

Nos. 24-3133, 24-3206, 24-3252

**IN THE UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT**

OHIO TELECOM ASSOCIATION; TEXAS ASSOCIATION OF BUSINESS;
CTIA – THE WIRELESS ASSOCIATION;
NCTA – THE INTERNET & TELEVISION ASSOCIATION;
USTELECOM – THE BROADBAND ASSOCIATION,

Petitioners,

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

PETITIONERS' OPENING BRIEF

Roman Martinez
Matthew A. Brill
Matthew T. Murchison
Charles S. Dameron
Christina R. Gay
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
(202) 637-2200
roman.martinez@lw.com

Counsel for Petitioners

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: Roman Martinez

Pursuant to 6th Cir. R. 26.1, Ohio Telecom 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 22, 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/Roman Martinez

Latham & Watkins LLP

Washington, DC 20004

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: 24-3206

Case Name: Texas Association of Business v. FCC, et al.

Name of counsel: Roman Martinez

Pursuant to 6th Cir. R. 26.1, Texas Association of Business

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 22, 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/Roman Martinez

Latham & Watkins LLP

Washington, DC 20004

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: 24-3252

Case Name: CTIA - The Wireless Ass'n, et al. v. FCC, et al.

Name of counsel: Roman Martinez

Pursuant to 6th Cir. R. 26.1, CTIA – The Wireless 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 22, 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/Roman Martinez

Latham & Watkins LLP

Washington, DC 20004

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: 24-3252

Case Name: CTIA - The Wireless Ass'n, et al. v. FCC, et al.

Name of counsel: Roman Martinez

Pursuant to 6th Cir. R. 26.1, NCTA – The Internet & Television 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 22, 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/Roman Martinez

Latham & Watkins LLP

Washington, DC 20004

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: 24-3252

Case Name: CTIA - The Wireless Ass'n, et al. v. FCC, et al.

Name of counsel: Roman Martinez

Pursuant to 6th Cir. R. 26.1, USTelecom – The 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 22, 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/Roman Martinez

Latham & Watkins LLP

Washington, DC 20004

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

	Page
DISCLOSURES OF CORPORATE AFFILIATIONS AND FINANCIAL INTEREST	i
TABLE OF AUTHORITIES	viii
STATEMENT IN SUPPORT OF ORAL ARGUMENT	1
JURISDICTIONAL STATEMENT	2
STATEMENT OF THE ISSUES.....	2
INTRODUCTION	3
STATEMENT OF THE CASE.....	7
A. Consumer Privacy Under The Communications Act.....	7
B. The 1998 CPNI Order And 2007 Reporting Rule.....	10
C. The Broadband Privacy Order And 2016 Reporting Rule.....	12
D. Congress’s Disapproval Of The Broadband Privacy Order Under The Congressional Review Act.....	13
E. The 2024 Reporting Rule	16
SUMMARY OF ARGUMENT	20
STANDARD OF REVIEW	22
ARGUMENT	23
I. The FCC Lacks Authority Under The Communications Act To Require Reporting Of Data Breaches Involving PII	23
A. Section 222 Permits The Regulation Of Customer Proprietary Network Information, Not Personally Identifiable Information	23
B. The FCC’s Contrary Arguments Lack Merit	31
II. The Congressional Review Act Bars The 2024 Reporting Rule’s Regulation Of PII.....	38

	Page
A. Congress’s 2017 Disapproval Resolution Forbids Issuance Of Any New Rule “Substantially The Same As” The 2016 Reporting Rule.....	39
B. The 2024 Reporting Rule Is Substantially The Same As The 2016 Reporting Rule	43
C. The FCC Cannot Reconcile The 2024 Reporting Rule With Congress’s Disapproval Resolution	47
CONCLUSION	58

TABLE OF AUTHORITIES

Page(s)

CASES

<i>Augustus v. Commissioner</i> , 118 F.2d 38 (6th Cir. 1941)	28
<i>Bais Yaakov of Spring Valley v. FCC</i> , 852 F.3d 1078 (D.C. Cir. 2017).....	23
<i>Bankamerica Corp. v. United States</i> , 462 U.S. 122 (1983).....	29, 37
<i>California Independent System Operator Corp. v. FERC</i> , 372 F.3d 395 (D.C. Cir. 2004).....	38
<i>Center for Biological Diversity v. Bernhardt</i> , 946 F.3d 553 (9th Cir. 2019)	40, 54
<i>FERC v. Electric Power Supply Association</i> , 577 U.S. 260 (2016).....	38
<i>Gustafson v. Alloyd Co.</i> , 513 U.S. 561 (1995).....	37
<i>KenAmerican Resources, Inc. v. United States Secretary of Labor</i> , 33 F.4th 884 (6th Cir. 2022)	23
<i>Louisiana Public Service Commission v. FCC</i> , 476 U.S. 355 (1986).....	3
<i>Middle South Energy, Inc. v. FERC</i> , 747 F.2d 763 (D.C. Cir. 1984).....	28
<i>Qwest Corp. v. Arizona Corp. Commission</i> , 567 F.3d 1109 (9th Cir. 2009)	36
<i>Qwest Corp. v. Minnesota Public Utilities Commission</i> , 684 F.3d 721 (8th Cir. 2012)	36
<i>RadLAX Gateway Hotel, LLC v. Amalgamated Bank</i> , 566 U.S. 639 (2012).....	35

	Page(s)
<i>Retail Ventures, Inc. v. National Union Fire Insurance Co. of Pittsburgh,</i> 691 F.3d 821 (6th Cir. 2012)	24, 31
<i>Russello v. United States,</i> 464 U.S. 16 (1983).....	36
<i>U.S. West, Inc. v. FCC,</i> 182 F.3d 1224 (10th Cir. 1999)	29
<i>United States v. Boulding,</i> 960 F.3d 774 (6th Cir. 2020)	50
<i>United States v. Pennsylvania Railroad Co,</i> 242 U.S. 208 (1916).....	37
<i>Utility Air Regulatory Group v. EPA,</i> 573 U.S. 302 (2014).....	37

ADMINISTRATIVE MATERIALS

<i>Implementation of the Telecommunications Act of 1996:</i> <i>Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information and Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended, Second Report and Order, 13 FCC Rcd 8061 (1998).....</i>	<i>8, 10, 29, 30</i>
<i>Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, Order on Reconsideration, 14 FCC Rcd 14409 (1999)</i>	<i>37</i>
<i>Implementation of the Telecommunications Act of 1996:</i> <i>Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information; Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended, Third Report and Order, 17 FCC Rcd 14860 (2002).....</i>	<i>29</i>

	Page(s)
<i>Implementation of the Telecommunications Act of 1996:</i>	
<i>Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, Notice of Proposed Rulemaking, 21 FCC Rcd 1782 (2006)</i>	30
<i>Implementation of the Telecommunications Act of 1996:</i>	
<i>Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, Report and Order, 22 FCC Rcd 6927 (2007).....</i>	<i>passim</i>
<i>Implementation of the Telecommunications Act of 1996:</i>	
<i>Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, Declaratory Ruling, 28 FCC Rcd 9609 (2013).....</i>	30
<i>Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,</i>	
<i>Report and Order, 31 FCC Rcd 13911 (2016).....</i>	<i>passim</i>

STATUTES AND REGULATIONS

5 U.S.C. § 551(4)	14, 40, 51
5 U.S.C. § 553(b)	48
5 U.S.C. § 706.....	22
5 U.S.C. § 706(2)(A).....	23, 43, 48
5 U.S.C. § 706(2)(C).....	23, 43, 48
5 U.S.C. §§ 801-08.....	13
5 U.S.C. § 801(a)	53
5 U.S.C. § 801(a)(1)(A)	14
5 U.S.C. § 801(a)(1)(B)	14
5 U.S.C. § 801(b)(1).....	14, 39, 41
5 U.S.C. § 801(b)(2).....	<i>passim</i>

	Page(s)
5 U.S.C. § 802(a)	14, 53
5 U.S.C. § 802(c)	14
5 U.S.C. § 802(d)	14
5 U.S.C. § 802(e)	14
5 U.S.C. § 804(3)	14, 40, 51
15 U.S.C. § 6501(8)	27
15 U.S.C. § 6809(4)	27
28 U.S.C. § 2342(1)	2
28 U.S.C. § 2344	2
42 U.S.C. § 1320d-2(d)	27
47 U.S.C. § 151 <i>et seq.</i>	2
47 U.S.C. § 201(b)	18, 34, 37
47 U.S.C. § 202	38
47 U.S.C. § 203	38
47 U.S.C. § 204	38
47 U.S.C. § 205	38
47 U.S.C. § 222	7
47 U.S.C. § 222(a)	8, 24
47 U.S.C. § 222(b)	8
47 U.S.C. § 222(c)	8, 25
47 U.S.C. § 222(c)(1)	3, 9, 25
47 U.S.C. § 222(c)(2)	25

	Page(s)
47 U.S.C. § 222(d)	9
47 U.S.C. § 222(e)	33
47 U.S.C. § 222(g)	9, 33
47 U.S.C. § 222(h)(1).....	3, 8
47 U.S.C. § 251(i)	36
47 U.S.C. § 338(i)	27
47 U.S.C. § 396(l)(4)(B)	32
47 U.S.C. § 402(a)	2
47 U.S.C. § 551	27
Pub. L. No. 98-549, 98 Stat. 2779 (1984).....	27
Pub. L. No. 100-618 (1988)	27
Pub. L. No. 104-121, 110 Stat. 868 (1996).....	13
Pub. L. No. 104-191, 110 Stat. 1936 (1996).....	27
Pub. L. No. 105-277 (1998)	27
Pub. L. No. 106-102 (1999)	27
Pub. L. No. 108-447, 118 Stat. 3393 (2004).....	27
Pub. L. No. 115-22, 131 Stat. 88 (2017).....	15, 41, 53
47 C.F.R. § 64.2002(c) (2016).....	12, 44, 46
47 C.F.R. § 64.2002(f) (2016)	12, 44, 45
47 C.F.R. § 64.2002(m) (2016).....	12, 45
47 C.F.R. § 64.2002(n) (2016).....	12
47 C.F.R. § 64.2006 (2016)	12

	Page(s)
47 C.F.R. § 64.2006(a) (2016).....	44, 47, 56
47 C.F.R. § 64.2006(b) (2016).....	44, 47
47 C.F.R. § 64.2006(c) (2016).....	44, 45
47 C.F.R. § 64.2009 (1998)	10
47 C.F.R. § 64.2011 (2008)	10
47 C.F.R. § 64.2011(a) (2024).....	44, 47
47 C.F.R. § 64.2011(b) (2024).....	44, 46, 47, 56
47 C.F.R. § 64.2011(b) (2008).....	11, 44
47 C.F.R. § 64.2011(c) (2008).....	11, 44, 47
47 C.F.R. § 64.2011(d) (2008).....	11
47 C.F.R. § 64.2011(e) (2008).....	11, 44, 46
47 C.F.R. § 64.2011(e)(1) (2024)	17, 44, 45, 46
47 C.F.R. § 64.2011(e)(2) (2024)	17, 44, 45
47 C.F.R. § 64.2011(e)(5) (2024)	17, 18, 31

LEGISLATIVE MATERIALS

142 Cong. Rec. 6922 (1996).....	13, 15, 55
142 Cong. Rec. 8196 (1996).....	15
H.R. Rep. No. 104-204 90 (1995), <i>as reprinted in</i> 1996 U.S.C.C.A.N. 10	7, 35
H.R. Rep. No. 104-458 (1995).....	35
H.R. Res. 230, 115th Cong. (2017)	15
S.J. Res. 34, 115th Cong. (2017)	15
S. Rep. No. 104-230 (1996) (Conf. Rep.).....	7

OTHER AUTHORITIES

82 Fed. Reg. 44118 (Sept. 21, 2017)15, 42, 49

86 Fed. Reg. 4662 (Jan. 15, 2021)56, 57

89 Fed. Reg. 9968 (Feb. 12, 2024)2, 52

Black’s Law Dictionary (11th ed. 2019).....24

Jody Freeman & Matthew C. Stephenson, *The Untapped Potential of
the Congressional Review Act*, 59 Harv. J. on Legis. 279 (2022).....16

Inc., *Proprietary Information* (Jan. 5, 2021),
<http://www.inc.com/encyclopedia/proprietary-information.html>24

Security Breach Notification Laws, National Conference of State
Legislatures (last updated Jan. 17, 2022),
[https://www.ncsl.org/research/telecommunications-and-
information-technology/security-breach-notification-laws.aspx](https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).....28

STATEMENT IN SUPPORT OF ORAL ARGUMENT

Pursuant to Circuit Rule 34(a), petitioners Ohio Telecom Association, Texas Association of Business, CTIA – The Wireless Association, NCTA – The Internet & Television Association, and USTelecom – The Broadband Association (collectively, “petitioners”) respectfully request oral argument in this case. As described below, this case implicates important questions regarding the construction of two federal statutes: the Communications Act and the Congressional Review Act. Petitioners submit that oral argument will aid this Court’s consideration of those questions, especially in the absence of precedent from this Court directly interpreting the relevant provisions.

JURISDICTIONAL STATEMENT

On February 12, 2024, pursuant to the Communications Act of 1934, as amended, *see* 47 U.S.C. § 151 *et seq.*, the Federal Communications Commission (“FCC”) published a final rule, titled Data Breach Reporting Requirements (“the 2024 Reporting Rule”), in the Federal Register. 89 Fed. Reg. 9968 (Feb. 12, 2024); *see* Petitioners’ Appendix (“A”) 1-104. Petitioners timely filed their petitions for review on February 20 and March 15, 2024. 28 U.S.C. § 2344; A105-19. This Court has jurisdiction under 28 U.S.C. § 2342(1) and 47 U.S.C. § 402(a).

STATEMENT OF THE ISSUES

1. Whether the 2024 Reporting Rule must be set aside under the Administrative Procedure Act (APA) because it exceeds the FCC’s statutory authority under the Communications Act.
2. Whether the 2024 Reporting Rule must be set aside under the APA because it violates the Congressional Review Act.

INTRODUCTION

This case involves the FCC’s brazen effort to claim regulatory authority that Congress not only declined to confer under the Communications Act but specifically rejected in enacting a “resolution of disapproval” under the Congressional Review Act (CRA). That effort must fail. It is a basic axiom of administrative law, rooted in the republican nature of government, that an administrative agency “has no power to act ... unless and until Congress confers power upon it.” *La. Pub. Serv. Comm’n v. FCC*, 476 U.S. 355, 374 (1986). And an agency’s lack of authority is all the more obvious where, as here, Congress has directly forbidden the agency’s action.

Under the Communications Act, telecommunications carriers bear certain duties to protect the confidentiality of a defined class of customer data called “customer proprietary network information” (CPNI). 47 U.S.C. § 222(c)(1). CPNI includes the records of customers’ phone calls, as well as related information about customers’ usage of specific telecommunications services and features. *Id.* § 222(h)(1). But the Communications Act imposes no such duties on telecommunications carriers with respect to consumer data other than CPNI. That is not surprising, as any company’s use and handling of *non*-CPNI data—including various forms of “personally identifiable information” (PII), such as a consumer’s medical data—is already subject to extensive regulatory oversight. For many years, the FCC respected the significance of that statutory distinction by enforcing its

sector-specific data-privacy regulations in a narrow manner, limited to carriers' use, disclosure, and safeguarding of CPNI.

In 2016, however, the FCC adopted an expansive new set of regulatory measures in an omnibus Broadband Privacy Order—a unique regime the FCC established for telecommunications carriers applicable to a wide swath of consumer data, including data *beyond* CPNI. One of the measures included in that Order, the 2016 Reporting Rule, imposed reporting and recordkeeping obligations on telecommunications carriers regarding consumer data breaches involving PII as well as CPNI. The FCC's sweeping new assertion of authority was controversial. It rested on a splintered, 3-2 vote among the commissioners of the FCC. The dissenting commissioners argued, among other things, that the FCC lacks authority to establish breach-reporting requirements for PII, as distinct from CPNI, under the Communications Act.

Shortly thereafter, Congress weighed in with a remarkable rebuke. Exercising its rarely used authority under the Congressional Review Act, Congress passed a resolution—which the President then signed—disapproving the Broadband Privacy Order in full. That disapproval resolution immediately deprived the 2016 Reporting Rule—and all the other rules adopted in the Order—of any legal effect. Under the plain terms of the CRA, Congress's resolution also meant that the 2016 Reporting Rule could not later be “reissued in substantially the same form.” 5 U.S.C.

§ 801(b)(2). Nor could the FCC adopt a “new rule” that is “substantially the same” as the previously disapproved rule or any portion thereof. *Id.*

The FCC has now defied Congress’s directive. Earlier this year, it published in the Federal Register a new consumer data-breach reporting rule (the 2024 Reporting Rule) that is substantially similar to the 2016 Reporting Rule disapproved by Congress. Most importantly, the 2024 Reporting Rule—like its 2016 predecessor—seeks to expand the range of customer data subject to the FCC’s authority by regulating customer PII that is not considered CPNI. Again, two commissioners dissented from the FCC’s action, explaining that Congress not only declined to give the FCC the power to regulate telecommunications carriers’ use of PII, as distinct from CPNI, but specifically foreclosed such a rule through the disapproval resolution. The FCC majority acknowledged Congress’s enactment of that extraordinary resolution, but asserted that Congress’s disapproval merely restrains the FCC from re-adopting the 2016 Broadband Privacy Order as a whole. According to the FCC, it may re-adopt seriatim the operative rules ultimately codified by that Order (such as the 2016 Reporting Rule).

The FCC majority is wrong—and its adoption of the 2024 Reporting Rule is contrary to law and must be set aside under the Administrative Procedure Act (APA)—for two basic reasons. First, the 2024 Reporting Rule, like the 2016 Reporting Rule, exceeds the FCC’s statutory authority to regulate CPNI by

prescribing data-privacy and security rules for an entirely new class of data—consumer PII. The FCC’s asserted justification for this enlargement of its authority disregards the text, structure, and history of the relevant provisions of the Communications Act.

Second, the FCC’s regulation of PII cannot be reconciled with the CRA. Congress recognized that the FCC overstepped its bounds in issuing the Broadband Privacy Order, so it enacted a joint resolution of disapproval of that Order and each of its constituent parts. Under the CRA, that resolution prevents the FCC from issuing a new rule that is “substantially the same” as the 2016 Reporting Rule, which was part of the Broadband Privacy Order. Yet the 2024 Reporting Rule and the 2016 Reporting Rule are materially identical in essential respects. Like the 2016 Reporting Rule, the new version imposes broad reporting and recordkeeping obligations with respect to data breaches involving customer PII. And it closely resembles the disapproved 2016 Reporting Rule in numerous other respects. Indeed, the FCC barely asserted otherwise in its rulemaking proceedings. Instead, the FCC argued that it could reimpose the 2016 Reporting Rule in full so long as it did not simultaneously reissue the other rules set forth in its 2016 Broadband Privacy Order. That argument rests on a misinterpretation of the CRA that would nullify that statute’s function as a check on administrative agency overreach.

Administrative agencies have only the powers that Congress gives them. They certainly lack any powers that Congress has expressly denied them. The 2024 Reporting Rule flouts both of these foundational principles. It should be set aside.

STATEMENT OF THE CASE

A. Consumer Privacy Under The Communications Act

In 1996, in the midst of a revolution in communications technology, Congress overhauled and updated the Communications Act of 1934 by enacting the Telecommunications Act of 1996. In doing so, it established a comprehensive “pro-competitive, de-regulatory national policy framework” for telecommunications services. S. Rep. No. 104-230, at 1 (1996) (Conf. Rep.).

Among the provisions of the 1996 Act was an entirely new statutory regime governing the use and disclosure of, and access to, certain customer data collected by telecommunications carriers. This regime, codified as Section 222 of the Communications Act, reflected a “careful balance of competing, often conflicting, considerations.” H.R. Rep. No. 104-204, at 90 (1995), *as reprinted in* 1996 U.S.C.C.A.N. 10, 57; *see* 47 U.S.C. § 222.

Section 222 imposes on all telecommunications carriers a duty to protect particular types of proprietary information collected in connection with the provision of a telecommunications service. Specifically, Section 222(a) states generally that “[e]very telecommunications carrier has a duty to protect the confidentiality of

proprietary information of[] ... other telecommunications carriers, equipment manufacturers, and customers.” 47 U.S.C. § 222(a). Previously, the FCC had imposed certain piecemeal restrictions on the use of proprietary information by a few incumbent telecommunications carriers—AT&T, the Bell Operating Companies (BOCs), and GTE Corporation—in order to protect “independent enhanced services providers” (i.e., nascent Internet service providers) from “discrimination by AT&T, the BOCs, and GTE.”¹ Section 222(a) applied these duties to all telecommunications carriers.

Sections 222(b) and (c) specify the particular types of information covered by the statute and identify each carrier’s particular duties with respect to such information. Section 222(b) governs the confidentiality of “carrier information,” and provides that any telecommunications carrier that receives “proprietary information from another carrier” shall use that information only to provide telecommunications, and not for “its own marketing efforts.” And Section 222(c) governs the confidentiality of *customer* data—specifically, “customer proprietary network information,” or CPNI. Section 222(h)(1) then defines CPNI to mean

¹ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information and Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, Second Report and Order, 13 FCC Rcd 8061, 8065-66, 8068-70 ¶¶ 3, 7 (1998) (1998 CPNI Order).

“information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and information contained in the bills ... received by a customer of a carrier.”

Under Section 222(c), a telecommunications carrier that receives CPNI generally may use, disclose, or permit access to that information only with the customer’s approval, unless such use, disclosure, or access is required by law or occurs in the course of providing “the telecommunications service from which such information is derived” or certain ancillary services. 47 U.S.C. § 222(c)(1). Section 222 provides additional exceptions to this consent requirement (1) when billing for telecommunications services, (2) to protect customers or the carrier against fraud, (3) in responding to customer-initiated inquiries, and (4) for various emergency purposes. *See id.* § 222(d), (g).

Congress sought to regulate CPNI partly to promote competition in the telephone services market and partly to protect consumers’ privacy interests in their proprietary information. Soon after Section 222 became law, the FCC explained that “the [Act’s] legislative history makes clear that Congress specifically intended [S]ection 222 to ensure that customers retained control over CPNI in the face of the powerful carrier incentives to use such CPNI to gain a foothold in new markets.”

1998 CPNI Order 8089-90 ¶ 37; *see id.* at 8112-13, 8120, 8130-31, 8145 ¶¶ 66, 75, 91 107 (similar). To that end, “[t]he Conference Report states that, through [S]ection 222, Congress sought to ‘balance both competitive and consumer privacy interests with respect to CPNI.’” *Id.* at 8089-90 ¶ 37.

B. The 1998 CPNI Order And 2007 Reporting Rule

In 1998, the FCC adopted its first rules implementing Section 222. *See* 1998 CPNI Order 8229 (codified at 47 C.F.R. § 64.2009). Consistent with the statute, those rules did not seek to regulate any form of customer information beyond CPNI. Instead, they established general restrictions on telecommunications carriers’ use and disclosure of, and access to, CPNI, as well as regulations requiring carriers to protect CPNI through recordkeeping and employee training. *See id.*

In 2007, the FCC adopted a new rule requiring telecommunications carriers and interconnected VoIP providers to report to customers and law-enforcement authorities any data breaches involving unauthorized disclosure of CPNI. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order, 22 FCC Rcd 6927 (2007) (2007 Reporting Rule) (codified at 47 C.F.R. § 64.2011). For purposes of the 2007 Reporting Rule, the FCC defined a “breach” as occurring “when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed

CPNI.” 47 C.F.R. § 64.2011(e). The rule required carriers to notify the Secret Service and the FBI of a CPNI breach within seven business days, and to notify affected customers thereafter. *Id.* § 64.2011(b), (c). It also required carriers to maintain records of any such CPNI breaches for at least two years. *Id.* § 64.2011(d).

The FCC claimed that its “general rulemaking authority”—including its authority under Section 201(b) to “prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this Act”—coupled with Section 222(a) gave it authority “to require carriers to report CPNI breaches.” 2007 Reporting Rule 6943 ¶ 27 n.94; *see id.* at 6930-31, 6945, 6956 ¶¶ 4, 6, 33, 56. As the Commission explained, “Section 222(a) imposes a general duty on telecommunications carriers to protect the confidentiality of proprietary information—a duty owed to other carriers, equipment manufacturers, and customers.” *Id.* at 6930 ¶ 4 n.6. Moreover, “Section 222(c) outlines the confidentiality protections applicable to [proprietary] *customer* information”—and that subsection discusses CPNI. *Id.* (emphasis added). Thus, in the FCC’s view, “[e]very telecommunications carrier has a general duty pursuant to section 222(a) to protect the confidentiality of CPNI.” *Id.* at 6931 ¶ 6. And “[n]otifying law enforcement of CPNI breaches is consistent with the goal of protecting CPNI.” *Id.* at 6943 ¶ 27.

C. The Broadband Privacy Order And 2016 Reporting Rule

In 2016, the FCC substantially revised its 2007 Reporting Rule as part of an omnibus Broadband Privacy Order. *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, 31 FCC Rcd 13911 (2016) (Broadband Privacy Order). The Order—adopted on a party-line, 3-2 vote—announced new privacy rules for providers of broadband Internet access services, *see id.* at 14080, and substantially modified the 2007 Reporting Rule by adopting a new 2016 Reporting Rule, *see id.* at 14080-81, 14085-86 (revised 47 C.F.R. §§ 64.2002(c), (f), (m), (n), 64.2006). Under the 2016 Reporting Rule, the FCC broadly expanded the regulatory definition of “breach” to cover a new category of information dubbed “customer proprietary information,” which the FCC defined to include CPNI as well as “[p]ersonally identifiable information (PII),” which was further defined to include information “linked or reasonably linkable to an individual,” such as a name, address, or health information. *Id.* at 14080-81 (noting changes to definitional provisions located at 47 C.F.R. § 64.2002(c), (f), (m)).

Commissioners Pai and O’Rielly dissented. While Commissioner Pai focused on the disconnect between the FTC’s existing regulatory approach and the new rules imposed by the FCC, Commissioner O’Rielly argued that the Order “exceed[ed] the Commission’s authority.” *Id.* at 14122. He specifically criticized the majority for expanding the definition of “breach” to cover a broader range of customer

information beyond CPNI. *Id.* at 14122-24. And he argued that the majority’s “made up” invocation of Section 222(a) to sweep in PII conflicted with Congress’s “deliberate[.]” choice not to refer to PII in Section 222, “unlike elsewhere in the [Communications] Act.” *Id.* at 14123.

D. Congress’s Disapproval Of The Broadband Privacy Order Under The Congressional Review Act

Given the controversy surrounding the 2016 Broadband Privacy Order, Congress immediately began scrutinizing the Order pursuant to the Congressional Review Act, 5 U.S.C. §§ 801-08. Enacted in 1996, the CRA empowers Congress to oversee—and, with the assent of the President, *overturn*—rules promulgated by federal agencies. *See* Pub. L. No. 104-121, § 251, 110 Stat. 868, 868-74 (1996) (codified at 5 U.S.C. §§ 801-08).

The CRA arose from a fundamental institutional concern that Congress had “effectively abdicated its constitutional role as the national legislature” in allowing federal agencies great latitude “in implementing and interpreting congressional enactments.” 142 Cong. Rec. 6922, 6926 (1996) (statement of Rep. Hyde). The CRA’s sponsors explained that the CRA would help restore “the appropriate roles of the Congress in enacting laws, and the Executive Branch in implementing those laws,” by “reclaiming for Congress some of its policy making authority, without requiring Congress to become a super regulatory agency.” *Id.*

Under the CRA, before any agency “rule” can take effect, the promulgating agency must submit to the Senate, House of Representatives, and Comptroller General a report containing, among other things, the rule and any necessary cost-benefit analysis. 5 U.S.C. § 801(a)(1)(A)-(B). The CRA incorporates the Administrative Procedure Act’s broad definition of “rule”: “[t]he whole or a part of an agency statement of general ... applicability and future effect designed to implement, interpret, or prescribe law or policy.” *Id.* § 551(4); *see id.* § 804(3).

After receiving an agency’s report, Congress may enact a “joint resolution of disapproval” of the rule within a statutorily defined timeframe. *See id.* § 802(a). Such a resolution may be subject to certain “fast track” procedures in the Senate. *See id.* § 802(c)-(e). The CRA tightly prescribes the form such resolution must take: “That Congress disapproves the rule submitted by the _____ relating to _____, and such rule shall have no force or effect.” *Id.* § 802(a). If both Houses of Congress pass such a resolution, the joint resolution is presented to the President. Absent a presidential veto, the disapproval resolution is enacted, and the CRA provides that the congressionally disapproved “rule shall not take effect (or continue).” *Id.* § 801(b)(1). The CRA then limits future agency action: A disapproved “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 legislation “specifically authoriz[ing]” the

rule. *Id.* § 801(b)(2). As the CRA’s bipartisan House and Senate sponsors later explained, “[s]ubsection 801(b)(2) is necessary to prevent circumvention of a resolution of disapproval.” 142 Cong. Rec. 8196-201 (1996) (statement of Sens. Nickles, Reid, and Stevens); 142 Cong. Rec. at 6922-26 (statement of Rep. Hyde).

Pursuant to the CRA, the FCC submitted the published 2016 Broadband Privacy Order to Congress for review shortly after the Order was adopted. Senator Jeff Flake and Representative Marsha Blackburn then promptly introduced a disapproval resolution that both Houses of Congress passed. *See* S.J. Res. 34, 115th Cong. (2017); H.R. Res. 230, 115th Cong. (2017). The resolution provided that “Congress disapproves the rule submitted by the Federal Communications Commission relating to ‘Protecting the Privacy of Customers of Broadband and Other Telecommunications Services’ (81 Fed. Reg. 87274) (December 2, 2016), and such rule shall have no force or effect.” Pub. L. No. 115-22, 131 Stat. 88, 88 (2017). The President signed Congress’s disapproval resolution into law on April 3, 2017. The FCC accordingly rescinded the provisions of the Broadband Privacy Order, including the 2016 Reporting Rule, and reinstated the 2007 Reporting Rule. *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 82 Fed. Reg. 44118, 44122-23 (Sept. 21, 2017).

Congress’s disapproval of the Broadband Privacy Order was a rare congressional rebuke. Before 2017, Congress and the President had successfully

disapproved agency rules only once since the CRA became law in 1996. *See* Jody Freeman & Matthew C. Stephenson, *The Untapped Potential of the Congressional Review Act*, 59 Harv. J. on Legis. 279, 286-87 (2022).

E. The 2024 Reporting Rule

1. In January 2023, the FCC again issued a Notice of Proposed Rulemaking seeking comment on amending the 2007 Reporting Rule. *See* A120-61 (*Data Breach Reporting Requirements*, Notice of Proposed Rulemaking, 38 FCC Rcd 566 (2023) (NPRM)). It sought comment on proposed amendments that were similar to provisions adopted in the disapproved 2016 Reporting Rule. Most notably, the FCC sought comment on whether it had authority under Section 222 to establish breach-reporting obligations for customer information “other than CPNI,” such as “Social Security Numbers and financial records.” A131 (NPRM ¶ 22). It also invited commenters to address “the impact of the Congressional disapproval of the *2016 Privacy Order* on the Commission’s legal authority to issue the rules proposed.” A127 (NPRM ¶ 11). But the FCC noted that it was “not seeking comment” on the issuance of “‘a new rule that is substantially the same as,’ the rule disapproved by Congress.” A143 (NPRM ¶ 52).

In response, numerous commenters explained why adoption of the proposed rule would exceed the FCC’s statutory authority and violate the CRA. Among them were four U.S. Senators, who noted that “the requirements in the [proposed rule]

governing notification to the [Commission], law enforcement, and consumers” are “clearly ‘substantially similar’ to the nullified 2016 rules.” A162 (Letter from Sen. Ted Cruz et al., to Hon. Jessica Rosenworcel, Chair, FCC (Dec. 12, 2023)). Thus, the Senators argued, the Commission was “defying clear and specific direction [under the CRA] not to issue requirements that are substantially similar to parts of a rule disapproved by Congress.” A163.

2. The FCC nevertheless adopted the 2024 Reporting Rule largely as proposed. *See* A1-104 (Order). As previewed in the FCC’s Notice of Proposed Rulemaking, the final rule—approved by the FCC on a party-line, 3-2 vote—adopted a sweeping definition of “breach” that mandated reporting duties with respect to CPNI as well as a broad class of “personally identifiable information.” 47 C.F.R. § 64.2011(e)(1), (2). The FCC defined PII to cover largely the same information captured in the FCC’s 2016 definition of PII, including (1) a customer’s “first name or first initial, and last name, in combination with any government-issued identification numbers or information issued on a government document used to verify the identity of a specific individual, or other unique identification number used for authentication purposes;” (2) any “user name or e-mail address, in combination with a password or security question and answer;” and (3) any “[u]nique biometric, genetic, or medical data.” *Id.* § 64.2011(e)(5); *see also* A11-12 (Order ¶ 20); A34 (Order ¶ 57 n.238). The FCC’s definition also covers “[a]ny

one” or “combination” of those discrete elements if such element or combination “would enable a person to commit identity theft or fraud.” 47 C.F.R. § 64.2011(e)(5)(iv)(B).

As with the 2016 Reporting Rule, the FCC claimed authority to regulate PII under Section 222(a). It argued that the “breadth of Section 222(a)” confirms that the FCC’s reporting rules “can and must apply to all PII rather than just to CPNI,” and it explicitly “disavow[ed]” its former longstanding position that its Section 222 authority was “coextensive with the definition of CPNI.” A58-59 (Order ¶¶ 118, 120). The FCC also claimed independent authority to regulate PII under Section 201(b), which gives the FCC authority to prohibit “unjust and unreasonable” “charges, practices, classifications, and regulations for and in connection with” a communications service, and to “prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of” the Act. 47 U.S.C. § 201(b). The FCC asserted that it was “implausible” that Congress would have exempted carriers from an obligation to protect private information that is not CPNI. A64 (Order ¶ 126).

Furthermore, the FCC expressly rejected commenters’ arguments that Congress’s 2017 disapproval of the 2016 Reporting Rule forbade adoption of a 2024 Reporting Rule incorporating substantially the same requirements. In its view, the CRA prohibits the FCC “from reissuing the *2016 Privacy Order* in whole, or in

substantially the same form, or from adopting another item that is substantially the same as the *2016 Privacy Order*.” A67 (Order ¶ 135). But the FCC posited that the CRA “does not prohibit the Commission from revising its *breach notification rules* in ways that are similar to, or even the same as, some of the revisions that were adopted in the *2016 Privacy Order*, unless the revisions adopted are the same, in substance, as the *2016 Privacy Order as a whole*.” *Id.* (emphasis added) (footnote omitted).

3. Commissioners Carr and Simington dissented. Both concluded that the 2024 Reporting Rule exceeded the FCC’s statutory authority. As Commissioner Simington explained, the FCC’s authority to regulate consumer data privacy had traditionally been “limited to ‘Customer Proprietary Network Information’ (CPNI), a term of art defined and used in Section 222’s grants of authority.” A102 (Simington Dissent). But the 2024 Reporting Rule “dramatically expands the kinds of data that the FCC has jurisdiction over,” contrary to “decades of FCC interpretation and practice,” and contrary to the “best interpretation of Section 222(a).” *Id.*; *see also* A99 (Carr Dissent) (“Congress never gave us authority to regulate PII in this manner”).

Both dissenters also concluded that the majority had “plainly violate[d]” Congress’s disapproval resolution under the CRA. A98 (Carr Dissent); *see* A102 (Simington Dissent). As Commissioner Carr noted, the majority itself

acknowledged that the 2016 Broadband Privacy Order “adopted several rules—all of which were nullified” by Congress’s 2017 disapproval resolution. A98. Among those rules was the 2016 “data breach rule ... nullified by the House, the Senate, and the President” in the disapproval resolution. *Id.*

Commissioner Carr pointed out that the FCC majority had “ma[de] no real attempt to explain how the data breach rule we adopt today” was not “the same or substantially similar to” that disapproved data breach rule. *Id.* Instead, the majority reasoned that the current rulemaking would not violate Congress’s disapproval resolution under the CRA so long as it did not “put *all* of th[e] 2016 rules back in place in this one decision.” *Id.* (emphasis added). On that view, an agency “could insulate any one of [its] rules from the CRA ... simply by packaging that one rule together with other rules in a single document. Then, ... the agency could always put that one rule back in place, provided it did not reenact those other rules that the agency packaged along with it.” *Id.* Both dissenters decried this reasoning, which would “read[] the CRA out of the United States Code altogether.” *Id.*; *see also* A102 (Simington Dissent) (warning that the majority’s “wooden reading” would make the CRA “a nullity”).

SUMMARY OF ARGUMENT

I. Congress never authorized the FCC to impose data-privacy obligations on telecommunications carriers with respect to customers’ personally identifiable

information (PII). The text, structure, and contemporaneous understanding of Section 222 of the Communications Act all indicate that Congress deliberately chose to impose such obligations only as to a carefully defined category of customer information: customer proprietary network information (CPNI). Indeed, elsewhere in the Communications Act, Congress specifically enacted data-privacy provisions applicable to PII. Congress's decision not to include PII within the scope of Section 222 was deliberate. And the FCC understood this limited scope when Section 222 was enacted: Its contemporaneous rulemaking—and the agency's rules and decisions for nearly two decades thereafter—treated CPNI as the only lawful subject of FCC regulation with respect to customer data under Section 222.

The FCC's contrary arguments are unavailing. Its reliance on Section 222(a) runs afoul of numerous canons of statutory construction, and would render superfluous or nonsensical entire swaths of Section 222. And its reliance on Section 201(b) of the Communications Act is equally flawed. Section 222—unlike many other sections of the Communications Act—clearly displaces the general authority conferred by Section 201(b) as it pertains to the use and disclosure of, and access to, telecommunications carriers' customer data. The FCC seeks to use Section 201(b) as an end-run around the carefully reticulated framework established by Congress in Section 222. The Court should reject that effort and set aside the 2024 Reporting Rule under the APA.

II. Congress’s express rejection of the 2016 Reporting Rule independently bars the FCC’s adoption of the 2024 Reporting Rule. Under the CRA, the FCC may not issue any rule that is “substantially the same as” a “rule” that Congress blocked from taking effect through a CRA joint resolution of disapproval. 5 U.S.C. § 801(b)(2). The 2016 Reporting Rule is a “rule” within the meaning of the CRA, and there is no dispute that it was nullified by the 2017 congressional disapproval resolution. The CRA thus bars the FCC from promulgating a new rule that is substantially the same as the 2016 Reporting Rule.

The 2024 Reporting Rule is substantially the same as the 2016 Reporting Rule. In the most crucial respect—the manner in which the 2024 and 2016 Rules expand data-breach reporting requirements to PII—the rules are virtually identical. And they are the same in numerous other particulars as well. The FCC has mustered no real argument to the contrary, instead justifying the 2024 Rule based on a plainly mistaken interpretation of the CRA. The 2024 Rule should be set aside under the APA for these reasons as well.

STANDARD OF REVIEW

In reviewing an agency action challenged under the APA, “the reviewing court shall decide all relevant questions of law” and “determine the meaning or applicability of the terms of an agency action.” 5 U.S.C. § 706. Accordingly, this Court reviews *de novo* the agency’s constructions of a federal statute. *See*

KenAmerican Res., Inc. v. U.S. Sec’y of Labor, 33 F.4th 884, 888 (6th Cir. 2022). “The reviewing court shall ... hold unlawful and set aside agency action, findings, and conclusions found to be ... arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law; ... [or] in excess of statutory jurisdiction, authority, or limitations, or short of statutory right.” 5 U.S.C. § 706(2)(A), (C).

ARGUMENT

I. THE FCC LACKS AUTHORITY UNDER THE COMMUNICATIONS ACT TO REQUIRE REPORTING OF DATA BREACHES INVOLVING PII

The Court should set aside the 2024 Reporting Rule for the simple reason that Congress never authorized it. “The FCC may only take action that Congress has authorized.” *Bais Yaakov of Spring Valley v. FCC*, 852 F.3d 1078, 1082 (D.C. Cir. 2017) (Kavanaugh, J.). Nothing in the Communications Act allows the FCC to establish data-breach reporting requirements with respect to “personally identifiable information” or PII, as distinct from CPNI.

A. Section 222 Permits The Regulation Of Customer Proprietary Network Information, Not Personally Identifiable Information

The text, structure, and history all indicate that the *only* customer data for which the FCC may establish breach-reporting requirements under Section 222 is CPNI. The 2024 Reporting Rule’s regulation of PII—a much broader class of data—exceeds the FCC’s statutory authority.

1. Section 222's Text Authorizes Regulation Of CPNI, Not Other Types Of Customer Data

a. Section 222's text and structure are straightforward. Section 222(a)—titled “In General”—articulates an overarching duty that is further specified with greater precision elsewhere in Section 222(c). Section 222(a) declares that “[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers.” 47 U.S.C. § 222(a). As relevant here, it identifies which entities are subject to Section 222—i.e., “[e]very telecommunications carrier”—and prescribes those carriers’ “general” duty to protect the “proprietary information” of “customers.” *Id.*

Under its ordinary meaning, the term “proprietary information” has a limited scope, covering only information in which an “owner” has a “protectable interest”—often a business interest, like a trade secret. *Black's Law Dictionary* (11th ed. 2019) (defining “proprietary information” as “[i]nformation in which the owner has a protectable interest. *See* TRADE SECRET.”); *see also Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh*, 691 F.3d 821, 833 (6th Cir. 2012) (“proprietary information” covers information “to which Plaintiffs own or hold single or sole right”). Unlike “personal information” or “personally identifiable information”—which can be disclosed, even publicly, without losing its character as such—“proprietary information” is kept confidential from third parties. *See Inc.*,

Proprietary Information (Jan. 5, 2021), <http://www.inc.com/encyclopedia/proprietary-information.html> (“Courts will not treat information readily available in public sources as proprietary.”).

Section 222(c)—titled “Confidentiality of customer proprietary network information”—clarifies what “customer” information Congress deemed to be “proprietary” under Section 222(a). It unambiguously limits the scope of such customer “proprietary” information to CPNI. In Section 222(c)(1)—titled “Privacy requirements for telecommunications carriers”—Congress enabled the FCC to impose restrictions on carriers’ ability to “permit access to individually identifiable [CPNI].” And in Section 222(c)(2), Congress granted customers the right to require disclosure of their “customer proprietary network information [CPNI]” upon request. Section 222(h)(1) then comprehensively defines CPNI to “mean[]” information related to the “quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service” that is “made available to the carrier by the customer solely by virtue of the carrier-customer relationship,” and “information contained in bills” pertaining to telephone service.

Taken together, the most natural reading of Section 222 is that subsection (a) sets forth a general mandate for telecommunications carriers to protect particular types of “proprietary” information, which is then more specifically described with respect to “customer proprietary” data in subsection (c), which in turn uses a term of

art (“customer proprietary network information”) that is precisely defined in subsection (h). It does not provide the Commission with any freestanding regulatory authority over other, broader categories of customer information.

Section 222 certainly does not encompass PII more broadly—i.e., any information that can be used to identify a natural person, such as the person’s name or address. A10-11 (Order ¶ 18); *see* A11-12 (Order ¶ 20); A34 (Order ¶ 57 n.238). In ordinary speech, it would be odd to refer to someone’s name and address as one’s “proprietary” information, insofar as customers routinely disclose such information to third parties. Nor does such PII come within Section 222(h)’s definition of CPNI. As the Commission previously explained, “practically speaking,” CPNI includes only “the phone numbers to be called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting.” 2007 Reporting Rule 6931 ¶ 5. CPNI thus does not include a broader swath of “personally identifiable information” that is already found in multiple places beyond one’s phone-call records and bills.

b. Other provisions of the Communications Act confirm that PII does not qualify as “customer proprietary information” or CPNI. When Congress sought to regulate a broad class of PII in the Communications Act, it did so explicitly—both before and after enacting Section 222 in 1996.

In 1984, for example, Congress imposed certain duties on cable operators to protect the privacy of “personally identifiable information” concerning subscribers. Cable Communications Policy Act of 1984, Pub. L. No. 98-549, § 631, 98 Stat. 2779, 2794-95 (codified at 47 U.S.C. § 551). Likewise, in 2004, Congress required satellite operators to protect the privacy of satellite subscribers’ “personally identifiable information.” Satellite Home Viewer and Reauthorization Act of 2004, Pub. L. No. 108-447, § 206(a), 118 Stat. 3393, 3425 (codified at 47 U.S.C. § 338(i)). The same year that Congress passed the Telecommunications Act, it passed the Health Insurance Portability and Accessibility Act, which authorizes the Department of Health and Human Services to establish rules protecting “individually identifiable health information.” Pub. L. No. 104-191, § 264(a), 110 Stat. 1936, 2033 (1996) (codified at 42 U.S.C. § 1320d-2(d)). Congress also expressly protected “personal information” and “personally identifiable information” in other statutes.² And state legislatures—recognizing that the FCC and FTC lack broad authority to issue general data-breach notification requirements—have imposed rules requiring

² See Children’s Online Privacy Protection Act, Pub. L. No. 105-277 (1998) (codifying definition of children’s “personal information” at 15 U.S.C. § 6501(8)); Gramm-Leach-Bliley Act, Pub. L. No. 106-102 (1999) (codifying definition of “nonpublic personal information” at 15 U.S.C. § 6809(4)); Video Privacy Protection Act, Pub. L. No. 100-618 (1988) (codifying definition of “personally identifiable information” at 18 U.S.C. § 2710).

businesses to notify individuals of breaches of “personal” or “personally identifiable” information in defined circumstances.³

These examples establish that when Congress and state legislatures want to protect “personally identifiable information,” they use express language to do so. Congress did not do that in Section 222.

2. The FCC’s Contemporaneous Understanding Of Section 222 Further Confirms This Reading

The FCC’s own contemporaneous understanding of Section 222 underscores that its authority to create notification rules for breaches of customer “proprietary” information encompasses only breaches of CPNI. Courts regard with “particular respect” the contemporaneous construction of a statute by the agency “initially charged with its enforcement.” *Middle S. Energy, Inc. v. FERC*, 747 F.2d 763, 769 (D.C. Cir. 1984). The reasoning is simple: “The first administrative interpretation of a provision as it appears in a new act often expresses the general understanding of the times or the actual understanding of those who played an important part when the statute was drafted.” *Augustus v. Commissioner*, 118 F.2d 38, 43 (6th Cir. 1941). And just as an agency’s “contemporaneous” practice sheds light on “the extent of power conveyed” by a statute, “the want of assertion of power by those who

³ See *Security Breach Notification Laws*, Nat’l Conference of State Legislatures (last updated Jan. 17, 2022), <https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

presumably would be alert to exercise it is equally significant in determining whether such power was actually conferred.” *Bankamerica Corp. v. United States*, 462 U.S. 122, 130-31 (1983).

Shortly after Section 222 became law, the FCC recognized Congress’s bestowal of authority to regulate CPNI—but not to go further. The FCC’s very first order implementing Section 222 rested on the understanding that “[S]ection 222 sets forth *three* categories of customer information to which different privacy protections and carrier obligations apply[:] [1] individually identifiable CPNI [covered by 47 U.S.C. § 222(c)(1), (2)], [2] aggregate customer information [covered by 47 U.S.C. § 222(c)(3)], and [3] subscriber list information [covered by 47 U.S.C. § 222(e)].” 1998 CPNI Order 8064-65 ¶ 2 (emphasis added); *see also U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1228 n.1 (10th Cir. 1999) (similar).⁴ The FCC did *not* state that Section 222 governed other types of “customer” information, such as PII.

The 2007 Reporting Rule likewise rested on the Commission’s understanding that its authority over customer “proprietary” information encompasses only CPNI.

⁴ *See also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information; Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, Third Report and Order, 17 FCC Rcd 14860, 14864 ¶ 6 (2002) (recognizing that “Congress laid out a framework for carriers’ use of customer information based on the sensitivity of the information” in Section 222).

It recognized that “[e]very telecommunications carrier has a general duty pursuant to section 222(a) to protect the confidentiality of CPNI”—because the FCC viewed carriers’ duties under subsection (a) and subsection (c) as co-extensive. 2007 Reporting Rule 6931 ¶ 6 (emphasis added). And many other FCC regulatory statements evince exactly the same understanding—namely, that “*only* that information that meets the definition of CPNI is subject to section 222.” *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd 9609, 9617 ¶ 24 (2013) (emphasis added).⁵

This unbroken regulatory history across nearly two decades underscores Section 222’s exclusive emphasis on CPNI with respect to protecting the confidentiality of customer information.

⁵ See also 1998 CPNI Order ¶ 208 (seeking comment on “the duty in section 222(a) upon all telecommunications carriers to protect the confidentiality of customers’ CPNI”); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Notice of Proposed Rulemaking, 21 FCC Rcd 1782, 1784 ¶ 4 (2006) (recognizing that “[e]very telecommunications carrier has a general duty pursuant to section 222(a) to protect the confidentiality of CPNI”).

B. The FCC’s Contrary Arguments Lack Merit

The FCC has asserted that both Section 222(a) and Section 201(b) authorize the extension of CPNI notification rules to breaches of PII. A58-64 (Order ¶¶ 117-26). The FCC is wrong as to each.

1. Section 222(a) Does Not Authorize FCC Regulation Of PII Breaches

The FCC claims that the “breadth of section 222(a)” signals that its “breach reporting rules can and must apply to all PII rather than just to CPNI.” A58 (Order ¶ 118). Specifically, the FCC asserts that it would be “inconsistent with” “section 222(a)’s use of the term ‘proprietary information of, and relating to, ... customers’” to conclude that “carriers have no [Communications Act] duty to protect the confidentiality of non-CPNI PII.” A59 (Order ¶ 120).

But it is the FCC’s view that creates inconsistency. By its plain terms, Section 222(a) requires carriers to “protect the confidentiality of *proprietary* information of ... customers.” Section 222(a) thus requires the *customers* to have a proprietary interest in the information. It is far from clear that the broad swaths of PII covered by the 2024 Reporting Rule would count. *See* 47 C.F.R. § 64.2011(e)(5). This Court has already held that information such as financial data that is “owned or held by many, including the customer [and other institutions]” is not “proprietary information” under that term’s “plain and ordinary meaning.” *Retail Ventures*, 691 F.3d at 833 (holding that an insurance plan’s exclusion of coverage for “proprietary

information” did not encompass customer payment and account information). And elsewhere in the Telecommunications Act, Congress expressly distinguished individuals’ “names” from protected “proprietary ... information.” 47 U.S.C. § 396(l)(4)(B). It is doubtful that PII under the FCC’s definition—which includes names, addresses, and telephone numbers not typically used for business purposes by customers, *see supra* at 17-18, 26—would qualify as proprietary.

The FCC attempts to sidestep this problem by denying that Section 222(a) requires the “proprietary information of customers” to be proprietary to *customers*. Instead, the FCC says, Section 222(a) requires only that the information “be ‘proprietary’ to the *carrier*—i.e., obtained in connection with establishing or maintaining a communications service.” A59 (Order ¶ 120). That interpretation misunderstands Section 222(a) and allows the agency to avoid any analysis of whether PII actually qualifies as *customer* “proprietary” information. More generally, the FCC expressly declined to explain why most PII qualifies as “proprietary information,” properly understood. *See* A59 (Order ¶ 120 n.428).

The FCC’s interpretation of Section 222(a) to require protection of PII also creates implausible anomalies throughout Section 222. For example, if Section 222(a) mandated a duty to protect PII, the exceptions Congress set forth in Section 222(d) would make little sense. Section 222(d) relieves carriers from obtaining customer approval for any use and disclosure of “CPNI” for certain purposes such

as billing, deterring fraud, and assisting law enforcement and emergency first responders. These exceptions do not extend to customer information other than CPNI. If the FCC were right that Section 222(a) independently requires carriers to keep PII private, the statute would permit a carrier to disclose CPNI—such as the total minutes a customer spent on the phone with his spouse the previous month—to first responders in the event of a threat to life. But it would *prohibit* the carrier from disclosing PII—such as a customer’s name, address, and medical information—to the same first responders. Congress could not have intended that absurd result. The fact that the Section 222(d) exceptions apply only to CPNI confirms that Section 222 does not govern PII.

Other features of Section 222’s structure reinforce the same point. For example, Section 222(e) requires carriers to disclose “subscriber list information” (i.e., customers’ names, addresses, and phone numbers) to third-party directory publishers when such information has been published by the carrier itself. Section 222(g) likewise requires carriers to disclose subscriber information to first responders. Both specify that such disclosure is authorized “notwithstanding subsections (b), (c), and (d),” which delineate carriers’ duties to protect CPNI. 47 U.S.C. § 222(e), (g). But if Section 222(a) imposes a broader duty to protect PII, then Congress would have added subsection (a) to the list of subsections—(b), (c), and (d)—that are trumped by the disclosure requirements. Doing so was

unnecessary, however, because Congress’s general instruction to protect “proprietary information” imposed no duties with respect to customer data beyond those later specified in subsection (c).

For all these reasons, the best interpretation of Section 222 is the one the FCC embraced for years: As to customer data, Section 222 applies only with respect to CPNI. The FCC’s efforts to expand Section 222(a) to cover PII ignore the structure and operation of the statutory scheme as a whole.

2. Section 201(b) Does Not Authorize The Regulation Of PII

The FCC’s reliance on Section 201(b) is equally misguided. A61-64 (Order ¶¶ 124-26). Enacted in 1934, Section 201(b) declares that any “unjust or unreasonable” “charge, practice, classification, or regulation” imposed by a carrier is “declared to be unlawful,” and it generally empowers the FCC to carry out that prohibition by regulation. 47 U.S.C. § 201(b). The FCC concludes that Section 201(b) provides “independent authority” for treating “PII as protected consumer information,” because failing to notify customers of a PII breach constitutes an “unjust or unlawful practice[.]” A61-62 (Order ¶ 124). That conclusion fails.

First, the specific protections Congress established in Section 222 supersede the general provisions of Section 201. Under the general/specific canon of construction, where a “limited, specific authorization” exists alongside a more “general authorization,” the statute must be read to avoid allowing the “specific

provision [to be] swallowed by the general one.” *RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 566 U.S. 639, 645 (2012).

Here, Section 201(b) is a classic “general” provision that “says nothing about” customer privacy, but instead generally prohibits unjust or unreasonable practices. *Id.* at 646. By contrast, Section 222 is specific—it is a “targeted” measure focused exclusively on the privacy and security of certain information obtained by telecommunications carriers through the services they provide. *Id.* at 645; *see* H.R. Rep. No. 104-204, at 90 (noting Section 222’s “careful balance of competing, often conflicting considerations”); H.R. Rep. No. 104-458, at 205 (1995) (similar). In Section 222, Congress chose to address a specific issue—the “Privacy of Customer Information”—with a self-contained, reticulated regime that sets forth the duties of telecommunications carriers with respect to customer information in minute detail. The FCC cannot now resort to Section 201(b)’s more general command to prohibit “unjust or unreasonable” practices as a basis for circumventing the carefully considered limitations of the Section 222 regime. Doing so undermines Congress’s carefully calibrated judgments with respect to data privacy.

Second, Congress chose not to include a savings clause in Section 222 preserving the FCC’s Section 201 authority. That directly contrasts with the savings clause Congress enacted in Section 251, which sets forth carriers’ duties for physically linking their networks and related obligations. In Section 251—which

Congress enacted alongside Section 222 in 1996—Congress expressly provided 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). Congress did not include any similar language in Section 222.

Congress’s use of a savings clause to preserve the FCC’s Section 201(b) authority in Section 251 shows that its omission of a savings clause from Section 222 was deliberate. Indeed, it confirms that Section 222 fully displaces Section 201 with respect to consumer privacy. *See Russello v. United States*, 464 U.S. 16, 23 (1983) (“[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.”); *accord Qwest Corp. v. Arizona Corp. Comm’n*, 567 F.3d 1109, 1117-18 (9th Cir. 2009) (comparing the absence of a “savings clause” in Section 271 of the Communications Act to one contained in Section 252); *Qwest Corp. v. Minnesota Pub. Utils. Comm’n*, 684 F.3d 721, 729 (8th Cir. 2012) (similar).

Third, the FCC itself previously recognized the exclusive and comprehensive nature of Section 222. Soon after Section 222 became law, the FCC (with a Democratic majority appointed by President Clinton) explained that the “specific consumer privacy and consumer choice protections established in [S]ection 222 supersede the general protections identified in [S]ections 201(b) and 202(a).”

Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Order on Reconsideration, 14 FCC Rcd 14409, 14491 ¶ 153 (1999). The FCC's more recent assertion that Section 201(b) supplies an independent power to regulate consumer privacy is particularly unconvincing in light of the conclusion reached by the FCC soon after Section 222 was enacted. *See Bankamerica*, 462 U.S. at 130-32. That the Commission has only recently purported to “discover” in Section 201(b) a significant power to regulate consumer privacy confirms the statute cannot plausibly be read to stretch that far. *See Utility Air Regul. Grp. v. EPA*, 573 U.S. 302, 324 (2014).

Finally, even assuming that Section 222 did not displace Section 201(b) with respect to consumer privacy, the 2024 Reporting Rule does not concern “practices ... in connection with” a communications service within the meaning of Section 201(b). 47 U.S.C. § 201(b). It is a basic principle of interpretation that a word is “known by the company it keeps” to avoid giving “unintended breadth to the Acts of Congress.” *Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995); *see United States v. Pennsylvania R.R. Co.*, 242 U.S. 208, 228-32 (1916) (applying this principle to narrowly construe the term “practices”). Here, “practices” is part of a statutory quartet that also includes the terms “charges, ... classifications, and regulations for and in connection with” a communications service. 47 U.S.C. § 201(b). In context, these terms all address carrier conduct that is an inherent or necessary aspect of

providing a communications service to customers—e.g., setting rates and classifying services. That limitation is inherent in the title of Section 201(b)—“Service and charges”—as well as in neighboring provisions’ use of the term “practices” to refer explicitly to things “affecting ... charges.” 47 U.S.C. § 203; *see id.* §§ 202, 204-05.

The term “practices” does not encompass a failure to notify the government of data breaches. As the D.C. Circuit explained when interpreting a similar provision of the Federal Power Act, it would be “quite a leap” to move from a context of transactional terms involving rates and charges “to an implication that by the word ‘practice,’ Congress empowered the Commission” to reach virtually any action a carrier takes in the course of its business. *California Indep. Sys. Operator Corp. v. FERC*, 372 F.3d 395, 400-03 (D.C. Cir. 2004); *see FERC v. Elec. Power Supply Ass’n*, 577 U.S. 260, 278 (2016) (“approv[ing]” the D.C. Circuit’s “commonsense construction” and explaining that terms like “in connection with” must be read narrowly “to prevent the statute from assuming near-infinite breadth”).

For all these reasons, Section 201(b) cannot rescue the FCC’s revisionist effort to expand its own authority and regulate data breaches of PII. The 2024 Reporting Rule is contrary to law and must be set aside under the APA.

II. THE CONGRESSIONAL REVIEW ACT BARS THE 2024 REPORTING RULE’S REGULATION OF PII

Even if the FCC’s regulation of PII in the 2024 Reporting Rule were authorized by the Communications Act—which it is not—it cannot be reconciled

with Congress’s resolution disapproving the 2016 Reporting Rule under the CRA. That resolution bars the FCC from “reissu[ing]” the 2016 Reporting Rule “in substantially the same form,” and it likewise prohibits the FCC from issuing a “new rule that is substantially the same as” the 2016 Reporting Rule. 5 U.S.C. § 801(b)(2).

As described below, the 2024 Reporting Rule and the 2016 Reporting Rule are substantially the same, both with respect to their novel regulation of PII and in other respects. Indeed, the FCC barely tried to distinguish the two. Instead, the FCC has asserted that it may simply reissue the 2016 Reporting Rule so long as it does not reissue the *entire* 2016 Broadband Privacy Order, of which the 2016 Reporting Rule was only a part. That argument runs afoul of the CRA’s text and would, if accepted, vitiate the basic operation of the statute. Congress took the extraordinary step of enacting legislation to nullify the FCC’s attempt to regulate PII in 2016. This Court should reject the FCC’s brazen effort to circumvent that disapproval.

A. Congress’s 2017 Disapproval Resolution Forbids Issuance Of Any New Rule “Substantially The Same As” The 2016 Reporting Rule

Under the CRA, when Congress disapproves an agency rule pursuant to the CRA’s procedures, then the “rule shall not take effect (or continue).” 5 U.S.C. § 801(b)(1). Furthermore, “[a] rule that does not take effect (or does not continue)” by reason of congressional disapproval “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” without new authorization from Congress. *Id.* § 801(b)(2). In this way, the

disapproval resolution not only deprives the disapproved rule of “any force or effect,” but also “validly amend[s]” the agency’s statutory authority to narrow its freedom of action with respect to future regulation. *Ctr. for Biological Diversity v. Bernhardt*, 946 F.3d 553, 562 (9th Cir. 2019); *see also Ctr. for Biological Diversity Appellees David Bernhardt and U.S. Dep’t of Interior Br. 21, ECF No. 38 (No. 18-35629)* (“Any authority that previously allowed [the agency] to promulgate the [disapproved rule] was thus narrowed with respect to this particular agency action.”).

Here, when the FCC adopted the 2016 Broadband Privacy Order, it submitted the entire omnibus order to Congress. *See Broadband Privacy Order 13940, 14078 ¶¶ 79, 397*. Encompassed within the Broadband Privacy Order were a host of more specific “rule[s],” as defined under the CRA and APA to mean “agency statement[s] of general ... applicability and future effect designed to ... prescribe law or policy.” 5 U.S.C. § 551(4); *see id.* § 804(3). Indeed, the Broadband Privacy Order prescribed significant changes to nine different sections of the Code of Federal Regulations, and included within each of those sections were a multitude of new rules specifying how the FCC intended to apply the Communications Act with respect to a host of different problems. The FCC’s 2016 submission to Congress expressly identified those rules as a (plural) set of “final *rules*” and “miscellaneous *rules*.” Broadband Privacy Order 14080 (emphasis added).

Most relevant here, the Broadband Privacy Order encompassed the 2016 Reporting Rule, which made various changes to the data-breach reporting rule that the FCC had adopted in 2007. *See id.* at 14085-86 (proposed 47 C.F.R. § 64.2006 and the corresponding definitional changes at proposed § 64.2002); *supra* at 12. These changes all qualified as rules within the meaning of the CRA. At the heart of the 2016 Reporting Rule was the FCC’s decision to depart from longstanding precedent and require telecommunications carriers to report data breaches involving not only CPNI, but also PII. The 2016 Reporting Rule sought to effectuate this change by (1) revising the regulatory definition of “breach” to refer to “customer proprietary information” instead of to “CPNI”; and then (2) adopting a new definition of “customer proprietary information” that encompassed both CPNI and PII. *See* 2016 Reporting Rule 14080 (proposed 47 C.F.R. §§ 64.2002(c), (f)).

When Congress issued its disapproval resolution under the CRA, *see* Pub. L. No. 115-22, 131 Stat. 88 (2017), such disapproval meant that the entire Broadband Privacy Order was invalidated and could “not take effect (or continue).” 5 U.S.C. § 801(b)(1). In disapproving the Broadband Privacy Order, the resolution necessarily invalidated all of the rules contained within the Order—including the 2016 Reporting Rule, its expanded definition of “breach,” and its new definition of “customer proprietary information” encompassing PII. As the FCC explained, the resolution “had the effect of nullifying each and every provision of the 2016

[Broadband] Privacy Order—each of those parts being rules under the APA.” A68 (Order ¶ 137); *see also* 82 Fed. Reg. at 44119 (recognizing that the disapproval effectuated “the nullification of any changes purported to have been made to the CFR by the [Broadband Privacy Order]”); *id.* at 44118 (rescinding “the *voided text of the rules*” disapproved by Congress).

As explained above, Section 801(b)(2) constrains the agency’s legal authority with respect to “[a] rule that does not take effect (or does not continue) under” a resolution of disapproval enacted pursuant to Section 801(b)(1). Most importantly, the agency may not issue a new rule “that is substantially the same as such a rule.” 5 U.S.C. § 801(b)(2). Here, the 2016 Reporting Rule undoubtedly qualifies as “[a] rule that d[id] not take effect (or d[id] not continue) under” Section 801(b)(1). As noted, Congress’s 2017 resolution of disapproval “had the effect of nullifying each and every provision of the 2016 *[Broadband] Privacy Order*—each of those parts being rules under the APA.” A68 (Order ¶ 137). The 2016 Reporting Rule is plainly among those “rules” that the disapproval resolution “nullif[ied].” *Id.*

Under Section 802(b)(2) the legal result of all this is straightforward: The 2017 resolution of disapproval eliminated the FCC’s authority to issue a new rule that is “substantially the same as” the 2016 Reporting Rule. 5 U.S.C. § 801(b)(2).

B. The 2024 Reporting Rule Is Substantially The Same As The 2016 Reporting Rule

Like the 2016 Reporting Rule, the 2024 Reporting Rule amends the 2007 Reporting Rule to require telecommunications carriers to report any data-breach incidents involving PII. In that crucial respect—along with many others—the two rules are “substantially the same” under Section 801(b)(2). The FCC’s attempt to adopt the 2024 Reporting Rule is therefore contrary to law and invalid under the APA. *See* 5 U.S.C. § 706(2)(A), (C).

As the chart below makes clear, the similarities between the 2016 and 2024 Rules—and the ways in which they depart from the 2007 Rule—are substantial:

	2007 REPORTING RULE	2016 REPORTING RULE	2024 REPORTING RULE
Regulatory scope	Imposes reporting duties with respect to CPNI	Imposes reporting duties with respect to CPNI and PII	Imposes reporting duties with respect to CPNI and PII
Definition of “breach”	“[W]hen a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.” 47 C.F.R. § 64.2011(e) (2008).	“[A]ny instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information.” 47 C.F.R. § 64.2002(c) (proposed 2016).	“[W]hen a person, without authorization or exceeding authorization, gains access to, uses, or discloses covered data.” 47 C.F.R. § 64.2011(e)(1) (2024).
Definition of protected data	Limited to “CPNI” only. 47 C.F.R. § 64.2011(e) (2008).	“Customer proprietary information” includes “CPNI” and “PII.” 47 C.F.R. § 64.2002(f) (proposed 2016).	“Covered data” includes “CPNI” and “personally identifiable information.” 47 C.F.R. § 64.2011(e)(2) (2024).
State of mind of the party responsible for the breach	Applies only where a person “intentionally” accesses or discloses covered data without authorization. 47 C.F.R. § 64.2011(e) (2008).	Drops the requirement of “intentional[]” access or disclosure. <i>See</i> 47 C.F.R. § 64.2002(c) (proposed 2016).	Drops the requirement of “intentional[]” access or disclosure. <i>See</i> 47 C.F.R. § 64.2011(e)(1) (2024).
Agencies to be notified	FBI and Secret Service. 47 C.F.R. § 64.2011(b) (2008).	FBI, Secret Service, and FCC. 47 C.F.R. § 64.2006(b)-(c) (proposed 2016).	FBI, Secret Service, and FCC. 47 C.F.R. § 64.2011(a) (2024).
Timeline for customer notification	No timeline. 47 C.F.R. § 64.2011(c) (2008).	“30 calendar days after the carrier reasonably determines that a breach has occurred.” 47 C.F.R. § 64.2006(a) (proposed 2016).	“30 days after reasonable determination of a breach.” 47 C.F.R. § 64.2011(b) (2024).

At the heart of both the 2016 and 2024 Reporting Rules is a fundamental shift away from the narrow reporting requirements established by the 2007 Reporting Rule. Whereas the 2007 Reporting Rule narrowly required telecommunications carriers to report data-breach incidents involving CPNI, the 2016 and 2024 Reporting Rules also require them to report data-breach incidents involving PII—which encompasses a far broader range of data.

As the chart indicates, the 2007 Reporting Rule defined a “breach” as “occurr[ing] when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.” 2007 Reporting Rule 6978 (47 C.F.R. § 64.2011(e)). The 2016 Reporting Rule and the 2024 Reporting Rule expand that definition in substantially the same way. The 2016 Reporting Rule redefined a “breach” as “any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information.” 2016 Reporting Rule 14080 (47 C.F.R. § 64.2002(c)). It then defined “customer proprietary information,” in turn, to include “CPNI” and “personally identifiable information.” *Id.* at 14080-81 (47 C.F.R. § 64.2002(f), (m)). Likewise, the 2024 Reporting Rule defines a “breach” as “occur[ring] when a person, without authorization or exceeding authorization, gains access to, uses, or discloses covered data.” 47 C.F.R. § 64.2011(e)(1). And it defines “covered data” to include “CPNI” and “personally identifiable information.” 47 C.F.R. § 64.2011(e)(2).

As already explained, the practical difference between CPNI and PII is significant. *See supra* at 26. Whereas CPNI is a limited and narrow class of customer information, PII—as defined in both the 2016 and 2024 Reporting Rules—covers a much wider class of customer information. By changing the definition of “breach” to encompass data breaches involving PII, both the 2016 Reporting Rule and the 2024 Reporting Rule dramatically enlarged the scope of carriers’ data-breach reporting obligations. That similarity itself suffices to show that the 2024 Reporting Rule is substantially the same as the 2016 Reporting Rule.

The 2024 Reporting Rule also substantially mirrors the 2016 Reporting Rule in other important ways. For example, the 2007 Reporting Rule defined only “intentional[]” acts of unauthorized access or disclosure as “breaches” triggering a reporting duty. 2007 Reporting Rule 6978 (47 C.F.R. § 64.2011(e)). The 2016 Reporting Rule swept in “any instance” of an unauthorized access to consumer data, regardless of whether such access was intentional. 2016 Reporting Rule 14080 (47 C.F.R. § 64.2002(c)). The 2024 Reporting Rule does the same thing. *See* 47 C.F.R. § 64.2011(e)(1).

Similarly, the 2007 Reporting Rule required carriers to notify only two law-enforcement agencies (the FBI and Secret Service) and affected customers of a data breach. *See* 2007 Reporting Rule 6977-78 (47 C.F.R. § 64.2011(b)). The 2016 Reporting Rule required carriers to notify the FCC itself as well. *See* 2016 Reporting

Rule 14085 (47 C.F.R. § 64.2006(b)). The 2024 Reporting Rule does the same. *See* 47 C.F.R. § 64.2011(a). And while the 2007 Reporting Rule specified that a carrier “shall notify its customers of a breach of those customers’ CPNI” after notifying law enforcement, 2007 Reporting Rule 6978 (47 C.F.R. § 64.2011(c)), it declined to set a particular timeline for such customer notification. The 2016 and 2024 Rules both set the same deadline: “30 days after reasonable determination of a breach.” 47 C.F.R. § 64.2011(b); *see* 2016 Reporting Rule 14085 (47 C.F.R. § 64.2006(a)).

All of these examples confirm that the 2016 Reporting Rule and the 2024 Reporting Rule are “substantially the same” for purposes of Section 801(b)(2). The 2024 Reporting Rule thus violates the CRA and must be set aside under the APA.

C. The FCC Cannot Reconcile The 2024 Reporting Rule With Congress’s Disapproval Resolution

In the recent rulemaking proceeding, the FCC sought to preempt any argument that the CRA renders the 2024 Reporting Rule unlawful. Notably, the FCC made little effort to argue that the 2024 Reporting Rule is dissimilar from the disapproved 2016 Reporting Rule. *See* A98 (Carr Dissent). Instead, the FCC asserted that the CRA allows it simply to reissue the entire 2016 Reporting Rule, so long as it does so in a narrower order that does not include the other rules that were incorporated within the 2016 Broadband Privacy Order. The FCC’s analysis, which rests on a plain misreading of the CRA that was not previewed in the FCC’s Notice

of Proposed Rulemaking, is arbitrary, capricious, and contrary to law under the APA. *See* 5 U.S.C. § 706(2)(A), (C).⁶

1. According to the FCC, the CRA “does not prohibit the Commission from revising its breach notification rules in ways that are similar to, or even the same as, some of the revisions that were adopted in the *2016 Privacy Order*, unless the revisions adopted are the same, in substance, as the *2016 Privacy Order* as a whole.” A67 (Order ¶ 135). The FCC’s argument turns on the point that Congress’s “joint resolution referred to the entirety of the *2016 Privacy Order*.” A68 (Order ¶ 136). In the FCC’s view, Congress’s disapproval resolution implicated only one “disapproved rule”—the Broadband Privacy Order as whole—and not any “individual pieces” of that rule. *Id.* (Order ¶ 137). That argument fails as a matter of statutory text and purpose.

As to the text, Section 801(b)(2) of the CRA provides that “[a] rule that does not take effect (or does not continue)” as the result of a congressional disapproval resolution “may not be reissued in substantially the same form,” and that “a new rule that is substantially the same as such a rule may not be issued,” absent intervening

⁶ Because the FCC did not provide notice of its flawed interpretation of the CRA in its NPRM, the rule also fails on procedural grounds under 5 U.S.C. § 553(b). *See* A98 (Carr Dissent) (arguing that the FCC’s decision “violates the APA” because the agency “expressly” declined to seek comment on “putting back in place ... a new rule that is the same as or substantially similar” to a disapproved one).

congressional authorization. 5 U.S.C. § 801(b)(2). Whether a “new rule” is subject to the rulemaking bar described in subsection (b)(2) depends on whether it is substantially the same as “[a] rule” that “[did] not take effect” or “[did] not continue” because of a congressional disapproval resolution. It does not depend on the precise language of Congress’s disapproval resolution, or on whether the resolution *specifically* disapproved of subsidiary rules contained within a broader “rule” expressly targeted by that resolution.

Here, therefore, the question is simply whether the 2024 Reporting Rule is substantially the same as “a rule that d[id] not take effect (or d[id] not continue)” because of a disapproval resolution. *Id.* For the reasons set forth above, the answer to that question is yes: The 2024 Reporting Rule closely mirrors the 2016 Reporting Rule, which did not take effect because of the 2017 resolution of disapproval. *Supra* at 41-42, 43-47.

Notably, the FCC has repeatedly acknowledged that the 2016 Reporting Rule—proposed to be codified in the Code of Federal Regulations (47 C.F.R. §§ 64.2002, 64.2006)—constituted an identifiable, discrete “rule” within the meaning of the CRA. *See* A67 (Order ¶ 135 n.478) (describing the “breach notification rule that was adopted by the *2016 Privacy Order*”). And it acknowledges that this rule was “nullif[ed]” by Congress’s disapproval resolution. A68 (Order ¶ 137); *see also* 82 Fed. Reg. at 44119 (acknowledging the disapproval’s

“nullification of any changes purported to have been made to the CFR [by the 2016 Broadband Privacy Order]”). Thus, under the proper analysis, the FCC may *not* “adopt a breach notification rule that is [substantially] the same as the breach notification rule that was adopted by the *2016 Privacy Order*” and subsequently disapproved by Congress. A67 (Order ¶ 135 n.478). Yet the FCC contends it may do just that, so long as it does not simultaneously re-adopt “the *2016 Privacy Order* as a whole.” *Id.* (Order ¶ 135).

The FCC offers two thin justifications for this result. First, it argues that the term “such a rule” in subsection (b)(2) must refer “to the rule specified in the joint resolution of disapproval,” which was “the entirety of the *2016 Privacy Order*.” A68 (Order ¶ 136). That argument disregards Section 802’s text. The term “such a rule” in subsection (b)(2) refers to its nearest reasonable referent, which appears at the very beginning of Section 801(b)(2): “[a] rule that does not take effect (or does not continue) under paragraph (1).” *See United States v. Boulding*, 960 F.3d 774, 781-82 (6th Cir. 2020) (describing how the “last antecedent canon” and “nearest-reasonable-referent” canons may “confirm” a statute’s “plain meaning”). Contrary to the FCC, Section 801(b)(2)’s reference to “such a rule” does not refer to the “rule specified in the joint resolution of disapproval.” A68 (Order ¶ 136). Indeed, those words—the “rule specified in the joint resolution of disapproval”—appear nowhere in Section 801. The FCC has simply conjured that phrase for its own convenience.

Even if the FCC were right that “such a rule” in Section 801(b)(2) refers to the rule identified in the joint resolution of disapproval addressed in Section 801(b)(1)—i.e., the Broadband Privacy Order—it would necessarily encompass *both* the Order as a whole, *and* its individual constituent rules (including the 2016 Reporting Rule). The CRA’s definition of “rule,” borrowed from the APA, expressly provides that Congress’s disapproval extends not only to the whole of an agency order, but also to all of the rules embedded therein: A rule is the “*whole or part* of an agency statement of general ... applicability and future effect.” 5 U.S.C. § 551(4) (emphasis added); *see id.* § 804(3). Thus, when Congress disapproves a bundled package of rules set forth in a single agency statement of general applicability and future effect, it does not merely disapprove the “whole” statement, but also “nullif[ies]” each operative “part[.]” of that statement. A68 (Order ¶ 137). Otherwise the disapproval resolution would not bar the agency from continuing to enforce some of those individual constituent rules, so long as it did not enforce all of them. Here, the FCC has rightly conceded that Section 801(b)(1) deprived the 2016 Reporting Rule from taking effect. *Supra* at 49-50. Section 801(b)(2) thus deprives the FCC from later issuing a rule that is “substantially the same as” that 2016 Reporting Rule.

Second, the FCC asserts that if Congress meant to bar the reissuance of any rule that was invalidated by reason of a disapproval resolution, it would have worded

subsection (b)(2) differently, by referring to “*Any rule* that does not take effect (or does not continue)” or “*Rules* that do not take effect (or do not continue).” 89 Fed. Reg. at 9994. But here there is no meaningful difference between “A rule,” “Any rule,” and “Rules.” Each of these formulations encompasses the 2016 Reporting Rule. Indeed, the FCC’s argument ignores the plain import of the words Congress utilized. The 2016 Reporting Rule is “[a] rule” that did not continue in effect by virtue of Congress’s disapproval resolution. Thus, by the plain terms of subsection (b)(2), the 2016 Reporting Rule may not be “reissued in substantially the same form,” and a “new rule that is substantially the same as [the 2016 Reporting Rule] may not be issued.” 5 U.S.C. § 801(b)(2). The FCC cannot run away from this conclusion just because Congress might have chosen another way of commanding the same result. The FCC’s strained semantic distinctions only highlight the weakness of its construction.

2. The FCC’s interpretation of Section 802(b)(2) also generates the strange result that a congressional disapproval resolution does not actually block readoption of *any* of the rules contained within an order disapproved by Congress, unless Congress systematically identifies and specifically disapproves each of the rules contained within that order. This result is textually untenable for two reasons.

First, as all agree, the CRA’s definition of “rule” ensures that Congress’s disapproval resolution “nullif[ied]” each operative “part[.]” of the 2016 Broadband

Privacy Order, not simply the “whole” of it. A68 (Order ¶ 137). As explained above, Congress did not need to identify each specific rule within the Broadband Privacy Order as disapproved, given that its disapproval of the whole ensured disapproval of each part. *Supra* at 51.

Second, the CRA’s text would not have permitted Congress to enumerate each and every rule embedded within the Broadband Privacy Order in its disapproval resolution. Rather, the CRA strictly limits the form of every disapproval resolution as follows: “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).” 5 U.S.C. § 802(a). That form follows from the procedure of the CRA, which instructs an agency to submit to Congress any “rule” promulgated by the agency. *Id.* § 801(a).

Here, Congress disapproved the Broadband Privacy Order submitted by the FCC in the language prescribed by the CRA. *See* Pub. L. No. 115-22, 131 Stat. at 88 (“Congress disapproves the rule submitted by the Federal Communications Commission relating to ‘Protecting the Privacy of Customers of Broadband and Other Telecommunications Services’ (81 Fed. Reg. 87274) (December 2, 2016), and such rule shall have no force or effect.”). Congress, operating within that restricted format, could not have more specifically disapproved each component rule of the Broadband Privacy Order.

Implicitly recognizing as much, the FCC has also noted that “Congress ... always remains free to enact laws outside the CRA process that reject agency rules with as much detail and precision as they wish.” A68 (Order ¶ 137 n.485). But the whole point of the CRA is to give Congress a streamlined mechanism to reject agency rules. The notion that Congress should forgo that mechanism—which includes “fast track” procedures that allow resolutions to bypass filibusters in the Senate—overlooks why Congress enacted the CRA in the first place. As the FCC’s dissenters explained, the FCC majority seeks nothing less than to “read[] the CRA out of the United States Code altogether.” A98 (Carr Dissent).

3. The whole thrust of the FCC’s reasoning in this rulemaking proceeding disregards the Ninth Circuit’s insight that a CRA disapproval resolution “validly amend[s]” whatever existing statutory authority might have supported the disapproved rule. *Ctr. for Biological Diversity*, 946 F.3d at 562. A CRA disapproval resolution does not just invalidate the disapproved agency action; it is an act of Congress that sets out new statutory limits on the agency’s authority. Under the FCC’s construction, however, any limits are easy to circumvent: An agency may simply separately reissue any of the individual parts of the disapproved rule. If the FCC were right, then Congress’s disapproval power would be most easily evaded (and therefore *least* consequential) with respect to the most significant and sweeping agency rulemakings involving the biggest bundles of rules.

That cannot be right. The central concern animating the CRA was that agency regulations are often “several orders of magnitude” more complex than the statutory provisions giving rise to those regulations, and that Congress “has effectively abandoned its constitutional role as the national legislature” by giving agencies “so much latitude in implementing and interpreting congressional enactments.” 142 Cong. Rec. at 6926. The CRA aimed to “reclaim[] for Congress” its lost policymaking authority. *Id.* Those concerns are at their zenith with respect to omnibus agency regulations like the 2016 Broadband Privacy Order, which set forth an entirely new and comprehensive regime of privacy rules for telecommunications carriers. If the CRA is to have any meaning, a resolution of disapproval must apply to any rules issued through such omnibus orders. Here, that means that Congress’s disapproval resolution bars reissuance of the 2016 Reporting Rule or adoption of any substantially similar rule.

4. The reason why the FCC has so implausibly fought to evade the plain meaning of Section 801(b)(2) is because the 2024 Reporting Rule is indeed “substantially the same” as the 2016 Reporting Rule. *Supra* at 43-47. That is also why, in its 2024 Order, the FCC barely even tried to argue that the 2024 Reporting Rule is distinct from the 2016 Reporting Rule. Indeed, it devoted just *three sentences* of its Order to identifying purported distinctions between the 2024 Reporting Rule and the 2016 Reporting Rule. *See* A70 (Order ¶ 142).

The scattered justifications the FCC offered up did not identify any substantial differences between the two rules. The FCC asserted, for example, that “the customer notification requirement we adopt here is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016.” *Id.* Yet a comparison of those provisions indicates hardly any differences, let alone substantial ones. The 2016 Reporting Rule required carriers to provide customers with the “date” or “date range” of the breach, along with a “description” of the breach, as well as certain contact information so that customers could make further inquiries. 2016 Reporting Rule 14085 (47 C.F.R. § 64.2006(a)). The 2024 Reporting Rule requires carriers to provide customers with the “date” or “estimated timeframe” of the breach, and commands that such notice shall otherwise “include sufficient information so as to make a reasonable customer aware that ... such a breach affected or may have affected the customer’s data.” 47 C.F.R. § 64.2011(b). Any differences between the two rules on this matter are minor.

The FCC’s order forms a striking contrast with a recent SEC rulemaking conducted against the backdrop of a prior CRA disapproval resolution. *See Disclosure of Payments by Resource Extraction Issuers*, 86 Fed. Reg. 4662 (Jan. 15, 2021). In that proceeding, the SEC took seriously its obligation to ensure that any “new rule” would not be “substantially the same as the disapproved rule.” *Id.* at 4665. In the SEC’s view, one “appropriate and reasonable way” to measure whether

the new rule accomplished this “is primarily by comparing the extent to which the [requirement] under the disapproved rule would differ from the [requirements] under the new rule.” *Id.* The SEC’s new rule included a change to a key definitional term, “project,” *id.*, which was “one of the two central discretionary determinations at the heart” of the disapproved rule, *id.* at 4665. And the SEC’s order otherwise transparently balanced the changes reflected in the new rule with the similarities to the disapproved rule. *See id.* at 4666-67. The SEC’s approach to the CRA—which recognized that a resolution of disapproval disempowers an agency from reissuing the significant components of a rejected rule—is far more faithful to the statute than the FCC’s attempted end-run here.

The CRA is not a regulatory straitjacket. It does not prohibit administrative agencies from finding regulatory solutions to problems that were the subject of previously disapproved rules. What it does not permit is what the FCC attempted here: a blatant re-run of a congressionally disapproved rule.

That the FCC made so little attempt to justify what it was doing makes this Court’s review all the more urgent. It is somewhat common for agencies to overstep the bounds of their existing statutory authority, as the FCC did here with respect to its regulation of PII. But it is exceedingly rare for an agency to flout an express congressional prohibition on regulation, as the FCC did with respect to its repeated

effort to impose data-breach reporting requirements involving PII. The clearly expressed will of Congress should count for more.

CONCLUSION

For the reasons set forth above, this Court should set aside the 2024 Reporting Rule as contrary to law and in excess of statutory authority.

Dated: May 22, 2024

Respectfully submitted,

s/ Roman Martinez

Roman Martinez

Matthew A. Brill

Matthew T. Murchison

Charles S. Dameron

Christina R. Gay

LATHAM & WATKINS LLP

555 Eleventh Street, NW

Suite 1000

Washington, DC 20004

(202) 637-2200

roman.martinez@lw.com

Counsel for Petitioners

CERTIFICATE OF COMPLIANCE

This brief complies with the type-face and type-style rules of Federal Rule of Appellate Procedure 32(a)(5) and (6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman font.

This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B) because it contains 12,982 words, including the text in graphics, and excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f) and 6th Cir. R. 32(b).

s/ Roman Martinez
Roman Martinez

CERTIFICATE OF SERVICE

I hereby certify that on May 22, 2024, I electronically filed the foregoing Petitioners' Opening Brief with the Clerk of Court of the United States Court of Appeals for the Sixth Circuit by using the CM/ECF system. Participants here are registered CM/ECF users and will be served by the CM/ECF system.

s/ Roman Martinez
Roman Martinez

ADDENDUM

Pursuant to Federal Rule of Appellate Procedure 28(f)

ADDENDUM
TABLE OF CONTENTS

Description	Page
5 U.S.C. § 551(4)	ADD-1
5 U.S.C. § 801	ADD-2
5 U.S.C. § 802	ADD-6
5 U.S.C. § 804(3)	ADD-9
47 U.S.C. § 201	ADD-10
47 U.S.C. § 222	ADD-11
47 C.F.R. § 64.2011	ADD-15

5 U.S.C. § 551

§ 551 Definitions

For the purpose of this subchapter—

* * *

(4) “rule” means the whole or a part of an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy or describing the organization, procedure, or practice requirements of an agency and includes the approval or prescription for the future of rates, wages, corporate or financial structures or reorganizations thereof, prices, facilities, appliances, services or allowances therefor or of valuations, costs, or accounting, or practices bearing on any of the foregoing;

* * *

5 U.S.C. § 801

§ 801 Congressional review

(a)(1)(A) Before a rule can take effect, the Federal agency promulgating such rule shall submit to each House of the Congress and to the Comptroller General a report containing—

- (i) a copy of the rule;
- (ii) a concise general statement relating to the rule, including whether it is a major rule; and
- (iii) the proposed effective date of the rule.

(B) On the date of the submission of the report under subparagraph (A), the Federal agency promulgating the rule shall submit to the Comptroller General and make available to each House of Congress—

- (i) a complete copy of the cost-benefit analysis of the rule, if any;
- (ii) the agency's actions relevant to sections 603, 604, 605, 607, and 609;
- (iii) the agency's actions relevant to sections 202, 203, 204, and 205 of the Unfunded Mandates Reform Act of 1995; and
- (iv) any other relevant information or requirements under any other Act and any relevant Executive orders.

(C) Upon receipt of a report submitted under subparagraph (A), each House shall provide copies of the report to the chairman and ranking member of each standing committee with jurisdiction under the rules of the House of Representatives or the Senate to report a bill to amend the provision of law under which the rule is issued.

(2)(A) The Comptroller General shall provide a report on each major rule to the committees of jurisdiction in each House of the Congress by the end of 15 calendar days after the submission or publication date as provided in section 802(b)(2). The report of the Comptroller General shall include an assessment of the agency's compliance with procedural steps required by paragraph (1)(B).

(B) Federal agencies shall cooperate with the Comptroller General by providing information relevant to the Comptroller General's report under subparagraph (A).

(3) A major rule relating to a report submitted under paragraph (1) shall take effect on the latest of—

- (A) the later of the date occurring 60 days after the date on which—
 - (i) the Congress receives the report submitted under paragraph (1); or

(ii) the rule is published in the Federal Register, if so published;

(B) if the Congress passes a joint resolution of disapproval described in section 802 relating to the rule, and the President signs a veto of such resolution, the earlier date—

(i) on which either House of Congress votes and fails to override the veto of the President; or

(ii) occurring 30 session days after the date on which the Congress received the veto and objections of the President; or

(C) the date the rule would have otherwise taken effect, if not for this section (unless a joint resolution of disapproval under section 802 is enacted).

(4) Except for a major rule, a rule shall take effect as otherwise provided by law after submission to Congress under paragraph (1).

(5) Notwithstanding paragraph (3), the effective date of a rule shall not be delayed by operation of this chapter beyond the date on which either House of Congress votes to reject a joint resolution of disapproval under section 802.

(b)(1) A rule shall not take effect (or continue), if the Congress enacts a joint resolution of disapproval, described under section 802, of the rule.

(2) A rule that does not take effect (or does not continue) under paragraph (1) 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, unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule.

(c)(1) Notwithstanding any other provision of this section (except subject to paragraph (3)), a rule that would not take effect by reason of subsection (a)(3) may take effect, if the President makes a determination under paragraph (2) and submits written notice of such determination to the Congress.

(2) Paragraph (1) applies to a determination made by the President by Executive order that the rule should take effect because such rule is—

(A) necessary because of an imminent threat to health or safety or other emergency;

(B) necessary for the enforcement of criminal laws;

(C) necessary for national security; or

(D) issued pursuant to any statute implementing an international trade agreement.

(3) An exercise by the President of the authority under this subsection shall have no effect on the procedures under section 802 or the effect of a joint resolution of disapproval under this section.

(d)(1) In addition to the opportunity for review otherwise provided under this chapter, in the case of any rule for which a report was submitted in accordance with subsection (a)(1)(A) during the period beginning on the date occurring—

(A) in the case of the Senate, 60 session days, or

(B) in the case of the House of Representatives, 60 legislative days,

before the date the Congress adjourns a session of Congress through the date on which the same or succeeding Congress first convenes its next session, section 802 shall apply to such rule in the succeeding session of Congress.

(2)(A) In applying section 802 for purposes of such additional review, a rule described under paragraph (1) shall be treated as though—

(i) such rule were published in the Federal Register (as a rule that shall take effect) on—

(I) in the case of the Senate, the 15th session day, or

(II) in the case of the House of Representatives, the 15th legislative day,

after the succeeding session of Congress first convenes; and

(ii) a report on such rule were submitted to Congress under subsection (a)(1) on such date.

(B) Nothing in this paragraph shall be construed to affect the requirement under subsection (a)(1) that a report shall be submitted to Congress before a rule can take effect.

(3) A rule described under paragraph (1) shall take effect as otherwise provided by law (including other subsections of this section).

(e)(1) For purposes of this subsection, section 802 shall also apply to any major rule promulgated between March 1, 1996, and the date of the enactment of this chapter.

(2) In applying section 802 for purposes of Congressional review, a rule described under paragraph (1) shall be treated as though—

(A) such rule were published in the Federal Register on the date of enactment of this chapter; and

(B) a report on such rule were submitted to Congress under subsection (a)(1) on such date.

(3) The effectiveness of a rule described under paragraph (1) shall be as otherwise provided by law, unless the rule is made of no force or effect under section 802.

(f) Any rule that takes effect and later is made of no force or effect by enactment of a joint resolution under section 802 shall be treated as though such rule had never taken effect.

(g) If the Congress does not enact a joint resolution of disapproval under section 802 respecting a rule, no court or agency may infer any intent of the Congress from any action or inaction of the Congress with regard to such rule, related statute, or joint resolution of disapproval.

5 U.S.C. § 802

§ 802 Congressional disapproval procedure

(a) For purposes of this section, the term “joint resolution” means only a joint resolution introduced in the period beginning on the date on which the report referred to in section 801(a)(1)(A) is received by Congress and ending 60 days thereafter (excluding days either House of Congress is adjourned for more than 3 days during a session of Congress), the matter after the resolving clause of which is as follows: “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).

(b)(1) A joint resolution described in subsection (a) shall be referred to the committees in each House of Congress with jurisdiction.

(2) For purposes of this section, the term “submission or publication date” means the later of the date on which—

(A) the Congress receives the report submitted under section 801(a)(1); or

(B) the rule is published in the Federal Register, if so published.

(c) In the Senate, if the committee to which is referred a joint resolution described in subsection (a) has not reported such joint resolution (or an identical joint resolution) at the end of 20 calendar days after the submission or publication date defined under subsection (b)(2), such committee may be discharged from further consideration of such joint resolution upon a petition supported in writing by 30 Members of the Senate, and such joint resolution shall be placed on the calendar.

(d)(1) In the Senate, when the committee to which a joint resolution is referred has reported, or when a committee is discharged (under subsection (c)) from further consideration of a joint resolution described in subsection (a), it is at any time thereafter in order (even though a previous motion to the same effect has been disagreed to) for a motion to proceed to the consideration of the joint resolution, and all points of order against the joint resolution (and against consideration of the joint resolution) are waived. The motion is not subject to amendment, or to a motion to postpone, or to a motion to proceed to the consideration of other business. A motion to reconsider the vote by which the motion is agreed to or disagreed to shall not be in order. If a motion to proceed to the consideration of the joint resolution is agreed to, the joint resolution shall remain the unfinished business of the Senate until disposed of.

(2) In the Senate, debate on the joint resolution, and on all debatable motions and appeals in connection therewith, shall be limited to not more than 10 hours,

which shall be divided equally between those favoring and those opposing the joint resolution. A motion further to limit debate is in order and not debatable. An amendment to, or a motion to postpone, or a motion to proceed to the consideration of other business, or a motion to recommit the joint resolution is not in order.

(3) In the Senate, immediately following the conclusion of the debate on a joint resolution described in subsection (a), and a single quorum call at the conclusion of the debate if requested in accordance with the rules of the Senate, the vote on final passage of the joint resolution shall occur.

(4) Appeals from the decisions of the Chair relating to the application of the rules of the Senate to the procedure relating to a joint resolution described in subsection (a) shall be decided without debate.

(e) In the Senate the procedure specified in subsection (c) or (d) shall not apply to the consideration of a joint resolution respecting a rule—

(1) after the expiration of the 60 session days beginning with the applicable submission or publication date, or

(2) if the report under section 801(a)(1)(A) was submitted during the period referred to in section 801(d)(1), after the expiration of the 60 session days beginning on the 15th session day after the succeeding session of Congress first convenes.

(f) If, before the passage by one House of a joint resolution of that House described in subsection (a), that House receives from the other House a joint resolution described in subsection (a), then the following procedures shall apply:

(1) The joint resolution of the other House shall not be referred to a committee.

(2) With respect to a joint resolution described in subsection (a) of the House receiving the joint resolution—

(A) the procedure in that House shall be the same as if no joint resolution had been received from the other House; but

(B) the vote on final passage shall be on the joint resolution of the other House.

(g) This section is enacted by Congress—

(1) as an exercise of the rulemaking power of the Senate and House of Representatives, respectively, and as such it is deemed a part of the rules of each House, respectively, but applicable only with respect to the procedure to be followed in that House in the case of a joint resolution described in subsection (a),

and it supersedes other rules only to the extent that it is inconsistent with such rules; and

(2) with full recognition of the constitutional right of either House to change the rules (so far as relating to the procedure of that House) at any time, in the same manner, and to the same extent as in the case of any other rule of that House.

5 U.S.C. § 804

§ 804 Definitions

For purposes of this chapter—

* * *

(3) The term “rule” has the meaning given such term in section 551, except that such term does not include—

(A) any rule of particular applicability, including a rule that approves or prescribes for the future rates, wages, prices, services, or allowances therefor, corporate or financial structures, reorganizations, mergers, or acquisitions thereof, or accounting practices or disclosures bearing on any of the foregoing;

(B) any rule relating to agency management or personnel; or

(C) any rule of agency organization, procedure, or practice that does not substantially affect the rights or obligations of non-agency parties.

47 U.S.C. § 201

§ 201. Service and charges

(a) It shall be the duty of every common carrier engaged in interstate or foreign communication by wire or radio to furnish such communication service upon reasonable request therefor; and, in accordance with the orders of the Commission, in cases where the Commission, after opportunity for hearing, finds such action necessary or desirable in the public interest, to establish physical connections with other carriers, to establish through routes and charges applicable thereto and the divisions of such charges, and to establish and provide facilities and regulations for operating such through routes.

(b) All charges, practices, classifications, and regulations for and in connection with such communication service, shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful: *Provided*, That communications by wire or radio subject to this chapter may be classified into day, night, repeated, unrepeated, letter, commercial, press, Government, and such other classes as the Commission may decide to be just and reasonable, and different charges may be made for the different classes of communications: *Provided further*, That nothing in this chapter or in any other provision of law shall be construed to prevent a common carrier subject to this chapter from entering into or operating under any contract with any common carrier not subject to this chapter, for the exchange of their services, if the Commission is of the opinion that such contract is not contrary to the public interest: *Provided further*, That nothing in this chapter or in any other provision of law shall prevent a common carrier subject to this chapter from furnishing reports of positions of ships at sea to newspapers of general circulation, either at a nominal charge or without charge, provided the name of such common carrier is displayed along with such ship position reports. The Commission 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. § 222

§ 222. Privacy of customer information

(a) In general

Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

(b) Confidentiality of carrier information

A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

(c) Confidentiality of customer proprietary network information

(1) Privacy requirements for telecommunications carriers

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

(2) Disclosure on request by customers

A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

(3) Aggregate customer information

A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1). A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefor.

(d) Exceptions

Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents—

(1) to initiate, render, bill, and collect for telecommunications services;

(2) to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services;

(3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service; and

(4) to provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title) or the user of an IP-enabled voice service (as such term is defined in section 615b of this title)—

(A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;

(B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

(C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

(e) Subscriber list information

Notwithstanding subsections (b), (c), and (d), a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

(f) Authority to use location information

For purposes of subsection (c)(1), without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to—

(1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title) or the user of an IP-enabled voice service (as such term is defined in section 615b of this title), other than in accordance with subsection (d)(4); or

(2) automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.

(g) Subscriber listed and unlisted information for emergency services

Notwithstanding subsections (b), (c), and (d), a telecommunications carrier that provides telephone exchange service or a provider of IP-enabled voice service (as such term is defined in section 615b of this title) shall provide information described in subsection (i)(3)(A)¹ (including information pertaining to subscribers whose information is unlisted or unpublished) that is in its possession or control (including information pertaining to subscribers of other carriers) on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions to providers of emergency services, and providers of emergency support services, solely for purposes of delivering or assisting in the delivery of emergency services.

(h) Definitions

As used in this section:

(1) Customer proprietary network information

The term “customer proprietary network information” means—

(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

except that such term does not include subscriber list information.

¹ So in original. Probably should be subsection “(h)(3)(A)”.

(2) Aggregate information

The term “aggregate customer information” means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

(3) Subscriber list information

The term “subscriber list information” means any information—

(A) identifying the listed names of subscribers of a carrier and such subscribers’ telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and

(B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.

(4) Public safety answering point

The term “public safety answering point” means a facility that has been designated to receive emergency calls and route them to emergency service personnel.

(5) Emergency services

The term “emergency services” means 9–1–1 emergency services and emergency notification services.

(6) Emergency notification services

The term “emergency notification services” means services that notify the public of an emergency.

(7) Emergency support services

The term “emergency support services” means information or data base management services used in support of emergency services.

47 C.F.R. § 64.2011

§ 64.2011 Notification of security breaches.

(a) *Commission and Federal Law Enforcement Notification.* Except as provided in paragraph (a)(3) of this section, as soon as practicable, but no later than seven business days, after reasonable determination of a breach, a telecommunications carrier shall electronically notify the Commission, the United States Secret Service (Secret Service), and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility on its website.

(1) A telecommunications carrier shall, at a minimum, include in its notification to the Commission, Secret Service, and FBI:

- (i) The carrier's address and contact information;
- (ii) A description of the breach incident;
- (iii) The method of compromise;
- (iv) The date range of the incident;
- (v) The approximate number of customers affected;
- (vi) An estimate of financial loss to the carrier and customers, if any; and
- (vii) The types of data breached.

(2) If the Commission, or a law enforcement or national security agency, notifies the carrier that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security.

(3) A telecommunications carrier is exempt from the requirement to provide notification to the Commission and law enforcement pursuant to paragraph (a) of this section of a breach that affects fewer than 500 customers and the carrier reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach. In circumstances where a carrier initially determined that it qualified for an exemption under this paragraph (a)(3), but later discovers

information such that this exemption no longer applies, the carrier must report the breach to Federal agencies as soon as practicable, but no later than within seven business days of this discovery, as required in this paragraph (a).

(b) *Customer notification.* Except as provided in paragraph (a)(2) of this section, a telecommunications carrier shall notify affected customers of a breach of covered data without unreasonable delay after notification to the Commission and law enforcement pursuant to paragraph (a) of this section, and no later than 30 days after reasonable determination of a breach. This notification shall include sufficient information so as to make a reasonable customer aware that a breach occurred on a certain date, or within a certain estimated timeframe, and that such a breach affected or may have affected that customer's data. Notwithstanding the foregoing, customer notification shall not be required where a carrier reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach, or where the breach solely involves encrypted data and the carrier has definitive evidence that the encryption key was not also accessed, used, or disclosed.

(c) *Recordkeeping.* All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the Commission, Secret Service, and the FBI pursuant to paragraph (a) of this section, and notifications made to customers pursuant to paragraph (b) of this section. The record shall include, if available, dates of discovery and notification, a detailed description of the covered data that was the subject of the breach, the circumstances of the breach, and the bases of any determinations regarding the number of affected customers or likelihood of harm as a result of the breach. Carriers shall retain the record for a minimum of 2 years.

(d) *Annual Reporting of Certain Small Breaches.* A telecommunications carrier shall have an officer, as an agent of the carrier, sign and file with the Commission, Secret Service, and FBI, a summary of all breaches occurring in the previous calendar year affecting fewer than 500 individuals and where the carrier could reasonably determine that no harm to customers was reasonably likely to occur as a result of the breach. This filing shall be made annually, on or before February 1 of each year, through the central reporting facility, for data pertaining to the previous calendar year.

(e) *Definitions.* (1) As used in this section, a "breach" occurs when a person, without authorization or exceeding authorization, gains access to, uses, or discloses covered data. A "breach" shall not include a good-faith acquisition of covered data by an employee or agent of a telecommunications carrier where such information is not used improperly or further disclosed.

(2) As used in this section, “covered data” includes both a customer’s CPNI, as defined by § 64.2003, and personally identifiable information.

(3) As used in this section, “encrypted data” means covered data that has been transformed through the use of an algorithmic process into a form that is unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security.

(4) As used in this section, “encryption key” means the confidential key or process designed to render encrypted data useable, readable, or decipherable.

(5) Except as provided in paragraph (e)(6) of this section, as used in this section, “personally identifiable information” means:

(i) An individual’s first name or first initial, and last name, in combination with any government-issued identification numbers or information issued on a government document used to verify the identity of a specific individual, or other unique identification number used for authentication purposes;

(ii) An individual’s username or email address, in combination with a password or security question and answer, or any other authentication method or information necessary to permit access to an account; or

(iii) Unique biometric, genetic, or medical data.

(iv) Notwithstanding the above:

(A) Dissociated data that, if linked, would constitute personally identifiable information is to be considered personally identifiable if the means to link the dissociated data were accessed in connection with access to the dissociated data; and

(B) Any one of the discrete data elements listed in paragraphs (e)(5)(i) through (iii) of this section, or any combination of the discrete data elements listed above is personally identifiable information if the data element or combination of data elements would enable a person to commit identity theft or fraud against the individual to whom the data element or elements pertain.

(6) As used in this section, “personally identifiable information” does not include information about an individual that is lawfully made available to the general public from Federal, State, or local government records or widely distributed media.