Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	
	)	
Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	CC Docket No. 96-115

ORDER

Adopted: June 26, 2017 **Released: June 29, 2017**

By the Commission: Chairman Pai issuing a statement; Commissioner Clyburn concurring in part, dissenting in part, and issuing a statement.

1. In this Order, we provide guidance that the Commission's rules implementing Section 222 of the Communications Act of 1934, as amended (the Act), for telecommunications carriers that were in existence prior to the *2016 Privacy Order*[1] are again in effect pursuant to the resolution of disapproval of that Order under the Congressional Review Act.[2] We also dismiss as moot 11 petitions for reconsideration of the Commission's *2016 Privacy Order*.

2. On October 27, 2016, the Commission adopted the *2016 Privacy Order*, which adopted rules to implement Section 222 of the Act as applied to broadband Internet service providers (ISPs), and revised the Commission's then-existing rules under Section 222 to harmonize the requirements for all telecommunications carriers.[3] The Commission published a summary of the *2016 Privacy Order* in the Federal Register on December 2, 2016, and thereafter submitted it to Congress pursuant to the Congressional Review Act. On April 3, 2017, the President signed Pub. Law 115-22,[4] which provides that the rule submitted by the Commission "shall have no force or effect." Because Pub. Law 115-22 was adopted pursuant to the Congressional Review Act, 5 U.S.C. § 801(f) provides that the *2016 Privacy Order* "shall be treated as though [it] had never taken effect."[5] As a result, the Commission rules implementing Section 222 at Part 64, Subpart U that were in effect prior to their amendment by the *2016*

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Report and Order, 31 FCC Rcd 13911 (2016) (*2016 Privacy Order*).

[2] 5 U.S.C. § 801(a)(1)(A).

[3] *See generally 2016 Privacy Order*, 31 FCC Rcd 13911.

[4] Joint Resolution, Pub. L. No. 155-22 (2017) ("*Resolved by the Senate and House of Representatives of the United States of America in Congress assembled,* 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.").

[5] 5 U.S.C. § 801(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."); *id.* § 801(b)(1) ("A rule shall not take effect (or continue), if the Congress enacts a joint resolution of disapproval . . . of the rule.").

Privacy Order are again in effect, including the annual compliance certification requirements and recordkeeping requirements set out in Section 64.2009(e) and (c). Therefore, barring further action by the Commission, carriers subject to the annual compliance certification requirement must file such a certification no later than March 1, 2018. The Section 222 rules that are again in effect are attached at Appendix A. We also remind ISPs that they remain subject to Section 222 but need not comply with the Commission's implementing rules as a result of the forbearance granted in the *Title II Order*.[6]

3. Pursuant to 5 U.S.C. § 553(b)(B), because we are simply recognizing the effect of the resolution of disapproval, we find that notice and public procedure are unnecessary to reflect this action in the Code of Federal Regulations. Pursuant to 5 U.S.C. § 553(d), because we are simply interpreting and implementing the resolution of disapproval, this action will be effective immediately upon publication in the *Federal Register*.

4. On December 21, 2016, Oracle Corporation filed a petition for reconsideration of the *2016 Privacy Order*.[7] On January 3, 2017, ten additional entities—U.S. Telecom Association (USTelecom), CTIA, American Cable Association, Association of National Advertisers, et al., Competitive Carriers Association, Consumer Technology Association, ITTA—The Voice of Mid-size Communications Companies, Level 3, NCTA—The Internet & Television Association, and Wireless Internet Service Providers Association—each filed separate petitions for reconsideration of the *2016 Privacy Order*.[8] Because the *2016 Privacy Order*, and the rules adopted therein, are no longer in effect, pursuant to Section 1.429(i) of our rules,[9] we dismiss as moot the 11 petitions seeking reconsideration of the *2016 Privacy Order*.

5. Accordingly, IT IS ORDERED that, pursuant to Section 1.429(i) of the Commission's rules, 47 CFR § 1.429(i), the Petitions for Reconsideration filed by Oracle Corporation on December 21, 2016, and by USTelecom, CTIA, American Cable Association, Association of National Advertisers et al.,

[6] *See Enforcement Bureau Guidance: Broadband Providers Should Take Reasonable, Good Faith Steps to Protect Consumer Privacy*, Public Notice, 30 FCC Rcd 4849 (EB 2015); *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5820-24, paras. 462-67 (2015) (*Title II Order*).

[7] Petition for Reconsideration of Oracle Corporation, WC Docket No. 16-106 (filed Dec. 21, 2016).

[8] Petition for Reconsideration of USTelecom, WC Docket No. 16-106 (filed Jan. 3, 2017); Petition for Reconsideration of CTIA, WC Docket No. 16-106 (filed Jan. 3, 2017); Petition for Reconsideration of American Cable Association, WC Docket No. 16-106 (filed Jan. 3, 2017); Petition for Reconsideration of Association of National Advertisers, et al., WC Docket No. 16-106 (filed Jan. 3, 2017); Petition for Reconsideration of Competitive Carriers Association, WC Docket No. 16-106 (filed Jan. 3, 2017); Petition for Reconsideration of Consumer Technology Association, WC Docket No. 16-106 (filed Jan. 3, 2017); Petition for Reconsideration of ITTA—The Voice of Mid-size Communications Companies, WC Docket No. 16-106 (filed Jan. 3, 2017); Petition for Reconsideration of Level 3, WC Docket No. 16-106 (filed Jan. 3, 2017); Petition for Reconsideration of NCTA—The Internet & Television Association, WC Docket No. 16-106 (filed Jan. 3, 2017); Petition for Reconsideration of Wireless Internet Service Providers Association, WC Docket No. 16-106 (filed Jan. 3, 2017).

[9] 47 CFR § 1.429(i) ("The Commission may grant the petition for reconsideration in whole or in part or may deny or dismiss the petition. Its order will contain a concise statement of the reasons for the action taken.").

Competitive Carriers Association, Consumer Technology Association, ITTA, Level 3, NCTA, and Wireless Internet Service Providers Association on January 3, 2017 in WC Docket No. 16-106 are DISMISSED.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

Rules

§ 64.2001 Basis and purpose.

(a) *Basis.* The rules in this subpart are issued pursuant to the Communications Act of 1934, as amended.

(b) *Purpose.* The purpose of the rules in this subpart is to implement section 222 of the Communications Act of 1934, as amended, 47 U.S.C. 222.

§ 64.2003 Definitions.

(a) *Account information.* "Account information" is information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill's amount.

(b) *Address of record.* An "address of record," whether postal or electronic, is an address that the carrier has associated with the customer's account for at least 30 days.

(c) *Affiliate.* The term "affiliate" has the same meaning given such term in section 3(1) of the Communications Act of 1934, as amended, 47 U.S.C. 153(1).

(d) *Call detail information.* Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

(e) *Communications-related services.* The term "communications-related services" means telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment.

(f) *Customer.* A customer of a telecommunications carrier is a person or entity to which the telecommunications carrier is currently providing service.

(g) *Customer proprietary network information (CPNI).* The term "customer proprietary network information (CPNI)" has the same meaning given to such term in section 222(h)(1) of the Communications Act of 1934, as amended, 47 U.S.C. 222(h)(1).

(h) *Customer premises equipment (CPE).* The term "customer premises equipment (CPE)" has the same meaning given to such term in section 3(14) of the Communications Act of 1934, as amended, 47 U.S.C. 153(14).

(i) *Information services typically provided by telecommunications carriers.* The phrase "information services typically provided by telecommunications carriers" means only those information services (as defined in section 3(20) of the Communication Act of 1934, as amended, 47 U.S.C. 153(20)) that are typically provided by telecommunications carriers, such as Internet access or voice mail services. Such phrase "information services typically provided by telecommunications carriers," as used in this subpart, shall not include retail consumer services provided using Internet Web sites (such as travel reservation services or mortgage lending services), whether or not such services may otherwise be considered to be information services.

(j) *Local exchange carrier (LEC).* The term "local exchange carrier (LEC)" has the same meaning given to such term in section 3(26) of the Communications Act of 1934, as amended, 47 U.S.C. 153(26).

(k) *Opt-in approval.* The term "opt-in approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request consistent with the requirements set forth in this subpart.

(l) *Opt-out approval.* The term "opt-out approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the waiting period described in § 64.2008(d)(1) after the customer is provided appropriate notification of the carrier's request for consent consistent with the rules in this subpart.

(m) *Readily available biographical information.* "Readily available biographical information" is information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth.

(n) *Subscriber list information (SLI).* The term "subscriber list information (SLI)" has the same meaning given to such term in section 222(h)(3) of the Communications Act of 1934, as amended, 47 U.S.C. 222(h)(3).

(o) *Telecommunications carrier or carrier.* The terms "telecommunications carrier" or "carrier" shall have the same meaning as set forth in section 3(44) of the Communications Act of 1934, as amended, 47 U.S.C. 153(44). For the purposes of this subpart, the term "telecommunications carrier" or "carrier" shall include an entity that provides interconnected VoIP service, as that term is defined in section 9.3 of these rules.

(p) *Telecommunications service.* The term "telecommunications service" has the same meaning given to such term in section 3(46) of the Communications Act of 1934, as amended, 47 U.S.C. 153(46).

(q) *Telephone number of record.* The telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."

(r) *Valid photo ID.* A "valid photo ID" is a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

§ 64.2005 Use of customer proprietary network information without customer approval.

(a) Any telecommunications carrier may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (*i.e.*, local, interexchange, and CMRS) to which the customer already subscribes from the same carrier, without customer approval.

(1) If a telecommunications carrier provides different categories of service, and a customer subscribes to more than one category of service offered by the carrier, the carrier is permitted to share CPNI among the carrier's affiliated entities that provide a service offering to the customer.

(2) If a telecommunications carrier provides different categories of service, but a customer does not subscribe to more than one offering by the carrier, the carrier is not permitted to share CPNI with its affiliates, except as provided in § 64.2007(b).

(b) A telecommunications carrier may not use, disclose, or permit access to CPNI to market to a customer service offerings that are within a category of service to which the subscriber does not already subscribe from that carrier, unless that carrier has customer approval to do so, except as described in paragraph (c) of this section.

(1) A wireless provider may use, disclose, or permit access to CPNI derived from its provision of CMRS, without customer approval, for the provision of CPE and information service(s). A wireline carrier may use, disclose or permit access to CPNI derived from its provision of local exchange service or interexchange service, without customer approval, for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

(2) A telecommunications carrier may not use, disclose or permit access to CPNI to identify or track customers that call competing service providers. For example, a local exchange carrier may not use local service CPNI to track all customers that call local service competitors.

(c) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, as described in this paragraph (c).

(1) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, in its provision of inside wiring installation, maintenance, and repair services.

(2) CMRS providers may use, disclose, or permit access to CPNI for the purpose of conducting research on the health effects of CMRS.

(3) LECs, CMRS providers, and entities that provide interconnected VoIP service as that term is defined in § 9.3 of this chapter, may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features.

(d) A telecommunications carrier may use, disclose, or permit access to CPNI 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.

§ 64.2007 Approval required for use of customer proprietary network information.

(a) A telecommunications carrier may obtain approval through written, oral or electronic methods.

(1) A telecommunications carrier relying on oral approval shall bear the burden of demonstrating that such approval has been given in compliance with the Commission's rules in this part.

(2) Approval or disapproval to use, disclose, or permit access to a customer's CPNI obtained by a telecommunications carrier must remain in effect until the customer revokes or limits such approval or disapproval.

(3) A telecommunications carrier must maintain records of approval, whether oral, written or electronic, for at least one year.

(b) *Use of Opt-Out and Opt-In Approval Processes.* A telecommunications carrier may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services. A telecommunications carrier may also permit such persons or entities to obtain access to such CPNI for such purposes. Except for use and disclosure of CPNI that is permitted without customer approval under section § 64.2005, or that is described in this paragraph, or as otherwise provided in section 222 of the Communications Act of 1934, as amended, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.

§ 64.2008 Notice required for use of customer proprietary network information.

(a) *Notification, Generally.*

(1) Prior to any solicitation for customer approval, a telecommunications carrier must provide notification to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.

(2) A telecommunications carrier must maintain records of notification, whether oral, written or electronic, for at least one year.

(b) Individual notice to customers must be provided when soliciting approval to use, disclose, or permit access to customers' CPNI.

(c) *Content of Notice.* Customer notification must provide sufficient information to enable the customer to make an informed decision as to whether to permit a carrier to use, disclose, or permit access to, the customer's CPNI.

(1) The notification must state that the customer has a right, and the carrier has a duty, under federal law, to protect the confidentiality of CPNI.

(2) The notification must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.

(3) The notification must advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes. However, carriers may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI.

(4) The notification must be comprehensible and must not be misleading.

(5) If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer.

(6) If any portion of a notification is translated into another language, then all portions of the notification must be translated into that language.

(7) A carrier may state in the notification that the customer's approval to use CPNI may enhance the carrier's ability to offer products and services tailored to the customer's needs. A carrier also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer.

(8) A carrier may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.

(9) The notification must state that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from that carrier is valid until the customer affirmatively revokes or limits such approval or denial.

(10) A telecommunications carrier's solicitation for approval must be proximate to the notification of a customer's CPNI rights.

(d) *Notice Requirements Specific to Opt-Out.* A telecommunications carrier must provide notification to obtain opt-out approval through electronic or written methods, but not by oral communication (except as provided in paragraph (f) of this section). The contents of any such notification must comply with the requirements of paragraph (c) of this section.

(1) Carriers must wait a 30-day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. A carrier may, in its discretion, provide for a longer period. Carriers must notify customers as to the applicable waiting period for a response before approval is assumed.

(i) In the case of an electronic form of notification, the waiting period shall begin to run from the date on which the notification was sent; and

(ii) In the case of notification by mail, the waiting period shall begin to run on the third day following the date that the notification was mailed.

(2) Carriers using the opt-out mechanism must provide notices to their customers every two years.

(3) Telecommunications carriers that use e-mail to provide opt-out notices must comply with the following requirements in addition to the requirements generally applicable to notification:

(i) Carriers must obtain express, verifiable, prior approval from consumers to send notices via e-mail regarding their service in general, or CPNI in particular;

(ii) Carriers must allow customers to reply directly to e-mails containing CPNI notices in order to opt-out;

(iii) Opt-out e-mail notices that are returned to the carrier as undeliverable must be sent to the customer in another form before carriers may consider the customer to have received notice;

(iv) Carriers that use e-mail to send CPNI notices must ensure that the subject line of the message clearly and accurately identifies the subject matter of the e-mail; and

(v) Telecommunications carriers must make available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week. Carriers may satisfy this requirement through a combination of methods, so long as all customers have the ability to opt-out at no cost and are able to effectuate that choice whenever they choose.

(e) *Notice Requirements Specific to Opt-In.* A telecommunications carrier may provide notification to obtain opt-in approval through oral, written, or electronic methods. The contents of any such notification must comply with the requirements of paragraph (c) of this section.

(f) *Notice Requirements Specific to One-Time Use of CPNI.*

(1) Carriers may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether carriers use opt-out or opt-in approval based on the nature of the contact.

(2) The contents of any such notification must comply with the requirements of paragraph (c) of this section, except that telecommunications carriers may omit any of the following notice provisions if not relevant to the limited use for which the carrier seeks CPNI:

(i) Carriers need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election;

(ii) Carriers need not advise customers that they may share CPNI with their affiliates or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party;

(iii) Carriers need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as carriers explain to customers that the scope of the approval the carrier seeks is limited to one-time use; and

(iv) Carriers may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the carrier clearly communicates that the customer can deny access to his CPNI for the call.

§ 64.2009 Safeguards required for use of customer proprietary network information.

(a) Telecommunications carriers must implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

(b) Telecommunications carriers must train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place.

(c) All carriers shall maintain a record, electronically or in some other manner, of their own and their affiliates' sales and marketing campaigns that use their customers' CPNI. All carriers shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record must include a description of each campaign, the specific CPNI that

was used in the campaign, and what products and services were offered as a part of the campaign. Carriers shall retain the record for a minimum of one year.

(d) Telecommunications carriers must establish a supervisory review process regarding carrier compliance with the rules in this subpart for outbound marketing situations and maintain records of carrier compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

(e) A telecommunications carrier must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis. The officer must state in the certification that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. The carrier must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart. In addition, the carrier must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. This filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year.

(f) Carriers must provide written notice within five business days to the Commission of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

(1) The notice shall be in the form of a letter, and shall include the carrier's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.

(2) Such notice must be submitted even if the carrier offers other methods by which consumers may opt-out.

§ 64.2010 Safeguards on the disclosure of customer proprietary network information.

(a) *Safeguarding CPNI.* Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.

(b) *Telephone access to CPNI.* Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, the telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.

(c) *Online access to CPNI.* A telecommunications carrier must authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information.

(d) *In-store access to CPNI.* A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.

(e) *Establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords.* To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, or account information. Telecommunications carriers may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

(f) *Notification of account changes.* Telecommunications carriers must notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.

(g) *Business customer exemption.* Telecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.

§ 64.2011 Notification of customer proprietary network information security breaches.

(a) A telecommunications carrier shall notify law enforcement of a breach of its customers' CPNI as provided in this section. The carrier shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement pursuant to paragraph (b) of this section.

(b) As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the telecommunications carrier shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni.

(1) Notwithstanding any state law to the contrary, the carrier shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in paragraphs (b)(2) and (b)(3) of this section.

(2) If the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (b)(1) of this section, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The carrier shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(3) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.

(c) *Customer notification.* After a telecommunications carrier has completed the process of notifying law enforcement pursuant to paragraph (b) of this section, it shall notify its customers of a breach of those customers' CPNI.

(d) *Recordkeeping.* All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (b) of this section, and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Carriers shall retain the record for a minimum of 2 years.

(e) *Definitions.* As used in this section, a "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

(f) This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.

STATEMENT OF
CHAIRMAN AJIT PAI

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106; *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket 96-115.

Today, the Commission releases a ministerial *Order* to implement the Congressional resolution disapproving the Commission's *2016 Privacy Order*, which had amended the Commission's rules implementing Section 222 of the Communications Act. Because Congress has invalidated the *2016 Privacy Order*, we simply make clear that the privacy rules that were in effect prior to 2016 are once again effective.

Originally, the Wireline Competition Bureau was slated to perform this ministerial act. But when Commissioner Clyburn asked for this matter to be addressed at the Commission level, we brought it up for a Commission vote. After doing so, Commissioner Clyburn did not ask for a single change to be made to this *Order*. I am therefore perplexed by her decision to dissent in part. When a Commissioner does not share her concerns about an item until after she casts her vote, it makes it difficult to work together to find common ground.

STATEMENT OF
COMMISSIONER MIGNON L. CLYBURN
CONCURRING IN PART AND DISSENTING IN PART

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106; *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket 96-115

Today nearly everything we do crosses the internet, from paying bills to seeking employment or researching a medical condition. Given the amount of personal data shared online, consumers are understandably concerned about their privacy. This is reflected in research showing that over 90 percent of consumers feel like they have lost control of their information online. That is why it is so important to have safeguards that govern all aspects of online privacy. Sadly, we continue to give broadband providers a hall pass today, even as we see 20 states step up and try to fill the void left by Congressional action and the FCC's refusal to reestablish robust privacy rules.

To be clear, I concur with giving guidance in the context of voice phone service. In an era where the FCC is taking a weed-whacker to rules to the detriment of regulatory certainty, it is some comfort to see the majority putting legacy rules back on the books that will at least provide some safeguards for voice customers. Reinstating the admittedly imperfect legacy voice rules, achieves that goal to some extent.

But I must disagree both with the simplistic treatment of the Congressional Review Act (CRA) found in this item, and more significantly, leaving out any requirements for broadband providers. I believe the better course would have been to close out the existing proceeding (or initiate a new proceeding) to come up with another holistic approach to voice and broadband.

First, it seems facile and bull-headed to move forward with an Order without seeking comment on how the CRA impacts this proceeding. This is the first time this legislative tool has ever been used on a set of FCC rules. In other novel contexts, the Commission has sought comment on how best to proceed. Even though the majority made clear they intend to move forward with Title II repeal, they still sought comment on the legal issue of how to classify broadband internet access service. Here, not only do we not seek comment, but in the first time the CRA is applied to FCC rules, we respond with "ministerial" changes to the Code of Federal Regulations.

Important and nuanced legal questions remain unanswered. Are aspects of the legacy voice rules substantially similar to the harmonized rules the Commission adopted last year? Does the CRA work to undo the modified adopted rule but leave in place the extinguishing of the original rule? We do not grapple with any of these fundamental interpretational issues.

Second, and more importantly, this Order shows that the majority is committed to reversing Title II for broadband and that they are willing to leave broadband consumers without privacy protections while this work is ongoing. There is a theory that we could actually move to adopt broadband privacy rules on the open notice from 2015. We should be using this item to adopt rules, or at a minimum seek comment on how to move forward with broadband privacy. Even if we did not adopt rules, we could adopt enforcement guidance or a policy statement using the voluntary code of conduct on which broadband providers seeking reconsideration were willing to agree. But no, the Commission is not even doing that. We now simply have the bare text of section 222 for broadband, and decade-old rules for legacy voice.

Just what does this all mean? For businesses: regulatory uncertainty regarding the enforcement of section 222. Broadband providers thought the bare text of section 222 was sufficiently uncertain to seek a stay of the *2015 Open Internet Order* two years ago. For consumers: they are almost wholly without recourse if a provider decides to not to adequately inform them, consult them before selling their data, or

fail to protect data that they do have. The only real recourse for them will be individual forced arbitration before an entity of their service provider's choosing . . . the very antithesis of putting #ConsumersFirst.

For all of the stated reasons, I vote to concur in part and dissent in part.