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
	)	

ORDER GRANTING STAY PETITION IN PART

Adopted: March 1, 2017 **Released: March 1, 2017**

By the Commission: Commissioner O'Rielly issuing a statement; Commissioner Clyburn dissenting and issuing a statement.

I. INTRODUCTION

1. On October 26, 2016, the Commission adopted the *2016 Privacy Order*.[1] By January 3, 2017, the Commission had received eleven separate timely petitions to reconsider that order.[2] On January 27, 2017, nine trade associations filed a petition for stay of those rules.[3] We grant the Stay Petition in part, and accordingly stay on an interim basis only one aspect of the requirements adopted in the *2016*

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, 31 FCC Rcd 13911 (2016) (*2016 Privacy Order* or *Order*).

[2] Petition of American Cable Association for Reconsideration, WC Docket No. 16-106 (filed Jan. 3, 2017), https://ecfsapi.fcc.gov/file/10104075594979/ACA_Privacy_Petition_for_Reconsideration_01032017_2.pdf; Petition of the Association of National Advertisers et al. for Reconsideration, WC Docket No. 16-106 (filed Jan. 3, 2017), https://ecfsapi.fcc.gov/file/1010300614650/Petition%20for%20Reconsideration%201.3.2017_2.pdf; Petition of CTIA for Reconsideration, WC Docket No. 16-106 (filed Jan. 3, 2017), https://ecfsapi.fcc.gov/file/101033094013829/160103%20CTIA%20Petition%20for%20Reconsideration%20WC%2016-106_2.pdf; Petition of the Competitive Carriers Association for Reconsideration, WC Docket No. 16-106 (filed Jan. 3, 2017), https://ecfsapi.fcc.gov/file/10103178455609/CCA%20Privacy%20Order%20Petition%20for%20Reconsideration%20(010317)%20_2.pdf; Petition of Consumer Technology Association for Reconsideration, WC Docket No. 16-106 (filed Jan. 3, 2017), https://ecfsapi.fcc.gov/file/10103091472650/CTA_FCC_Privacy_Petition_for_Reconsideration_2.pdf; Petition of ITTA for Reconsideration, WC Docket No. 16-106 (filed Jan. 3, 2017), https://ecfsapi.fcc.gov/file/10103777424694/ITTA%20Broadband%20Privacy%20PFR%20As%20Filed%20010317_2.pdf; Petition of Level 3 Communications, LLC, for Reconsideration, WC Docket No. 16-106 (filed Jan. 3, 2017), https://ecfsapi.fcc.gov/file/10103280069637/Level%203%20Petition%20for%20Reconsideration%20(1.3.2017)_2.pdf; Petition of NCTA for Reconsideration, WC Docket No. 16-106 (filed Jan. 3, 2017), https://ecfsapi.fcc.gov/file/10103104689995/NCTA%20Recon%20Petition%20WC%2016-106_2.pdf (NCTA Reconsideration Petition); Petition of Oracle Corp. for Reconsideration, WC Docket No. 16-106 (filed Dec. 21, 2016), https://ecfsapi.fcc.gov/file/1221003408004/Oracle_Broadband_Privacy_Petition_for_Reconsideration.pdf; Petition of the United States Telecom Association for Reconsideration, WC Docket No. 16-106 (filed Jan. 3, 2017), https://ecfsapi.fcc.gov/file/1010364854858/Privacy_PFR_01.03.17_lf_krs%20_2.pdf; Petition of the Wireless Internet Service Providers Association for Reconsideration, WC Docket No. 16-106 (filed Jan. 3, 2017), https://ecfsapi.fcc.gov/file/101032162706335/WISPA%20Petition%20for%20Reconsideration%3B%20WC%20Docket%20No.%2016-106_2.pdf.

[3] *See* Joint Petition of American Cable Association et al. (Petitioners) for Stay, WC Docket No. 16-106 (filed Jan. 27, 2017), https://ecfsapi.fcc.gov/file/101270254521574/012717%20Petition%20for%20Stay.pdf (Stay Petition).

Privacy Order related to data security, which are those aspects of the rule scheduled to become effective on March 2, 2017. This interim stay extends until the Commission can act on the petitions for reconsideration pending in this proceeding. We do not take action at this time on Petitioners' request for stay of other provisions of the *2016 Privacy Order*, in particular, the new notice requirements, customer approval requirements, and data breach notification requirements, which are all subject to Office of Management and Budget approval under the Paperwork Reduction Act.[4] The Commission should be able to resolve the petitions for reconsideration before those rules become effective. Additionally, this Order does not address those rules that became effective before the Stay Petition was filed.

II. BACKGROUND

2. In March 2016, the Commission "propose[d] to apply the traditional privacy requirements of the Communications Act to . . . broadband Internet access service (BIAS)."[5] Seven months later, in October 2016, the Commission somewhat shifted its approach and adopted new notice requirements, customer approval requirements, data security requirements, and data breach notification requirements.[6]

3. With respect to data security, the *Order* requires BIAS providers and other telecommunications carriers to "take reasonable measures to protect customer [proprietary information] from unauthorized use, disclosure, or access."[7] It states that "the reasonableness of a provider's data security practices will depend significantly on context" and identifies factors that a provider must consider, specifically, the nature and scope of its activities; the sensitivity of the data it collects; its size; and technical feasibility.[8] The *Order* describes practices that the Commission "presently consider[s] exemplary of a reasonable and evolving standard of data security."[9] It also identifies that "existing privacy and data security laws, best practices, and public-private initiatives" are each "a potential source of guidance on practices that may be implemented to protect the confidentiality of customer [proprietary information]."[10] Finally, the *Order* adopts harmonized data security requirements for BIAS providers and telecommunications carriers that were subject to the Commission's predecessor customer proprietary network information rules.[11] These data security requirements are scheduled to become effective on March 2, 2017.

4. The Stay Petition contends that the Commission should stay many of the rules adopted in the *Order* until the Commission acts upon the petitions for reconsideration filed in this proceeding, which the Stay Petition incorporates by reference.[12] As to data security, Petitioners argue that although the *Order* "appropriately adopts a 'reasonable measures' standard," its articulation of that standard's meaning "substantially widen[s] the uncertainty and compliance burdens imposed upon ISPs relative to all other Internet entities and heighten[s] the risks of different interpretations."[13] Similarly, the NCTA

[4] *See generally* Stay Petition; *2016 Privacy Order*, 31 FCC Rcd at 14080, Appx. A (Sections 64.2003, 64.2004, 64. 2006, 64.2011(b)).

[5] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500, 2501, para. 2 (2016).

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

[7] 47 CFR § 64.2005(a).

[8] *2016 Privacy Order*, 31 FCC Rcd at 14009, para. 242.

[9] *Id.* at 14013, para. 248.

[10] *Id.*

[11] *Id.* at 14018-19, paras. 256-60.

[12] *See* Stay Petition at 1-3.

[13] *Id.* at 22-23.

Reconsideration Petition asserts that the *Order* erred in that "there is no specific mechanism to ensure that the FCC interprets th[e] test in the same manner as the" Federal Trade Commission (FTC) and that "[t]o the contrary, the *Order* expresses its intention to look beyond the FTC's administration of that [reasonable measures] test."[14]

5. Petitioners argue that they will bear substantial costs and burdens complying with the new rules, and that these costs and burdens constitute irreparable harm and are contrary to the public interest because they will not be recoverable in the event that the Commission grants the pending petitions for reconsideration.[15] With respect to the new data security requirements, they also represent that ISPs "have relied on a voluntary set of privacy and data security principles that are consistent with the FTC's long-standing framework, and have committed to continue adhering to these obligations."[16] These "ISP Privacy Principles" include a commitment to take reasonable measures to protect customer information from unauthorized use, disclosure, or access, taking into account the nature and scope of their activities, the sensitivity of the data, the size of the ISP, and technical feasibility. The signatories to these principles include Altice, AT&T, Charter, Citizens Telephone and Cablevision, Comcast, Cox, Dickey Rural Networks, Inland Telephone Company, Northeast Louisiana Telephone, SCTelcom, T-Mobile, Verizon, VTX1, Wheat State Telephone, and the following associations: ACA, CTIA, ITTA, NCTA, NTCA, USTelecom, WISPA, and WTA.[17]

6. On February 3, 2017, eleven organizations filed an opposition to the Stay Petition.[18] The Opposition argues that Petitioners are not likely to succeed on the merits of the petitions for reconsideration, because their arguments "have previously been presented and considered by the Commission."[19] As to the data security and other requirements of the rules, it contends that a stay would harm consumers "because they will not be able to exercise effective options to protect their private information."[20] It asserts that the FTC cannot require ISPs to comply with their voluntary privacy policies; that ISPs lack the market incentives to protect customer information; and that Petitioners' claims of irreparable harm are theoretical, grossly exaggerated, or routine costs associated with compliance.[21]

III. DISCUSSION

7. Section 1.429(k) of the Commission's rules permits the Commission for good cause to stay the effective date of a rule pending a decision on a petition for reconsideration.[22] It is well-settled that in determining whether to stay the effectiveness of one of its Orders, the Commission applies the traditional four-factor test established by the U.S. Court of Appeals for the District of Columbia Circuit

[14] NCTA Reconsideration Petition at 25.

[15] Stay Petition at 24 & n.91, 32-33; *see also* para. 7, *infra*.

[16] *Id.* at 32.

[17] *Id.* Appx. A.

[18] *See* Joint Opposition of National Priorities Consumer Action et al. to Petition for Stay, WC Docket No. 16-106 (filed Feb. 3, 2017), https://ecfsapi.fcc.gov/file/10204239884547/Opposition%20to%20Petition%20for%20Stay%20-%20Final.pdf (Opposition). The additional opposition filed in this proceeding on February 8 is untimely and will be disregarded. *See* 47 CFR § 1.45(d) ("Oppositions to a request for stay of any order or to a request for other temporary relief shall be filed within 7 days after the request is filed."); Opposition of Curtis J. Neely to Frivolous Joint Petition for Stay, WC Docket No. 16-106 (filed Feb. 8, 2017), https://ecfsapi.fcc.gov/file/10208985919369/16-106_Opposition%20to%20Stay.pdf.

[19] Opposition at 5.

[20] *Id.* at 7.

[21] *Id.* at 7, 12.

[22] 47 CFR § 1.429(k).

("D.C. Circuit").[23] To qualify for a stay, a petitioner must show that: (1) it is likely to prevail on the merits; (2) it will suffer irreparable harm absent the grant of preliminary relief; (3) other interested parties will not be harmed if the stay is granted; and (4) the public interest would favor grant of the stay. The Commission's consideration of each factor is weighed against the others, with no single factor dispositive.[24] Thus, "injury held insufficient to justify a stay in one case may well be sufficient to justify it in another, where the applicant has demonstrated a higher probability of success on the merits."[25]

8. We find that Petitioners meet the test for a stay with respect to the data security requirements (new Section 64.2005) in the *2016 Privacy Order*. For the reasons explained below, Petitioners are uniquely likely to succeed on the merits of their claim on reconsideration with respect to these requirements, and they would be entitled to a stay pending Commission action on that claim given their showing with respect to the other three factors. But we believe they would be entitled to a stay even if they had not demonstrated "a higher probability of success on the merits." Consistent with action in similar contexts where petitions for reconsideration of Commission rulemaking orders are pending,[26] we determine that it is in the public interest for the Commission to address and resolve, prior to the to rule taking effect, the parties' claims that the data security requirements need to be clarified or reconsidered, so that (1) consumers are not subject to two different privacy regimes, vitiating their uniform expectation of online privacy, and (2) BIAS providers and other telecommunications carriers do not incur substantial and unnecessary compliance costs while the possibility of changes to the requirements still exist. On our own motion, we also stay the application of new Section 64.2005 to non-BIAS carriers because the same reasoning that justifies a stay to BIAS applies equally to other telecommunications services.[27]

A. Likelihood of Success on the Merits

9. With respect to data security requirements, the *Order* expressly states that the Commission will look beyond the FTC's interpretation of "reasonable measures" and take into account the requirements of other privacy regimes such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm Leach Bliley Act (GLBA), as well as best practices and public-private initiatives.[28] In this case, Petitioners are uniquely likely to succeed on their claim on reconsideration that

[23] *See Washington Metro. Area Transit Comm'n v. Holiday Tours, Inc.*, 559 F.2d 841, 843 (D.C. Cir. 1977) (*Holiday Tours*); *Virginia Petroleum Jobbers Ass'n v. Federal Power Comm'n*, 259 F.2d 921, 925 (D.C. Cir. 1958) (*VA Petroleum Jobbers*).

[24] *AT&T Corp. v. Ameritech Corp.*, 13 FCC Rcd 14508, para. 14 (1998); *Cuomo v. NRC*, 772 F.2d 972, 974 (D.C. Cir. 1985) ("Probability of success is inversely proportional to the degree of irreparable injury evidenced. A stay may be granted with either a high probability of success and some injury, or vice versa.").

[25] *VA Petroleum Jobbers*, 259 F.2d at 925; *accord Holiday Tours*, 559 F.2d at 844.

[26] *See Billed Party Preference for InterLATA 0+ Calls*, Order, 13 FCC Rcd 12576 (CCB 1998); *Regulatory Treatment of LEC Provision of Interexchange Services Originating in the LEC's Local Exchange Area and Policy and Rules Concerning the Interstate, Interexchange Marketplace*, Order, 13 FCC Rcd 6427 (CCB 1998); *Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, Order, 12 FCC Rcd 15313 (WTB 1997).

[27] The Stay Petition focuses on the application of the *2016 Privacy Order* to BIAS providers. *See* Stay Petition at 2 n.2.

[28] Stay Petition at 23; *see also 2016 Privacy Order*, 31 FCC Rcd at 14012-13, para. 248 ("[T]he requirement to engage in reasonable data security practices is set against a backdrop of existing privacy and data security laws, best practices, and public-private initiatives. Each of these is a potential source of guidance on practices that may be implemented to protect the confidentiality of customer [proprietary information]."); *2016 Privacy Order*, 31 FCC Rcd at 14012-13, para. 248 n.714 (citing, as examples of existing privacy and data security laws, the FTC Act, HIPAA, GLBA, and four states' data security laws); *2016 Privacy Order*, 31 FCC Rcd at 14012-13, para. 248 n.715 (citing, as examples of best practices, the 2015 FTC Security Guide for Business and FCC Communications Security, Reliability, and Interoperability Council Best Practices); *2016 Privacy Order*, 31 FCC Rcd at 14012-13, (continued….)

this requirement sweeps too broadly and too vaguely, "substantially widening the uncertainty and compliance burdens imposed upon ISPs relative to all other Internet entities and heightening the risks of different interpretations."[29] The data security requirements, as they currently stand, would subject ISPs to more burdensome regulation than other participants in the Internet ecosystem are subjected to by the FTC.

10. Moreover, a majority of the current Commission dissented from the *2016 Privacy Order* because it did not agree with such an approach. Then-Commissioner Pai explained that the *Order* should have "paralleled the FTC's framework as closely as possible," thereby avoiding "unique rules on ISPs that do not apply to all online actors that collect and use consumer data."[30] Similarly, Commissioner O'Rielly in his dissent expressed concerns about the departure of the adopted rules from the FTC's framework, as well about providing insufficient time for providers to come into compliance with the new data security rules. He specifically noted that "there has been no evidence of any privacy harms, and "no benefit to be gained from increased regulations," while the *Order* "places substantial, unjustified costs on businesses and consumers."[31] In these circumstances, we find that Petitioners have a substantial likelihood of success on the merits of the new data security rules being subject to revisions.

11. Further, contrary to the Opposition's assertion that the Commission's authority to grant petitions for reconsideration is limited to those which rely on facts or arguments which have not been previously presented to the Commission,[32] the Commission's rules simply permit the dismissal or denial of a petition that relies "on arguments that have been fully considered and rejected by the Commission within the same proceeding."[33] The rules do not *require* such a dismissal or denial. Moreover, the Commission as it is currently constituted has not considered and rejected any arguments pertaining to the data security rule raised in the Petitions for Reconsideration.

B. The Balance of the Equities Also Favors Petitioners

12. As noted above, in this context the very strong likelihood of success on the merits of the petitions for reconsideration militates heavily in favor of a stay of the data security requirements of the rules. But the remaining *VA Petroleum Jobbers* factors also warrant a stay of those requirements.

13. Several general principles govern the irreparable injury inquiry. First, "the injury must be both certain and great; it must be actual and not theoretical."[34] A petitioner must also "substantiate the claim that the irreparable injury is 'likely' to occur. . . . Bare allegations of what is likely to occur are of no value since the court must decide whether the harm will in fact occur."[35] While the general rule is that costs of compliance with a regulatory scheme do not constitute irreparable injury,[36] we conclude in these circumstances that the public interest would not be served by requiring BIAS providers to incur excessive costs of compliance when (1) there is an inability to recoup those costs, (2) such costs would be of

(Continued from previous page)
para. 248 n.716 (citing, as an example of a public-private initiative, the National Institute of Standards and Technology Cybersecurity Framework).

[29] Stay Petition at 23.

[30] *2016 Privacy Order*, 31 FCC Rcd at 14121 (Statement of Commissioner Pai).

[31] *Id.* at 14129 (Statement of Commissioner O'Rielly).

[32] Stay Opposition at 13.

[33] 47 CFR § 1.429(l)(3).

[34] *Wisconsin Gas Co. v. FERC*, 758 F.2d 669, 674 (D.C. Cir. 1985).

[35] *Id.* at 674.

[36] *See American Hospital Ass'n v. Harris*, 625 F.2d 1328, 1331 (7th Cir. 1980).

questionable additional benefit, and (3) there is substantial likelihood that Petitioners may persuade the Commission on reconsideration to revisit such requirements.[37]

14. We disagree with the Opposition's general assertion that the economic harms described by Petitioners are either theoretical, grossly exaggerated, or routine costs associated with compliance.[38] The *2016 Privacy Order* outlines a number of practices that companies should consider implementing in order to comply with the new data security rule.[39] These recommended practices include changes to a company's internal business structure, potential modifications to its customer authentication methods, and changes to its information handling practices to incorporate data minimization practices.[40] Petitioners explain that BIAS providers will need to take substantial technical measures to reconfigure data-collection and data-use protocols; establish new internal business rules; and modify employee training programs. Some companies, such as small rural providers, must hire additional employees or procure the services of third parties to manage the transition to new rules.[41] Requiring these companies to incur additional costs and allocate significant resources toward implementing requirements that the Commission is reasonably likely to revise upon reconsideration is wasteful and counterproductive to the public interest. This is particularly the case from a consumer perspective because those resources could be better spent developing new offerings, upgrading networks, or improving security (and, relatedly, because the rule's implementation would create a bifurcated privacy regime contrary to consumers' uniform expectation of online privacy).

15. Further, Petitioners demonstrate that providers already are incurring costs associated with analyzing the changes to their network operations and businesses practices that the new rules necessitate.[42] For example, "many thousands of company personnel [will need to be] trained" and "small rural providers, must hire additional employees or procure the services of third parties" to comply.[43] To the extent that the Commission ultimately decides to substantially revise the data security rule adopted in the *Order*, these implementation costs will be unrecoverable and will be compounded by additional costs associated with reverting back to practices permitted prior to establishment of the vacated or revised obligations.

16. The weighting of "data security requirements under HIPAA, GLBA, and other relevant statutory frameworks"[44] and other indicia of reasonable data security required by the *Order* would be resource-intensive, and providers could not be sure that they would weigh the factors in the same manner as this or any future Commission. The fact that the *Order* contains no specific mechanism to ensure that the Commission will interpret the "reasonable measures" standard in the same manner as the FTC undermines the Commission's goals regarding the importance of consistent application of the "reasonable measures" standard across the Internet ecosystem, heightens the risk of different interpretations, and thereby increases the uncertainties and associated costs regarding compliance.[45] Petitioners are also

[37] *See Central Valley Chrysler-Plymouth v. California Air Resources Bd.*, 2002 WL 34499459 (E.D. Cal. June 11, 2002), at *7; *Texas Food Industry v. Dept. of Agriculture*, 842 F.Supp. 254, 260–61 (W.D. Tex. 1993); *see also National Medical Care, Inc. v. Shalala*, 1995 WL 465650 (D.D.C. 1995) ("[G]iven the overwhelming likelihood that the Plaintiffs will eventually succeed on the merits of their retroactivity claim, it would be absurd to allow the Defendant to impose these costs [of compliance] upon the Plaintiffs at all.").

[38] Stay Opposition at 12.

[39] *See 2016 Privacy Order*, 31 FCC Rcd at 14012-018, paras. 248-55.

[40] *Id.*

[41] Stay Petition at 25.

[42] *Id.* at 27.

[43] *Id.*

[44] *2016 Privacy Order*, 31 FCC Rcd at 14015, 4para. 250.

[45] *See* NCTA Petition for Reconsideration at 25.

correct that this represents a departure from the status quo, in which BIAS providers have long operated under the FTC's interpretations of the FTC Act's Section 5 prohibition against unfair or deceptive acts or practices, and other telecommunications carriers have operated under the Commission's existing rules addressing data security.[46] Thus, the resources that BIAS providers and other telecommunications carriers would be required to devote to assessing the interplay between these and other privacy regimes and their existing data security practices are substantial. BIAS providers and other telecommunications carriers would also be required to potentially institute technical and operational measures to alter existing practices to be consistent with these other regimes, which could require substantial staff and resources and may impose hardships on small providers.

17. Conversely, granting Petitioners' request for a stay of the data security rule will maintain a status quo that has been in place for nearly two years with respect to BIAS providers—since the Commission reclassified BIAS as a telecommunications service—and nearly a decade with respect to other telecommunications carriers, with the Commission's adoption of heightened authentication requirements in 2007. While BIAS providers have not been subject to specific implementing rules for nearly two years now, they have been obligated to comply with Section 222 of the Communications Act of 1934, as amended; the Commission's interim guidance; and other applicable federal and state privacy, data security, and breach notification laws.[47] The record contains no evidence of harm to consumers as a result. Furthermore, as noted above, BIAS providers have released a voluntary set of "ISP Privacy Principles" that are consistent with the FTC's long-standing framework, and have committed to continue adhering to these obligations regardless of whether the Commission's broadband privacy rules are stayed, thereby further minimizing the risk of harm to other parties.[48] The Opposition's arguments about ISPs' "economic incentives"[49] fail to differentiate among the various privacy rules, the vast bulk of which are not the subject of this Stay Order, and also fail to demonstrate that BIAS providers have not complied with these commitments or why they would be likely not to do so during the pendency of the stay. For other telecommunications carriers, our existing rules governing data security—which address, among other things, employee training, supervisory review processes, and customer authentication requirements—will remain in place.[50]

18. The Opposition argues that "[i]f it were true" as "Petitioners suggest, that different regulatory standards for different types of entities inherently create competitive disadvantages, granting a stay would necessarily harm edge providers."[51] But creating and eliminating regulatory asymmetries are not the same. An agency tasked with promoting competition cannot treat as cognizable a "harm" that results simply from removing a regulatory disparity. Moreover, to the extent that consumers have a uniform expectation of privacy when they go online, removing such disparities and creating a level regulatory framework better serves their interests.

19. In the foregoing circumstances, we conclude that preserving the status quo pending further examination of whether to uphold the *Order*'s deviation from the FTC's successful data security framework would benefit consumers, competition, innovation and the digital economy—and thus further the public interest. Therefore, the public interest disfavors compelling BIAS providers and other

[46] *See* 47 CFR §§ 64.2009, 64.2010.

[47] Stay Petition at 8. For this reason, consumers will retain multiple avenues to raise objections to data security practices, contrary to the Opposition's assertions. *Cf.* Opposition at 6 (stating that a stay "would mean that consumers would have essentially no protections"); Opposition at 7 (asserting that a stay will leave consumers with no redress).

[48] Stay Petition at 32.

[49] Opposition at 7-8.

[50] 47 CFR § 64.2009(a), (b), (d), (f); 47 CFR § 64.2010.

[51] Opposition at 9.

telecommunications carriers to incur substantial costs and burdens to implement the data security rule pending our reconsideration of that rule.

20. For these reasons, we grant in part the Stay Petition and stay on an interim basis the data security requirements established by the *Order*, i.e., new section 64.2005, until the Commission has decided the petitions for reconsideration pending in this proceeding. The *Order* states that "until the new privacy rules are effective and implemented with respect to voice services, the existing rules remain in place."[52] Accordingly, services that were subject to the Commission's preexisting data security requirements remain subject to those rules—specifically, such services remain subject to Section 64.2010 and subsections 64.2009(a)-(b), (d), and (f) of the Commission's rules as they existed prior to the *Order*.[53] The *Order* eliminated the specific compliance recordkeeping and annual certification requirements in preexisting Sections 64.2009(c) and (e), and therefore those provisions are no longer applicable to any entity.[54]

IV. ORDERING CLAUSES

21. Accordingly, IT IS ORDERED that, pursuant to Sections 1, 2, 4(i)-(j), 201, 202, 222, 303(b), 303(r), 316, 338(i), 631, and 705 of the Communications Act of 1934, as amended, and Section 706 of the Telecommunications Act of 1996, as amended, 47 U.S.C. §§ 151, 152, 154(i)-(j), 201, 202, 222, 303(b), 303(r), 316, 338(i), 551, 605, 1302, and Section 1.429(k) of the Commission's rules, 47 CFR § 1.429(k), this Order IS ADOPTED.

22. IT IS FURTHER ORDERED that the Joint Petition of American Cable Association et al. for Stay IS GRANTED IN PART to the extent described herein.

23. IT IS FURTHER ORDERED that this Order SHALL BE EFFECTIVE upon release, in accordance with section 1.102(b)(1) of the Commission's rules, 47 CFR § 1.102(b)(1).

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[52] *2016 Privacy Order*, 31 FCC Rcd at 14044, para. 316; *id.* at 14042, para. 310 ("Until these rules become effective, Section 222 applies to all telecommunications services, including BIAS, and our current implementing rules continue to apply to telecommunications services other than BIAS and to interconnected VoIP.").

[53] In construing the pre-*Order* rules, the definitions in 47 CFR § 64.2003 as it existed prior to adoption of the *Order* remain applicable.

[54] *See 2016 Privacy Order*, 31 FCC Rcd at 14005, para. 234; *Wireline Competition Bureau Announces Effective Dates of Broadband Privacy Rules*, Public Notice, 31 FCC Rcd 13170, 13170-11 (WCB 2016) ("[T]he *2016 Privacy Order* relieved telecommunications carriers and interconnected VoIP providers of the specific compliance recordkeeping and annual certification requirements in existing section 64.2009, specifically subsections (c) and (e). Thus, once the *Order* becomes effective on January 3, 2017, telecommunications carriers and interconnected VoIP providers no longer will be required to comply with the requirements in subsections (c) and (e) of section 64.2009."); *see also* Voice on the Net (VON) Coalition Comments, WC Docket No. 16-106, at 4-5 (Feb. 3, 2017) (asking the Commission not to reinstate the preexisting compliance recordkeeping and annual certification requirements); Letter from Nicholas G. Alexander, Associate General Counsel, Level 3 Communications, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed Feb. 10, 2017); Letter from Christopher L. Shipley, Attorney & Policy Advisor, INCOMPAS, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed Feb. 10, 2017).

STATEMENT OF
COMMISSIONER MICHAEL O'RIELLY

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.

I support this decision to stay the broadband data security rules while the Commission and Congress consider an appropriate resolution of the broader Net Neutrality proceeding.

To be clear, I think the law and Commission precedent are quite straightforward: the FCC lacks authority to adopt data security rules for any type of provider. Data security is not mentioned anywhere in the Communications Act, and other statutes and legislative efforts that have addressed the topic do not afford the FCC any role. I consistently objected to the prior Commission's unlawful attempts to freelance in this area long before the *Net Neutrality Order* and *Privacy Order* were adopted. I also pointed out that the Commission's attempts to saddle the communications sector with experimental regulations could conflict with well-established FTC precedents that have served as a predictable road map for businesses and consumers alike.

Finally, I appreciate the opportunity to vote on this order at the Commission level. While I welcome greater participation by the full Commission in general, I think that Commission-level action on significant decisions like this one are particularly helpful to provide a clear and final statement of the agency's position, which promotes transparency and certainty for all interested parties.

DISSENTING STATEMENT OF
COMMISSIONER MIGNON L. CLYBURN

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.

On the very same day a major content distribution network revealed that the private data of millions of users from thousands of websites had been exposed for several months, the FCC announced its intention to indefinitely suspend rules requiring broadband providers to protect users' private data. The irony here is inescapable. With a stroke of the proverbial pen, the Federal Communications Commission—the same agency that should be the "cop on the beat" when it comes to ensuring appropriate consumer protections—is leaving broadband customers without assurances that their providers will keep their data secure.

It is for this reason, that I must issue this unequivocal dissent.

In this Order, the majority fells a tree to ostensibly prune a branch. Rather than interpret a duly-adopted, flexible rule in a manner that would be consistent with the majority's understanding of its proper scope, they have chosen to gut the rule entirely. If the problem with the data security rule is, for example, the ability of the Commission to look to other Congressional mandates for guidance, then simply issue interpretive guidance that narrows the scope of the rule. In another context, the majority allowed rules to go into effect with a letter of intent not to enforce until the rules were modified. So my question is why does the same approach not work here?

The painful answer is this: Because with the new FCC, the ends justify the means. This Order is but a proxy for gutting the Commission's duly adopted privacy rules—and it does so with very little finesse. First, the Order alleges deleterious divergence from FTC standards, when in actuality there is little daylight between the approaches taken by the two agencies. Both agencies require only reasonable data security measures, with caveats for the sensitivity of the data, size of the company and technical feasibility. Even the voluntary framework that providers submit with their stay request, which the Order cites approvingly, uses the exact text from the FCC rule as the baseline for broadband provider compliance efforts. This view was reiterated last week by FTC Commissioner Terrell McSweeny who stated that "[t]he rules the FCC adopted conform to long standing FTC practice and provide clear rules on how broadband companies should protect their customers' personal information." Further, the FCC gave helpful guidance, stressed that the standards it set out were not the only way to comply with the rule, and stated unequivocally that the rules were not a strict liability standard. The Order wrongly cites these as additional requirements imposed on broadband providers.

Second, the Order alleges significant harm to service providers, but cites absolutely nothing to prove it. In fact, the stay request does not even begin to estimate the costs associated with compliance. Contrast this with the stay requests for the *2015 Open Internet Order*, where providers offered affidavits involving allegations of specific harms. There, the Commission denied those stay petitions, finding that the harms alleged were insufficient to meet the high bar of a stay. Here, petitioners do not even attempt to quantify the costs associated with all of the privacy rules, much less the data security rule. Again, the rule adopted requires only reasonable data security. It does not put providers at a competitive disadvantage, it does not require massive reporting obligations, nor does it even really require providers to change their existing conduct.

The outcome of this Order is not relief of regulatory burdens, as is evidenced by providers seeking a stay *using the text of the FCC's rule as the basis for their voluntary code of conduct*. What it actually does is permit providers to shift the costs for corporate negligence onto private citizens. Because of the 9th Circuit decision that seriously called into question the ability of the FTC to regulate any business that has a common carrier component, the Commission's action today means that a voluntary

industry code is the only comprehensive federal protection for broadband data security. If a provider simply decides not to adequately protect a customer's information and does not notify them when a breach inevitably occurs, there will be no recompense as a matter of course. The only recourse for customers will be *individual forced arbitration* before an entity of their *service provider's choosing*. Rather than the Commission being able to spearhead an investigation and remuneration for consumers, each individual will have to discover the breach and prosecute it on their own. This is the antithesis of putting #ConsumersFirst.

Finally, I must express my disappointment that the Chairman even entertained this item being adopted on delegated authority. This would have marked the first time in which the Wireline Competition Bureau actually granted a petition for stay. Thankfully, my request to have this considered by the Commission preserved some degree of procedural integrity at the FCC.

Thank you to the staff of the Wireline Competition Bureau. While I dissent, I continue to appreciate your efforts.