Brownstein Hyatt Farber Schreck

October 27, 2017

Michael H. Pryor
Attorney at Law
202.383.4706 tel
202.296.7009 fax
mpryor@bhfs.com

VIA ELECTRONIC FILING

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Restoring Internet Freedom, WC Docket No. 17-108

Dear Ms. Dortch:

In its previous comments in this proceeding, ADT Corporation ("ADT") urged the Commission to maintain core net neutrality protections to ensure that wireline or wireless broadband providers transmit alarm data over their broadband connections quickly and accurately.[1] ADT thus supports efforts to prevent blocking or throttling (or any form of degradation) of lawful applications and content, and to bar discrimination by precluding anticompetitive prioritization schemes that would favor broadband affiliated operations, including alarm monitoring services.[2] At the same time, ADT has advocated for a "light touch regulatory approach."[3]

In this ex parte letter, ADT proffers a reasonable, limited jurisdictional basis to underpin the Commission's authority to continue such protections for independent alarm companies. Specifically, the Commission has ancillary jurisdiction to adopt these specific net neutrality protections based on the Commission's mandated responsibility in Section 275 of the Act to prevent discrimination against alarm companies by network providers themselves engaged in the provision of alarm monitoring. Section 275's nondiscrimination obligations apply to Bell Operating Companies ("BOCS"), Incumbent Local Exchange Carriers ("ILECs"), Local Exchange

[1] Comments of the ADT Corporation, WC Docket 17-108, at 2 (July 17, 2017). ("ADT Comments").
[2] A number of broadband providers have agreed to abide by these core net neutrality protections, including codifying them pursuant to the Commission's authority under section 706. *See, e.g.,* Comments of AT&T, WC Docket 17-108 at 102-103 (July 17, 2017) ("AT&T Comments"); Reply Comments of Verizon, WC Docket 17-108, at 15 (Aug. 30, 2017). In this ex parte submission, ADT proffers an alternative basis of jurisdiction to apply such protections to the ensure that vital, public safety transmissions are protected and to preserve competition in the alarm monitoring industry.
[3] ADT Comments at 5.

Carriers ("LECs"), and, importantly, to their affiliates providing broadband internet access service ("BIAS"). ADT requests that the Commission use its ancillary authority to prevent discrimination against alarm companies by all BIAS providers offering competing services, not just those affiliated with traditional telecommunications carriers.

The nondiscrimination protections requested here are narrowly targeted to the alarm industry and reflect the unique status afforded the industry by Congress, the courts and this Commission. Codification of the net neutrality rules described above - no blocking, no throttling, and no anticompetitive prioritization of alarm data - does not require the Commission to classify broadband providers under Title II nor would it confer common carrier status. ADT is simply seeking to extend to broadband networks the unique pro-competitive protections that Congress and this Commission have long afforded the alarm monitoring industry in order to preserve those protections as traditional wireline connections to homes and offices are rapidly replaced by wireline and wireless broadband connections.

Background

ADT provides alarm monitoring services to approximately 7 million homeowners and businesses. Increasingly, ADT's services are connected to homes and businesses over wireline or wireless broadband internet access services or BIAS.

While small packets of alarm data can run over traditional copper lines or over cellular networks, broadband service is generally required for ADT's enhanced Pulse® alarm service that allows customers to view security camera footage, remotely arm and disarm their systems, and lock and unlock their doors. The need for security cameras is growing, as some large municipalities, including Detroit, Las Vegas, Milwaukee and Salt Lake City, have adopted verified response policies where video or on-the-ground confirmation of an emergency is required before police and/or fire departments will respond to the alarm.

Today, approximately 70% of ADT's new customers opt for it's Pulse® service when they sign up with ADT, growing the percentage of ADT's alarm monitoring customers that rely on broadband connections to protect their families, homes and businesses by leaps and bounds. Many of those BIAS providers are also fierce competitors for alarm and home monitoring services. This creates the classic discrimination paradigm that has animated competition policy since the breakup of AT&T -- network providers have the incentive and the ability to discriminate against companies in the same line of business as the network provider.[4]

[4] *See, e.g., United States v. AT&T*, 552 F. Supp. 131, 189 (D.D.C.1982), *aff'd sub nom. Maryland v. United States*, 460 U.S. 1001 (1983) (barring Bell Operating Companies from providing information services, such as alarm monitoring, because of their ability and incentive to discriminate against competing information service providers). The court ultimately lifted the information services line of business restriction, noting the Department of Justice's determination that the protections afforded by the FCC's *Computer Inquiry* nondiscrimination rules minimize risk. *U.S. v. Western Elec. Co.* 767 F. Supp. 308 (D.D.C. 1991).

ADT's Alarm Data Has Been Blocked by ISPs

Concerns that BIAS providers would interfere with ADT's transmissions are not merely theoretical. Broadband providers have blocked ADT's data, preventing ADT's customers from using enhanced alarm monitoring features such as remote operation through smart phone apps and video surveillance. In 2015, a large swath of ADT's customers in Puerto Rico using a specific broadband internet access service provider suddenly lost the ability to use ADT's Pulse® service, ADT's home automation service that enables customers to control their alarm systems remotely or to access their video surveillance cameras. Upon being approached by ADT's technicians, the ISP initially disclaimed any responsibility, notwithstanding that all of ADT's customers using this ISP lost Pulse® service. Further analysis showed that, in fact, this ISP was blocking a critical timing port that rendered the service unusable. The issue took nearly two-and-a-half months to resolve, during which time ADT's customers were without this service and ADT stopped offering the service to residential and business customers using this ISP's internet service. This blocking occurred during a time that net neutrality rules were not in effect. Service was finally restored after the net neutrality rules were released and were about to be implemented.

A similar instance occurred in 2016. A smaller, mainland ISP blocked certain ports shutting down ADT's customers' ability to utilize Pulse® services. This ISP, however, was more responsive and the blocking was resolved after approximately two-and-a-half weeks. It is noteworthy that this incident occurred during a time that the no-blocking rule was in effect.[5]

ADT does not have evidence to suggest that these instances of blocking were the result of a specific intent to discriminate against ADT. The ISP that blocked services in Puerto Rico did not provide competing alarm monitoring services although the mainland ISP described in the second example did offer competing services. Whether there was an in intent to harm ADT, however, is of no particular importance to ADT's customers who were without the ability to utilize ADT's services for an extended period of time, substantially diminishing their ability to protect themselves or their property. What is clear, however, is that no BIAS provider would block its own alarm monitoring customers' service for any extended period of time.

These examples illustrate the need for a no blocking rule that ensures that ADT's services will be treated the same as an ISP's own alarm monitoring services and indicates that the existence of such a rule provides a strong incentive quickly to address network issues as they arise. If ADT, the country's largest alarm monitoring provider cannot resolve a blocking issue for months, the many thousands of much smaller alarm monitoring providers will have little hope to withstand ISP blocking or anticompetitive conduct in the absence of readily enforceable net neutrality rules and their deterrent effect.

[5] Other, more isolated instances of blocking have also occurred. In at least four instances in the past year, ADT's customers' ability to use Pulse was blocked by the ISP. One instance involved alarm monitoring services to a retirement community and another involved such services at a dentist's office.

The Courts, the Congress and the FCC Have All Protected Alarm Monitoring Companies from Potential Anti-competitive Behavior of Network Providers

The Commission has long regulated the alarm monitoring services provided by the Bell Operating Companies (BOCs) and incumbent local exchange carriers to ensure that they are not given unfair advantages. Under *Computer III*, for example, the Commission regulated BOC-provided alarm monitoring services as enhanced services subject to the *Computer III* non-discrimination safeguards.[6] Bell companies engaged in the provision of alarm monitoring services were required to submit comparably efficient interconnection (CEI) plans spelling out how they would make underlying transmission facilities available to competing alarm providers on a nondiscriminatory basis.[7]

Concern that BOCs and incumbent local exchange companies would discriminate against competing alarm monitoring companies carried over to the 1996 Act. Section 275 of the 1996 Act contains numerous protections for independent alarm monitoring companies from possible anticompetitive behavior of competing network providers. These protections include: banning Bell Operating Company entry into the alarm services market for the first five years after the passage of the 1996 Act;[8] barring ILECs from using local service revenues directly or indirectly to subsidize their alarm monitoring services;[9] and, barring LECs from using for marketing purposes the information they derive from transmitting alarms or calls to the alarm monitoring centers of independent alarm companies.[10]

A central protection of section 275 is its nondiscrimination obligation. It requires ILECs "engaged in the provision of alarm monitoring services" to "provide nonaffiliated entities, upon reasonable request, with the network services it provides to its own alarm monitoring operations,

---

[6] *In the Matter of Implementation of the Telecommunications Act of 1996: Telemessaging, Electronic Publishing, and Alarm Monitoring Services*, 12 FCC Rcd 3824, 3844, ¶ 45 (1997)(*Alarm Monitoring Order*) ("Prior to the Act, alarm monitoring services were regulated as enhanced services and were subject to the nondiscrimination requirements established under the Commission's *Computer II* and *Computer III* regimes."). That order recognized that, after the 1996 Act, alarm monitoring services that had been designated as enhanced services would also be information services. *Id.* at 3826, ¶ 4, n. 10. The Commission ruled that section 275 conferred jurisdiction over intrastate alarm services, as well as interstate services, and preempted inconsistent state regulations. *Id.* at 3828, ¶ 8, 3831, ¶ 16.

[7] *See, e.g., Bell Operating Companies Joint Petition for Waiver of Computer II Rules*, 10 FCC Rcd 13758, 13769, ¶ 72(1995) (approving Ameritech's CEI plan for its "SecurityLink" alarm monitoring services).

[8] 47 U.S.C. § 275(a) (barring BOCs or their affiliates from entering the market for five years, subject to grandfathering of existing services).

[9] 47 U.S.C. § 275(b)(2).

[10] 47 U.S.C. § 275(d). *See also*, 11 FCC Rcd 9553, 9557 ¶ 9 (1996)(interpreting section 275 to preclude use of alarm-related customer proprietary network information ("CPNI") for marketing, even if the LECs' customer otherwise granted authorization to obtain CPNI generally). Section 275, similar to the overall structure of the Act, imposes various obligations on BOCs, ILECs and LECs. For example, whereas Section 275 empowers the Commission to enjoin harmful discriminatory conduct by all ILECs and their affiliates, (§ 275(c)), only BOCs were prevented from market entry for the first five years (§275 (a)(1)).

on nondiscriminatory terms and conditions."[11] The Commission has determined that the non-discrimination ban in section 275 is a more stringent standard than that found in sections 201 and 202 of the Act because section 275's nondiscrimination standard is not qualified by the terms unjust and unreasonable.[12] To ensure swift relief, Congress adopted an expedited, 120-day complaint process for independent alarm companies to bring complaints for violations of the non-discrimination and cross subsidization provisions.[13] Congress also specifically distinguished between alarm monitoring service, which, as noted, the Commission has long defined as an enhanced or information service, and the underlying transmission facilities "of a local exchange carrier or one of its affiliates" used to transmit the alarm signal.[14]

The Commission Should Use its Ancillary Authority To Bar BIAS Providers from Discriminating Against Unaffiliated Alarm Monitoring Services

The clear intent of Congress and the Commission is to protect alarm companies from unfair competition by providers of the network service upon which they depend. Section 275 is a "specifically delegated power" directing the Commission to ensure nondiscriminatory treatment of alarm companies.[15] During the *Computer Inquiry* proceedings through passage of the 1996 Act, concerns about discriminatory treatment centered on the Bell companies and local exchange carriers, which were the primary, if not sole, providers of transmission capacity for alarm companies. Today, alarm data is increasingly likely to traverse broadband wireline or wireless networks, whether provided by ILECs (and their affiliates) or other BIAS providers.

The underlying competitive concern nevertheless remains the same. Broadband internet access service providers that engage in the provision of alarm monitoring service have the same incentive and ability to discriminate in favor of their own alarm monitoring services as do the BOCs, ILECs, or LECs operating TDM networks. To preserve the protections against anti-competitive discrimination, the Commission should use its ancillary authority to extend Section 275 to all BIAS providers, both wireline and wireless. Barring broadband providers from blocking, throttling or engaging in anticompetitive prioritization are the net neutrality equivalents

[11] 47 U.S.C. § 275(b)(1). In the 1997 *Alarm Monitoring Order*, the Commission interpreted the term "network services" to include all "telecommunications services" used by the ILEC for its own alarm monitoring services, and did not require ILECs to provide "information services" because "there is little danger of discrimination in the provision of such services." *Alarm Monitoring Order*, 12 FCC Rcd at 3848, ¶ 54. This justification for excluding "information services," based on 1997 access technologies has little application today when ILEC and non-ILEC affiliated BIAS providers offer their own monitoring services over their broadband connections.
[12] *Alarm Monitoring Order*, 12 FCC Rcd at 3848, ¶ 53.
[13] 47 U.S.C. § 275(c).
[14] 47 U.S.C. § 275(e). This provision defines "alarm monitoring service" as "a service that uses a device located at a residence, place of business, or other fixed premises – (1) to receive signals from other devices located at or about such premises regarding a possible threat to such premises to life, safety or property, from burglary, fire, vandalism, bodily injury, or other emergency; and (2) to transmit a signal regarding such threat by means for transmission facilities of a local exchange carrier or one of its affiliates to a remote monitoring center to alert a person at such center of the need to inform the customer or another person or police, fire, rescue, security, or public safety personnel of such threat." This definition excludes medical monitoring devices attached to an individual.
[15] *Comcast Corp. v. FCC*, 600 F.3d 642, 659 (D.C. Cir. 2010).

of section 275's obligation to provide network access on "nondiscriminatory terms and conditions."

Extending section 275 to broadband providers is hardly a stretch. Section 275 already applies to the broadband affiliates of ILECs and LECs, no matter how those broadband affiliates are classified. Section 275 encompasses all affiliates of such entities and bars them from violating this section.[16] The plain language of 275 applies to "affiliates" without limitation and the Act defines affiliates as "a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person. For purposes of this paragraph, the term 'own' means to own an equity interest (or the equivalent thereof) of more than 10 percent."[17] It requires no great jurisdictional leap to go from regulating ILEC and LEC-affiliated broadband providers to regulating other broadband providers that also compete with alarm companies.

Extension of Section 275 to Broadband Providers is the Paradigmatic Use of Ancillary Jurisdiction.

Relying on the express authority of section 275 to regulate broadband providers' treatment of competing alarm companies readily meets both prongs of the ancillary jurisdiction test: (1) the subject of the regulation must be covered by the Commission's general grant of jurisdiction under Title 1 of the Communications Act; and (2) the subject of the regulation must be "reasonably ancillary to the effective performance of [the Commission's] statutorily mandated responsibilities."[18] As to the first prong, the transmission of alarm signals over broadband networks easily falls within the Commission's general grant of jurisdiction over "all interstate and foreign communication by wire or radio."[19]

The second part of the test, which is generally the central point of contention in analyzing ancillary jurisdiction, is also easily met. The subject of the regulation at issue is nondiscriminatory access to network services for unaffiliated alarm monitoring service providers. Section 275 confers upon the Commission the "statutorily mandated responsibilit[y]" to protect the independent alarm industry from harmful discrimination by competing network providers. The effective performance of this responsibility requires that not only traditional LECs and their affiliates (including broadband affiliates) refrain from discrimination, but that all network operators provide independent alarm companies access to the same network services used by their own alarm monitoring operations on nondiscriminatory terms and conditions. As more and more

[16] *See, e.g.,* 47 U.S.C. § 275 (a) (No Bell operating company *or affiliate* thereof . . .); *id.*at § 275(c) (if a complainant makes an appropriate showing of a discrimination violation, the Commission shall order the ILEC "*and its affiliates*" to "cease engaging in such violation"); *id.* at§ 275(e) (alarm monitoring service is transmitted "by means of transmission facilities of a local exchange carrier *or one of its affiliates*.") (emphasis added to all citations).
[17] 47 U.S.C. § 153(1).
[18] *Comcast Corp. v. FCC*, 600 F.3d 642, 644 (D.C. Cir. 2010) (*quoting Am. Library Ass'n. v FCC*, 406 F.3d 689, 692 (D.C. Cir. 2005)).
[19] 47 U.S.C. § 152(a).

homes and businesses use broadband connections, ensuring that broadband providers offer nondiscriminatory access is needed to "prevent the frustration of a regulatory scheme expressly authorized by statute."[20] As AT&T noted in its comments, "the Commission could invoke ancillary authority to prohibit an ISP from anticompetitively excluding online services that directly compete with its own regulated services whenever doing so 'is necessary to further [the Commission's] regulation of activities over which it [has] express statutory authority' under Titles II, III or IV."[21]

Finally, to effectuate the Commission's responsibilities under Section 275, the Commission should preclude discrimination against competing alarm companies whether the alarm customer is a residential customer or an enterprise customer, notwithstanding prior Commission determinations that defined the broadband internet access service subject to net neutrality regulation as a mass market service limited largely to residential consumers, small business and schools and libraries.[22] Businesses rely on ADT and other alarm monitoring services to prevent theft or to protect property and section 275 does not distinguish between residential or business alarm customers.

Applying the section 275 nondiscrimination obligation to broadband providers would not confer on them common carrier status. As explained by the D.C. Circuit in *Verizon* when striking down the FCC's efforts to use ancillary jurisdiction to impose a general nondiscrimination standard in the *2010 Open Internet Order*,[23] a general common carriage obligation is readily distinguishable from a more narrow carriage obligation designed to "remedy[] a specific perceived evil."[24] The Court articulated the distinction by contrasting the broad nondiscrimination rule proposed in the *2010 Open Internet Order*, with the specific and targeted nondiscrimination obligation sustained in *Southwestern Cable.*

> *Southwestern Cable* involved a Commission rule that, among other things, compelled cable operators to transmit the signals of local broadcasters when cable operators imported the competing signals of other broadcasters into the local service area. Such a rule is plainly distinguishable from the *Open Internet Order*'s anti-discrimination rule because the *Southwestern Cable* regulation imposed no obligation on cable operators to hold their facilities open to the public generally, but only to certain specific broadcasters if and when the cable operators acted in ways that might harm those broadcasters. As the

[20] *See, e.g., Comcast Corp. v. FCC*, 600 F.3d 642, 656 (D.C. Cir. 2010) (contrasting lack of identifiable statutory authority to impose common carrier obligations on information service providers with the Commission's *Computer II Order*, which "like the Supreme Court viewed the regulations at issue in S*outhwestern Cable* – as regulation of services otherwise beyond the Commission's authority in order to prevent frustration of a regulatory scheme expressly authorized by statute.")
[21] AT&T Comments at 109.
[22] *See, e.g., In the Matter of Protecting and Promoting the Open Internet*, Report and Order, 30 FCC Rcd 5601, 5683 ¶ 189 (2015).
[23] *In the Matter of Preserving the Open Internet*, Report and Order, 25 FCC Rcd 17905 (2015) (*2010 Open Internet Order*).
[24] *Verizon v. FCC*, 740 F.3d 623, 656 (D.C. Cir. 2014) .

> Court later explained in *Midwest Video II*, the *Southwestern Cable* rule "was limited to remedying a specific perceived evil," and "did not amount to a duty to hold out facilities indifferently for public use." The *Open Internet Order*'s anti-discrimination provision is not so limited, as the compelled carriage obligation applies in all circumstances and with respect to all edge providers.[25]

Imposing a requirement on BIAS providers to provide network facilities to competing, unaffiliated alarm monitoring companies does not compel carriage in all circumstances or to all edge providers. Rather, like *Southwestern Cable*, applying section 275 to BIAS providers would only require nondiscriminatory network access to a narrowly defined group, competing alarm companies, and would do so only to prevent harm to those alarm companies.

To Effectuate the Congressional Scheme, the Commission Should Also Apply Section 275's Expedited Complaint Process

A number of broadband providers have already promised to abide by net neutrality rules similar to those requested here by ADT to protect alarm companies from discrimination– no blocking, no throttling and no anti-competitive prioritization.[26] Providers have also noted that such promises would be enforceable by the Federal Trade Commission.[27] The Commission too has asked whether concerns about discriminatory or anticompetitive behavior would be sufficiently addressed through enforcement of the anti-trust laws.[28]

These remedies are not sufficient, however, to effectuate the specific statutory scheme entrusted to the Commission to protect alarm monitoring service providers. Congress established a specific expedited enforcement process for alarm companies. This process, set forth in section 275(c), is designed to provide prompt relief to an alarm company suffering "material financial harm" as a result of discriminatory treatment. The Act requires the Commission to issue an order to stop discriminatory behavior within 60 days of receiving a complaint that contains "an appropriate showing that the alleged violation occurred" and to make a final determination within 120 days.[29]

Section 275's expedited complaint process is an integral component of that section's non-discrimination protections. The promise of quick enforcement, including an order enjoining

---

[25] *Verizon v. FCC*, 740 F.3d 623, 656 (D.C. Cir. 2014) (citations omitted).
[26] *See, e.g.*, Comments of AT&T Corp., WC Docket 17-108, at 101 (July 17, 2017)(supporting a set of bright-line rules that prohibit blocking and throttling that reflect "long-standing industry norms and are thus essentially cost free); Comments of ACA, WC Docket 17-108, at 67-68 (July 17, 2017); Comments of Frontier Communications Corp. WC Docket 17-108, at 5-6 (July 17, 2017); Comments of Verizon, WC Docket 17-108, at 4 (July 17, 2017)("Verizon Comments"); Comments of Comcast Corporation, WC Docket 17-108, at 52 (July 17, 2017) (supporting prohibiting blocking, throttling and anticompetitive paid prioritization).
[27] *See, e.g.*, Verizon Comments at 15-17.
[28] *See, e.g., In the Matter of Restoring Internet Freedom*, Notice of Proposed Rulemaking, 32 FCC Rcd 4434, 4460 ¶ 78 (2017).
[29] 47 U.S.C. §275(c).

discriminatory conduct within 60 days, provides a strong deterrent to such behavior. It precludes the ability of larger, more powerful companies to defeat complaints through litigation by attrition strategies. The availability of an FCC-enforced expedited complaint process is particularly crucial for the thousands of smaller alarm companies that have neither the resources nor the staying power to litigate a drawn-out complaint process. The Commission's exercise of ancillary jurisdiction to apply Section 275's non-discrimination obligations to broadband providers should therefor include that section's tailored enforcement provisions as well, ensuring consistent treatment across all network providers that are also offering competition alarm monitory services.

The Commission Should Also Bar Use of Alarm Information for Marketing Purposes

Section 275 also bars "local exchange carriers" from using independent alarm company data to market their own or any other entity's, affiliated or unaffiliated, alarm services. Specifically, section 275(d) states that "local exchange carriers may not record or use in any fashion the occurrence or content of calls received by providers of alarm monitoring services for the purposes of marketing such services on behalf of such local exchange carrier, or any other entity."[30] Unlike other provisions of section 275, the marketing rule in this subsection (d) applies to all LECs, regardless of whether they are providing their own alarm monitoring service. In implementing this subsection, the Commission concluded that a LEC may not use the information identified in section 275, even if the customer had authorized access to his or her customer proprietary network information ("CPNI") under section 222(c) of the Act.[31]

As with other protections in section 275, the ban on using alarm data for marketing purposes should be applied to BIAS providers using ancillary jurisdiction. To be meaningful, the Commission should also take into account the particular opportunities for anticompetitive conduct that can occur when an alarm customer switches to broadband. Broadband providers should not be allowed to use the switch as an opportunity to market or promote its own alarm services by misrepresenting that the existing alarm company's services will not function on the broadband connection or will not function as well over the broadband connection than the BIAS provider's own monitoring services. Such assertions would violate the spirit of the nondiscrimation requirements.

The Commission Should Prohibit All Network Providers from Blocking Critical Public Safety Transmissions

Blocking or throttling of alarm monitoring data should not be tolerated by any network provider, regardless if they offer a competing alarm monitoring service. Blocking or throttling, in this context has life threatening consequences. ADT thus respectfully requests that the

[30] 47 U.S.C. § 275(d).

[31] *See, In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information; Use of Data Regarding Alarm Monitoring Service Providers*, Report and Order, 11 FCC Rcd, 9553, 9557, ¶ 9 (1996). The Commission did not otherwise adopt regulations implementing this provision's statutory bar finding that it was "clear on its face." *Id*. at 9558, ¶ 10.

Commission bar all blocking and/or throttling of alarm monitoring data. Using ancillary jurisdiction to apply section 275's nondiscrimination standard may not address instances of blocking by network providers that do not offer their own alarm monitoring services, but the consequences of blocking and throttling are no less severe, as the example of blocking effecting ADT's customers in Puerto Rico demonstrates. The Commission has frequently relied on ancillary jurisdiction to apply non-economic forms of regulation, including vital public safety regulations, to ensure the consumers remain protected when using communication services not classified as telecommunications services.[32] Alarm monitoring services are a critical component of the nation's public safety communications infrastructure. Today's technology enables the use of safety-enhancing functionality, such as that provided by ADT's Pulse® services, that utilize broadband connections. The Commission should ensure that these functions remain fully available to consumers who depend on reliable service to protect their homes and property.

Specific Rules

In light of the foregoing, ADT proposes that the Commission utilize its ancillary jurisdiction and adopt the following rules to protect the alarm industry:

1. A person engaged in the provision of broadband internet access service, insofar as such person is engaged, and to the extent such person, directly or through an affiliate, is also engaged in the provision of alarm monitoring services, shall not block, throttle, impair or degrade the transmission of alarm monitoring data of an unaffiliated alarm monitoring service provider.

2. A person engaged in the provision of broadband internet access service, insofar as such person is engaged, and to the extent such person, directly or through an affiliate, is also engaged in the provision of alarm monitoring services, shall not engage in prioritization with respect to such services. Prioritization refers to the management of a broadband provider's network to directly or indirectly favor its alarm monitoring service over that of an unaffiliated alarm monitoring service provider.

3. A person engaged in the provision of broadband internet access service, insofar as such person is engaged, shall not record or use in any fashion the occurrence or contents of calls received by providers of alarm monitoring services for the purpose of marketing such services on behalf of such broadband internet access service provider, or any other entity. No broadband internet access service provider shall misrepresent to an existing customer of an unaffiliated alarm

[32] *See, e.g., IP-Enabled Services and E911 Requirements for IP-Enabled Service Providers*, First Report and Order, 20 FCC Rcd 10245, ¶ 26 (2005)("We find that regardless of regulatory classification, the Commission has ancillary jurisdiction to promote public safety by adopting E911 rules for interconnected VoIP services."), *aff'd sub nom. Nuvio Corp. v. FCC*, 473 F.3d 302 (D.C. Cir. 2006); *Proposed Extension of Part 4 of the Commission's Rules Regarding Outage Reporting to Interconnection Voice Over Internet Protocol Service Providers and Broadband Service Providers*, Report and Order, 27 FCC Rcd 2650, 2678, ¶ 66 (2012) ("VoIP Outage Order") (concluding that "the Commission has ancillary authority to ensure both that interconnected VoIP providers fulfill their duty to provide 9-1-1 services and to address major obstacles to their doing so, such as failures in underlying communications networks.")

monitoring service that: (a) such service is incompatible with the internet access service or (b) that such internet access service will be provisioned in a manner that provides superior network performance for the broadband internet access service provider's own alarm monitoring service.

4. A person engaged in the provision of broadband internet access services, insofar as such person is engaged, shall not block or throttle alarm monitoring data.

Please contact the undersigned if you have any questions.

Sincerely,

/s/ Michael H. Pryor

Michael H. Pryor
Brownstein, Hyatt, Farber, Schreck, LLP
1155 F Street NW, Suite 1200
Washington, DC 20004
Telephone: (202) 383-4706

cc: Amy Bender (via email)
Travis Litman (via email)
Jay Schwarz (via email)
Claude Aiken (via email)
Jamie Susskind (via email)

MHP:kjs