No. 24-3133

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

OHIO TELECOM ASSOCIATION,

Petitioner,

HAMILTON RELAY, INC.,

Intervenor.

v.

FEDERAL COMMUNICATIONS COMMISSION; UNITED STATES OF AMERICA,

Respondents.

On Petitions for Review of an Order of the
Federal Communications Commission, Agency No. 23-111

JOINT BRIEF OF ACA CONNECTS, CCA, NTCA, WISPA, AND WTA AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

Craig E. Gilmore
Daniel H. Kahn
Wilkinson Barker Knauer, LLP
1800 M Street NW, Suite 800N
Washington, DC 20036
(202) 783-4141
cgilmore@wbklaw.com
dkahn@wbklaw.com
Counsel for ACA Connects, CCA, NTCA, WISPA, and WTA

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: Craig E. Gilmore

Pursuant to 6th Cir. R. 26.1, ACA Connects – America's Communications Association
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 May 29, 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/ Craig E. Gilmore
Wilkinson Barker Knauer, LLP
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: Craig E. Gilmore

Pursuant to 6th Cir. R. 26.1, Competitive Carriers Association
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 May 29, 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/ Craig E. Gilmore
Wilkinson Barker Knauer, LLP
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: Craig E. Gilmore

Pursuant to 6th Cir. R. 26.1, NTCA – The Rural Broadband Association
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 May 29, 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/ Craig E. Gilmore
Wilkinson Barker Knauer, LLP
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: Craig E. Gilmore

Pursuant to 6th Cir. R. 26.1, WISPA – The Association for Broadband Without Boundaries
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 May 29, 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/ Craig E. Gilmore
Wilkinson Barker Knauer, LLP
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: Craig E. Gilmore

Pursuant to 6th Cir. R. 26.1, WTA – Advocates for Rural Broadband
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 May 29, 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/ Craig E. Gilmore
Wilkinson Barker Knauer, LLP
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

TABLE OF AUTHORITIES

CASES

STATUTES AND REGULATIONS

LEGISLATIVE MATERIALS

ADMINISTRATIVE MATERIALS

OTHER AUTHORITIES

INTEREST OF AMICI CURIAE[1]

ACA Connects – America's Communications Association ("ACA Connects") is a non-profit association representing more than 500 small and medium-sized independent communications providers that operate in communities throughout the United States. ACA Connects members provide an array of communications services to homes and businesses, including telecommunications services and interconnected Voice over Internet Protocol services, that are crucial to the economic prosperity of the communities they serve.

Competitive Carriers Association ("CCA") is the nation's leading association for competitive wireless providers and stakeholders. Members range from small, rural carriers serving fewer than 5,000 customers to regional and national providers, as well as vendors and suppliers that provide products and services throughout the wireless communications ecosystem.

NTCA – The Rural Broadband Association ("NTCA") is a non-profit organization representing small, locally operated telephone and broadband providers in rural communities throughout the United States. With rare exception, all NTCA telecommunications members are small businesses according to Small Business

[1] Counsel for all parties consented in writing to the filing of this brief. No counsel for a party authored this brief in whole or in part, and no person or entity other than *amici curiae* made a monetary contribution that was intended to fund the preparation or submission of this brief.

Association North American Industry Classification Codes, on average employing 35 people and serving approximately 6,000 fixed broadband service customer accounts.

WISPA – The Association for Broadband Without Boundaries ("WISPA") is a trade association with approximately 600 small businesses that provide mass-market, retail broadband to consumers in rural, exurban, and other unserved and underserved geographic areas. The vast majority of these broadband providers use fixed wireless technologies but a growing percentage are incorporating fiber optics in their networks. The vast majority of WISPA's broadband provider members have 10 or fewer employees. WISPA's membership also includes more than 300 engineers, technical consultants, equipment manufacturers, and other companies that support WISPA's small broadband provider members' deployment efforts.

WTA – Advocates for Rural Broadband ("WTA") is a national trade association that represents approximately 400 rural local exchange carriers that provide voice and broadband services to some of the most rural, remote, rugged, sparsely populated, and expensive-to-serve areas of the United States. The typical WTA member company serves fewer than 5,000 customers per service area and has fewer than 50 employees.

Members of ACA Connects, CCA, NTCA, WISPA, and WTA (the "Associations," and each an "Association") are regulated by the Federal

Communications Commission ("FCC") *Order* that is the subject of the instant appeal. *Data Breach Reporting Requirements*, Report and Order, FCC 23-111 (rel. Dec. 21, 2023) ("*Order*") (Petitioners' Appendix ("A") 1–104). The Associations take special interest in the impact of the *Order* on their small business members. These members generally lack access to resources and economies of scale to make it practical for them to absorb substantial regulatory changes or to comply with conflicting and overlapping rules across jurisdictions. The costs of compliance with novel and overlapping regulatory obligations such as those adopted in the *Order* detract from the core work of the Associations' members to connect existing and new customers in hard-to-serve areas and close the digital divide. In representing members' interests, each Association participated in the underlying FCC rulemaking proceeding.

SUMMARY OF ARGUMENT

The *Order* begins by observing that communications services "are a ubiquitous feature of modern life, and they provide a vital lifeline for consumers." A2 (*Order* ¶ 1). But the FCC then undercuts Congress's fundamental connectivity goals by adopting burdensome data breach reporting requirements that exceed the FCC's legal authority.

Congress has made connecting Americans to high-speed broadband communications central to the FCC's mission, stating that the agency "shall

encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans." 47 U.S.C. § 1302(a). Members of the Associations play an essential role in delivering high-speed broadband connectivity, leveraging limited resources to invest in their communities, many of which would be overlooked but for Association members' ongoing efforts and investment. The *Order* undermines Congress's connectivity goals by unnecessarily and unlawfully imposing significant compliance costs on Association members, most of which are small businesses that lack dedicated privacy teams and in-house attorneys to navigate the requirements that the FCC has stacked atop existing state and federal data breach notification laws.

The *Order* exceeds the FCC's authority in multiple respects. First, it applies data breach reporting requirements to a broad swath of personally identifiable information ("PII"), which the FCC is not generally empowered to regulate absent specific direction from Congress. A2–3 (*Order* ¶ 3). Consistent with the Communications Act of 1934, as amended (the "Act"), the FCC has long maintained data breach requirements governing customer proprietary network information ("CPNI"), which is a narrower set of telecommunications-specific customer data. 47 U.S.C. § 222; *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed

Rulemaking, 22 FCC Rcd 6927 (2007) ("*2007 Order*"). But the FCC has no unique privacy expertise, and Congress has given it no charge to regulate telecommunications carriers regarding non-CPNI PII. Second, Congress previously disapproved of substantially the same regulation pursuant to the Congressional Review Act ("CRA"). 5 U.S.C. §§ 801–808; Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Pub. L. No. 115-22, 131 Stat 88 (2017) ("Resolution"); *see also Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, 31 FCC Rcd 13911 (2016) ("*2016 Order*"). Attempting to overrule Congress's clear disapproval is inconsistent with the CRA and thus violates the Administrative Procedure Act ("APA"). The FCC also failed to provide notice that satisfies the APA. Through the Act and the Resolution, Congress directed the FCC to take a measured approach to privacy that aligns with Congress's connectivity goals. The FCC has disregarded Congress's direction, and the Court should set aside the *Order*.

ARGUMENT

I. THE FCC ERRED IN EXTENDING ITS BREACH NOTICE REQUIREMENTS BEYOND CUSTOMER PROPRIETARY NETWORK INFORMATION.

Existing state data breach reporting requirements already establish carriers' reporting obligations for breaches of PII. The FCC's attempt to fill a contrived "gap" contradicts policy goals articulated by Congress by hindering the efforts of small

providers serving rural and other high-cost areas to continue to close the digital divide and serve their customers.[2] Beyond contradicting Congress's policy goals, the FCC's assertion of authority over carriers regarding breaches of PII exceeds its statutory authority.

A. The *Order*'s Regulation of Personally Identifiable Information Harms Small Providers' Ability to Deploy Networks and Serve Their Communities.

The FCC's unlawful expansion of its data breach reporting requirements to encompass non-CPNI PII conflicts with Congress's fundamental policy goals for reliable advanced connectivity, including broadband.[3] Congress created the FCC "to make available, so far as possible, to all the people of the United States, . . . a rapid, efficient, Nation-wide, and world-wide wire and radio communication service

---

[2] The *Order* joins with other aspects of the FCC's ongoing regulatory onslaught that will siphon resources away from Congress's broadband investment goals and into counterproductive regulatory compliance efforts, especially for smaller providers. The FCC has asserted vast and unprecedented authority to regulate virtually all aspects of the provision of broadband in its recent net neutrality and digital discrimination orders. *See Safeguarding and Securing the Open Internet et al.*, Declaratory Ruling, Order, Report and Order, and Order on Reconsideration, FCC 24-52 (rel. May 7, 2024) ("*Title II Order*"); *Implementing the Infrastructure Investment and Jobs Act: Prevention and Elimination of Digital Discrimination*, Report and Order and Further Notice of Proposed Rulemaking, FCC 23-100 (rel. Nov. 20, 2023).

[3] While the *Order* focuses on voice service, the resources that service providers expend on added compliance burdens as a result of the *Order* cannot be invested in broadband. *See generally* A2 (*Order* ¶ 1) (addressing telecommunications carriers and interconnected Voice over Internet Protocol providers).

with adequate facilities at reasonable charges." 47 U.S.C. § 151. Thus, the FCC must tailor its regulatory approach to amplify private sector efforts to connect communities. In the Bipartisan Infrastructure Law enacted in 2021, Congress emphasized that "[a]ccess to affordable, reliable, high-speed broadband is essential to full participation in modern life in the United States" and that "[t]he persistent 'digital divide' in the United States is a barrier to the economic competitiveness of the United States and equitable distribution of essential public services, including health care and education." *Id.* § 1701(1)–(2).

The Associations' service provider members play a unique and essential role in achieving Congress's connectivity goals. Most are small businesses that lack dedicated in-house privacy and regulatory compliance teams. They predominantly operate in rural or other hard-to-reach communities that require special expertise, investment, and commitment to serve. Absent Association members' ongoing investments, these communities may lack the broadband connectivity that is essential to participation in the modern economy, access to health care and education, and civic engagement. As federal and state authorities are poised to make unprecedented investments in universal connectivity via the Bipartisan Infrastructure Law's $42.5 billion Broadband Equity, Access, and Deployment

Program and other programs,[4] the Associations' members are well-positioned to seek and make use of support to serve their communities more effectively than ever.

But the *Order* hinders such participation and other broadband connectivity efforts by imposing additional, unnecessary regulatory compliance costs on these small businesses. Congress recognized the harm of overregulation in establishing that "[i]t is the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." *Id.* § 230(b)(2). Small providers that disproportionately operate in hard-to-serve areas are especially sensitive to heightened regulatory compliance costs because they lack the ability to prorate costs across large customer bases. Because of their small staffs, they often must seek out and pay for specialized assistance to review, update, and implement internal procedures for new regulations and to ensure compliance once new regulations are in effect. *See, e.g.,* Letter from Angela Simpson, Senior Vice President & General Counsel, CCA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 22-21, at 3 (Dec. 8, 2023); Letter from Michael Romano, Executive Vice President, NTCA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 22-21, at 2 (Dec. 6, 2023).

[4] *See generally* National Telecommunications and Information Administration, Internet for All, Programs, https://www.internetforall.gov/programs (last visited May 29, 2024).

Association members are committed to customer privacy and are especially sensitive to the privacy needs of their small customer bases. Overregulation saps resources that could otherwise be invested to address customers' (as opposed to regulators') privacy preferences. Moreover, Association members generally are already subject to state data breach notification laws applicable to PII (or personal information), as the FCC itself acknowledges. A6 (*Order* ¶ 12) (stating that "all 50 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have laws requiring covered entities to notify individuals of data breaches"); *id.* 8–9 (*Order* ¶ 16) (stating that "[a]ll state data breach notification requirements explicitly include categories of sensitive personal information within their scope"); 47 C.F.R. § 64.2011(f) ("This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency."). Thus, consumers are already protected by those state laws in the manner each respective state deems appropriate. Carriers' practices and state data breach laws will continue to evolve, but the *Order* prejudges the correct approach nationwide.

The FCC's definition of PII extends further than many state laws in several respects, imposing potentially significant new costs on Association members and greatly complicating efforts to discern what may constitute a breach and what

obligations then attach. Of note, only about half of state data breach laws encompass medical data, fewer than half encompass biometric data, and only a handful encompass genetic data. *See generally Security Breach Notification Laws*, National Conference of State Legislatures (last updated Jan. 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws. In contrast, carriers will be subject to breach notification obligations to the FCC for such data nationwide under the *Order*. The FCC has indicated that it may extend its regulations beyond the information within the scope of the *Order*, meaning its definition of PII could further diverge from state practices. *See* A11 (*Order* ¶ 19) (cautioning that "[n]otwithstanding these limitations, we will monitor the data security landscape and will not hesitate to revisit and revise the list of data elements in a future rulemaking as necessary to ensure that carriers adequately protect sensitive customer data").

Association members cannot be certain of whether the FCC's approach to the scope of a reportable breach of PII diverges from or creates a legal conflict with state law. The FCC does not define the various forms of information it included within the scope of PII, such as "information necessary to permit access to an account" or "medical data." *Id.* 10–11 (*Order* ¶ 18); *id.* 77–78 (*Order* App. A, 47 C.F.R. § 64.2011(e)(5)). While the FCC lists examples of each form of information, it is careful to state that each such form merely "[i]nclude[s], but [is] not limited to" those

specific examples. *Id.* 10–11 (*Order* ¶ 18 nn.53-56). Thus, if a carrier suffers a loss of data that includes, for example, information that relates to health, it cannot conclusively know if the FCC would deem that occurrence a breach. The need to evaluate potential conflict and divergence between federal and state law creates uncertainty and adds costs for carriers.

Even where the FCC's definition of PII and a state's definition of personal information or PII completely overlap, the FCC's expansion of its rules to encompass PII can impose significant additional burdens. For example, the FCC requires notice to federal law enforcement officials that state laws do not require. *Compare* Carol M. Hayes, *Comparative Analysis of Data Breach Laws: Comprehension, Interpretation, and External Sources of Legislative Text*, 23 Lewis & Clark L. Rev. 1221, 1255 (2020) ("Hayes") ("There are three main recipients of data breach notifications: the consumer, the state Attorney General, and credit reporting agencies."), *with* A76–77 (*Order* App. A, 47 C.F.R. § 64.2011(a)) (requiring notice to the FCC, the U.S. Secret Service, and the Federal Bureau of Investigation). The FCC also requires notice to consumers when state law would not require it. *See infra* Section II.A. Accordingly, carriers may face added notification costs because of the FCC expanding its breach rule to encompass PII.

In sum, the *Order*'s expansion of the FCC's data breach rule to encompass PII undermines Congress's policy goals and Association members' ability to invest

in and serve their communities. Not surprisingly given Congress's clear policy goals, it also exceeds the statutory authority Congress granted to the Commission, as explained in detail below.

B. The FCC Lacks Authority to Regulate Carrier Notification of Breaches of Personally Identifiable Information.

Congress did not give the FCC the authority it asserts to require carrier notifications of breaches of non-CPNI PII. Although the FCC asserts authority under Sections 222 and 201(b) of the Act, neither provides the requisite authority, and accordingly, the FCC's *Order* is invalid. *See generally La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986) (stating that the FCC "literally has no power to act" absent a statutory delegation of authority).

Via Section 222, Congress gave the FCC responsibility over CPNI, which Congress defined as certain types of information that carriers possess because of their specific role of providing telecommunications services such as legacy telephone service. *See* 47 U.S.C. § 222(h)(1)(A)–(B) (defining CPNI as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service . . . and that is made available . . . solely by virtue of the carrier-customer relationship; and information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier"); *cf. Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer*

Proprietary Network Information and Other Customer Information, Order, 13 FCC Rcd 12390, 12395 ¶ 8 (CCB 1998) ("We clarify that a customer's name, address, and telephone number do not fall within the definition of CPNI . . . ."). Congress laid out carriers' duties, and exceptions from those duties, with respect to CPNI in considerable detail. *See* 47 U.S.C. § 222(c)–(g). But it made no such pronouncement in Section 222 regarding PII.

The FCC points to Section 222(a), which sets forth the general proposition that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, . . . customers," as supporting its assertion of authority over breaches involving PII. *Id.* § 222(a); A58 (*Order* ¶ 118). But that conclusion flies in the face of the text and structure of Section 222. While the statute defines CPNI in detail, it does not otherwise define customer "proprietary information." *See* 47 U.S.C. § 222. And while Section 222 also prescribes carriers' duties with regard to CPNI in detail, it does not set forth any detail regarding a distinct "duty" of confidentiality with respect to any other customer "proprietary information," whether PII or otherwise.

The only correct interpretation is that the customer "proprietary information" to which Section 222(a) refers is CPNI, and the contours of the customer confidentiality duty referenced in Section 222(a) are articulated in the remainder of Section 222. This reading explains why Section 222 does not reference PII, in

contrast to other provisions of the Act. *See* 47 U.S.C. §§ 338(i), 551; *see also Bittner v. United States*, 598 U.S. 85, 94; 143 S. Ct. 713, 720 (2023). It comports with the title of Section 222(a), "In general." 47 U.S.C. § 222(a); *see also Rudisill v. McDonough*, 144 S. Ct. 945, 955 (2024) (stating that "[s]ection headings supply cues as to what Congress intended") (cleaned up). It explains the title of Section 222(c)(1), "Privacy requirements for telecommunications carriers," which suggests that additional customer privacy requirements for carriers are not to be found elsewhere unannounced. 47 U.S.C. § 222(c)(1). And it aligns with the well-established canon of statutory construction that specific provisions control more general ones. *Metro. Detroit Area Hosp. Servs. v. United States*, 634 F.2d 330, 334 (6th Cir. 1980) ("It is an elementary rule of statutory construction that a specific provision controls when the same subject matter is addressed by a more general provision.").[5]

Nor does Section 201(b) provide the authority that the FCC claims. A61–62 (*Order* ¶ 124). Section 201(b) states that "[a]ll charges, practices, classifications, and regulations for and in connection with such communication service, shall be just

[5] The FCC's reading, by contrast, unreasonably assumes that Congress wished to direct privacy protections for CPNI in detail but gave the FCC greater discretion to determine how to regulate telecommunications carrier privacy practices for the broader category of PII. *See* A9–10 (*Order* ¶ 17) (asserting that "CPNI is a subset of PII"). It defies reason to assume that Congress felt the expert telecommunications agency had less competence to determine how to regulate the treatment of telecommunications-specific information (i.e., CPNI) than PII.

and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful," and that the FCC may "prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter." 47 U.S.C. § 201(b). The FCC's assertion contradicts the basic canon of statutory construction that a specific statutory provision (i.e., Section 222) supersedes the more general one (i.e., Section 201(b)). *See Metro. Detroit*, 634 F.2d at 334.

The broader statutory structure and legislative history confirm that Section 201(b) does not provide authority for the FCC to regulate breaches involving PII. In enacting Section 222, Congress chose not to include the savings clause it inserted into Section 251, stating that "[n]othing in this section shall be construed to limit or otherwise affect the Commission's authority under section 201 of this title." 47 U.S.C. § 251(i); *see also* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, 66 (1996). "When Congress includes particular language in one section of a statute but omits it from a neighbor, we normally understand that difference in language to convey a difference in meaning (*expressio unius est exclusio alterius*)." *Bittner*, 598 U.S. at 94; 143 S. Ct. at 720. The legislative history confirms that Congress expected Section 222 to "protect all consumers" and explained that it "strives to balance both competitive and consumer privacy interests." S. Rep. No. 104-230, at 204–05 (1996) (Conf. Rep.). Congress thus understood that the FCC

would rely on Section 222 and not other authority to address telecommunications privacy.

In sum, if Congress wanted the FCC to regulate telecommunications carriers regarding customer notification of breaches of PII, it could have said so. It did not, and the FCC cannot proceed without the requisite authority.

II. THE CONGRESSIONAL REVIEW ACT PRECLUDES THE FCC'S DATA BREACH NOTIFICATION RULE.

The *Order* violates the CRA by effectively reissuing the data breach notification rule that Congress disapproved. In 2016, the FCC adopted an order that sought to apply new privacy requirements to both broadband Internet access service providers and to voice carriers and others already subject to its CPNI rules. *2016 Order*, 31 FCC Rcd at 13911. As a part of that decision, the FCC adopted a revised data breach notification rule that is substantially the same as the one set forth in the *Order*. The *2016 Order* was short-lived; Congress swiftly enacted a resolution of disapproval that, under the CRA, made the breach notification rule "have no force or effect" and barred the FCC from adopting substantially the same rule in the future. In adopting the Resolution, Congress reenforced its preference for measured policy that avoids needless costs that disproportionately harm Association members and the customers they serve.

Yet contrary to the CRA, the FCC adopted the *Order*, which effectively reissues the *2016 Order*'s breach notification rule. The FCC asserts that it may do

so because Congress only disapproved the entirety of the *2016 Order*, not its individual components. However, this interpretation is contrary to the text of the CRA and, if adopted by the courts, would effectively write the CRA out of the U.S. Code.

A. Retreading the Ground of the *2016 Order* Harms Small Carriers and Their Current and Potential Customers.

In adopting substantially the same breach notification reporting rule as in the *2016 Order*, the FCC undermines Congress's goal of facilitating investment and customer service by Association members. By contradicting the Resolution, the FCC's *Order* runs counter to the policy preferences that necessarily underlie the Resolution. Further, by imposing significant requirements on providers in comparison to what would otherwise apply under current state law, the requirements that the FCC adopts in contravention of the CRA impose unnecessary and burdensome costs that hinder small providers from achieving Congress's connectivity goals and from serving their customers efficiently.

First and most significantly, the *2016 Order* breach notification rule encompassed PII, just like the *Order*. *2016 Order*, 31 FCC Rcd at 13928 ¶ 46, 14025–26 ¶ 274. By again regulating PII, the *Order* imposes significant new costs on Association members because, as discussed above, the FCC's definition of PII extends further than many state laws and requires additional data breach notifications. *Supra* Section I.A. The more types of information that a breach

notification rule covers, the more notifications that carriers may have to send to customers.

Second, the *Order* follows the model of the *2016 Order* by taking an overbroad and vague approach to defining cognizable "harm." The *Order* requires carriers to notify customers after reasonable determination of a breach, subject to certain exceptions. A77 (*Order* App. A, 47 C.F.R. § 64.2011(b)). One exception is the "harm-based trigger": where a carrier reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach, customer notification is not required, and, for breaches that affect fewer than 500 customers, notification to government agencies is only required through an annual report. *Id.* 76–77 (*Order* App. A, 47 C.F.R. § 64.2011(a)(3), (b), (d)). The *2016 Order* also adopted a harm-based trigger. *2016 Order*, 31 FCC Rcd at 14020–21 ¶ 263. Like the FCC's approach, many state laws have harm-based triggers to notification requirements. *See*, *e.g.*, Wis. Stat. § 134.98(2)(cm)(1); Ariz. Rev. Stat. § 18-552(J); Fla. Stat. § 501.171; Ind. Code § 24-4.9-3-1; Utah Code § 13-44-202(1); W.V. Code § 46A-2A-102(a).

As to the harms they contemplate, state data breach notification laws "are almost always focused on the breach of personal information that could facilitate identity theft." Hayes, 23 Lewis & Clark L. Rev. at 1253. For instance, customer notification is not required by Wisconsin law unless the acquisition of information

creates a "material risk of identity theft or fraud," Wis. Stat. § 134.98, and not required by Arizona law if the breach has not or is not reasonably likely to result in "substantial economic loss to affected individuals." Ariz. Rev. Stat. §18-552 (J).

In contrast, in 2016, the FCC "disagree[d] with commenters who assert that financial loss or identity theft should be the primary metrics for determining the level of harm or whether harm exists." *2016 Order*, 31 FCC Rcd at 14022 ¶ 266. Reusing similar language, it again "disagree[s] with commenters arguing that 'harm' should only include the risk of identity theft or financial harm" in the *Order*. A33 (*Order* ¶ 56). Instead, the *Order* takes a "broad approach" to the definition of harm. *Id.* 32–33 (*Order* ¶ 55). The FCC defines harm to include, for instance, "the disclosure of private facts." *Id.* Carriers generally, but particularly small carriers with fewer resources, are not well-positioned to determine which facts are "private." Further, the FCC's definition of "harm" is unbounded, in that it "include[s], but is not limited to" the specific categories of harm enumerated by the FCC and encompasses "other similar types of dangers" to those listed. *Id.* The *Order* sets forth a nebulous list of factors to consider when evaluating the likelihood of harm, but it does not explain how those factors should be employed. *Id.* 34–35 (*Order* ¶ 57). Association members are left to guess at what "harm" might include.

The burden of this ambiguity is amplified by the fact that as in 2016, the onus is on carriers to demonstrate that there is not a likelihood of "harm" to customers to

overcome the rebuttable presumption. *Id.* 31–32 (*Order* ¶ 53); *see also 2016 Order*, 31 FCC Rcd at 14022 ¶ 265. In contrast to the FCC's repeated approach, not all states with breach notification laws presume harm. *See, e.g.*, Haw. Rev. Stat. §§ 487N-1 to -2; N.C. Gen. Stat. §§ 75-61(14), 75-65(a). Because of the FCC's willingness to again take an expansive and vague approach despite the Resolution, carriers may be more likely to err on the side of determining that a harm may occur and thus send more notifications than otherwise necessary under state laws. The costs of these obligations fall particularly hard on smaller carriers.

As a final example, the FCC's decision to again remove the intent limitation from the definition of breach also expands the number of incidents that trigger customer notification, even when such notification may not provide a commensurate benefit to customers or their safety. *See 2016 Order*, 31 FCC Rcd at 14024 ¶ 270; A12 (*Order* ¶ 21). To obtain information from employees or contractors for every inadvertent access, use, or disclosure of covered information, carriers will have to implement costly and burdensome processes, particularly considering the FCC's expansive definition of covered information. *See, e.g.,* Comments of NTCA, WC Docket No. 22-21, at 4 (Feb. 22, 2023); Reply Comments of WTA, WC Docket No. 22-21, at 2 (Mar. 24, 2023). Due to their expenditures typically comprising a small part of a contractor's revenue, small providers may have particular difficulty exerting pressure on vendors to comply with FCC regulations.

The FCC's decision to violate the CRA by (among other things) again addressing PII, adopting a broad definition of "harm," and removing intentionality from its definition of "breach" harms consumers in addition to Association members. First, contrary to Congress's pro-connectivity policies, the FCC's requirements force providers to divert resources from connecting and serving communities around the country. Second, contrary to the careful balance Congress struck in Section 222, the FCC's approach will lead to "notice fatigue," which occurs when customers receive so many notifications that they disregard notifications and risks to their security. *See* Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. Ill. L. Rev. 803, 822 (2021). Data breach notifications impose costs on customers, including time, stress, anxiety, and disengagement. *Id.* As consumers receive more and more notifications from varying sources, they are more and more likely to ignore those notifications despite the security risks. Finally, small carriers will expend resources that could otherwise be invested in privacy protections to keep up with emerging threats.

B. The FCC May Not Overrule Congress or Set Aside Its Direction.

Under the CRA, the enactment of the resolution disapproving the FCC's *2016 Order* prohibits the FCC from adopting the data breach notification rules in its *Order*. The CRA establishes the processes whereby Congress can void agency actions by enacting a joint resolution of disapproval of the rule. 5 U.S.C. § 802. If

the resolution of disapproval is enacted, "[a] rule shall not take effect (or continue)." *Id.* § 801(b)(1). After enactment, "[a] rule that does not take effect (or does not continue) . . . may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued," absent subsequent enactment of a law specifically authorizing the new rule. *Id.* § 801(b)(2).

The *2016 Order* and the *Order* altered the breach notification rule that the FCC adopted in 2007 in ways that are substantially the same. Most significantly, the *2016 Order*, like the *Order*, established carrier breach notification obligations with respect to PII. *See 2016 Order*, 31 FCC Rcd at 14025–26 ¶ 274; A8–12 (*Order* ¶¶ 15–20). Other examples abound. Both decisions adopted an overbroad harm-based trigger for customer notice and eliminated the limitation of the preexisting data breach notification rule to covering only intentional data access. *See 2016 Order*, 31 FCC Rcd at 14020–21 ¶ 263, 14024 ¶ 270; A12–16, 30–36 (*Order* ¶¶ 121–25, 52–58); *see also supra* Section II.A. Both decisions added the FCC to the government entities that carriers must notify of certain breaches. *2016 Order*, 31 FCC Rcd at 14026 ¶ 276; A18 (*Order* ¶ 28). And both established the same deadlines for notifying customers of a breach. *2016 Order*, 31 FCC Rcd at 14029 ¶ 284; A77 (*Order* App. A, 47 C.F.R. § 64.2011(b)). Because the *Order* substantially tracks the same rule that was disapproved due to the Resolution passed by Congress, the CRA bars the FCC from adopting the *Order*.

1. The FCC May Not Ignore Congress by Separately Adopting Components of the *2016 Order*.

In the *Order*, the FCC posits that because "the joint resolution referred to the entirety of the [*2016 Order*]," the reissuance prohibition only applies to a "rule" that is "the entire [*2016 Order*] with all of the rule revisions adopted therein." A68 (*Order* ¶ 136). Thus, under the FCC's interpretation, it may issue any rules contained within the *2016 Order* as long as it does not adopt the whole of the *2016 Order*. *Id*.

However, the CRA does not permit agencies, including the FCC, to sidestep Congress's disapproval. The CRA prohibits agencies from reissuing "[a] rule that does not take effect (or does not continue)" as a result of a resolution of disapproval. 5 U.S.C. § 801(b)(2). The *2016 Order* data breach notification rule was "a rule" that was halted because of the Resolution. Thus, the common-sense meaning of the statute bars reissuance of a component rule, as well as the entirety, of the *2016 Order*.

Indeed, the FCC has implicitly acknowledged that the data breach notification rule it adopted in the *2016 Order* was a rule within the ordinary meaning of that term. In 2016, the FCC identified that the separate rules that made up the *2016 Order*, including the data breach rule to be codified at 47 C.F.R. § 64.2006, were themselves rules. *See 2016 Order*, 31 FCC Rcd at 14080 (App. A, 47 C.F.R. § 64.2001) (re-adopting into the Code of Federal Regulations references to the "rules

in this subpart" and the "purpose of the rules" in describing the rules adopted in the *2016 Order*).

The FCC's new interpretation also is inconsistent with the statutory definition of a "rule." The CRA incorporates the APA definition of "rule" to mean "the whole or *a part of* an agency statement of general . . . applicability and future effect designed to . . . prescribe law or policy." 5 U.S.C. § 804(3); *id.* § 551(4) (emphasis added). The term "rule" therefore refers both to an entire agency statement that prescribes obligations *and* every component part of that statement. The data breach notification rule is plainly a component part of the *2016 Order* that prescribes legal obligations; therefore, it is a "rule" within the meaning of the CRA.

The FCC's current position implies that Congress should have identified specific provisions in the Resolution. However, there is no requirement in the CRA that Congress identify specific provisions. To the contrary, the CRA requires resolutions of disapproval to include a statement using the specific formula, "'That Congress disapproves the rule submitted by the __ relating to __, and such rule shall have no force or effect.' (The blank spaces being appropriately filled in)." *Id.* § 802(a). Congress followed this formula here. *See* Resolution. Congress thus understood itself to have disapproved of "the whole" and each "part of" the *2016 Order*, including the data breach reporting rule. And indeed, the record reflects that the breach notification rule contributed to Congress's disapproval of the *2016 Order*.

163 Cong. Rec. H2479 (daily ed. Mar. 28, 2017) (statement of Rep. Burgess) (explaining that he disapproved of the *2016 Order* in part because it may "result in more frequent breach notifications, leading to a weaker focus on security by consumers who do suffer from notification fatigue"); *see also supra* Section II.A.

The FCC's position that the CRA only prevents an agency from reissuing a decision "in whole, or in substantially the same form," is untenable. A67 (*Order* ¶ 135). The FCC's theory is self-defeating because it effectively leaves an agency free to adopt portions of the disapproved decision, part by part, until the whole has been recreated. Even if that were out of bounds, the FCC's approach leads to bedeviling line-drawing exercises regarding how much recreation of the disapproved decision is "too much." The FCC's approach would empower agencies to treat legislation as a mere bump in the road. However, "[i]t is axiomatic that an administrative agency's power to promulgate legislative regulations is limited to the authority delegated by Congress." *Bowen v. Georgetown Univ. Hosp.*, 488 U.S. 204, 208 (1988).

The possibility of piecemeal reenactment is not merely hypothetical. The FCC asserts that it is not, through the *Order*, "adopting something substantially the same as the [*2016 Order*] as a whole through the aggregate effect of individual Commission actions." A71 (*Order* ¶ 143). Even if true, this statement does not bind the FCC going forward. The FCC recently asserted that broadband Internet access

service is a common carriage service subject to Section 222. *See Title II Order* ¶¶ 67–68, 349–359 (asserting authority over broadband Internet access service provider privacy practices, including with respect to PII). Although the FCC waived application of rules implementing Section 222 to broadband, the *Title II Order* leaves the door open for future application of the FCC's privacy rules to broadband Internet access service providers, including by revisiting its waiver of application of those rules to broadband at any time. *See id.*

2. The *Order* Violates the Administrative Procedure Act.

The FCC's violation of the CRA further violates the APA's prohibition against agency actions that are "not in accordance with the law." 5 U.S.C. § 706(2)(A). As discussed above, Congress disapproved of the *2016 Order*, including its component rules. *See supra* Section II.B.1. Yet the FCC issued the *Order*, which is "substantially the same" as the breach notification rule contained within the *2016 Order*, without new authorization from Congress. 5 U.S.C. § 801(b)(2). This issuance violated the CRA, and thus the APA.

Additionally, the FCC failed to provide sufficient notice as required under the APA. The APA requires that agencies provide notice of proposed rules and an opportunity for interested persons to participate in the rulemaking proceeding. *Id.* § 553(b)–(c). To satisfy the notice requirement, the final rule must be a "logical outgrowth" of the proposed rule. *See Long Island Care at Home, Ltd. v. Coke*, 551

U.S. 158, 174 (2007). However, in the Notice of Proposed Rulemaking issued prior to the *Order*, the FCC made no indication that it was issuing a new rule that is "substantially the same" as the breach notification rule in the *2016 Order*. *See* A98 (*Order* Statement of Commissioner Brendan Carr); *id.* 102–103 (*Order* Statement of Commissioner Nathan Simington). *See generally id.* 120–161 (*Data Breach Reporting Requirements*, Notice of Proposed Rulemaking, 38 FCC Rcd 566 (2022) ("*Notice*")). Indeed, the FCC explicitly stated that it was *not* seeking comment on reissuing a rule in substantially the same form or substantially the same as the disapproved rule. *Id.* 143 (*Notice*, 28 FCC Rcd at 589 ¶ 52). Under the logical outgrowth test, an agency may not "pull a surprise switcheroo on regulated entities." *Env't Integrity Project v. EPA*, 425 F.3d 992, 996 (D.C. Cir. 2005). Additionally, the FCC gave no indication regarding its interpretation of the CRA. *See* A143 (*Notice*, 28 FCC Rcd at 589 ¶ 53). This lack of notice denied interested parties, including Association members, of their right to participate in the development of the FCC's *Order* and thus violated the APA.

III. CONCLUSION.

For these reasons, this Court should hold unlawful and set aside the *Order*.

Respectfully submitted,

/s/ Craig E. Gilmore
Craig E. Gilmore
Daniel H. Kahn
Wilkinson Barker Knauer, LLP
1800 M Street NW, Suite 800N
Washington, DC 20036
(202) 783-4141
cgilmore@wbklaw.com
dkahn@wbklaw.com
Counsel for ACA Connects, CCA, NTCA, WISPA, and WTA

May 29, 2024

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitations of Fed. R. App. P. 29(a)(5) because this brief contains 6,377 words, excluding the parts of the brief exempted by Fed. R. App. 32(f) and 6 Cir. R. 32(b)(1).

2. This brief 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) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word using 14-point Times New Roman font.

/s/ Craig E. Gilmore
Craig E. Gilmore

CERTIFICATE OF FILING AND SERVICE

I hereby certify that on May 29, 2024, I filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the Sixth Circuit using the electronic CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the CM/ECF system.

/s/ Craig E. Gilmore
Craig E. Gilmore