

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
and UNITED STATES OF AMERICA,

Respondents.

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

BRIEF FOR RESPONDENTS

Jonathan S. Kanter
Assistant Attorney General

Robert B. Nicholson
Attorney

U.S. DEPARTMENT OF JUSTICE
ANTITRUST DIVISION
950 Pennsylvania Ave. NW
Washington, DC 20530

P. Michele Ellison
General Counsel

Jacob M. Lewis
Deputy General Counsel

Sarah E. Citrin
Deputy Associate General Counsel

Adam L. Sorensen
Counsel

FEDERAL COMMUNICATIONS
COMMISSION
45 L Street NE
Washington, DC 20554
(202) 418-1740
fcclitigation@fcc.gov

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES	v
STATEMENT IN SUPPORT OF ORAL ARGUMENT	xii
INTRODUCTION.....	1
STATEMENT OF THE ISSUES	5
STATEMENT OF THE CASE.....	5
A. Statutory And Regulatory Background.....	5
1. Consumer privacy under the Communications Act.....	5
a. Section 201(b).....	5
b. Section 222	5
c. Section 225	7
2. The Commission’s rulemaking authority	7
3. The Commission’s privacy orders	8
a. The 1998 CPNI Order	8
b. The 2007 Notification Rule	8
c. The 2013 Relay Service Order	9
d. The 2016 Broadband Privacy Order.....	9
4. The Congressional Review Act and the 2017 Disapproval Resolution of the 2016 Broadband Privacy Order	11
B. The Data Breach Order.....	12
1. Data breach obligations	13
2. Legal authority.....	15
a. Section 222	16
b. Section 201(b).....	16
c. Section 225	17
d. Congressional disapproval.....	17

TABLE OF CONTENTS
(continued)

	Page
STANDARD OF REVIEW	18
SUMMARY OF THE ARGUMENT.....	19
ARGUMENT	21
I. SECTION 201(B) OF THE COMMUNICATIONS ACT AUTHORIZES THE COMMISSION TO PROTECT TELECOMMUNICATIONS CUSTOMERS’ PERSONALLY IDENTIFIABLE INFORMATION.....	21
A. The Commission Engaged In Reasoned Decisionmaking Within Section 201(b)’s Boundaries	21
B. Statutory Structure And Sound Policy Support The Commission’s Reading	25
C. Petitioners Misread Section 201(b).....	27
II. PERSONALLY IDENTIFIABLE INFORMATION IS CONSUMER “[P]ROPRIETARY [I]NFORMATION” UNDER SECTION 222(A).....	34
A. The Ordinary Meaning of Section 222(a) Supports the Commission’s Reading	34
B. Petitioners Misread Section 222	37
III. THE COMMISSION’S BREACH NOTIFICATION RULES FOR TELECOMMUNICATIONS RELAY SERVICE PROVIDERS ARE AUTHORIZED UNDER SECTION 225 AND THE COMMISSION’S ANCILLARY AUTHORITY.....	44
IV. THE COMMISSION’S DATA BREACH REPORTING RULES ARE CONSISTENT WITH THE CONGRESSIONAL REVIEW ACT	47
A. The Congressional Review Act’s Disapproval Bar Is Limited To “Substantially The Same” Rule	48
1. The CRA and Congress’s disapproval resolution apply only to the 2016 order as a whole	48
2. Petitioners’ interpretation of the CRA is mistaken	52

TABLE OF CONTENTS
(continued)

	Page
B. The Challenged Order Is Not “Substantially The Same” As The 2016 Broadband Privacy Order.....	57
CONCLUSION	63
CERTIFICATE OF COMPLIANCE	64

TABLE OF AUTHORITIES*

Cases

<i>Alaska v. Haaland</i> , 143 S. Ct. 1002 (2023).....	49
<i>Calif. Indep. Sys. Operator Corp. v. FERC</i> , 372 F.3d 395 (D.C. Cir. 2004).....	28
<i>Chicago & N. W. Ry. Co. v. United Transp. Union</i> , 402 U.S. 570 (1971).....	38
<i>City of Eugene, Oregon v. FCC</i> , 998 F.3d 701 (6th Cir. 2021).....	19
<i>Ctr. for Biological Diversity</i> , 946 F.3d 553 (9th Cir. 2019).....	57
<i>Epic Sys. Corp. v. Lewis</i> , 584 U.S. 497 (2018)	31
<i>FTC v. AT&T Mobility LLC</i> , 883 F.3d 848 (9th Cir. 2018)	26
<i>FTC v. Wyndham Worldwide Corp.</i> , 799 F.3d 236 (3d Cir. 2015).....	26
<i>Glob. Crossing Telecomms., Inc. v. Metrophones Telecomms., Inc.</i> , 550 U.S. 45 (2007).....	22, 28
<i>Graham Cnty. Soil & Water Conservation Dist. v. U.S. ex rel. Wilson</i> , 559 U.S. 280 (2010).....	27
<i>In re Davis</i> , 960 F.3d 346 (6th Cir. 2020)	37
<i>In re Jackson Masonry, LLC</i> , 906 F.3d 494 (6th Cir. 2018)	35
<i>Loper Bright Enters. v. Raimondo</i> , 603 U.S. ___, 144 S. Ct. 2244, 2262 (2024).....	19, 22
<i>Qwest Corp. v. Ariz. Corp. Comm’n</i> , 567 F.3d 1109 (9th Cir. 2009).....	32
<i>RadLAX Gateway Hotel, LLC v. Amalgamated Bank</i> , 566 U.S. 639 (2012).....	30

TABLE OF AUTHORITIES
(continued)

	Page(s)
<i>Razete v. United States</i> , 199 F.2d 44 (6th Cir. 1952).....	28
<i>Retail Ventures, Inc. v. Nat’l Union Fire Ins. Co. of Pittsburgh, Pa.</i> , 691 F.3d 821 (6th Cir. 2012).....	39
<i>Safari Club Int’l v. Haaland</i> , 31 F.4th 1157 (9th Cir. 2022), <i>cert.</i> <i>denied sub nom. Alaska v. Haaland</i> , 143 S. Ct. 1002 (2023) 49, 50, 57, 62	
<i>Skilling v. United States</i> , 561 U.S. 358 (2010)	30
<i>United States Telecom Ass’n v. FCC</i> , 825 F.3d 674 (D.C. Cir. 2016) 10, 36	
<i>United States v. Dairy Farmers of Am., Inc.</i> , 426 F.3d 850 (6th Cir. 2005).....	62
<i>United States v. Fitzgerald</i> , 906 F.3d 437 (6th Cir. 2018).....	55
<i>United States v. Small</i> , 988 F.3d 241 (6th Cir. 2021).....	34
 Statutes	
5 U.S.C. § 551(4).....	54, 55
5 U.S.C. § 553(b).....	62
5 U.S.C. § 801(b).....	11, 48, 53, 62
5 U.S.C. § 801(f).....	56
15 U.S.C. § 44	26
15 U.S.C. § 45(a).....	26
15 U.S.C. § 6501(8).....	41
15 U.S.C. § 6809(4).....	41
16 U.S.C. § 824e(a)	28

TABLE OF AUTHORITIES
(continued)

	Page(s)
47 U.S.C. § 154(i).....	46
47 U.S.C. § 1602(a).....	38
47 U.S.C. § 201(b).....	<i>passim</i>
47 U.S.C. § 222.....	5
47 U.S.C. § 222(a).....	<i>passim</i>
47 U.S.C. § 222(b).....	6
47 U.S.C. § 222(c).....	6, 36
47 U.S.C. § 222(c)(1).....	40
47 U.S.C. § 222(h)(1).....	6, 35, 36, 41
47 U.S.C. § 225.....	<i>passim</i>
47 U.S.C. § 228(a).....	38
47 U.S.C. § 251.....	32
47 U.S.C. § 252.....	32
47 U.S.C. § 256(a).....	38
47 U.S.C. § 303(r).....	7
47 U.S.C. § 343(a).....	38
47 U.S.C. § 394(a).....	38
47 U.S.C. § 395(a).....	38
47 U.S.C. § 532(a).....	38
47 U.S.C. § 548(a).....	38

TABLE OF AUTHORITIES
(continued)

	Page(s)
47 U.S.C. § 614(a).....	38
47 U.S.C. § 1411(a).....	38
47 U.S.C. § 1428(a).....	38
Ala. Code § 8-38-2.....	41
Telecommunications Act of 1996, Pub. L. 104-104, 110 Stat. 56 (1996).....	31
 Regulations	
47 C.F.R. § 64.2009	8
 Administrative Materials	
<i>Disclosure of Payments by Resource Extraction Issuers</i> , SEC, 86 Fed. Reg. 4662 (Jan. 15, 2021)	61
<i>Implementation of the Telecommunications Act of 1996</i> , 13 FCC Rcd 8061 (1998).....	8, 25, 42, 43
<i>Implementation of the Telecommunications Act of 1996</i> , 22 FCC Rcd 6927 (2007).....	9
<i>Lifeline & Link Up Reform & Modernization</i> , 30 FCC Rcd 7818 (2015).....	25
<i>Protecting and Promoting the Open Internet</i> , 30 FCC Rcd 5601 (2015), <i>aff'd</i> , <i>United States Telecom Ass'n v. FCC</i> , 825 F.3d 674 (D.C. Cir. 2016)	10
<i>Protecting the Privacy of Customers of Broadband and Other Telecommunications Services</i> , 31 FCC Rcd 13911 (2016).....	<i>passim</i>

TABLE OF AUTHORITIES
(continued)

	Page(s)
<i>Re Second Computer Inquiry</i> , 77 FCC.2d 384, 440, 499 (1980), <i>aff'd sub nom. Computer and Communications Industry Ass'n v. FCC</i> , 693 F.2d 198 (D.C. Cir. 1982).....	24
<i>Regulatory & Policy Problems Presented by the Interdependence of Computer & Communication Services & Facilities</i> , 28 FCC.2d 291 (1970), <i>aff'd in part sub nom. GTE Serv. Corp. v. FCC</i> , 474 F.2d 724 (2d Cir. 1973)	24
<i>Restoring Internet Freedom</i> , 33 FCC Rcd 311 (2017)	10
<i>Safeguarding and Securing the Open Internet Restoring Internet Freedom</i> , 2024 WL 2109860 (May 7, 2024), <i>petition for review filed, In re MCP No. 185</i> , No. 24-7000 (6th Cir.).....	10, 58
<i>Structure and Practices of the Video Relay Service Program; Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities</i> , 28 FCC Rcd 8618 (2013)	9, 45, 46
<i>Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information</i> , 14 FCC Rcd 14409 (1999).....	33
<i>TerraCom, Inc. and YourTel America, Inc.</i> , 29 FCC Rcd 13325 (2014).....	17, 23, 25, 43
 Legislative Materials	
H.R. Rep. No. 104-204	31
H.R. Rep. No. 104-458	31
Joint Resolution, Pub. L. No. 115-22, 131 Stat. 88 (2017) ...	11, 48, 53, 54

TABLE OF AUTHORITIES
(continued)

	Page(s)
Providing for Congressional Disapproval of a Rule Submitted by the Federal Communications Commission, 163 Cong. Rec. H2478 (daily ed. Mar. 28, 2017)	50
Providing for Congressional Disapproval of a Rule Submitted by the Federal Communications Commission, 163 Cong. Rec. H2479 (daily ed. Mar. 28, 2017)	51
<i>Providing for Congressional Disapproval of a Rule Submitted by the Federal Communications Commission</i> , 163 Cong. Rec. H2489 (daily ed. Mar. 28, 2017)	51
Providing for Congressional Disapproval of a Rule Submitted by the Federal Communications Commission, 163 Cong. Rec. S1925 (daily ed. Mar. 22, 2017)	50
 Treatise	
Antonin Scalia & Bryan A. Garner, <i>Reading Law: The Interpretation of Legal Texts</i> (2012)	36
 Other Materials	
Adam M. Finkel & Jason W. Sullivan, <i>A Cost-Benefit Interpretation of the “Substantially Similar” Hurdle in the Congressional Review Act: Can OSHA Ever Utter the E-Word (Ergonomics) Again?</i> , 63 Admin. L. Rev. 707 (2011)	49, 52
<i>Black’s Law Dictionary</i> (6th ed. 1990)	35, 48
Hamilton Relay Comments (Feb. 22, 2023).....	45
Matt Egan & Sean Lyngaas, <i>Nearly all AT&T cell customers’ call and text records exposed in a massive breach</i> , CNN (July 12, 2024).....	12
Merriam Webster Online	39

TABLE OF AUTHORITIES
(continued)

	Page(s)
Michael J. Cole, <i>Interpreting the Congressional Review Act: Why the Courts Should Assert Judicial Review, Narrowly Construe “Substantially the Same,” and Decline to Defer to Agencies Under Chevron</i> , 70 Admin. L. Rev. 53 (2018)	49

STATEMENT IN SUPPORT OF ORAL ARGUMENT

Respondents believe that the Court could find oral argument helpful.

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
and UNITED STATES OF AMERICA,

Respondents.

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

BRIEF FOR RESPONDENTS

INTRODUCTION

Responding to a startling increase in the frequency and sophistication of attacks targeting telecommunications customers' personal data, the Federal Communications Commission revised its privacy rules to ensure that carriers are adequately protecting their customers. *See Data Breach Reporting Requirements*, FCC 23-111, 2023

WL 8889606 (released Dec. 21, 2023), Petitioners’ Appendix (“A”) 1–104. Among other things, the revised rules clarified that carriers are obligated to protect customers’ “personally identifiable information”—including their names, government identification numbers, and medical data. At the same time, the Commission redefined the term “breach” to account for carriers’ good faith, updated carriers’ reporting responsibilities, and extended those rules to providers of telecommunications relay services to individuals with hearing and speech impairments.

The Commission grounded these changes on three independent bases of statutory authority. First, Section 201(b) of the Communications Act empowers the Commission to ensure that carriers’ “practices” in offering communication services are “just and reasonable.” 47 U.S.C. § 201(b). Second, Section 222(a) authorizes the Commission to enforce carriers’ duty to protect “proprietary information of, and relating to . . . customers.” 47 U.S.C. § 222(a). And third, with respect to relay services, Section 225 obligates the Commission to ensure those services are “functionally equivalent” to service provided to consumers without hearing or speech impairments. 47 U.S.C. § 225.

In this challenge to the Commission’s updated privacy rules, Petitioners ask this Court to impose sweeping new restraints on the

federal government’s ability to protect the personal information of telecommunications customers. If adopted, those restraints would not only leave tens of millions of such consumers without any federal regulatory protection for their most private data held by carriers—including social security numbers and biometrics—but would also permanently forbid the Commission from issuing similar protections. Such an outcome would needlessly expose the private data of every American who uses a telecommunications device and is flatly inconsistent with the expressed will of Congress.

Petitioners advance a series of novel statutory arguments that would rewrite the text of the Communications Act and disregard the Commission’s long history of protecting telecommunications customer privacy. Largely ignoring Section 201(b)’s broad prohibition of “unjust and unreasonable” carrier practices, 47 U.S.C. § 201(b), Petitioners argue that their obligation to protect consumer data is controlled by Section 222’s privacy protections. Yet they point to virtually no evidence of Congress’s intent to narrow Section 201(b) in that manner. Petitioners likewise attempt to read their general obligation to protect the “proprietary information of, and relating to . . . customers” under Section 222(a) out of the Communications Act, arguing that provision has no

independent meaning. Finally, Intervenor provides no reason to think the Commission's rules respecting relay service providers are not authorized by Section 225's instruction that such service be "functionally equivalent" to other telecommunications services. 47 U.S.C. § 225(a)(3).

Petitioners' argument that the challenged order is prohibited by Congress's disapproval of an earlier rule under the Congressional Review Act (or "CRA") is equally misguided. The CRA prohibits an agency from reissuing "substantially the same" rule as one Congress has previously disapproved, but it does not prohibit an agency from adopting an approach with similar or overlapping features. Petitioners' contrary interpretation is unfaithful to the text of the CRA and would produce absurd results, permanently barring agencies from readopting even the most routine parts of disapproved orders, such as legal definitions. Even under Petitioners' reading, the disapproved rule on which they rely—a broad 2016 privacy order targeting broadband Internet service providers—differed dramatically in scope, focus, and approach from the order challenged here. And even at the most granular level, the disapproved rule's breach notification provisions contained key differences from those in the challenged order.

The petitions for review should be denied.

STATEMENT OF THE ISSUES

1. Whether the Commission acted within its statutory authority in promulgating the challenged data breach notification rule.
2. Whether the Commission complied with the Congressional Review Act in promulgating the challenged data breach notification rule.

STATEMENT OF THE CASE

A. Statutory And Regulatory Background

1. Consumer privacy under the Communications Act

a. Section 201(b)

Section 201(b) of the Communications Act provides that “[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service [by wire or radio] shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful.” 47 U.S.C. § 201(b).

b. Section 222

Section 222, entitled “Privacy of customer information,” requires telecommunications carriers to protect the confidentiality of certain information belonging to other carriers, equipment manufacturers, and customers. 47 U.S.C. § 222.

Subsection (a) lays out broad obligations for telecommunications carriers: “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.” 47 U.S.C. § 222(a).

Subsection (b) restricts the use of proprietary information one carrier receives from another, limiting its use to “providing any telecommunications service.” *Id.* § 222(b).

Subsection (c) restricts carriers’ use of “customer proprietary network information” (“CPNI”), *id.* § 222(c), a statutorily defined term that 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.

Id. § 222(h)(1).

c. Section 225

Section 225 charges the Commission with ensuring the availability and efficiency of “telecommunications relay services”—“telephone transmission services that provide the ability for an individual who is deaf, hard of hearing, deaf-blind, or who has a speech disability to engage in communication by wire or radio . . . in a manner that is functionally equivalent to the ability of a hearing individual who does not have a speech disability.” 47 U.S.C. § 225(a)(3).

2. The Commission’s rulemaking authority

The Communications Act provides the Commission with broad rulemaking authority to carry out its provisions.

Section 201(b) authorizes the Commission to “prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter.” 47 U.S.C. § 201(b). Similarly, Section 303(r) empowers the Commission to “[m]ake such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this chapter.” *Id.* § 303(r). And Section 225(d) empowers the Commission to “establish functional requirements, guidelines, and operations procedures for telecommunications relay services” and “establish minimum standards

that shall be met in carrying out” the provision of those services. *Id.* § 225(d)(1).

3. The Commission’s privacy orders

The Commission’s privacy rulemaking and enforcement efforts have evolved over time to keep pace with emerging threats to consumers and carriers, as well other changes in the legal and regulatory landscape.

a. The 1998 CPNI Order

After Congress enacted Section 222 in 1996, the Commission adopted implementing rules that established restrictions on telecommunications carriers’ use and disclosure of CPNI, and required carriers to take effective steps to protect CPNI. *Implementation of the Telecommunications Act of 1996*, 13 FCC Rcd 8061, 8195, ¶193 (1998) (1998 CPNI Order). Among other things, the 1998 CPNI Order required carriers to train their personnel on handling customer information, and to maintain records that track access to CPNI. *See* 1998 CPNI Order at 8198, ¶¶198–199; 47 C.F.R. § 64.2009(b)–(c).

b. The 2007 Notification Rule

In 2007, responding to the rising incidence of “pretexting” scams—in which a party seeking access to a customer’s private communications records pretends to be a customer or authorized user to obtain that

information—the Commission amended its customer privacy rules to, among other things, require carriers to notify law enforcement and customers of security breaches involving CPNI. *Implementation of the Telecommunications Act of 1996*, 22 FCC Rcd 6927, 6943–45, ¶¶26–32.

c. The 2013 Relay Service Order

In 2013, the Commission adopted rules to protect the privacy of customer information relating to telecommunications relay services. *Structure and Practices of the Video Relay Service Program; Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, 28 FCC Rcd 8618 (2013) (2013 Relay Service Order). Responding to rampant fraud and abuse in the provision of relay services, *id.* at 8620, ¶1, the Commission applied CPNI protections to relay service providers that largely mirrored preexisting rules applicable to other telecommunications service providers. *Id.* at 8684–85, ¶¶164–169.

d. The 2016 Broadband Privacy Order

In 2015, the Commission reclassified broadband Internet access service as a telecommunications service subject to Title II of the Communications Act. *See Protecting and Promoting the Open Internet*,

30 FCC Rcd 5601, 5733, ¶306 (2015), *aff'd*, *United States Telecom Ass'n v. FCC*, 825 F.3d 674 (D.C. Cir. 2016).¹

In the wake of that decision, the Commission in 2016 issued a wide-ranging order adopting a host of privacy regulations primarily addressing broadband Internet service providers. *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 31 FCC Rcd 13911 (2016) (2016 Broadband Privacy Order).

In the course of that proceeding, the Commission also adopted revisions to its privacy rules governing telecommunications carriers. Among other things, the Commission clarified that the information protected by its rules included not only CPNI, but also “personally identifiable information” and the “content of communications.” *Id.* at 13913–14, ¶6. It further required telecommunications providers to inform customers “clearly and accurately . . . about what confidential information the carriers collect” and how they use it, *id.* at 13914, ¶8; set

¹ The Commission subsequently reversed its 2015 classification decision, *see Restoring Internet Freedom*, 33 FCC Rcd 311 (2017), but has more recently returned to its classification of broadband Internet access service as a Title II telecommunications service, *see Safeguarding and Securing the Open Internet Restoring Internet Freedom*, 2024 WL 2109860 (May 7, 2024) (2024 Open Internet Order), *petition for review filed*, *In re MCP No. 185*, No. 24-7000 (6th Cir.).

different standards for customer approval of a carrier’s use of sensitive vs. non-sensitive customer information, *id.* at 13915, ¶9; instituted new data security requirements, *id.* at 13915, ¶10; and adopted breach notification rules requiring carriers to notify affected customers and federal authorities, *id.* at 13915, ¶11.

4. The Congressional Review Act and the 2017 Disapproval Resolution of the 2016 Broadband Privacy Order

The CRA provides, in relevant part, that an agency “rule shall not take effect (or continue), if the Congress enacts a joint resolution of disapproval.” 5 U.S.C. § 801(b)(1). Such a disapproved rule “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 specifically authorized by Congress. 5 U.S.C. § 801(b)(2).

The resolution disapproving the 2016 Broadband Privacy Order 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.” Joint Resolution, Pub. L. No. 115-22, 131 Stat. 88 (2017).

B. The Data Breach Order

Concerned with the rising frequency and sophistication of customer data breaches, the Commission in 2023 proposed new rules updating the breach notification obligations of telecommunications carriers and relay service providers. *See* A120–21 (*Data Breach Reporting Requirements*, 38 FCC Rcd 566, 566–67, ¶1 & n.3 (2023)).

As the Commission explained in the order it ultimately adopted, A1–104 (*Data Breach Reporting Requirements*, FCC 23-111 (Order)), telecommunications “providers often collect large quantities of sensitive customer data,” which can be exploited to provide insight into myriad aspects of customers’ private lives, including “medical conditions, religious beliefs, [and] personal associations.” A2 (Order ¶1). Telecommunications carriers have proven particularly vulnerable to attack in recent years, with one major provider experiencing a customer data breach each year between 2018 and 2023, including one event affecting 37 million customers. *See* A2 (Order ¶3 & n.5).²

² That trend has continued since the Commission’s order. AT&T recently disclosed that “nearly all” of its tens of millions of cellular customers’ call and text logs were exposed in a data breach. *See* Matt Egan & Sean Lyngaas, *Nearly all AT&T cell customers’ call and text records exposed in a massive breach*, CNN (July 12, 2024) (available at (cont’d)

1. Data breach obligations

In response to these evolving threats, the Commission adopted six primary changes to its data breach rules. *See* A2–3 (Order ¶¶3–4).

a. First, the Commission expanded the scope of its breach notification rules to cover not just CPNI, but also consumers’ “personally identifiable information” (or “PII”). A8–12 (Order ¶¶15–20). PII means “information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.” A9–10 (Order ¶17). For purposes of the notification rules, covered PII is limited to information obtained “in connection with the customer relationship,” A9 (Order ¶16), and that specifically includes:

- (1) 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) user name or e-mail 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
- (3) unique biometric, genetic, or medical data.

<https://www.cnn.com/2024/07/12/business/att-customers-massive-breach/index.html>).

A10 (Order ¶18).

b. Second, the Commission altered its definition of a “breach” for telecommunications carriers to include inadvertent access, use, or disclosure of customer information, except in those cases where such information is acquired in good faith by an employee or agent of a carrier, and such information is not used improperly or further disclosed. A12–17 (Order ¶¶21–27).

c. Third, the Commission required carriers to notify the Commission, the Secret Service, and the FBI as soon as practicable after a reasonable determination of a breach, but no later than seven business days following such determination. A18–30 (Order ¶¶28–51).

d. Fourth, the Commission eliminated its previous requirement that carriers notify customers of a breach in cases where a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. A30–36 (Order ¶¶52–58).

e. Fifth, the Commission eliminated a mandatory waiting period for carriers to notify customers, and instead required carriers to notify customers without unreasonable delay after notification to federal agencies, and in no case more than 30 days following reasonable

determination of a breach (unless a delay is requested by law enforcement). A36–37 (Order ¶¶59–61).

f. Finally, to fulfill its statutory duty to ensure that people who rely on relay services receive equivalent protections to other telecommunications consumers, the Commission adopted equivalent changes to the data breach obligations of telecommunications relay service providers. A39–57 (Order ¶¶65–116).

2. Legal authority

The Commission also analyzed its statutory authority to enact the challenged order, concluding that “sections 201(b), 222, 225, and 251(e)” of the Communications Act provided it “with authority to adopt the breach notification rules enumerated in this Order,” and that “Congress’ nullification of the Commission’s revisions to its data breach rules in the 2016 Privacy Order” did not preclude the adopted rules. A58 (Order ¶117). *See id.* A58–71 (Order ¶¶117–143).³

³ Section 251(e) authorizes the Commission’s breach notification rule with respect to interconnected Voice over Internet Protocol (VoIP) providers. *See* A65 (Order ¶129). Because neither Petitioners nor Intervenor challenge that aspect of the order, this brief does not address it.

a. Section 222

The Commission first discussed its authority under subsections 222(a) and 222(c). While the latter “imposes more specific requirements on carriers” with respect to CPNI, the Commission explained that subsection 222(a) imposes a more general duty on carriers to “protect the confidentiality of proprietary information of, and relating to’ customers, fellow carriers, and equipment manufacturers.” A58 (Order ¶118). “[T]he breadth of section 222(a)” offered “additional clarity that the Commission’s breach reporting rules can” apply to all PII, not just to CPNI. *Id.* That conclusion was consistent with previous Commission practice, and it was confirmed by the structure of the statute. A59–60 (Order ¶¶120–122).

b. Section 201(b)

Independent of Section 222, the Commission also grounded its statutory authority for the data breach notification rules in Section 201(b)’s requirement that common carriers’ practices be just and reasonable. A61–64 (Order ¶¶124–126). Section 201(b) may be “violated when carriers fail[] to notify customers whose personal information ha[s] been breached by the carriers’ inadequate data-security policies.” A61–62 (Order ¶124) (citing *TerraCom, Inc. and YourTel America, Inc.*, 29

FCC Rcd 13325 (2014) (*TerraCom*)). That conclusion was consistent with Section 201(b)'s plain language, did not conflict with Section 222, and was further confirmed by Congress's choice to exempt telecommunications carriers from comparable federal regulation by the Federal Trade Commission. A62–64 (Order ¶¶125–126).

c. Section 225

The Commission further concluded it had independent authority to amend its data breach requirements for telecommunications relay services under Section 225. A65–66 (Order ¶¶130–132). Because that provision directs the Commission to ensure that relay services enable communication in a manner that is “functionally equivalent” to telecommunications services provided to consumers without hearing or speech impairments, the Commission concluded it had “ample legal authority” to amend its data breach rules in this area. *Id.*

d. Congressional disapproval

Finally, the Commission determined that Congress's disapproval of the 2016 Broadband Privacy Order under the CRA did not preclude the rule. A66–71 (Order ¶¶133–143).

The Commission concluded that “the CRA is best interpreted as prohibiting the Commission 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). The statute does not “prohibit the [agency] 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.” *Id.* The Commission further explained why this conclusion was consistent with the plain text of both the CRA and the 2017 disapproval resolution, as well as with the legislative history of the resolution. A68 (Order ¶136–137).

Even if that were not the case, the Commission also found the new rules differed substantially from those in the 2016 Broadband Privacy Order. A70 (Order ¶142). Critical differences included less prescriptive customer notification requirements, the addition of a good-faith exception to the definition of a “breach,” and different disclosure requirements for federal reporting. *Id.*

STANDARD OF REVIEW

In reviewing agency action under the Administrative Procedure Act, this Court must “determine whether the agency rules at issue are ‘arbitrary, capricious, an abuse of discretion, or otherwise not in

accordance with law[.]” *City of Eugene, Oregon v. FCC*, 998 F.3d 701, 707 (6th Cir. 2021).

Courts “must exercise independent judgment in determining the meaning of statutory provisions.” *Loper Bright Enters. v. Raimondo*, 603 U.S. ___, 144 S. Ct. 2244, 2262 (2024). Nonetheless, where Congress has “empower[ed] an agency to prescribe rules to ‘fill up the details’ of a statutory scheme, or to regulate subject to the limits imposed by a term or phrase—such as “reasonable”—that ‘leaves agencies with flexibility,’” courts must “recognize[] [Congress’s] constitutional delegations” to agency expertise and, in interpreting such a statute, should merely “ensur[e] the agency has engaged in ‘reasoned decisionmaking’ within those boundaries.” *Id.* at 2263.

SUMMARY OF THE ARGUMENT

I. The challenged breach notification rule falls within the Commission’s broad powers under Section 201(b) of the Communications Act, which authorizes the Commission, in pertinent part, to ensure that “[a]ll . . . practices . . . for and in connection with” a “communication service” are “just and reasonable.” Privacy rules under this provision are nothing new, and Congress delegated significant discretion to the Commission to regulate in this area. Contrary to Petitioners’ argument,

Section 222 has not silently superseded Section 201(b)'s plain text and well-established meaning.

II. Section 222(a) also authorizes the Commission to require telecommunications carriers to protect customers' personally identifiable information. It plainly states that the Commission has authority over all of telecommunications carriers' customers' "proprietary information," not only their proprietary network information as protected elsewhere in the statute.

III. The Commission likewise has authority to apply its protection of personally identifiable information to telecommunications relay service providers. Section 225 of the Communications Act obligates the Commission to do so, and the Commission's ancillary powers under Section 222 provide further authority for this portion of the Commission's order.

IV. Congress's 2017 disapproval of a prior Commission order under the Congressional Review Act does not bar this new rule.

The plain text of the Congressional Review Act, as well as that of the 2017 disapproval resolution, make clear that Congress disapproves of a single "rule" as a whole, not an unnamed constituent part. That straightforward conclusion is confirmed by the legislative history, which

shows that Congress did not have data breach notification rules in mind when it disapproved the 2016 Broadband Privacy Order. Moreover, it would make little to sense to forbid agencies from making small but meaningful changes to address Congress’s concerns, or to require them to discard policies Congress supported or did not consider.

In any event, the breach notification rule challenged here is not “substantially the same” as either the 2016 Broadband Privacy Order as a whole, or the breach notification provision contained within that order. The challenged order differs in overall coverage and approach, and includes substantial changes from the disapproved rule including a redefinition of the key regulatory term “breach.”

ARGUMENT

I. SECTION 201(b) OF THE COMMUNICATIONS ACT AUTHORIZES THE COMMISSION TO PROTECT TELECOMMUNICATIONS CUSTOMERS’ PERSONALLY IDENTIFIABLE INFORMATION

A. The Commission Engaged In Reasoned Decisionmaking Within Section 201(b)’s Boundaries

1. Section 201(b) provides that “[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation

that is unjust or unreasonable is declared to be unlawful.” 47 U.S.C. § 201(b). Congress further empowered the Commission to “prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of” the Communications Act. *Id.*

In using broad terms to delineate the scope of the agency’s regulatory authority—directing the Commission to do what is “necessary” in the “public interest” to ensure that carriers’ “practices” “for and in connection with” communications services are “reasonable”—Congress gave the agency substantial regulatory discretion. *See Loper Bright*, 144 S. Ct. at 2263–64.

The Commission’s decision to require carriers to protect customers’ personally identifiable information falls within Congress’s delegation of authority to the agency. Section 201(b)’s reference to “practices” has long been understood to authorize the Commission to “insist upon certain carrier practices, while . . . prohibiting others as unjust or unreasonable.” *Glob. Crossing Telecomms., Inc. v. Metrophones Telecomms., Inc.*, 550 U.S. 45, 53 (2007).

Because unsafe or inadequate data security practices that result in the disclosure of personally identifiable information can be “unjust and unreasonable” “practices” “in connection with” the provision of

communications services, Section 201(b) authorizes the Commission to prescribe breach notification rules aimed at addressing that harm. As the Commission explained, “any information collected from a customer or prospective customer related to establishing or maintaining the provision of a communications service” is “in connection with” communications services because it relates to those services. A62 (Order ¶125).

Likewise, poor data security manifestly can be “unjust and unreasonable.” 47 U.S.C. § 201(b). In one example cited by the Commission, two telecommunications companies collected the names, addresses, Social Security numbers, and driver’s licenses of their customers, and then stored them in “publicly accessible folders on the Internet without password protection or encryption” despite “representing to consumers in the Companies’ privacy policies that they employed appropriate technologies to protect consumers’ [personal information].” *TerraCom*, 29 FCC Rcd at 13325, ¶¶1–2. Such a complete failure to protect customer information violates Section 201(b), and the Commission reasonably interpreted its authority to address such failures in the challenged order. A61–63 (Order ¶¶124–125).

2. The Commission’s reliance on Section 201(b) in regulating telecommunications customer data security is nothing new. As early as 1970, the Commission recognized its “fixed and continuing responsibility with respect to the privacy and integrity of intelligence traversing the communications networks of this country,” and cited its authority under 201(b) as part of the basis for rules governing the provision of data processing services by common carriers. *See Regulatory & Policy Problems Presented by the Interdependence of Computer & Communication Services & Facilities*, 28 FCC.2d 291, 295, 300 (1970), *aff’d in part sub nom. GTE Serv. Corp. v. FCC*, 474 F.2d 724 (2d Cir. 1973); *see also Re Second Computer Inquiry*, 77 FCC.2d 384, 440, 499 (1980) (discussing “broad consumer rights under Section 201(b) and 202(a) of the Act” and adopting rules that, among other things, prohibited certain common carriers from disclosing “any customer proprietary information unless such information is available to any member of the public on the same terms and conditions”), *aff’d sub nom. Computer and Communications Industry Ass’n v. FCC*, 693 F.2d 198 (D.C. Cir. 1982).

The Commission continued to rely on its 201(b) authority in this area even after Congress enacted more specific data security measures in Section 222. In the 1998 CPNI Order, for example, the Commission

made clear that “section 201(b) remains fully applicable where it is demonstrated that carrier behavior is unreasonable and anticompetitive.” 13 FCC Rcd at 8126, ¶85 & n.316. What is more, the Commission has specifically relied on 201(b) in the context of data breaches of sensitive personal information of telecommunications customers that is not CPNI. A decade ago, in *TerraCom*, 29 FCC Rcd 13325, the Commission found two companies’ data security practices likely violated 201(b) because they “failed to employ even the most basic and readily available technologies and security features for protecting consumers” personal information. *Id.* at 13336, ¶32. While *TerraCom* was a notice of apparent liability, not a rulemaking, its understanding of 201(b) has been reflected in multiple Commission orders since. *See, e.g., Lifeline & Link Up Reform & Modernization*, 30 FCC Rcd 7818, 7846, 7896 ¶¶65, 235 & n.168 (2015) (“confirm[ing] the general interpretation of sections 201 and 222 reflected in the TerraCom NAL”).

B. Statutory Structure And Sound Policy Support The Commission’s Reading

The Communications Act’s relationship to the Federal Trade Commission Act (FTC Act) likewise demonstrates that Congress in

Section 201(b) intended to give the Commission authority to regulate common carriers' protection of personally identifiable information.

In the FTC Act, Congress gave the Federal Trade Commission broad authority to prevent businesses from engaging in “unfair or deceptive” practices, 15 U.S.C. § 45(a), including by implementing inadequate data security and misleading privacy policies. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247 (3d Cir. 2015) (holding that the FTC has statutory authority to regulate data security and privacy practices under § 45(a)). But businesses are exempt from this provision of the FTC Act when they act as telecommunications carriers. *See* 15 U.S.C. § 45(a)(2) (exempting from FTC authority “common carriers subject to the Acts to regulate commerce”); *id.* § 44 (defining “Acts to regulate commerce” as including “the Communications Act of 1934 and all Acts amendatory thereof and supplementary thereto”). Congress designed this scheme to create complementary powers in the FCC and FTC, while “avoid[ing] interagency conflict.” *FTC v. AT&T Mobility LLC*, 883 F.3d 848, 855 (9th Cir. 2018).

As the Commission explained, Section 201(b) ensures that customers of telecommunications carriers do not fall into a regulatory gap in which there is no federal protection against carriers' mishandling

their personally identifiable information that is not CPNI. A64 (Order ¶126). Indeed, if Petitioners prevail, telecommunications carriers would be the only major businesses in the United States that are not subject to federal requirements imposing reasonable data security protections.

C. Petitioners Misread Section 201(b)

1. Petitioners are mistaken in arguing that the statutory phrase “practices . . . in connection with’ a communications service” cannot “encompass a failure to notify the government of data breaches” because the surrounding words “all address carrier conduct that is an inherent or necessary aspect of providing a communications service to customers.” Pet. Br. 37–38.

To start, Petitioners do not dispute that the plain meaning of the term “practices” can encompass data security practices. Instead, they rely on the interpretive canon that “a word is ‘known by the company it keeps,’” Pet. Br. 37, to argue that the term “practices” here should be limited to less than its ordinary meaning. Not so. That interpretive canon cannot “rob” a statutory term “of its independent and ordinary significance.” *Graham Cnty. Soil & Water Conservation Dist. v. U.S. ex rel. Wilson*, 559 U.S. 280, 288 (2010).

In any event, the surrounding statutory terms—“[a]ll charges, . . . classifications, and regulations”—are nearly if not equally as broad as the term “practices.” 47 U.S.C. § 201(b). And Petitioners nowhere explain why the capacious statutory phrase “in connection with”—which simply means “related to,” *see Razete v. United States*, 199 F.2d 44, 49 (6th Cir. 1952)—should instead be read to mean “an inherent or necessary aspect of.” Pet. Br. 37. As explained above, *supra* 22–23, Section 201(b) has long been understood to reach a wide variety of carrier business practices, including practices that would not ordinarily be described as “inherent” to telecommunications. *See* A62 (*Order* n.446). For example, “exclusive contracts with commercial building owners,” *see Glob. Crossing Telecommunications*, 550 U.S. at 54, are not an inherent or necessary aspect of communications services, but nonetheless fall within Section 201(b)’s reference to “practices.”

California Independent System Operator Corp. v. FERC, 372 F.3d 395 (D.C. Cir. 2004), is not to the contrary. Pet. Br. 38. There, the D.C. Circuit concluded that the term “practice” in 16 U.S.C. § 824e(a) did not authorize the Federal Energy Regulatory Commission “to replace the governing board of” a utility, which had been “chosen according to a method dictated by California statute.” 372 F.3d at 396. The

Commission’s application of Section 201(b) has no such far-reaching ambition. It merely reaches carriers’ data collection practices in their ordinary service relationships with their customers. *See* A62 (*Order* n.446).

Even if Petitioners were correct that the phrase “practices . . . in connection with . . . communication service” should be read to mean “carrier conduct that is an inherent or necessary aspect of providing a communications service to customers,” Pet. Br. 37–38, that meaning would still cover the challenged rule. As the Commission found, communications services are a “ubiquitous feature of modern life” in which providers “often collect large quantities of sensitive customer data.” A2 (*Order* ¶1). That sensitive information is not strictly limited to network data—for example, telecommunications carriers routinely collect identifying information and financial data for billing purposes. For these reasons, collecting and protecting customer information is, in fact, “an inherent or necessary aspect of providing a communications service to customers.” Pet. Br. 37–38. Thus, even under Petitioners’ reading, the Commission would have acted within its authority under Section 201(b).

2. Petitioners are likewise mistaken that “the specific protections Congress established in Section 222 supersede the general provisions of Section 201.” Pet. Br. 34–35 (citing *RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 566 U.S. 639, 645 (2012)). They point to nothing in Section 222’s text or history that suggests Congress intended to restrict, rather than augment, the Commission’s existing authority over telecommunications customer privacy in enacting that provision.

The specific-general canon of statutory construction may apply where necessary to avoid “the superfluity of a specific provision [from being] swallowed by the general one.” *RadLAX*, 566 U.S. at 645. While the Commission’s powers under Section 201(b) are broad enough to encompass rules governing customer proprietary information, *see supra* 21–27, it does not “swallow” the particular concerns Congress chose to address in Section 222. The former provision authorizes the Commission to regulate business practices—including data collection—that are unjust or unreasonable, while the latter authorizes the Commission to protect telecommunications customers’ proprietary data regardless of whether they are unjust or unreasonable. The fact that one statute may “[o]verlap with other federal statutes does not render [it] superfluous.” *Skilling v. United States*, 561 U.S. 358, 413 n.45 (2010).

In arguing otherwise, Petitioners exclusively rely on a vague statement from the legislative history that Section 222 balanced “competing, often conflicting considerations.” Pet. Br. 35 (citing H.R. Rep. No. 104-204, at 90, H.R. Rep. No. 104-458, at 205). But the same is true of virtually any statutory provision.

This Court should decline to infer inter-statutory conflict from such thin evidence. “It is [a] [c]ourt’s duty to interpret Congress’s statutes as a harmonious whole rather than at war with one another.” *Epic Sys. Corp. v. Lewis*, 584 U.S. 497, 502 (2018). Because there is no necessary conflict between the two provisions, Petitioners are mistaken in reading Section 222 as silently overriding the Commission’s 201(b) authority.

3. Petitioners are also wrong that Section 222’s lack of a savings clause “confirms that Section 222 fully displaces Section 201 with respect to consumer privacy.” Pet. Br. 35–36. In adopting the 1996 amendments to the Communications Act—including Section 222—Congress expressly disavowed such an implied effect, providing that “the amendments made by this Act shall not be construed to modify, impair, or supersede Federal, State, or local law unless expressly so provided in such Act or amendments.” Telecommunications Act of 1996, Pub. L. 104-104, 110 Stat. 56, § 601(c)(1) (1996) (codified at 47 U.S.C. § 152 note). Petitioners

point to no such “express[]” command in Section 222. Instead, Petitioners seek to draw a negative inference from the absence in Section 222 of additional savings language because Congress chose to include such clauses in other, unrelated, provisions. Pet. Br. 36 (citing 47 U.S.C. §§ 251 & 252).

But the other savings clauses Petitioners point to in the Communications Act would be unnecessary in Section 222, which, again, does not conflict with 201(b). Section 252 contains savings clauses preserving state authority, not the Commission’s own powers. See 47 U.S.C. § 252(e)(3), (f)(2); *Qwest Corp. v. Ariz. Corp. Comm’n*, 567 F.3d 1109, 1117 (9th Cir. 2009). And “[w]hile it is not entirely clear why Congress felt the need for an additional savings clause in section 251(i),” the Commission observed, “it might simply have done so ‘to be doubly sure,’ particularly given the responsibilities assigned to the states in the implementation of sections 251 and 252.” A62–63 (Order n.449). It is hardly uncommon for Congress to take a belt-and-suspenders approach to statutory drafting, and the absence of a savings clause in 222 is, at most, inconclusive.

4. Contrary to Petitioners’ suggestion, the Commission has not “recently purported to ‘discover’ in Section 201(b) a significant power to

regulate consumer privacy.” Pet. Br. 36–37. As explained above, *supra* 24–25, the Commission has long relied on its Section 201(b) powers in this area.

Petitioners locate a single Commission statement from 1999 that they assert aligns with their view that Section 222 superseded privacy protections under Section 201(b). Pet. Br. 36–37 (citing *Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, 14 FCC Rcd 14409, 14491 ¶153 (1999)). But, as the Commission explained, A63 (Order n.451), that statement must be understood in context. In the 1999 order, the Commission was clarifying that “where consumer privacy issues addressed specifically in section 222 are implicated, the requirements of section 222 are controlling over more general protections in section 201(b) and 202(a) that are unrelated to privacy—such as advancing competitive neutrality.” *See id.*; 14 FCC Rcd at 14491 ¶153. In other words, the Commission was saying that carriers could not leverage competition rules to defeat privacy protections, not that Section 222 displaced all other privacy authority under Section 201. In any event, that single regulatory statement is hardly compelling evidence that the Commission, let alone Congress, understood Section 222 to supersede Section 201(b).

II. PERSONALLY IDENTIFIABLE INFORMATION IS CONSUMER “[P]ROPRIETARY [I]NFORMATION” UNDER SECTION 222(a)

Apart from Section 201(b), Section 222 also provides independent authority for the Commission’s data breach requirements.

A. The Ordinary Meaning of Section 222(a) Supports the Commission’s Reading

Section 222(a) provides that “[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, . . . customers.” 47 U.S.C. § 222(a). In conjunction with the Commission’s rulemaking powers to carry out the provisions of the Communications Act, this subsection authorizes the Commission to oversee how carriers protect customers’ personally identifiable information.

When interpreting a statutory term, this Court “give[s] it the ‘ordinary meaning,’” guided if necessary by dictionary definitions. *United States v. Small*, 988 F.3d 241, 254 (6th Cir. 2021). PII—information that alone or in aggregate identifies individual customers, A9–10 (Order ¶17)—is “proprietary information of, and relating to, . . . customers” subject to section 222(a) because, by ordinary meaning, it is obtained by a business through a service relationship with its customers.

The term “proprietary” is commonly understood to mean “belonging or pertaining to a proprietor.” *Black’s Law Dictionary* 1219 (6th ed. 1990). Because a telecommunications carrier acquires the information that identifies their customers “by virtue of its service relationship with them,” A62 (Order n.446), it is “proprietary information of, and relating to” those customers, and telecommunications carriers are obligated to protect it.

Indeed, Congress recognized this ordinary meaning of “proprietary” in its statutory definition of the narrower term CPNI, which is a subset of customer proprietary information. In Section 222(h), Congress made clear that certain network information is “proprietary”—and thus covered by the statute—because it “is made available to the carrier by the customer solely by virtue of the carrier-customer relationship.” 47 U.S.C. § 222(h)(1). Unlike 222(c), however, 222(a) is not limited to “network” information, and extends to all “proprietary information of, and relating to, . . . customers.”

This straightforward interpretation of Section 222(a) is confirmed by well-established canons of interpretation. It is axiomatic that “the same words in the same statute mean the same thing.” *In re Jackson Masonry, LLC*, 906 F.3d 494, 501 (6th Cir. 2018). An important corollary

of this principle is that “a material variation in terms suggests a variation in meaning.” See Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* § 25 (2012). For example, in *U.S. Telecom Association v. FCC*, 825 F.3d 674 (D.C. Cir. 2016), the D.C. Circuit interpreted the statutory phrase “public switched network” to reach “beyond telephone networks alone” because Congress used the narrower term “public switched telephone network” elsewhere in the statute. *Id.* at 717–18.

Applying these commonsense rules here, Section 222(a)’s reference to “proprietary information of, and relating to, . . . customers” must mean something beyond just CPNI, a precise term defined elsewhere in the statute. See 47 U.S.C. § 222(c), (h)(1). If Congress had meant to protect only customer proprietary network information in Section 222(a), it would have used that term or, at very least, used the word “network.” It did not. The broader language of 222(a) thus “suggests a variation in meaning,” Scalia & Garner, *Reading Law*, § 25, that the Commission correctly interpreted as extending to personally identifiable information, not only CPNI. A58–59 (Order ¶120).

Section 222(a)’s independent meaning is likewise confirmed by another interpretive canon: the rule against surplusage. That “familiar

rule” provides “that courts should ‘give effect, if possible, to every word Congress used.’” *In re Davis*, 960 F.3d 346, 354–55 (6th Cir. 2020). Interpreting Section 222(a)’s reference to “proprietary information of, and relating to, other telecommunication carriers, *equipment manufacturers*, and customers” (emphasis added) as only to CPNI would violate this rule. After all, the term “equipment manufacturers” appears nowhere else in the statute, and declining to read 222(a) as offering broader protections than 222(c) with respect to customers would effectively read “equipment manufacturers” out of the statute. A59–60 (Order ¶¶120). Indeed, if Section 222(a) merely encompassed CPNI, it is unclear what effect Section 222(a) would have at all.

B. Petitioners Misread Section 222

Petitioners’ limitation of Section 222 to CPNI alone is unsound.

1. Petitioners first err by arguing that Section 222(a) has no independent significance other than to introduce the more specific provisions that follow—a sort of statutory master of ceremonies. Pet. Br. 25–26.

Had Congress in 222(a) wished only to state its purposes in enacting the rest of Section 222, it would have said so. Congress has enacted such hortatory “purpose” statements in several provisions of the

Communications Act. *See, e.g.*, 47 U.S.C. §§ 228(a), 256(a), 394(a), 395(a), 532(a), 548(a), 614(a). These provisions all follow a familiar pattern: they use the word “purpose,” not the phrase “in general,” nor do they expressly impose a legal “duty” as does Section 222(a). *Id.*; *see* A59 (Order ¶120). Meanwhile, statutes that introduce a specific legal obligation with the phrase “in general” include 47 U.S.C. §§ 343(a) (prohibiting commercial terrestrial operations in a particular spectrum band); 1411(a) (reallocating spectrum for public safety entities); 1428(a) (authorizing certain fees); 1602(a) (prohibiting certain uses of federal subsidies). Courts read such “general” obligation provisions as creating binding legal duties, not as merely announcing a statutory purpose. *Accord Chicago & N. W. Ry. Co. v. United Transp. Union*, 402 U.S. 570, 575–76 (1971) (holding that provision of the Railway Labor Act imposing “General duties” is not “merely hortatory”).

2. Petitioners also misread the phrase “proprietary information.” Relying on a dictionary definition, they argue that this term refers to ownership in a “protectable interest.” Pet. Br. 24. But Petitioners fail to ground this meaning in Section 222. For example, they do not explain how anyone owns a protectable interest in the customer network

information described in 222(h), as opposed to merely acquiring it through the carrier-customer relationship as Congress specified.

Next—in reliance on a 2021 definition from “inc.com”—Petitioners claim that “proprietary information” necessarily means non-public information. Pet. Br. 24–25. But “proprietary” is not exclusively understood to mean non-public. For example, a patent may be “proprietary” in the sense that it “is used, produced, or marketed under exclusive legal right of the inventor or maker,” even though a patent is necessarily public. See “Proprietary,” Merriam Webster Online (using “patent” as an example of something that is “proprietary”).⁴

Retail Ventures, Inc. v. National Union Fire Insurance Co. of Pittsburgh, Pa., 691 F.3d 821 (6th Cir. 2012), Pet. Br. 31–32, is not to the contrary. That decision upheld a district court’s determination that “customer credit card and checking account information” was not “proprietary information” in the context of an insurance policy exclusion from liability. 691 F.3d at 833. But unlike Section 222(a), the policy in *Retail Ventures* had no language tying “proprietary information” to customer data.

⁴ <https://www.merriam-webster.com/dictionary/proprietary>.

Petitioners’ argument that “proprietary information” means non-public is further confused by its position that customer “proprietary information” has no independent meaning in 222(a) at all, and simply refers to “consumer proprietary network information” as described in 222(c) and defined in 222(h). Pet. Br. 25–26. Again, such an interpretation violates bedrock interpretative principles, *see supra* 35–37, and is also inconsistent with Petitioners’ own argument that proprietary means non-public. Neither 222(c) nor 222(h) gives any indication that consumer proprietary network information is so limited. To the contrary, 222(c) contemplates that some CPNI may be used in “publishing of directories.” *See* 47 U.S.C. § 222(c)(1). Because “proprietary” in Section 222 refers to information obtained through a communications service relationship, and makes no reference to its non-public character, it is irrelevant that “customers routinely disclose [names and addresses] to third parties.” Pet. Br. 26.

Petitioners are likewise mistaken that “Section 222(a) requires the ‘proprietary information of customers’ to be proprietary to customers.” Pet. Br. 32. As the text of the statute makes clear, protected information can be “of . . . customers”—i.e., belonging to them—or “relating to . . . customers”—i.e., information belonging to carriers that has a connection

to customers. 47 U.S.C. § 222(a). It is “proprietary”—and thus covered by the statute—because it is “obtained in connection with establishing or maintaining a communications service.” A59 (Order ¶120). Far from “sidestep[ping]” the plain meaning of the statute, Pet. Br. 32, that interpretation accounts for both the ordinary meaning of the term “proprietary” and Congress’s understanding of that term reflected in 222(h)(1). *See supra* 34–37. Petitioners’ interpretation does not. Indeed, it would make little sense to say, for example, that customers own a protectable interest in the “technical configuration” of their telecommunications service. 47 U.S.C. § 222(h)(1).

3. The fact that other statutory provisions refer to PII with different language, Pet. Br. 26–28, does not compel the conclusion that Section 222 cannot be read to reach the same result without using the exact phrase “personally identifiable information.” Petitioners argue that “[w]hen Congress sought to regulate a broad class of PII . . . it did so explicitly.” *Id.* But as the statutes Petitioners cite illustrate, legislatures refer to personally identifiable information in a variety of ways. *See, e.g.*, 15 U.S.C. § 6501(8) (“personal information”); *id.* § 6809(4) (“nonpublic personal information”); Ala. Code § 8-38-2(6) (“sensitive personally identifying information”). The fact that Congress chose to use the phrase

“proprietary information of, and relating to . . . customers” in 222(a) thus does not compel Petitioners’ interpretation that Section 222(a) does not cover PII.

4. Petitioners are also mistaken that the Commission understood Section 222 as strictly limited to CPNI in prior orders. Pet. Br. 28–30. In the 1998 CPNI Order’s discussion of legal authority, the Commission made clear that it understood that provision to govern “disclosure of CPNI *and other customer information.*” 13 FCC Rcd 8073 ¶14 (emphasis added). That order’s introductory discussion of “three categories of customer information” in Section 222, Pet. Br. 29, is not reasonably interpreted as a comprehensive statement on the Commission’s understanding of its authority under the statute.

The other orders on which Petitioners rely, Pet. Br. 30, also do not support their position. For example, the Commission’s statement in the 2007 Notification Rule that “[e]very telecommunications carrier has a general duty pursuant to section 222(a) to protect the confidentiality of CPNI” (22 FCC Rcd at 6931) is in no way inconsistent with the challenged order’s interpretation of 222(a) because, as the Commission explained, “CPNI is a subset of PII.” A10 (Order ¶17).

At most, the regulatory language Petitioners cite indicates that the Commission proceeded incrementally in implementing Section 222, beginning with CPNI before implementing broader PII rules. The Commission has contemplated that Section 222' could cover "other customer information" from the beginning, 1998 CPNI Order, 13 FCC Rcd at 8073 ¶14, and has specifically applied 222's protections to non-CPNI for at least a decade, *see TerraCom*, 29 FCC Rcd 13325.

5. Nor does the Commission's interpretation of Section 222(a) "create[] implausible anomalies" elsewhere in the statute. Pet. Br. 32. Reading 222(a) to impose a broad duty to protect customer information (as its text commands) is not inconsistent with the exceptions laid out in 222(d). "[I]t is understandable the Congress made a point of establishing express exceptions" in 222(d) directed at "the more detailed statutory specification of carriers' requirements regarding CPNI" in 222(c). A60 (Order ¶122). But this does not mean that the same exceptions cannot apply to carriers' obligations under 222(a). Indeed, the Commission expressly disavowed the "anomalous" reading Petitioners insist it created. *See* A60 (Order ¶122 ("[W]e do not interpret the grounds for disclosure authorized by section 222(d) as violating carriers' obligation to protect the confidentiality of proprietary information imposed by section

222(a).”). Petitioners are thus mistaken that “Section 222(d) exceptions apply only to CPNI.” Pet. Br. 33.

The same reasoning applies to the exceptions Petitioners point to in 222(e) and 222(g). Again, the Commission harmonized these provisions with 222(a), declining to “interpret section 222(a) to impose obligations inconsistent with those disclosure requirements, either.” A60–61 (Order ¶122).

III. THE COMMISSION’S BREACH NOTIFICATION RULES FOR TELECOMMUNICATIONS RELAY SERVICE PROVIDERS ARE AUTHORIZED UNDER SECTION 225 AND THE COMMISSION’S ANCILLARY AUTHORITY

Section 225 provides “ample legal authority” for the Commission to prescribe breach notification rules for telecommunications relay service providers. A66 (Order ¶132).

As the Commission explained, A65–66 (Order ¶¶130–132), that provision not only authorizes but obligates the Commission to ensure that relay services are functionally equivalent to telephone voice services for consumers without hearing or speech impairments, and to establish “functional requirements, guidelines, and operations procedures” for relay services providers in pursuit of that goal. *See id.* The plain text of

the statute authorizes the challenged rules here as they apply to relay service providers.

The Commission’s privacy rules are necessary to ensure that relay services offer the same sort of protections that voice services offer to customers that are not hearing or speech impaired. Relay services without similar privacy protections that apply to voice services would not be “functionally equivalent” to those voice services. Indeed, the Commission has protected relay service customer information since well before its 2013 order applying CPNI protections to relay service users. *See* 2013 Relay Service Order, 28 FCC Rcd at 8680–81, ¶¶158–159. Just like previous protections, the breach notification rules here are a “functional requirement[], guideline, [or] operating procedure” that advances Section 225’s functional equivalency requirement. 47 U.S.C. § 225. As even Intervenor Hamilton Relay Inc. acknowledged before the Commission, Section 225 “provides sufficient authority to impose CPNI data breach notification obligations on [relay service] providers.” Hamilton Relay Comments at 9 (Feb. 22, 2023), available at <https://www.fcc.gov/ecfs/document/10222802816908/1>. Extending the same protections to other personally identifiable information when the Commission has done so for consumers that are not hearing or speech

impaired is thus well within the bounds of the Commission’s authority under Section 225.

Subjecting relay service providers to privacy regulations—including data breach rules covering personally identifiable information—also falls within the Commission’s ancillary authority under Sections 222 and 225. *See* A66 (Order ¶131); 2013 Relay Service Order, 28 FCC Rcd at 8685, ¶170–171. The Commission’s ancillary authority derives from 47 U.S.C. § 154(i), which empowers the Commission to “perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions.” *Id.*

Intervenor does not contest the Commission’s conclusion that its privacy rules for relay service providers are reasonably ancillary to section 225. And with respect to authority ancillary to section 222, because ordinary telecommunications service subscribers place and receive calls from relay service users, and relay service “call records include call detail information concerning all calling and called parties,” A66 (Order ¶131), the same reasons that support the Commission’s statutory authority over regular telecommunications services, *supra* 21–43, also extend to relay service providers.

Intervenor’s argument that Section 222 is “limited to regulating the practices of telecommunications carriers, not protections for subscribers,” Intervenor’s Br. 24, cannot be squared with the plain text of the statute. The whole point of regulating telecommunications carriers’ practices is to protect their subscribers. That is why Section 222(a) unambiguously protects “proprietary information of, and relating to . . . customers.” 47 U.S.C. § 222(a). The Commission’s relay service privacy rules thus fall well within the scope of its ancillary authority under that provision.

IV. THE COMMISSION’S DATA BREACH REPORTING RULES ARE CONSISTENT WITH THE CONGRESSIONAL REVIEW ACT

The challenged breach notification rules are also consistent with the Congressional Review Act and Congress’s 2017 disapproval resolution. The CRA prohibits the Commission from reissuing “substantially the same” rule as the 2016 Broadband Privacy Order, not simply a similar or partially overlapping rule. And the challenged rule differs significantly from the previously disapproved order.

A. The Congressional Review Act’s Disapproval Bar Is Limited To “Substantially The Same” Rule

1. The CRA and Congress’s disapproval resolution apply only to the 2016 order as a whole

a. The CRA’s disapproval bar applies to two kinds of rule: (1) a disapproved “rule . . . reissued in substantially the same form” and (2) “a new rule that is substantially the same as such a rule.” 5 U.S.C. § 801(b)(2). “Substantially” means “[e]ssentially; without material qualification,” or “in substance.” Black’s Law Dictionary, *supra*, 1340. The word “same” means “[i]dentical, equal” or “equivalent.” Black’s Law Dictionary, *supra*, 1428–29. Thus, the CRA bars an agency from reissuing a rule that is substantively identical to a disapproved rule, not merely one that shares some characteristics or policies. A rule that only partly overlaps with a disapproved rule is not “substantially the same.”

That commonsense interpretation is further confirmed by the text of the 2017 disapproval resolution, which applies to “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)).” Joint Resolution, Pub. L. No. 115-22, 131 Stat. 88 (2017). As the Commission explained, that language “referred to the 2016 Privacy Order in its entirety.” A67

(Order ¶136). Notably, both the CRA and the 2017 disapproval resolution refer to a single “rule,” not “rules,” and not to each of its constituent parts individually, further confirming that Congress disapproved of the 2016 Broadband Privacy Order in toto.

This reading of the CRA is consistent with the only court of appeals decision to consider the scope of congressional disapproval under the CRA.⁵ In *Safari Club Int’l v. Haaland*, the Ninth Circuit concluded that a Department of Interior rule prohibiting baiting brown bears in Alaska’s Kenai National Wildlife Refuge was not barred by Congress’s disapproval of a broader rule banning brown bear baiting in all national wildlife refuges in Alaska, including Kenai. 31 F.4th 1157, 1169–70 (9th Cir. 2022), *cert. denied sub nom. Alaska v. Haaland*, 143 S. Ct. 1002 (2023). As the Court explained, Congress’s disapproval resolution concerned only “the Refuges Rule or a new administrative rule that is substantively

⁵ Legal scholars have reached similar conclusions. See Michael J. Cole, *Interpreting the Congressional Review Act: Why the Courts Should Assert Judicial Review, Narrowly Construe “Substantially the Same,” and Decline to Defer to Agencies Under Chevron*, 70 Admin. L. Rev. 53, 83–94 (2018); Adam M. Finkel & Jason W. Sullivan, *A Cost-Benefit Interpretation of the “Substantially Similar” Hurdle in the Congressional Review Act: Can OSHA Ever Utter the E-Word (Ergonomics) Again?*, 63 Admin. L. Rev. 707, 740–41 (2011).

identical,” and thus did not bar the narrower Kenai rule, which “only forbids baiting of brown bears in the Kenai Refuge.” *Id.* While the circumstances in *Safari Club* were not identical to those here—the narrower Kenai Rule predated rather than followed congressional disapproval—the Court’s sound reasoning applies with equal force. A rule that contains some but not all of the same measures as a disapproved rule is not “substantively identical” within the meaning of the CRA. *Id.*

b. The Commission’s interpretation of the CRA is likewise supported by the legislative history of the disapproval resolution, which demonstrates that the Commission’s breach notification rules did not animate Congress’s disapproval.⁶ Indeed, breach notification rules are barely mentioned in that history. Instead, congressional debate focused on regulation of broadband internet service providers and the potential for duplicative jurisdiction with the Federal Trade Commission. *See, e.g., Providing for Congressional Disapproval of a Rule Submitted by the*

⁶ The legislative history is at *Providing for Congressional Disapproval of a Rule Submitted by the Federal Communications Commission*, 163 Cong. Rec. S1925-55 (daily ed. Mar. 22, 2017); *Providing for Congressional Disapproval of a Rule Submitted by the Federal Communications Commission*, 163 Cong. Rec. H2478-86 (daily ed. Mar. 28, 2017).

Federal Communications Commission, 163 Cong. Rec. H2489, H2489 (2017) (statement of Rep. Blackburn) (arguing that “having two privacy cops on the beat will create confusion within the internet ecosystem and will end up harming consumers”).

In the few places where breach notification was mentioned, it was only in the context of broadband Internet service providers. *See* 163 Cong. Rec. H2479 (daily ed. Mar. 28, 2017) (statement of Rep. Burgess) (referencing the 2016 data breach consumer notice requirements in the context of “treat[ing] internet service providers differently from the rest of the internet”). And even then, Congress made no mention of Petitioners’ central objection here—applying breach notification rules to personally identifiable information.

c. Sound policy reasons likewise counsel in favor of the Commission’s conclusion that congressional disapproval under the CRA prohibits reissuance of substantially the same rule as a whole, not merely a similar or overlapping rule.

To start, an overbroad interpretation of the disapproval bar would prevent agencies from making small but significant changes to address Congress’s objections. As Professors Finkel and Sullivan point out, “it would be bizarre to constrain the agency from attempting to satisfy

congressional concerns by fundamentally changing the substance and import of a vetoed rule merely because doing so might affect only a small fraction of the individual words in the regulatory text.” Finkel & Sullivan, *supra*, 63 Admin. L. Rev. at 735–36.

At the same time, an overbroad disapproval bar would permanently prohibit policies Congress did not oppose. Even where Congress disapproves of a rule overall, it may still approve of some of its constituent parts. “Since the CRA strikes down an entire rule even though Congress may support certain portions of that rule, it only makes sense to read the substantial similarity provision as allowing the nonoffending provisions to be incorporated into a future rule.” Finkel & Sullivan, *supra*, 63 Admin. L. Rev. at 750–51. A contrary interpretation would be not just “draconian” but “nonsensical.” *Id.*

2. Petitioners’ interpretation of the CRA is mistaken

Petitioners read the Congressional Review Act’s disapproval bar as permanently removing the Commission’s authority to make any “statement[] of general ... applicability and future effect designed to ... prescribe law or policy” that is “contained within” a disapproved order. Pet. Br. 40. That reading is mistaken.

To start, Petitioners disregard Congress’s choice—in both the CRA and the 2017 disapproval resolution—to refer to disapproving a single “rule,” not multiple “rules.” *See supra* 47–50; 5 U.S.C. § 801(b) (repeatedly referring to “a rule”); Joint Resolution, Pub. L. No. 115-22, 131 Stat. 88 (2017) (referring to “the rule” and identifying the 2016 Broadband Privacy Order). Congress could have easily specified in the CRA that a disapproval resolution precludes readopting all constituent portions of a rule, but it did not.

Petitioners attempt to evade the this straightforward reading by arguing that “Section 801(b)(2)’s reference to ‘such a rule’ does not refer to the ‘rule specified in the joint resolution of disapproval,’” and instead refers to the statutory phrase “[a] rule that does not take effect (or does not continue) under paragraph (1).” Pet. Br. 50. That is a distinction without a difference. “Paragraph (1)” means 5 U.S.C. § 801(b)(1), which reads: “A rule shall not take effect (or continue), if the Congress enacts *a joint resolution of disapproval*, described under section 802, *of the rule*.” (Emphases added.) Here, “the rule” that was subject to “a joint resolution of disapproval” is, of course, “the ‘rule specified in the joint resolution of disapproval’”—specifically, “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)).” Joint Resolution, Pub. L. No. 115-22, 131 Stat. 88 (2017). Because that single “rule” is the 2016 Broadband Privacy Order in its entirety, not some unnamed constituent part, Petitioners’ interpretation is incorrect.

The statutory definition of the term “rule” does not compel a contrary result. Pet. Br. 51. The CRA incorporates the APA’s definition of “rule”—“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.” 5 U.S.C. § 551(4), as referenced in 804(3). As the Commission acknowledged, A68 (Order ¶136), that definition can be read in the abstract to “refer to parts of such a [disapproved] decision, or to various requirements as adopted or amended by such a decision.” But the Commission rightly chose not to read it that way because the 2017 disapproval resolution rejected the 2016 Broadband Privacy Order as a whole.

Moreover, Petitioners’ reading will produce demonstrably bad results. As explained above, *supra* 51–52, disregarding constituent policies that Congress did not consider (or even actively supported) would

be “draconian” and “nonsensical.” And under Petitioners’ reading, any formal legal definition adopted in the course of a disapproved order—undoubtedly a “statement[] of general . . . applicability and future effect designed to . . . prescribe law”—would be permanently prohibited. *See* Pet. Br. 41 (arguing that the challenged order’s “definitional changes” are prohibited rules). For example, under such a reading the Commission would be barred—forever—from defining a “customer” as “a current or former subscriber to a telecommunications service” or “applicant for a telecommunications service.” 2016 Broadband Privacy Order, 31 FCC Rcd at 13925–26. Even the Commission’s routine application of the Paperwork Reduction Act, *id.* at 14077–78, would be prohibited under Petitioners’ logic because it is “part of an agency statement . . . describing the organization, procedure, or practice requirements of an agency” contained within a disapproved rule. 5 U.S.C. § 551(4). Such absurd results cannot be what Congress intended. *United States v. Fitzgerald*, 906 F.3d 437, 447 (6th Cir. 2018).

Nor would the Commission’s interpretation of the CRA allow an agency to “continu[e] to enforce some . . . individual constituent” disapproved rules or make Congress’s disapproval power “easy to circumvent.” Pet. Br. 52–55. As all parties agree, congressional

disapproval renders a rule “of no force or effect.” 5 U.S.C. § 801(f); A66–67 (Order ¶133); Pet. Br. 52–53. The Commission, however, nowhere suggested it could choose to enforce some parts of a disapproved rule without further rulemaking. Nor did the agency claim or suggest that it could simply reissue every identical part of a disapproved rule separately. *Contra* Pet. Br. 54. The Commission merely concluded that the CRA does not prevent it from reissuing a similar or overlapping *portion* of a disapproved rule through appropriate rulemaking. A67 (Order ¶135).

Petitioners are mistaken that Congress “could not have more specifically disapproved each component rule of the Broadband Privacy Order” under the CRA’s prescribed procedures. Pet. Br. 53. Nothing in that law prohibits Congress from specifying some subpart of an agency rule in a disapproval resolution. Here, for example, Congress could have provided that “Congress disapproves the rule submitted by the Federal Communications Commission relating to Breach Notification Requirements in ‘Protecting the Privacy of Customers of Broadband and Other Telecommunications Services’ (81 Fed. Reg. 87274 (December 2, 2016)), as codified at 47 C.F.R. § 64.2006, and such rule shall have no force or effect.” It did not. And, of course, Congress could always nullify

an agency's new rule through another CRA disapproval resolution, or otherwise amend the agency's statutory authority. A68 (Order n.485).

Center for Biological Diversity, 946 F.3d 553 (9th Cir. 2019), Pet. Br. 54, does not support Petitioners' interpretation. There, the Ninth Circuit upheld the constitutionality of Congress's disapproval of the Interior Department's Refuges Rule, concluding that the disapproval resolution "validly amended" the Interior Department's statutory authority, 946 F.3d at 562. But the question here is not about the constitutional validity of congressional disapproval, but rather its scope. *Center for Biological Diversity* did not purport to interpret the scope of congressional disapproval under the CRA, *see id.* at 563–64, and the only court of appeals decision to do so supports the Commission's interpretation, not Petitioners'. *See supra* 48–50; *Safari Club Int'l*, 31 F.4th 1157.

B. The Challenged Order Is Not “Substantially The Same” As The 2016 Broadband Privacy Order

1. Comparing the challenged rules with the 2016 Broadband Privacy Order as a whole reveals significant differences in focus. As the Commission explained—and as the legislative history discussed above illustrates, *supra* 50–51—the 2016 order “focused in large part on

adopting privacy rules for broadband Internet access service.” A70 (Order ¶141). Here, by contrast, the challenged order does not apply to broadband providers at all. And while the Commission has subsequently determined that broadband providers should be classified as telecommunications carriers, it has waived the data breach notification rules to the extent they might have been applicable. *See* 2024 Open Internet Order, at *138 ¶359. Finally, unlike the 2016 order, the challenged order extends the data breach notification rules to an entirely different category of regulated entity: telecommunications relay service providers. *See* A39–57 (Order ¶¶65–116).

The 2016 Broadband Privacy Order was also much broader in scope than just breach notification rules. Among other things, that order “required carriers to disclose their privacy practices, revised the framework for customer choice regarding carriers’ access, use, and disclosure of the customers’ information, and imposed data security requirements in addition to data breach notification requirements.” A70 (Order ¶141); 2016 Broadband Privacy Order, 31 FCC Rcd at 13913–16, ¶¶6–18. By contrast, the rules challenged here are targeted to breach notification alone. *See* A2–3 (Order ¶¶3–4). Viewed as a whole, it is thus

“clear that there is at most a small conceptual overlap between” the two orders. A70 (Order ¶141).

Even looking only to the two orders’ particular breach notification rules, there are substantial differences in approach. The customer notification requirement now at issue “is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016.” A70 (Order ¶142). The 2016 order required, among other things, written or electronic notification of a breach, a description of the data exposed, instructions for contacting federal authorities, and guidance on protecting against identify theft. 31 FCC Rcd at 14085, Appx. A, section 64.2006(a). By contrast, the challenged order merely requires “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.” A77 (Order Appx. A, section 64.2011(b)).

The two orders even define the term “breach” differently. Notably, the 2016 data breach notification rules did not include the substantial exception for carriers’ good faith adopted in the challenged order. *See* 31 FCC Rcd at 14080, Appx. A, section 64.2002(c) (defining “breach”). Again,

by contrast the challenged rule excludes from the term “breach” any “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.” A77 (Order Appx. A, section 64.2011(e)(1)).

Other provisions also differ significantly between the two orders. For example, the federal agency notification requirements in the challenged order apply to breaches affecting far fewer customers—500 or more, compared to 5,000 or more in the 2016 Order—and include extensive recordkeeping requirements, which reflect the Commission’s demonstrated need to understand the scope of data breaches. *Compare* 31 FCC Rcd at 14085, Appx. A section 64.2006(b), (c) *with* A76 (Order Appx. A, section 64.2011(a)); A70 (Order ¶142).

2. Petitioners disregard these significant differences between the 2016 and 2024 privacy rules. As Petitioners acknowledge, the Broadband Privacy Order “appl[ied] the Communications Act with respect to a host of different problems,” not just data breach notification. Pet. Br. 40. That alone is enough to conclude that the challenged order is not “substantially the same” as the 2016 Broadband Privacy Order. *See supra* 57–58. If

someone orders a large pizza and receives a single slice, they have not gotten “substantially the same” thing.

But even assuming some version of Petitioners’ extreme interpretation of the CRA’s disapproval bar applied, their argument would still fail. As explained above, *supra* 58–60, significant differences distinguish the 2016 data breach rules from those challenged here: among other things, the order adopts a different definition of “breach,” changing that key term to exclude certain good-faith exposures. *Id.*

Petitioners fail to grapple with these important distinctions. The only difference they address is the content of customer notification, Pet. Br. 56, but they fail to mention that the 2016 Broadband Privacy Order’s breach notification rules, unlike those here, required written or electronic notification and required carriers to provide a description of the compromised data, as well as resources for contacting federal authorities and guarding against identity theft. *See* 31 FCC Rcd at 14085.

The Securities and Exchange Commission rulemaking Petitioners cite reinforces the Commission’s position. Pet. Br. 56–57 (discussing *Disclosure of Payments by Resource Extraction Issuers*, 86 Fed. Reg. 4662 (Jan. 15, 2021)). According to Petitioners, the SEC’s new rule was permissible because it “included a change to a key definitional term” from

the disapproved rule. *Id.* It is hard to imagine a more “key definitional term” in the data breach notification context than the term “breach,” which, again, the Commission redefined here to exclude certain good-faith actions.

To be sure, Petitioners identify similarities between the two orders: both cover personally identifiable information, both require reporting to federal agencies, and both set a 30-day timeline for notifying customers after discovering a breach. Pet. Br. 44. But the CRA does not bar the Commission from issuing a rule with some similarities. It bars “substantially the same” one. 5 U.S.C. § 801(b). Because Petitioners fail to show that the challenged order is “substantively identical” to the 2016 Broadband Privacy Order or its constituent breach notification rules, *Safari Club Int’l*, 31 F.4th at 1169–70, it is not barred by the CRA.⁷

⁷ Only in a footnote, Petitioners argue that the Commission did not provide adequate notice of its interpretation of the CRA. Pet. Br. 48 n.6. “An argument contained only in a footnote does not preserve an issue for [this Court’s] review.” *United States v. Dairy Farmers of Am., Inc.*, 426 F.3d 850, 856 (6th Cir. 2005). Because Petitioners’ notice argument is limited to a single footnote and does not appear in the statement of issues, this Court should not reach it. In any event, Petitioners are mistaken. The APA requires only a “reference to the legal authority under which the rule is proposed” and “either the terms or substance of the proposed rule or a description of the subjects and issues involved.” 5 U.S.C. § 553(b)(2), (3). The Data Breach
(cont’d)

CONCLUSION

The petitions for review should be denied.

Dated: July 29, 2024

Respectfully submitted,

/s/ Adam Sorensen

Jonathan S. Kanter
Assistant Attorney General

P. Michele Ellison
General Counsel

Robert B. Nicholson
Attorneys

Jacob M. Lewis
Deputy General Counsel

U.S. DEPARTMENT OF JUSTICE
ANTITRUST DIVISION
950 Pennsylvania Ave. NW
Washington, DC 20530

Sarah E. Citrin
Deputy Associate General Counsel

*Counsel for Respondent
United States of America*

Adam L. Sorensen
Counsel

FEDERAL COMMUNICATIONS
COMMISSION
45 L Street NE
Washington, DC 20554
(202) 418-1740
fcclitigation@fcc.gov

*Counsel for Respondent Federal
Communications Commission*

Notice specifically sought comment on “the effect and scope of the Congressional disapproval of the 2016 Privacy Order.” A143 (Data Breach Notice ¶52). That was sufficient.

CERTIFICATE OF COMPLIANCE

Certificate of Compliance With Type-Volume Limitation, Typeface Requirements and Type Style Requirements

1. This document complies with the type-volume limit of Fed. R. App. P. 32(a)(7)(B) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f):
 - this document contains 11,820 words, *or*
 - this document uses a monospaced typeface and contains _____ lines of text.

2. This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because:
 - this document has been prepared in a proportionally spaced typeface using Microsoft Word for Office 365 in 14-point Century Schoolbook, *or*
 - this document has been prepared in a monospaced spaced typeface using _____ with _____.

/s/ Adam Sorensen
Adam Sorensen
Counsel for Respondents

STATUTORY ADDENDUM

STATUTORY ADDENDUM CONTENTS

	Page
5 U.S.C. § 551	Add. 2
5 U.S.C. § 801	Add. 3
47 U.S.C. § 201	Add. 7
47 U.S.C. § 222	Add. 8
47 U.S.C. § 225	Add. 13

5 U.S.C. § 551 provides in pertinent part:

(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 provides:

§ 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), and shall in addition include an assessment of the agency's compliance with such requirements of the Administrative Pay-As-You-Go Act of 2023 as may be applicable.

(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.

47 U.S.C. § 201 provides in pertinent part:

(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, unrepeatd, 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 provides:

§ 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.

(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 U.S.C. § 225 provides in pertinent part:

(a) Definitions

As used in this section--

(1) Common carrier or carrier

The term “common carrier” or “carrier” includes any common carrier engaged in interstate communication by wire or radio as defined in section 153 of this title and any common carrier engaged in intrastate communication by wire or radio, notwithstanding sections 152(b) and 221(b) of this title.

(2) TDD

The term “TDD” means a Telecommunications Device for the Deaf, which is a machine that employs graphic communication in the transmission of coded signals through a wire or radio communication system.

(3) Telecommunications relay services

The term “telecommunications relay services” means telephone transmission services that provide the ability for an individual who is deaf, hard of hearing, deaf-blind, or who has a speech disability to engage in communication by wire or radio with one or more individuals, in a manner that is functionally equivalent to the ability of a hearing individual who does not have a speech disability to communicate using voice communication services by wire or radio.

(b) Availability of telecommunications relay services

(1) In general

In order to carry out the purposes established under section 151 of this title, to make available to all individuals in the United States a rapid, efficient nationwide communication service, and to increase the utility of the telephone system of the Nation, the Commission shall ensure that interstate and intrastate telecommunications relay services are available, to the extent possible and in the most efficient manner, to hearing-impaired and speech-impaired individuals in the United States.

(2) Use of general authority and remedies

For the purposes of administering and enforcing the provisions of this section and the regulations prescribed thereunder, the Commission shall have the same authority, power, and functions

with respect to common carriers engaged in intrastate communication as the Commission has in administering and enforcing the provisions of this subchapter with respect to any common carrier engaged in interstate communication. Any violation of this section by any common carrier engaged in intrastate communication shall be subject to the same remedies, penalties, and procedures as are applicable to a violation of this chapter by a common carrier engaged in interstate communication.

(c) Provision of services

Each common carrier providing telephone voice transmission services shall, not later than 3 years after July 26, 1990, provide in compliance with the regulations prescribed under this section, throughout the area in which it offers service, telecommunications relay services, individually, through designees, through a competitively selected vendor, or in concert with other carriers. A common carrier shall be considered to be in compliance with such regulations--

- (1) with respect to intrastate telecommunications relay services in any State that does not have a certified program under subsection (f) and with respect to interstate telecommunications relay services, if such common carrier (or other entity through which the carrier is providing such relay services) is in compliance with the Commission's regulations under subsection (d); or
- (2) with respect to intrastate telecommunications relay services in any State that has a certified program under subsection (f) for such State, if such common carrier (or other entity through which the carrier is providing such relay services) is in compliance with the program certified under subsection (f) for such State.

(d) Regulations

(1) In general

The Commission shall, not later than 1 year after July 26, 1990, prescribe regulations to implement this section, including regulations that--

- (A) establish functional requirements, guidelines, and operations procedures for telecommunications relay services;
- (B) establish minimum standards that shall be met in carrying out subsection (c);

.....