DISSENTING STATEMENT OF
COMMISSIONER MICHAEL O'RIELLY

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

Today, the Commission attempts to solve a problem of its own making and, in the process, creates a host of new ones. Having reclassified broadband Internet access service as a telecommunications service, the FCC usurped part of the FTC's role in overseeing broadband privacy. Not content to inherit a system that, by almost all accounts, was working quite well to protect consumers, the FCC quickly embarked on an expansionist mission, seeking to impose situationally-defective new requirements that are stricter than most consumers would ever want or expect and that exceed the Commission's authority. Finding itself out of its depth, the FCC was forced to rein in some of the most extreme proposals and align itself better with the FTC framework. Landing in a less bad spot, however, should not be confused with setting sound policy. I must dissent for a number of reasons.

Beginning with legal authority, the Commission's attempt to fit broadband into section 222 is fundamentally flawed. The plain language of the statute speaks in terms of telephone service.[1] Accordingly, in its effort to shoehorn broadband into this regime, the Commission is forced to ignore or explain away language that clearly contradicts its position, regulate by analogy, or simply create new obligations out of thin air.[2]

To start, there is no independent authority in section 222(a) to regulate privacy or data security, regardless of the technology. As I have said before, the purpose of section 222(a) was to set forth the general parameters of *who* would be covered by the new rules contained in the other subsections. Before the 1996 Act, the rules only applied to AT&T, the BOCs, and GTE. Section 222(a) changed that by extending the general duty to protect proprietary information to *all* telecommunications carriers, while sections 222(b) and (c) detail *when and how* that duty is to be exercised. Specifically, section 222(b) protects other carriers from anti-competitive practices by requiring the confidentiality of carrier proprietary information, while section 222(c) protects the privacy expectations of consumers with respect to their call records by requiring the confidentiality of "customer proprietary network information", or CPNI. Given this three-part structure, it is not surprising that section 222(a) employs a term – proprietary information – that encompasses both the carrier proprietary information used in 222(b) as well as the CPNI used in section 222(c). It does not give the Commission license to ignore its own history and read section 222(a) and its terminology out of context.

Additionally, the use of "equipment manufacturers" in subsection (a) does not provide or authenticate any independent authority to act under the subsection, as the Commission tries to imagine in this item. Instead, it merely functions to cross reference overall concerns that some believed that equipment procurement by old-school Bell Operating Companies would lead to sharing of improper information from manufacturers. To the extent that concern existed, it was addressed directly in various places in section 273 with specific authority to act provided to the Commission in subsection (g) and, thus, it is inappropriate to read such authority into section 222(a).

---

[1] *See, e.g.,* CTIA Comments at 16-23; Comcast Comments at 67.

[2] Interestingly, when deciding that the section 222(e) exception for subscriber list information does not apply to broadband subscriber information, the order takes pains to examine the intent of Congress regarding the exception and analyzes the publishing technologies and information sharing practices that were in place at the time of enactment. In deciding that the rest of section 222 applies to broadband, however, the order breezes right past Congressional intent. Accordingly, section 222(e) is focused on "telephone books" or "direct equivalents" (no "functional equivalents" here) but somehow section 222(c) covers applications.

Commenters supplied additional reasons that refute the FCC's interpretation. They point out that the FCC's expansive interpretation of section 222(a) cannot stand because it would nullify other provisions of section 222.[3] And they show that Congress carefully crafted Section 222 to regulate CPNI and deliberately chose not to use the broader category of "personally identifiable information," or PII, unlike elsewhere in the Act.[4] These arguments further demonstrate that the order's interpretation of section 222(a) is not a permissible or reasonable one. Only a court intent on ignoring its obligations could not understand what the Commission is attempting to do here.

Since there is no independent authority in section 222(a), the categories of information that the FCC made up within section 222(a) – "customer proprietary information" and its subset "personally identifiable information" – are outside the scope of the provision. Yet even if the Commission attempted to ground its rules solely in section 222(c), which I do not concede applies to broadband either, it would still face significant legal problems. Many of the elements that the Commission wants to capture within its rules are not "customer proprietary network information".

First, proprietary information is "information that a person or entity owns to the exclusion of others," and thus it is not proprietary "if other individuals or entities can access the information and use it for their own commercial purposes."[5] That is why, in defining CPNI in section 222(h), Congress specified that it is limited to information that is made available to carriers "solely by virtue of the carrier-customer relationship."[6] Unlike traditional voice calls where the only parties that had access to call records were those already subject to section 222(c) – the local exchange carrier and in some instances the interexchange carrier – multiple parties that are unregulated by section 222 have access to an end user's online activities.[7] Indeed, "an ISP need not rely on its own relationship with its customers to collect information about their online activities because it could obtain the same information independently (at a price) from data brokers or other unregulated third parties."[8] Accordingly, this information would fall outside the scope of section 222(c).[9]

The order responds that proprietary information can't mean information kept secret from everyone else, because other personal information would not be protected by the CPNI rules. And it resorts to platitudes that adhering to the law as it is drafted would "undermine the privacy protective purpose of the statute." But those arguments misunderstand the limited purpose of section 222. It was never intended to cover all information about a person. It defines and protects a specific set of call record information, and until just recently, that has been the Commission's interpretation as well.[10] Far from

---

[3] *See, e.g.,* CTIA Comments at 27; AT&T Comments at 105-107; Verizon Comments at 57-58.

[4] Verizon Comments at 58-59 (citing Whitman v. American Trucking Ass'ns, Inc., 531 U.S. 457, 468 (2001); Dole Food Co. v. Patrickson, 538 U.S. 468, 476 (2003)).

[5] CTIA Comments at 34.

[6] 47 U.S.C. § 222(h).

[7] AT&T Comments at 101.

[8] *Id*. at 102.

[9] Even under the Commission's erroneous theory, to which I do not subscribe, that section 222(a) provides independent authority, this type of information would have to be excluded because section 222(a) likewise uses the term proprietary. Accordingly, section 222(a) also does not cover PII. Verizon also makes the point that, at most, section 222(a) requires "that carriers 'protect the confidentiality' of information; it does not govern permissible *uses* of information" and, therefore, "is far too thin a reed to authorize the entire regulatory apparatus the Commission proposes to erect for PII that is not CPNI." Verizon Comments at 59.

[10] *See, e.g.,* Verizon Comments at 56 ("The fact that the Commission has only now — after 18 years — claimed to discover new authority within Section 222 over all PII held by all telecommunications carriers, rather than only CPNI, belies that novel statutory interpretation. As the Supreme Court has cautioned, '[w]hen an agency claims to discover in a long-extant statute an unheralded power to regulate a significant portion of the American economy, we typically greet its announcement with a measure of skepticism. We expect Congress to speak clearly if it wishes to

(continued….)

creating a gap, as the order claims, Congress made an intentional allocation of responsibility. Section 222 directs the Commission to protect a discrete category of information and, to the extent Congress is concerned about other types of information, it has enacted other laws covering them, and it can enact additional laws going forward. The FCC is not empowered to supplement its own authority, even if it believes it has policy reasons to do so.[11]

At times, the order runs circles around itself. For instance, the order takes the position that "proprietary information" covers "information that should not be exposed widely to the public." But when confronted with the fact that IP addresses are necessarily disclosed on the open Internet to make the service work, the order responds that "whether information is available to third parties does not affect whether it meets the statutory definition of CPNI."[12]

Second, section 222(c)(1) is limited to "individually identifiable" CPNI. Therefore, the order's inclusion of information that is reasonably linked or linkable to a person *or device* is impermissibly broad.[13] If a device "cannot be linked to a specific individual[,] . . . information that may be linked to the device would fall outside the scope of the statute and should not be subject to these rules."[14]

As a backstop, the order also lists a number of other provisions that provide absolutely no authority for these rules.[15] As I've said before, those provisions were never intended to regulate privacy or data security. In addition, by specifically enacting section 222, Congress made clear that the authority to regulate privacy is found in that provision. Any other reading would render section 222 superfluous.

While the FCC has no authority to adopt broadband privacy rules, I am compelled to comment on the serious deficiencies in the rules themselves in the event that somehow a court erroneously, irresponsibly and lawlessly finds that there is authority for them. In particular, the order fails to adequately justify the rules, including why it takes a different approach from the FTC in several key respects, leaving ISPs with substantially greater burdens than other Internet companies. The order falls back on the tired refrain that broadband providers are "gatekeepers" and that, in that role, they are able to see more information about their customers than edge providers. This ridiculous notion has been thoroughly debunked in the record.[16] The fact that consumers use multiple platforms to access the Internet, coupled with the increasing prevalence of encryption, significantly undermines the order's

(Continued from previous page)
assign to an agency decisions of vast economic and political significance.'") (citing Utility Air Regulatory Grp. v. EPA, 134 S. Ct. 2427, 2444 (2014) (citation and internal quotation marks omitted)).

[11] For example, the order now claims that a broad definition of protected information is required to better align FCC rules with the FTC approach. Putting aside for a moment the fact that the FCC does not actually line up with the FTC approach in several key respects, the FCC cannot exceed the limits of the authority delegated to it by Congress. As one commenter noted: "The law is clear that an agency cannot 'use its definitional authority to expand its own jurisdiction.'" Comcast Comments at 68 (citing Am. Bankers Ass'n v. SEC, 804 F.2d 739, 754-55 (D.C. Cir. 1986)).

[12] Of course, IP addresses do not qualify as CPNI in any event, as commenters have demonstrated. *See, e.g.,* Comcast Comments at 77-81.

[13] *See, e.g.,* AT&T Oct. 17, 2016 *Ex Parte* at 4.

[14] *Id*.

[15] *See also* AT&T Comments at 108-113; CTIA Comments at 59-73.

[16] *See, e.g.*, Peter Swire, Associate Director, The Institute for Information Security & Privacy at Georgia Tech, et al., Working Paper, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* at 24-25 (filed May 27, 2016); EPIC Comments at 16 ("The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company."); Comcast Comments at 26-34; Verizon Comments at 16-24.

claims that broadband providers have unique or unparalleled access to customers and their information. The Commission's lame attempt at discounting the traffic subject to encryption does a disservice to common sense and ignores the plain fact that consumer traffic from the most popular Internet sites is already encrypted with more to come. Accordingly, to the extent that the rules rely on the faulty gatekeeper proposition, the Commission should be overturned for that reason alone.

The FCC claims that, in moving to a sensitivity-based framework, the rules will be "more properly calibrated to customer and business expectations." But requiring opt-in notice for web browsing history and application usage data is a significant departure from the FTC approach, which is the basis for current expectations.[17] Under the FTC approach, those categories have not been treated as sensitive. While this approach has been in effect, there has been no evidence of any privacy harms, and businesses have been able to "provide great value to consumers in the form of discounts, convenient features, and other new and innovative services."[18] Requiring opt-in consent for these categories will destroy that value and upend years of settled expectations, burdening rather than benefitting most users.[19]

It will also create confusion. Consumers will receive notices from the broadband providers asking them to opt in. If they do not opt in, but continue to see advertisements based on their web browsing and application usage, some will understandably assume that their broadband providers are violating their privacy policies when, in fact, the ads originate from third parties not subject to FCC rules.[20]

It is also unnecessary. As commenters pointed out, to the extent that web browsing history and application usage data concerns sensitive information, such as health or financial records, it is already covered by the other categories that the FTC, and now the FCC, consider to be sensitive.[21] Commenters also submitted documentation into the record showing how broadband providers and other Internet companies currently differentiate and avoid the use of sensitive web browsing and application usage information under the current FTC framework.[22] Therefore, there is no reason to adopt an added layer of sensitivity that sweeps too broadly.

---

[17] *See, e.g.,* ITTA Oct. 21, 2016 *Ex Parte* at 2-3 (noting that "Web browsing and app usage history are not considered sensitive by the FTC" that "the FTC's Privacy Report endorsed an opt-out approach towards web browsing data used for behavioral advertising" and that "[a]gainst the backdrop of the longstanding, embedded commercial practice of consumers benefiting from targeted advertising based on web browsing history, consumers do not have the same expectations of privacy in this context as they do with other categories of information.").

[18] T-Mobile Oct. 14, 2016 *Ex Parte* at 2. *See also, e.g.,* Comcast Comments at 26-34; Verizon Comments at 17-24.

[19] *See, e.g.,* Comcast Comments at 44-52; T-Mobile Oct. 14, 2016 *Ex Parte* at 1-2.

[20] *See, e.g.,* Comcast Comments at 43; ITTA Oct. 21, 2016 *Ex Parte* at 3.

[21] Comcast Comments at 43.

[22] *See, e.g.,* Internet Commerce Coalition Oct. 18, 2016 *Ex Parte* at 2-3 (describing how ISPs and Internet companies use a combination of "white lists" and "black lists" that "isolate and exclude data categorized as sensitive by the FTC"); AT&T Oct. 17 *Ex Parte* at 3 ("Like any other Internet company, a broadband provider can avoid the use of sensitive information by categorizing website and app usage based on standard industry interest categories established by the Interactive Advertising Bureau ('IAB') and other leading industry associations. This process involves correlating non-content web address or app information (e.g., visit to a sports website) with a pre-established "white list" of permissible interest categories (e.g., sports lover) available from the IAB. The list of interest categories can be refined as needed to exclude any sensitive categories."); American Association of Advertising Agencies et. al Oct. 21, 2016 *Ex Parte* at 2 ("[C]ompanies across the Internet, including ISPs, have for decades used a combination of administrative and technical controls to limit the use of sensitive data for marketing and advertising purposes, absent consumer consent. These practices were developed to comply with the FTC's privacy framework and the self-regulatory program administered by the DAA."); Future of Privacy Forum Reply at 8; Google Oct. 3, 2016 *Ex Parte* at 1; NCTA Oct. 20, 2016 *Ex Parte* at 3-5; INCOMPAS Oct. 21, 2016 *Ex Parte* at 3.

The order responds that it is better to be overinclusive because what is non-sensitive to most people could be sensitive to some. But, again, given that there has been no evidence of harm while this approach has been in effect at the FTC, there is no reason to re-draw the line in a way that will burden most consumers. That is not to say that privacy conscious consumers should have no remedy at all. Rather, they should be presented with clear notice of how their providers differentiate sensitive information and have the ability to opt out if they do not think methods are sufficient to protect them.[23]

The Commission must realize that an overly broad opt-in regime has significant consequences for consumers because "[i]t is well understood that an opt-in consent mechanism results in far fewer individuals conveying their consent than is the case under an opt-out consent mechanism" even when substantial benefits are at stake.[24] As one commenter noted: "In the marketing context, a rough rule of thumb is that opt-out consent mechanisms may yield approximately 82% or much higher of individuals preserving their consent, whereas an opt-in consent model may yield only approximately 18% or much lower of individuals consenting."[25] While the Commission anticipates that, in an opt-in regime, many consumers will wish to affirmatively exercise choice options, the "statistics on opt-in consent rates cited above show that this is not the case, and that many individuals will simply not pay attention to the choice or skip past it to get to the service."[26] This isn't consumer choice, it's recognition of consumer apathy.

Perhaps most troubling is that the order explicitly contemplates that it will apply to the Internet of Things. And, it makes this sweeping power grab without explaining how it has authority to do so. When I first cautioned that reclassifying broadband would lead to the FCC regulating edge providers and applications, some scoffed. Then it happened and now it is front and center again. Here, the FCC is refreshingly honest about its ambitions in this item, and I have every reason to expect that the Commission will make good on this vast new stake it has claimed. Those in the edge community should reconsider their belief that the FCC will never venture into their business models: The Commission is intentionally setting itself on a collision course with the FTC's definition with the intention to up the burdens on edge providers and all technology companies, either here or at the FTC.

The ultimate absurdity of these rules is that broadband providers remain free to purchase and use the information they need from those other Internet companies, including edge providers, because these other companies, not covered by the rules, will continue to operate under the FTC's opt-out regime. The rules prohibit a broadband provider from using sensitive "customer proprietary information" without opt-in consent, but "customer proprietary information" is limited to information that the provider "acquires in connection with its provision of telecommunications service." Information obtained from an edge provider does not meet that definition.[27]

Therefore, all that the FCC has really done is raise the transaction costs. The FCC, in its typical nanny state fashion, seems to assume that consumers prefer an opt-in regime. But when consumers find

---

[23] ITIF Oct. 20, 2016 *Ex Parte* at 2.

[24] Comcast Comments at 48; Technology Policy Institute Oct. 17, 2016 *Ex Parte* at 2 ("All available research suggests that opt-in consent dramatically reduces participation. Any data classified under opt-in is less likely to be available to support services, innovation, and competition, as we and others discussed in previous filings.") (citing Tom Lenard and Scott Wallsten, Technology Policy Institute, *An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking* (May 2016); Avi Goldfarb, Catherine E. Tucker and Liad Wagman, *Comments on Notice of Proposed Rule Making: 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services'* (May 20, 2016)).

[25] Comcast Comments at 48 (citing Mindi Chahal, *Consumers less likely to 'opt in' to marketing than to 'opt out,' Marketing Week* (May 7, 2014), https://www.marketingweek.com/2014/05/07/consumers-less-likely-to-opt-in-to-marketing-than-to-opt-out/).

[26] *Id.* at 52.

[27] And even if the Commission "fixed" the definition, it would still be precluded by the statute from placing restrictions on a broadband provider's purchase or use of third-party data. *See, e.g.,* Comcast Comments at 75-76.

out the end result is that they may have to pay more for heightened privacy rules that they never asked for, I doubt they will be grateful that the FCC intervened on their behalf. Indeed, this is a grandiose attempt to enact legacy talking points into rules so that Commission leadership can pat itself on the back while consumers receive no actual, practical protections. Added costs and burdens for providers? Yes. Benefits for consumers? No.

In another departure from the FTC framework and widespread consumer expectations, the order limits inferred consent to first party marketing within a service category, as well as the marketing of customer premises equipment (CPE) and "communications services commonly bundled together with the subscriber's telecommunications service." Here again, there is no rational reason to place undue restrictions on broadband providers.[28] While allowing providers to inform their customers about certain bundled offerings is a welcome change to the original, untenable draft, I would have extended inferred consent to the marketing of all products and services offered by broadband providers and affiliates as long as the affiliated relationship is clear to consumers.[29] Therefore, at a minimum, I would not require opt out consent to market new products and services that are "reasonably understood by customers as within the existing service relationship."[30] As the record demonstrated, consumers expect to receive information from their providers about new products, services, and discounts.[31] In addition, if broadband providers "cannot market new products and services on the same terms as online companies – or even other brick and mortar businesses – there will be less incentive to invest and develop new services."[32]

---

[28] *See, e.g.,* NCTA Oct. 20, 2016 *Ex Parte* at 8 ("The FCC has recognized that the statute permits carriers to use customer data to market products and services distinct from the underlying telecommunications service from which the data is collected. In interpreting the degree to which Section 222 accommodates first party marketing, the Commission stated that the relevant inquiry should focus on 'the customer's reasonable expectations of privacy in connection with CPNI.'") (citing *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, para. 41 (1999) (*1999 CPNI Order*)).

[29] *See* 2012 FTC Privacy Report at 41-42; Internet Commerce Coalition Oct. 18, 2016 *Ex Parte* at 4 (explaining that "first-party marketing of an ISP's other products and services should be permissible based on implied consent, as both the FTC and Administration have previously concluded"); NCTA Oct. 20, 2016 *Ex Parte* at 8 (noting that "both the FTC and White House privacy frameworks afford companies flexibility to use customer data to engage in first-party marketing and advertising of their own services based on implied consent") (citing 2012 FTC Privacy Report at 40 ("[M]ost first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice"); The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 17 (2012) ("[C]ompanies may infer consent to use personal data to conduct marketing in the context of most first-party relationships, given the familiarity of this activity in digital and in person commerce, the visibility of this kind of marketing, the presence of an easily identifiable party to contact to provide feedback, and consumers' opportunity to end their relationship with a company if they are dissatisfied with it.")); ITTA Oct. 21, 2016 *Ex Parte* at 2-3.

[30] AT&T Oct. 17, 2016 *Ex Parte* at 2 (*1999 CPNI Order*, 14 FCC Rcd 14409, para. 42). *See also* NCTA Oct. 20, 2016 *Ex Parte* at 8; ITTA Oct. 21, 2016 *Ex Parte* at 2-3.

[31] *See, e.g.,* Cox Communications Inc. October 20, 2016 *Ex Parte* at 2 ("Regulatory authorities and experts recognize first-party marketing is a wide-spread practice and a well understood tool for establishing and maintaining . . . customer relationships. Both the FTC and the White House privacy frameworks specifically recognize this commonly accepted practice and permit companies to use customer data to communicate with their customers and personalize their customers' experience based on the customer's implied consent in most instances. Even existing FCC CPNI rules permit carriers to use CPNI to engage in some first-party marketing, without customer approval. Regulating such activities here would be unprecedented and would not reflect customers' current expectations of their broadband providers: to anticipate what they want and when they want it, to provide maximum value, and then tell them about it.") (citations omitted); NCTA Oct. 20, 2016 *Ex Parte* at 7-8 (also noting that broadband providers are new entrants to many products and services offered by large edge providers).

[32] Cox Communications Inc. October 20, 2016 *Ex Parte* at 3.

In addition, I was appalled to see a case-by-case approach imported to review mislabeled "pay for privacy" offers. These are consumer incentives offered every day in the real world and now ISPs will need to obtain a blessing from an agency that has no privacy experience.[33] The result is that broadband providers will be reluctant to extend, and may even forgo, valuable offers and discounts that consumers would want for fear that they will fall into another zero-rating style abyss. From that experience, we know that the game is perpetually on hold awaiting heavenly intervention, and some players have just stopped playing. Trying that again here in the privacy context does not make any sense, unless the real intention is to effectively ban pay for privacy offers without actually saying so in an attempt to avoid a legal challenge.

Moreover, I reject the Commission's effort to insert itself into mandatory arbitration clauses by committing to initiate a proceeding on the issue. As commenters explained in the record, mandatory arbitration clauses have benefitted both companies and consumers. In particular, "[m]ultiple studies have found that consumers obtain relief in arbitration at rates higher than they do in court, while being less costly and time-consuming for consumers than litigation."[34] I have heard the argument that eliminating these clauses will enable consumers to band together in class action lawsuits, but that is unrealistic. The fact-specific nature of many of the disputes that end up in arbitration – such as an incorrect bill – do not lend themselves to class certification.[35]

Any foray into mandatory arbitration clauses is unlikely to withstand legal challenge, so committing to initiate a proceeding is a complete waste of Commission resources. Under the Federal Arbitration Act (FAA), any "written provision in any . . . contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction . . . shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract."[36] Supreme Court precedent has made clear that Congressional intent to override the FAA can only be demonstrated through a "contrary congressional command" that is "discernible from the text, history, or purposes of the statute" and it must be explicit.[37] Accordingly, "given the stringency of this test, the Supreme Court has never held that any federal statute overrides the FAA."[38] And nothing in section 222 or the Communications Act generally meets that high hurdle.[39] In short, the Commission would be asking for another muni broadband style reversal.

Shifting to data security and data breach, I recognize that the Commission has significantly moved away from the irrationally strict and unworkable proposals in the NPRM by adopting a reasonableness standard for data security and a harm-based approach for data breach notifications.

---

[33] Technology Policy Institute Oct. 17, 2016 *Ex Parte* at 1 ("Requiring regulatory approval for new business models is likely to reduce experimentation, and reducing the number of potential methods of paying for service is likely to harm consumers."); Nokia Oct. 14, 2016 *Ex Parte* at 2 (describing the benefits of such offers).

[34] Verizon Oct. 21, 2016 *Ex Parte* at 2. *See also* CTIA Comments at 50-55.

[35] *See* CTIA Comments at 50 ("Most wrongs suffered by wireless consumers are relatively small and individualized, involving excess charges on a bill, a defective piece of equipment, or the like. These claims are simply too small to justify paying a lawyer to handle the matter and, in any event, most consumers do not have the resources to do so—and a lawyer is needed to navigate the complicated procedures that apply in court. And claims of this sort cannot be brought as class actions because they involve facts specific to an individual consumer's situation. . . . For this large category of consumer claims, arbitration provides the only realistic option for obtaining a fair resolution of the dispute.").

[36] Verizon Oct. 21, 2016 *Ex Parte* at 2 (citing 9 U.S.C. § 2).

[37] CTIA Comments at 56 (citing Shearson/Am. Express, Inc. v. McMahon, 482 U.S. 220, 226-227 (1987); CompuCredit Corp. v. Greenwood, 132 S. Ct. 665, 673 (2012)).

[38] CTIA Comments at 56.

[39] *See, e.g.,* Verizon Comments at 74; CTIA Comments at 56-58.

However, the Commission still lacks authority to adopt all of these rules, and I remain concerned that the Commission is not giving providers sufficient time to come into compliance.[40] Even the larger providers requested at least 12 months,[41] but the Commission does not even afford the smallest providers that much time. The training and auditing alone could take more time than what is given. If it is so important to act on data security and data breach notifications, then the Commission should at least ensure that it is done right rather than right now.

As a whole, this order places substantial, unjustified costs on businesses and consumers. Had the FCC conducted a cost-benefit analysis, which it committed to do but failed to live up to once again, it would have been unable to justify adopting these significant additional restrictions. Given that consumer privacy has been adequately protected under the current FTC framework and that there has been no evidence of any privacy harms, there is no benefit to be gained from increased regulation. On the other hand, there are substantial costs, including the increased transaction costs to purchase the information from unregulated Internet companies that will ultimately be passed on to consumers, the lost opportunity and revenues for broadband providers precluded from competing against Internet companies in the online advertising space, the foreclosure of innovative services that providers won't be able to offer and consumers won't receive, and the costs to consumers themselves who will be forced to participate in the opt-in regime and will pay more as a result.

While there are some statements about changes made to reduce compliance costs (i.e., one type of cost that is reviewed, in part, by the Office of Management and Budget), there is no overall analysis of the costs and benefits of this order. To the extent Commission leadership promised that rulemakings would serve as cost-benefit analyses, which I have explained is not adequate to comply with the relevant Executive Orders in any event, this order never engages in a serious discussion of the costs raised by commenters, failing to deliver even on that meager promise.

Finally, I want to point out that, despite my fundamental objections to this item based on the lack of statutory authority to adopt broadband privacy rules, I was willing to try to find common ground on specific issues, including the treatment of web browsing and app usage information, in order to mitigate the most harmful aspects of the order. My overtures were completely rebuffed by my colleagues. If anyone thinks that the only thing standing in the way of a more bipartisan Commission is an intransigent Commission minority, then this proceeding has proven, once again, that is absolutely incorrect.

[40] *See, e.g.,* WISPA Comments at 27-28 (seeking a two-year extension for all the Commission rules); ITTA Sept. 30, 2016 *Ex Parte* at 3 (same).

[41] *See, e.g.,* Verizon Sept. 23, 2016 *Ex Parte* at 1 ("Once rules are adopted, providers must go through an extensive and complex implementation process. Specifically, providers must perform an assessment of their existing processes and systems to determine what changes must be made; review, update, and negotiate supplier and other contracts; update written requirements documents; research, design, code, and test updates to customer care, self-serve, and back-office applications and systems; train employees and suppliers; draft customer communications; develop notice methods and periods; and set up a system for ensuring ongoing compliance. These actions will take a significant amount of time to complete, requiring approximately 18 months from the date rules are adopted.").