No. 24-3133

IN THE UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

OHIO TELECOM ASSOCIATION, *et al.*,

Petitioners,

v.

FEDERAL COMMUNICATIONS COMMISSION
and UNITED STATES OF AMERICA,

Respondents.

On Petition for Review of an Order of
the Federal Communications Commission

Brief of Amici Curiae Electronic Privacy Information Center, Privacy Rights Clearinghouse, and Public Knowledge in support of the Federal Communications Commission and United States of America.

Counsel for Amici Curiae
Alan Butler
Christopher Frascella
Electronic Privacy Information Center
1519 New Hampshire Ave NW
Washington DC 20008
202-483-1140
butler@epic.org

Dated: August 5, 2024

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 24-03133 Case Name: Ohio Telecom Association v. FCC, et al

Name of counsel: Alan Butler

Pursuant to 6th Cir. R. 26.1, Electronic Privacy Information Center
Name of Party
makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

No.

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

No.

CERTIFICATE OF SERVICE

I certify that on August 5, 2024 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Alan Butler
1519 New Hampshire Ave NW
Washington DC 20036

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 24-3133 Case Name: Ohio Telecom Association v. FCC, et al

Name of counsel: Alan Butler

Pursuant to 6th Cir. R. 26.1, Public Knowledge
Name of Party
makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

No

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

No

CERTIFICATE OF SERVICE

I certify that on August 6 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Alan Butler
1519 New Hampshire Ave. NW
Washington, DC 20036

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 24-3133 Case Name: Ohio Telecom Association v. FCC, et al

Name of counsel: Alan Butler

Pursuant to 6th Cir. R. 26.1, Privacy Rights Clearinghouse
Name of Party
makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

No

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

No

CERTIFICATE OF SERVICE

I certify that on August 6 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Alan Butler
1519 New Hampshire Ave. NW
Washington, DC 20036

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

TABLE OF CONTENTS

DISCLOSURE OF CORPORATE AFFILIATIONS AND FINANCIAL INTEREST ii

TABLE OF AUTHORITIES iv

INTEREST OF AMICI 1

SUMMARY OF ARGUMENT 2

ARGUMENT 4

I. Data Breach Notifications Rules Help Both Customers and Telecommunications Carriers Manage the Aftermath of a Breach. 6

a. Breach notifications help subscribers avoid downstream harms. 11

b. Breach notification is a bare minimum transparency measure that applies as a commonsense requirement across other industries. 14

II. The FCC Is the Best-Positioned to Enforce Telecommunications Data Breach Obligations. 16

a. The FCC has ample relevant authority to promulgate this breach notification rule under Section 222, which protects more than just Customer Proprietary Network Information (CPNI). 17

b. The FCC also has broad authority to update its breach notification rule under Section 201(b). 19

c. The FCC is better suited than other federal and state agencies because of its relationship to telecommunications companies. 21

III. The Congressional Review Act (CRA) Should Not Be a Bar to Agencies Improving Portions of Disapproved Rules. 22

a. Petitioners' interpretation of the CRA would create permanent regulatory gaps. 23

b. The Court should find that the rule under review is not "substantially the same" under the CRA because it has a different scope, different underlying facts, and different reasoning from the 2016 broadband privacy rule. 25

CONCLUSION 29

CERTIFICATE OF COMPLIANCE 31

CERTIFICATE OF SERVICE 32

TABLE OF AUTHORITIES

Cases

Conroy v. Aniskoff, 507 U.S. 511 (1993) 33

Galaria v. Nationwide Mut. Ins. Co., 663 Fed. Appx. 384 (6th Cir. 2016) 17, 18

Gonzales v. Oregon, 546 U.S. 243 (2006) 26

Statutes

47 U.S.C. § 201(b).....4, 20, 21

47 U.S.C. § 222 .....4, 18, 19

5 U.S.C. § 801 .....4, 24

5 U.S.C. § 801(b)(2) 4

Other Authorities

2009 Data Breach Investigation Report, Verizon Bus. (2009) 10

2014 Internet Crime Report, FBI (2014).....9

2016 Internet Crime Report, FBI (2016).....9

2021 in review Data Breach Annual Report: Identity Theft Compromises: From the Era of Identity Theft to the Age of Identity Fraud, ITRC (Jan. 2022) 10

2023 Internet Crime Report, FBI (2023).....9

2024 Data Breach Investigation Report, Verizon Bus. (2024) 9

Adam M. Finkel & Jason W. Sullivan, *A Cost-Benefit Interpretation of the 'Substantially Similar' Hurdle in the Congressional Review Act: Can OSHA Ever Utter the E-Word (Ergonomics) Again?,* 63 Admin. L. Rev. 4 (2011).27, 29

AT&T Privacy Notice, AT&T Privacy Center (July 25, 2024) 19

Complaint, *In the Matter of Global Tel*Link Corp. et al.*, Fed. Trade Comm'n. No. C-4801 (2023) 14

Crooks Steal Phone, SMS Records for Nearly All AT&T Customers, KrebsonSecurity (Jul. 12, 2024) 11

Data Breach Response: A Guide for Business, Fed. Trade Comm'n (Feb. 2021) ..13

Emily Heaslip, *How to Communicate a Data Breach to Customers,* U.S. Chamber of Commerce (Jan. 26, 2022) 14

EPIC *et al.* Reply Comments, *Data Breach Reporting Requirements*, FCC 23-111 (Mar. 24, 2023) 8

FCC-FTC Consumer Protection Memorandum of Understanding (Nov. 16, 2015) 21

H.J.R. 107, 118th Cong. (2024) 28

H.J.R. 153, 118th Cong. (2024) 28

In re China Unicom (Americas) Operations Ltd., FCC 22-9, 37 FCC Rcd 1480 (rel. Feb. 2, 2022) 20

In re Quadrant Holdings LLC, Q Link Wireless LLC, and Hello Mobile LLC, DA-22-825, 37 FCC Rcd 9304 (rel. Aug. 5, 2022) 20

In re TerraCom, Inc. and YourTel America, Inc., FCC 14-173, 29 FCC Rcd 13325 (rel. Oct. 24, 2014) 20, 21

Ionut Arghire, *Millions of AT&T Customers Notified of Data Breach at Third-Party Vendor*, SecurityWeek (Mar. 10, 2023) 11

Jesper Zerlang, *The Pandemic's Lasting Effects: Are Cyber Attacks One of Them?,* Forbes (Jul. 20, 2022) 8

Karl Paul, *How remote work opened the floodgates to ransomware,* The Guardian (Jun. 17, 2021) 8

Kat Cammack et al., Letter to Chair Rosenworcel (Dec. 12, 2023).....29

Kim Zetter, *Hackers Detail How They Allegedly Stole Ticketmaster Data From Snowflake,* Wired (Jun. 17, 2024).....12

Martin Ignatovski, *Healthcare Breaches During COVID-19: The Effect of the Healthcare Entity Type on the Number of Impacted Individuals, 19 Perspectives in Health Info. Mgmt. (2022)* 8

Mobile: Breach Exposed SSN/DOB of 40M+ People, KrebsonSecurity (Aug. 18, 2021) 11

New T-Mobile Breach Affects 37 Million Accounts, KrebsonSecurity (Jan. 19, 2023) 11

Press Release, *NJ to Receive Roughly $500k from $16M Settlements Over 2012 and 2015 Experian Data Breaches*, N.J. Att'y Gen. (Nov. 7, 2022).....22

S. J. Res. 34, 115th Cong. (2017).....5

Targeted Cyberattacks Fuel Massive Increase in Breach Victim Counts, ITRC (2024).....10

The Congressional Review Act (CRA): Frequently Asked Questions, Cong. Rsch. Serv. (Nov. 12, 2021).....27, 28, 29

T-Mobile Privacy Notice, T-Mobile Privacy Center (May 13, 2024).....19

Verizon Customer Data for Sale on Dark Web, New Data Breach Suspected, The Cyber Express (Feb. 16, 2023).....11

Verizon's 2016 DBIR finds cybercriminals are exploiting human nature, Verizon News Ctr. (Apr. 29, 2016).....9

When Information is Lost or Exposed, Fed. Trade Comm'n (last visited Aug. 2, 2024) 13

Zack Whittaker, *AT&T says criminals stole phone records of 'nearly all' customers in new data breach,* TechCrunch (Jul. 12, 2024).....12

Rules

Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, 88 Fed. Reg. 20212 (Apr. 5, 2023).....16

Standards for Safeguarding Consumer Data, 86 Fed. Reg. 70062 (Dec. 9, 2021).16

Regulations

Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 47 C.F.R. § 64 (2016) 5

INTEREST OF *AMICI*

The Electronic Privacy Information Center ("EPIC") is a non-profit public interest research center in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.[1] EPIC routinely participates as *amicus curiae* before federal and state courts in cases concerning the privacy and security of consumer data.

Privacy Rights Clearinghouse ("PRC") is a nonprofit organization based in San Diego, California, established in 1992 to advance privacy for all by empowering individuals and advocating for positive change. PRC has championed strong data breach notification laws since 2005, when the world's first such law was passed in California.

Public Knowledge ("PK") is non-profit consumer rights organization that advocates for technology policy that serves the public interest. PK advocates before Congress, the courts, the Federal Communications Commission (FCC), and other agencies to support consumer rights, including the right of consumers to have their confidential personal information protected.

---

[1] All parties have consented to the filing of this brief. In accordance with Federal Rule of Appellate Procedure 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief. This brief was not authored, in whole or in part, by counsel for a party. EPIC would like to thank EPIC Summer IPIOP Clerk Anna Young for her contribution to this brief.

The undersigned *Amici* routinely submit comments and civil society input on the Commission's regulatory dockets to promote stronger protections for consumer data, robust privacy rules, and strict enforcement to prevent downstream harms.

SUMMARY OF ARGUMENT

Data breaches are a constant and urgent threat to the privacy of American consumers today. And telecommunications subscribers are uniquely vulnerable because they rely on carrier services to engage in their day-to-day activities; these users can't avoid having their communications, payment, and other personal data collected in order to access essential services. The Federal Communications Commission (FCC) seeks in the rulemaking under review, *Data Breach Reporting Requirements*, FCC 23-111, 2023 WL 8889606 (released Dec. 21, 2023), Pet'rs' App. ("A") 1–104, to establish strong, uniform rules to ensure that carriers' practices in handling customer data breaches are just and reasonable.

The Petitioners challenging this rule argue that the broad statutory authority Congress granted the Commission is not sufficient to permit this modification to the data breach notification rules. The implication of this argument is that Congress intended for breaches of telecommunications customers' sensitive personal information (including Social Security Numbers, biometric data, and other identifiers) to fall outside any existing federal regulatory jurisdiction. This is nothing more than a cynical attempt at regulatory arbitrage to avoid liability for

weak cybersecurity practices and for inadequate responses when the sensitive data of millions of their customers has been mishandled. It is evident from the text of Section 201 and 222, and is consistent with the FCC's unique role in regulating the business practices of telecommunications carriers, that the Commission has wide latitude to promulgate the necessary data breach notification rules, as well as other data security and privacy rules. Telecommunications carriers are free to advocate to Congress that regulatory authority over data breaches be vested in a different agency (such as the Federal Trade Commission), but it is not the role of courts to improperly narrow the Commission's authority under 47 U.S.C. § 201(b) and 47 U.S.C. § 222, and thereby create a regulatory loophole for this industry.

The Petitioners' arguments that the Congressional Review Act (CRA), 5 U.S.C. § 801, bars the data breach reporting rule similarly miss the mark. The CRA only prohibits the reissuance of a disapproved rule in "substantially the same form" or the issuance of a new rule that is "substantially the same as such a rule." 5 U.S.C. § 801(b)(2). This narrow restriction on agency rulemakings effectuates Congress's response to a specific regulatory action at a specific point in time, and does not alter the scope of FCC (or any other agency's) authority to promulgate other rules. Furthermore, the 2017 disapproval resolution cited by Petitioners was a narrow and specific response by Congress to a particular rule—*Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 47

C.F.R. § 64 (2016)—as it existed at that time. *See* S. J. Res. 34, 115th Cong. (2017), *enacted as* Pub. L. No. 115-22, 131 Stat. 88 (2017). The data breach notification rule under review is not a reissuance of the 2016 broadband privacy rule, and it is not substantially the same as that rule. The CRA does not bar this regulation, and it is well within the scope of the Commission's authority. The Court should deny the Petition for Review.

ARGUMENT

Authority to impose data breach reporting requirements, which have been applied and established across many industries, should not be eliminated for telecommunications carriers. Congress established the Federal Communications Commission ("FCC" or "Commission") to regulate telecommunications carriers and specifically authorized the Commission to promulgate rules concerning the handling of customers' private information. Data breach notification rules for telecommunications carriers are an essential piece of the regulatory patchwork that protects American consumers from identity theft and abuse. Timely breach notifications are key to mitigating the downstream harms of breaches and these requirements benefit both the customers and the carriers themselves.

The Court should not improperly cabin the FCC's authority to protect the privacy of customer information, and Congress's past disapproval of a broader set of privacy regulations for broadband providers does not eliminate or diminish that

well-established authority. It would be especially dangerous to adopt a sweeping and atextual interpretation of the Congressional Review Act ("CRA") here when the Commission's needs to have the ability to respond quickly to urgent and ongoing threats of data misuse and tech-facilitated fraud and where Congress has chosen not to establish a comprehensive federal privacy regime with jurisdiction vested in a different entity.

Breaches of consumer data have become more prevalent and more severe since the FCC's 1998, 2007, and 2013 privacy rulemakings and even since the 2016 broadband privacy rule was promulgated. These data breaches can lead to identity theft, account compromise, and other monetary and non-monetary losses, and timely breach notification can equip consumers to mitigate these downstream harms. For this reason, timely breach notification has become a well-established business practice across industries; notification is an essential, beneficial step in incident response. Indeed, in the U.S. National Cybersecurity Strategy Implementation Plan, the White House charged the Office of the National Cyber Director with harmonizing these types of cybersecurity standards across industries to ensure that personal data is protected. The current regulatory patchwork for data security includes Securities and Exchange Commission's (SEC's) disclosure requirements to investors and the Federal Trade Commission's (FTC's) data

security guidance for and enforcement actions against companies that are not acting as common carriers.

The FCC's updated breach notification rule requires carriers to provide consumers with detailed notification of breaches in a timely manner. Barring this rule would create a major gap in the regulatory patchwork that would unfairly privilege telecommunications carriers. The FCC has historically regulated these entities, including their privacy and cybersecurity practices, under Title II of the Communications Act. While there is concurrent jurisdiction in some contexts, denying the FCC authority here would weaken accountability for carriers.

I. Data Breach Notifications Rules Help Both Customers and Telecommunications Carriers Manage the Aftermath of a Breach.

Data breaches happen all too frequently, and many worry that it could be a question of when, not if, their data will be breached. But the response to a breach can be as important, and in some cases more important, than the steps taken to prevent or mitigate the risks beforehand. That is because the harmful consequences that flow from a breach, including identity theft, loss of control of accounts, harassment, and invasions of privacy, can often be avoided if there is a warning in time to implement protective measures and prevent the worst from happening. And companies similarly have an interest in implementing a predictable and efficient process for responding to a breach. Clear data breach notification rules provide a

useful rubric for responding to a crisis and mitigating foreseeable downstream harms, and they provide legal clarity to all sides to reduce unnecessary litigation.

The need for the FCC's rule has never been more evident. As undersigned *amici* and others made clear in their comments on the rulemaking, the threat of data breaches has grown progressively worse since 2016. *See, e.g.*, EPIC *et al.* Reply Comments, *Data Breach Reporting Requirements*, FCC 23-111, at 13-15 (Mar. 24, 2023).[2] When the COVID-19 pandemic forced people to conduct their business and their lives remotely, hackers increased their activities. *See, e.g.*, Martin Ignatovski, *Healthcare Breaches During COVID-19: The Effect of the Healthcare Entity Type on the Number of Impacted Individuals, 19 Perspectives in Health Info. Mgmt. 4, 1c (2022);*[3] Jesper Zerlang, *The Pandemic's Lasting Effects: Are Cyber Attacks One of Them?,* Forbes (Jul. 20, 2022);[4] Karl Paul, *How remote work opened the floodgates to ransomware,* The Guardian (Jun. 17, 2021).[5] Multiple credible authorities on the prevalence and severity of breaches have reported significant upticks over the last fifteen years, especially since the FCC's

[2] https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814.
[3] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9635044/.
[4] https://www.forbes.com/sites/forbestechcouncil/2022/07/20/the-pandemics-lasting-effects-are-cyber-attacks-one-of-them/.
[5] https://www.theguardian.com/technology/2021/jun/17/ransomware-working-from-home-russia.

most recent attempt to protect consumers from these harms in 2016 and again after the COVID-19 pandemic caused lockdowns in early 2020.

Indeed, reports of aggregate data breach statistics from law enforcement, corporate, and civil society groups all demonstrate the need for strong data security and breach regulations. Each year the Federal Bureau of Investigation (FBI) releases an Internet Crime Report that catalogues cybercrime incidents, including personal data breach complaints. In 2023, there were 55,851 complaints related to personal data breaches; this compares with 38,218 complaints in 2019, *2023 Internet Crime Report*, FBI 8 (2023);[6] 27,573 complaints in 2016, *2016 Internet Crime Report*, FBI 17 (2016);[7] and 5,145 complaints in 2014. *2014 Internet Crime Report*, FBI 47 (2014).[8] In its 2024 Data Breach Investigation Report (DBIR), Verizon analyzed 30,458 global data breach incidents, with a record-high of 10,626 unique data breaches. *2024 DBIR,* Verizon Bus. 5 (2024).[9] That is compared with more than 2,260 breaches in Verizon's 2016 report, *Verizon's 2016 DBIR finds cybercriminals are exploiting human nature*, Verizon News Ctr. (Apr. 29, 2016),[10] and 90 confirmed data breaches in its 2009 report, *2009 DBIR*,

[6] https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.
[7] https://www.ic3.gov/Media/PDF/AnnualReport/2016_IC3Report.pdf.
[8] https://www.ic3.gov/Media/PDF/AnnualReport/2014_IC3Report.pdf.
[9] https://www.verizon.com/business/resources/T597/reports/2024-dbir-executive-summary.pdf.
[10] https://www.verizon.com/about/news/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human.

Verizon Bus. 2 (2009).[11] An analysis done by the Identify Theft Resource Center (ITRC) showed that the number of people affected by data breaches within the first six months of 2024 was more than one billion, a 490% increase from the first half of 2023. *See Targeted Cyberattacks Fuel Massive Increase in Breach Victim Counts*, ITRC 6 (2024).[12] Like the FBI and Verizon, ITRC's reports on data breaches similarly tracks an upward trend—from 785 compromises in 2015 to 1,099 in 2016, *2021 in review Data Breach Annual Report: Identity Theft Compromises: From the Era of Identity Theft to the Age of Identity Fraud*, ITRC 6 (Jan. 2022); to 1,801 in 2022, to 3,203 in 2023. *Targeted Cyberattacks* 5. The ITRC estimates that 2024 had approximately 14% more breaches in the first six months than in the first six months of 2023 (already a record-breaking year), suggesting 2024 could be even worse. *See id.* at 1.

As Commission outlines in its brief, carriers in particular have had several recent high-profile breaches impacting millions of customers. Resp'ts Br. 12. In 2023, news broke that nine million AT&T accounts had their data accessed, and data on 7.5 million Verizon customers were stolen by hackers. *See, e.g.*, Ionut Arghire, *Millions of AT&T Customers Notified of Data Breach at Third-Party*

---

11 https://www.fbiic.gov/public/2009/april/VBA60069WPDBIR8x1109pdfv1singleR.pdf.

12 https://www.idtheftcenter.org/publication/itrc-h1-data-breach-analysis/.

Vendor, SecurityWeek (Mar. 10, 2023);[13] *Verizon Customer Data for Sale on Dark Web, New Data Breach Suspected,* The Cyber Express (Feb. 16, 2023).[14] T-Mobile reported that the personally identifiable information (PII) of 37 million costumers was stolen in 2023, just two years after PII was reported stolen from 40 million of its customers. *New T-Mobile Breach Affects 37 Million Accounts,* KrebsonSecurity (Jan. 19, 2023);[15] *T-Mobile: Breach Exposed SSN/DOB of 40M+ People*, KrebsonSecurity (Aug. 18, 2021).[16] Most recently and egregiously, AT&T disclosed a breach impacting over 100 million people—nearly all of its customers as well as some non-customers. *Crooks Steal Phone, SMS Records for Nearly All AT&T Customers,* KrebsonSecurity (Jul. 12, 2024).[17] And that is only the most recent news about breaches at the largest carriers.

Current regulations and enforcement actions alone are not sufficient to reverse this trend, but they are a necessary step and new rulemaking progress should not be halted. In an era of pronounced remote and hybrid work, the ability to use a victim's personal data to access online accounts becomes even more

[13] https://www.securityweek.com/millions-of-att-customers-notified-of-data-breach-at-third-party-vendor/.
[14] https://thecyberexpress.com/verizon-customer-data-for-sale-on-dark-web/.
[15] https://krebsonsecurity.com/2023/01/new-t-mobile-breach-affects-37-million-accounts/.
[16] https://krebsonsecurity.com/2021/08/t-mobile-breach-exposed-ssn-dob-of-40m-people/.
[17] https://krebsonsecurity.com/2024/07/hackers-steal-phone-sms-records-for-nearly-all-att-customers/.

impactful. For example, the unprecedented AT&T breach was accomplished by using employee credentials obtained from a separate data breach. *See, e.g.*, Kim Zetter, *Hackers Detail How They Allegedly Stole Ticketmaster Data From Snowflake,* Wired (Jun. 17, 2024).[18]

a. Breach notifications help subscribers avoid downstream harms.

Rules that require timely and informative notification to consumers after their personal information is breached are important to make sure that they can take the necessary steps to prevent further harm. Countermeasures can include a credit freeze, credit monitoring, changing passwords, or exercising greater scrutiny on communications that may be phishing attempts bolstered by data obtained in a breach. These steps impose monetary and time costs that consumer would not have spend but for their data being stolen, and already represent significant harm, but that harm can at least be mitigated through timely notice. The same is true when a carrier's vendor entrusted with consumer data experiences a breach. *See e.g.*, Zack Whittaker, *AT&T says criminals stole phone records of 'nearly all' customers in new data breach,* TechCrunch (Jul. 12, 2024) (subscriber data breached through vendor).[19]

[18] https://www.wired.com/story/epam-snowflake-ticketmaster-breach-shinyhunters/.
[19] https://techcrunch.com/2024/07/12/att-phone-records-stolen-data-breach/.

The Federal Trade Commission has published detailed guidance on data breach response that highlights the important role timely notice plays in the process. *See, e.g.*, *Data Breach Response: A Guide for Business,* Fed. Trade Comm'n (Feb. 2021);[20] *When Information is Lost or Exposed,* Fed. Trade Comm'n (last visited Aug. 2, 2024).[21] For example, if an individual's social security number is exposed, they need to consider freezing their credit, check their accounts for unknown charges, and set up an E-Verify account to lock their number. *See When Information is Lost or Exposed.* If someone's debit or credit card number or bank account information is taken, they will need to close their card or account, review their transactions, get any fraudulent charges removed, and lastly, check their credit report. *See id.*

Even the U.S. Chamber of Commerce acknowledges in its recommendations that companies should send breach notifications (1) as quickly as possible ("[t]he sooner you can alert customers, the sooner they can take steps to protect themselves from fraud"); (2) with adequate information; and (3) through "multiple communication channels to make sure that all affected parties are notified of the breach," because consumers have the best opportunity to mitigate harm if notified that additional security precautions are necessary. Emily Heaslip, *How to*

[20] https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business.
[21] https://www.identitytheft.gov/Info-Lost-or-Stolen.

Communicate a Data Breach to Customers, U.S. Chamber of Com. (Jan. 26, 2022).[22]

This Court has also recognized in its own data breach decisions that it is important to limit downstream harms caused by data breaches. In *Galaria v. Nationwide Mut. Ins. Co.*, consumer plaintiffs survived a motion to dismiss on appeal because the court found they had been injured by the costs they reasonably incurred to mitigate future harms. 663 Fed. Appx. 384, 386–87 (6th Cir. 2016) (unpublished). The court agreed that while it's not "'literally certain' that the Plaintiff's data will be misused," there is enough "risk of harm that incurring mitigation costs is reasonable." *Id.* at 388. But this mitigation cannot occur without notification.

Unfortunately, companies have been known to understate the severity of the data breaches they experience, making regulations like the FCC's all the more important. Delaying accurate notification to their consumers means the affected individuals are at a great disadvantage in attempting to protect themselves from identity theft. *See* Complaint, *In the Matter of Global Tel*Link Corp. et al.*, Fed. Trade Comm'n. No. C-4801, ¶ 41 (2023).[23] For example, Telmate, a voice over IP (VoIP) provider, knowingly reported to consumers that "no medical data,

[22] https://www.uschamber.com/co/grow/customers/how-to-communicate-data-breach-to-customers.
[23] https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-GlobalTelLink.pdf.

passwords, or consumer payment information" were affected in a recent breach that did in fact implicate medical data and credit card numbers. *See id.* at ¶¶ 38-40. Additionally, Telmate took eight months to notify impacted customers. *Id.* Because Telmate delayed notifying its consumers, the affected individuals could not take actions to protect themselves from identity theft. *See id.* at ¶ 41.

b. Breach notification is a bare minimum transparency measure that applies as a commonsense requirement across other industries.

The Commission's data breach notification regulations are the bare minimum rules necessary to ensure that consumers have the necessary information to protect themselves in the aftermath of their personal information being exposed. While our country is sorely in need of baseline cybersecurity regulations, and the FCC has ample established authority to enact such regulations, *see* Section II *infra*, this rulemaking is a commonsense approach to the regulatory baseline. If the Commission doesn't have the authority to take these steps, as the Petitioners argue, then telecommunications customers are significantly at risk and swift legislative action will be necessary to fill this regulatory void.

The Commission's approach imposes minimal regulatory burdens on carriers also because the agency strove to harmonize this rule with approaches "already deployed by our partners in federal and state government." A3 ¶ 4. The FCC is not the only agency working to reduce the impact of breaches, but is uniquely positioned to do so where the breached entity is a common carrier or its

vendor. The SEC has explained that personal information being exposed can have "severe consequences" for the impacted individual, including that data being "used to steal their identities or access their accounts at financial institutions to steal assets held in those accounts." *Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents,* 88 Fed. Reg. 20,212, 20,253 (Apr. 5, 2023).[24] The FTC made the same point in its Safeguards Rule proceeding. *Standards for Safeguarding Consumer Data,* 86 Fed. Reg. 70062, 70066 (Dec. 9, 2021).[25]

The FCC rule also gives carriers tremendous flexibility in the form and content of the breach notifications. The rule offers suggestions for what would best protect consumers, A38-39 ¶ 63 (recommendations, not requirements), but only requires that the notification "include sufficient information so as to make a reasonable customer aware that a breach occurred . . . within a certain estimated timeframe, and that such a breach . . . may have affected that customer's data."

[24] https://www.federalregister.gov/documents/2023/04/05/2023-05767/cybersecurity-risk-management-rule-for-broker-dealers-clearing-agencies-major-security-based-swap#p-665.
[25] https://www.federalregister.gov/documents/2021/12/09/2021-25064/standards-for-safeguarding-customer-information#p-73.

A37-38 ¶ 62. Furthermore, a provider is not required to issue a breach notification at all if the provider "can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach." A3 ¶ 4; A8 ¶ 14.

Because of the FCC's attention to flexibility and harmonization, one breach notification can satisfy multiple, different regulatory requirements, making it hard for carriers to argue that this would impose a significant burden or would be inconsistent with other existing breach notification requirements that apply across industries. By mandating a timely notification, the Commission's rule gives carriers certainty and guidance that can also narrow the scope of possible consumer litigation for untimely notices.

The Court should not prevent the best-equipped regulator from imposing a minimally burdensome requirement on carriers that clarifies liability and helps millions of consumers protect themselves from a persistent and growing threat.

II. The FCC Is the Best-Positioned to Enforce Telecommunications Data Breach Obligations.

The FCC has the established authority to update its breach notification protections for consumers under Sections 222 and 201(b) of the Communications Act, and the Commission is well-suited to oversee the industry's breach notification regime due to its role as their primary regulator. For nearly two decades, the Commission has required that carriers report data breaches of their customer's personal information under the agency's authorities. A58 ¶ 119.

a. The FCC has ample relevant authority to promulgate this breach notification rule under Section 222, which protects more than just Customer Proprietary Network Information (CPNI).

In Section 222, Congress tasked the FCC with ensuring that every telecommunications carrier protects the confidentiality of proprietary information of and relating to its customers. This is vital because carriers are exempt in many cases from authority under Section 5 of the FTC Act when they are acting in their capacity as common carriers. Resp'ts Br. 26. If the FCC lacks jurisdiction here, there would be a critical gap in regulatory authority over data breach requirements that would benefit telecommunications carriers. This would have far-reaching implications for consumers who rely on these services every day.

That Section 222 authorizes the Commission to hold carriers accountable for broad categories of consumer data is evident from its title—"privacy of customer information"—as well as from the explicit duty the statute creates in its first provision. Petitioners attempt to flip traditional canons of statutory interpretation on their head, arguing that the use of a more specific term later in a statute ("CPNI") narrows the prior more general provision of the statute ("privacy of customer information" and rules regarding "customer proprietary information" ("CPI")). The general CPI provision in Section 222(a) is broader than the specific CPNI rules in Section 222(c); the choice to define and use the narrower term in subsection (c) should not be treated as surplusage. And the carriers know well that

they have obligations to protect the confidentiality of the broader set of customer information that they collect, as is evident from their own privacy policies. *See, e.g.*, *AT&T Privacy Notice*, AT&T Privacy Center (July 25, 2024), ("Account Information. You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including [CPNI].");[26] *T-Mobile Privacy Notice*, T-Mobile Privacy Center (May 13, 2024), (noting "account creation & billing" as a separate category from CPNI).[27]

Not only is CPNI defined as a narrower subset of customer information, but it excludes highly sensitive data that Congress would not have intended to exclude from the protections of Section 222(a). Some categories of sensitive personal information are not considered CPNI protected under 222(c), as the Commission noted in its Order: "[i]t is implausible that Congress would have exempted common carriers from any obligation to protect their customers' private information that is not CPNI." A64 ¶ 126. Indeed, the FCC has cited to its mandate under Section 222 to protect subscriber data other than CPNI for more than a decade. *See, e.g.*, *In re TerraCom, Inc. and YourTel America, Inc.*, FCC 14-173, 29

[26] https://about.att.com/privacy/privacy-notice.html.
[27] https://www.t-mobile.com/privacy-center/privacy-notices/t-mobile-privacy-notice.html.

FCC Rcd 13325, ¶ 2 (rel. Oct. 24, 2014)[28] ("failed to employ reasonable data security practices to protect consumers' [proprietary information]"); *In re Quadrant Holdings LLC, Q Link Wireless LLC, and Hello Mobile LLC*, DA-22-825, 37 FCC Rcd 9304, 9307 n. 25 (rel. Aug. 5, 2022)[29] ("[t]he scope of "proprietary information" covered by section 222 extends beyond CPNI data to include private or sensitive data that a customer would normally wish to protect"); *In re China Unicom (Americas) Operations Ltd.*, FCC 22-9, 37 FCC Rcd 1480, 1539, ¶ 83 (rel. Feb. 2, 2022)[30] ("The Commission expressed concern…that CUA's service offerings provide CUA with access to both customer PII and CPNI…") (internal citations omitted).

b. The FCC also has broad authority to update its breach notification rule under Section 201(b).

In Section 201(b), Congress delegated rulemaking authority that is also sufficient to support the proposed regulations even without Section 222. As the Commission has detailed in its brief, Section 201(b) mirrors the consumer protection authority granted to the Federal Trade Commission, but unlike the FTC's authority, Section 201(b) applies to telecommunications carriers without qualification. Resp'ts Br. 26–27. Without this complementary regime, common

[28] https://docs.fcc.gov/public/attachments/FCC-14-173A1.pdf.
[29] https://docs.fcc.gov/public/attachments/DA-22-825A1.pdf.
[30] https://docs.fcc.gov/public/attachments/FCC-22-9A1.pdf.

carriers could seek to evade scrutiny of their unreasonable business practices altogether.

Historically, the FCC has used Section 201(b) to address practices beyond charges for services—for example, to enforce violations of basic data security practices and failure to notify consumers of a breach. *See, e.g.*, *TerraCom, Inc. and YourTel America, Inc.* ¶ 12. Petitioners' and other *amici*'s claims that Section 222 narrows Section 201(b)'s scope not only contort the provisions they rely on, Resp'ts Br. 32, but also disregard more recent and unambiguous Supreme Court precedent about the FCC's authority under 201(b) being express and far-reaching, including "broad power to enforce all provisions of the statute." *Gonzales v. Oregon*, 546 U.S. 243, 259 (2006) (citing to *Nat'l. Cable & Telecomm. Ass'n v. Brand X Internet Services*, 545 U.S. 967, 980 (2005)).

The parallel authority to regulate the trade practices of carriers held by the FCC is outlined in detail in the 2015 Consumer Protection Memorandum of Understanding between the FCC and the FTC. *See* FCC-FTC Consumer Protection Memorandum of Understanding 1 (Nov. 16, 2015) ("Whereas the [FCC] . . . requires all common carrier charges, practices, classifications, and regulations . . . to be just and reasonable . . . , Whereas Congress has directed the [FTC] to . . . . prevent unfair or deceptive acts or practices . . . The FCC and the FTC will

continue to work together to protect consumers from acts and practices that are deceptive, unfair, unjust and/or unreasonable…").[31]

c. The FCC is better suited than other federal and state agencies because of its relationship to telecommunications companies.

States and other federal agencies have important roles to play in breach notification, but when it comes to the telecom industry specifically, the FCC is and should continue to be the best equipped enforcement authority. While every state has its own breach notification law, there has only been one significant breach notification-related action brought by state attorneys general against a carrier in the last five years despite the numerous serious telecommunications data breaches. *See* Press Release, *NJ to Receive Roughly $500k from $16M Settlements Over 2012 and 2015 Experian Data Breaches*, N.J. Att'y Gen. (Nov. 7, 2022).[32] Moreover, while the FCC has attempted to harmonize the regulations at issue with corresponding state laws to minimize any additional burden on carriers, the FCC needs clear enforcement authority to add teeth to these requirements. A37-39 ¶¶ 62-63; A55-56 ¶ 111. The FCC is in the best position to take necessary regulatory action to combat this significant risk to consumers.

[31] https://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db1116/DOC-336405A1.pdf.
[32] https://www.njoag.gov/nj-to-receive-roughly-500k-from-16m-settlements-over-2012-and-2015-experian-data-breaches/.

Other federal agencies are simply not as well positioned to enforce data breach reporting regulations against the large carriers. The FTC, the main federal 'cop on the beat' for data security, has never brought a breach notification-related action against a non-VoIP telephone provider, such as one of the big three carriers. Resp'ts Br. 26. Additionally, the FCC has experience and familiarity with the practices of carriers—certainly moreso than any other regulator.

Clear authority and enforcement capacity is necessary to ensure that companies have a strong incentive to provide timely, meaningful, and relevant breach notifications to impacted consumers; the FCC holds that authority.

III. The Congressional Review Act (CRA) Should Not Be a Bar to Agencies Improving Portions of Disapproved Rules.

No court has held that an agency is barred from promulgating a rule simply because it includes some provisions that had also been included in an earlier regulation subject to a Congressional Review Act joint resolution of disapproval—because that is not what the law requires. The Court should reject Petitioners' strained arguments to read this broad jurisdiction stripping into the CRA.

A disapproval resolution issued under the CRA reflects Congress's response to a specific rulemaking action at a specific point in time; such a regulation does not limit the underlying statutory authority of the agency, and nothing in the statute or the legislative record provides support for the sweeping deregulatory argument made by the Petitioners here. Indeed, affirming the Petitioners' interpretation of the

CRA would create regulatory lacunae; in the instant case, this would privilege some businesses over others. Petitioners' interpretation would also have tremendous repercussions for the role of the administrative state, hindering the ability of federal agencies to carry out their statutory mandates.

In order for a regulation to be "substantially the same" under 5 U.S.C. § 801, the Court must find that it is the same in (1) scope and subject matter; (2) underlying factual predicates; and (3) articulated agency reasoning. If any *one* of these elements is not substantially the same, then the rule itself cannot be said to be substantially the same. In this instance, *none* of these three elements are substantially the same, and so there can be no basis to find that Congress's 2017 resolution of disapproval precludes the issuance of this 2023 rule.

a. Petitioners' interpretation of the CRA would create permanent regulatory gaps.

Adopting Petitioners' broad interpretation of the CRA would have a permanent preclusive effect on federal consumer protection efforts and more immediately allow carriers to evade federal consumer breach notification regulation. Through the CRA, Congress nullifies a specific regulatory action; it does not claw back existing agency authorities. If all it takes is a single CRA disapproval to preclude an agency from enacting rules until an act of Congress reverses it, agencies could be quietly (and even accidentally) stripped of authority granted under their organic statutes. Congress is empowered to circumscribe an

agency's mandate or even its existence *ex post*, but the CRA is not the vehicle by which Congress exercises that power. Petitioners' interpretation, if adopted, could—and likely is meant to—lead to regulatory gaps where no agency is able to regulate an industry because the rules attempting to do so have been subject to CRA resolutions. On Petitioners' view, agencies would need to wait until Congress eventually enacts a new statute reaffirming existing authority in order to use it. That would undermine the very reason Congress created the administrative agency in the first place: to be more nimble than Congress can be. This is especially true where technology and technology-facilitated fraud is concerned, as advances in technology and its use by bad actors occur at a more rapid pace than statutory text can keep up with. In the instant case, this would complicate enforcement of federal breach notification regulations, but only against common carriers and other entities subject to regulation only under Title II of the Communications Act. VoIP providers, for instance, would still be subject to regulation under the FTC, but the largest carriers would argue exemption from the FTC's authority by virtue of their status as common carriers. We also caution the Court that Petitioners' interpretation could prohibit an agency from ever acknowledging factual findings contained within a disapproved rule.

Petitioners' interpretation of the CRA does not stand up to scrutiny, not only because of its far-reaching repercussions but also because it ignores the purpose of

the statute. Congress intended for the CRA to put the ball back in the agency's court, not to put any impetus on Congress. If the Court interprets any CRA resolution as being a total prohibition against that agency reissuing any portion of the disapproved rule, the Court would thereby inject a requirement into the CRA that Congress take additional steps to undo any resulting collateral damage from each CRA resolution. For example, if Congress disapproved of a regulation due to one of ten topics within the regulation, the Court should not require Congress to pass a law re-authorizing the agency to reissue rules on the other nine topics where such authority already exists in the statute.

The Court should avoid the risks of stripping an agency of its jurisdiction forever and of burdening Congress with additional steps to avoid throwing the baby out with the bathwater. This is especially true because Congress can more easily fix a problem of overreach in a new regulation through a future CRA disapproval, which does not require the same extensive legislative steps that would be involved in creating or extending statutory authority.

b. The Court should find that the rule under review is not "substantially the same" under the CRA because it has a different scope, different underlying facts, and different reasoning from the 2016 broadband privacy rule.

The FCC's 2023 Rule is not "substantially the same" as the 2016 Broadband Privacy Order (BPO) under any logical interpretation of the CRA. A disapproval resolution applies to a specific regulation *in toto*; the CRA does not instruct courts

to abandon all canons of legal reasoning and interpretation in favor of drawing lines and counting words and comparing percentages within those bounds. As such, it cannot apply to each individual word, phrase, or provision contained within the disapproved regulation, but rather must apply to the rule as a whole. If (1) the scope or subject matter, (2) the underlying factual predicates, or (3) the articulated reasoning of the new rule is different, then the rule the agency has issued is not substantially the same.

The CRA does not define the meaning or scope of "substantially the same," but that phrasing implies some factor-based analysis, as Congress deliberately chose that wording rather than simply "the same." We submit that scope, facts, and reasoning are the three most salient factors. Scholars suggest that interpretations of "substantially the same" include asking whether the agency has addressed "the specific problems Congress identified," whether external conditions have changed, and whether the agency "has devised 'a wholly different regulatory approach.'" *The Congressional Review Act (CRA): Frequently Asked Questions*, Cong. Rsch. Serv. 19 n.107 (Nov. 12, 2021)[33] (citing Adam M. Finkel & Jason W. Sullivan, *A Cost-Benefit Interpretation of the 'Substantially Similar' Hurdle in the Congressional Review Act: Can OSHA Ever Utter the E-Word (Ergonomics) Again?,* 63 Admin. L. Rev. 4, 710 (2011) [hereinafter "Finkel & Sullivan"])..

[33] https://sgp.fas.org/crs/misc/R43992.pdf.

We urge the Court to consider scope and subject matter of the regulation itself as the primary source for evaluating whether a previously disapproved regulation is substantially the same as a new one. It is possible that the specifics of a Congressional debate leading up to a CRA resolution of disapproval could provide guidance on next steps to the agency in terms of the animating justifications for striking down the rule in the first place, *see The Congressional Review Act (CRA): Frequently Asked Questions*, Cong. Rsch. Serv. 19-20 (Nov. 12, 2021) (citing to Rep. Henry Hyde, Congressional Record, daily edition, vol. 142, (April 19, 1996), p. E577,[34] but any inferences from this debate may be arbitrary, as Justice Scalia once observed, *see Conroy v. Aniskoff*, 507 U.S. 511, 519 (1993) (referring to Judge Harold Leventhal analogizing legislative history to picking out one's friends in a crowded party). For example, as *amicus* ACA Connects noted, only a single member of Congress once made an offhand reference to notification fatigue due to breach reporting. Am. Br. of ACA Connects *et al.* 24-25, ECF No. 36. Members of Congress have introduced CRA resolutions for multiple FCC rules since January 2024, *see, e.g.,* H.J.R. 153, 118th Cong. (2024); H.J.R. 107, 118th Cong. (2024), yet there does not seem to be nearly the same level of interest in disapproving of this breach notification rule. *See* Kat

[34] https://www.congress.gov/congressional-record/volume-142/issue-51/extensions-of-remarks-section/article/E571-1.

Cammack et al., Letter to Chair Rosenworcel (Dec. 12, 2023).[35] Rather than looking to floor debate, the court would be better served to focus on whether the scope or subject matter of the rule has changed. Here, the FCC outlines how it has: for example, the 2016 rule applied to carriers and broadband Internet access service providers, whereas the 2023 rule applied to carriers and telecommunications relay service providers. Resp'ts Br. 57-58.

External conditions, or factual predicates, are relevant because a rule that Congress disapproved of at one time may be wholly appropriate at a different time, or in a different context—e.g., after a different cost-benefit analysis. *See The Congressional Review Act (CRA): Frequently Asked Questions*, Cong. Rsch. Serv. 19 (Nov. 12, 2021) (citing Finkel & Sullivan). The increasing and well documented prevalence of data breaches easily satisfies this criterion. *See* Section I *supra*.

We urge the court to consider an agency's articulated reasoning—including its underlying assumptions and definitions—rather than whether a rule represents a "wholly different regulatory approach." The CRA prohibits a rule that is "substantially the same"; it does not require a "wholly different" rule. An agency's attempt to reissue a rule need only avoid the problems that caused it to be

[35] https://cammack.house.gov/sites/evo-subsites/cammack.house.gov/files/evo-media-document/final-cra-letter_12.13.pdf.

disapproved of in the first place, even if it bears multiple similarities to a previously disapproved rule. Here, the FCC articulated how its reasoning about breach notification had changed, including the agency redefining the term "breach" itself. Resp'ts Br. 59-62.

Even if the Court decides that the CRA empowers it to draw lines around portions of disapproved rules and compare the contours of the shape it has chosen with the shape of a subsequent rule in its entirety, the FCC's rule would still pass muster. As the FCC notes, even within the data breach notification section itself, there are substantial differences between the 2016 and 2023 Orders. Resp'ts Br. 59-60.

The FCC did not attempt a "blatant re-run" of its nullified 2016 BPO in 2023, as Petitioners allege, Pets. Br. 57—but undertook a distinct process with a different scope, considered different facts, articulated different reasoning, and produced a rule that achieves a partially similar goal but not in substantially the same form.

CONCLUSION

We urge the Court to consider the implications of its ruling for the firmly established authority of the FCC and other federal agencies to protect consumers and their personal information. The Petition for Review should be denied.

Respectfully submitted:

This the 5th day of August, 2024.

Counsel for Amici Curiae

Alan Butler
Christopher Frascella
Electronic Privacy Information Center
1519 New Hampshire Ave NW
Washington DC 20008
202-483-1140
butler@epic.org

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(a)(7)(B) because it contains 6,287 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f) and 6 Cir. R. 32(b)(1). This brief also complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6).

August 5, 2024 /s/ Alan Butler

Alan Butler
Counsel for *Amici Curiae*

CERTIFICATE OF SERVICE

I hereby certify that on August 5, 2024, this brief was electronically filed with the Clerk of the Court for the United States Court of Appeals for the Sixth Circuit through 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.

August 5, 2024 /s/ Alan Butler
Alan Butler
Counsel for *Amici Curiae*

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 24-3133 Case Name: Ohio Telecom Association v. FCC, et al

Name of counsel: Alan Butler

Pursuant to 6th Cir. R. 26.1, Public Knowledge
Name of Party
makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

No

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

No

CERTIFICATE OF SERVICE

I certify that on August 6 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Alan Butler
1519 New Hampshire Ave. NW
Washington, DC 20036

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

6th Cir. R. 26.1
DISCLOSURE OF CORPORATE AFFILIATIONS AND FINANCIAL INTEREST

(a) **Parties Required to Make Disclosure**. With the exception of the United States government or agencies thereof or a state government or agencies or political subdivisions thereof, all parties and amici curiae to a civil or bankruptcy case, agency review proceeding, or original proceedings, and all corporate defendants in a criminal case shall file a corporate affiliate/financial interest disclosure statement. A negative report is required except in the case of individual criminal defendants.

(b) **Financial Interest to Be Disclosed**.

(1) Whenever a corporation that is a party to an appeal, or which appears as amicus curiae, is a subsidiary or affiliate of any publicly owned corporation not named in the appeal, counsel for the corporation that is a party or amicus shall advise the clerk in the manner provided by subdivision (c) of this rule of the identity of the parent corporation or affiliate and the relationship between it and the corporation that is a party or amicus to the appeal. A corporation shall be considered an affiliate of a publicly owned corporation for purposes of this rule if it controls, is controlled by, or is under common control with a publicly owned corporation.

(2) Whenever, by reason of insurance, a franchise agreement, or indemnity agreement, a publicly owned corporation or its affiliate, not a party to the appeal, nor an amicus, has a substantial financial interest in the outcome of litigation, counsel for the party or amicus whose interest is aligned with that of the publicly owned corporation or its affiliate shall advise the clerk in the manner provided by subdivision (c) of this rule of the identity of the publicly owned corporation and the nature of its or its affiliate's substantial financial interest in the outcome of the litigation.

(c) Form and Time of Disclosure. The disclosure statement shall be made on a form provided by the clerk and filed with the brief of a party or amicus or upon filing a motion, response, petition, or answer in this Court, whichever first occurs.