

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

In the Matter of	)	
	)	
Matter of Restoring Internet Freedom	)	WC Docket No. 17-108
	)	
	)	
	)	

**COMMENTS OF THE ADT CORPORATION**

The ADT Corporation (“ADT”) submits these Comments in response to the Federal Communication Commission’s Notice of Proposed Rulemaking (“Notice”) in the Restoring Internet Freedom proceeding. ADT appreciates the opportunity to assist the Commission consider ways to “benefit consumers through greater innovation, investment and competition.”<sup>1</sup>

ADT is the nation’s largest provider of home and business automation and alarm monitoring services in the United States and Canada, serving more than seven million residential and commercial customers. ADT offers a wide range of services for: i) residential security, including burglar alarm monitoring, fire and smoke monitoring, carbon monoxide monitoring, flood and temperature monitoring, panic buttons, and video; ii) small and large businesses, including intrusion detection and monitoring, access control systems and management, video surveillance, and automated business control tools; iii) home and business automation; and iv) home health, including push of a button assistance and 24/7 monitoring. Nationwide, there are six ADT-operated monitoring centers, which provide 24/7 service and notify local police, fire and emergency services when alarm data is received.

---

<sup>1</sup> *In the Matter of Restoring Internet Freedom*, WC Docket No. 17- 108, FCC 17-60, Notice of Proposed Rulemaking (“Notice”) (rel. May 23, 2017).

Consumers, schools, businesses, commercial/industrial properties and governments all depend heavily on reliable security and monitoring services such as those offered by ADT and its competitors. Most importantly, users depend on properly functioning alarm services, whether they are dealing with life safety threats resulting from an intrusion, a health crisis, a flood, carbon monoxide (CO) threat, or a fire. Such services require reliable and immediate connections to professional alarm monitoring centers and, in turn, public safety officials and first responders.

Increasingly, such connections are over customer-provided broadband networks, such as the Internet, rather than traditional telephone networks. Many of the Internet Service Providers (ISPs) that own these connections now offer competing alarm services, thus offering these ISPs the ability and incentive to degrade competing alarm service signals in favor of their own.

Whatever happens in this proceeding, the Commission must be mindful to safeguard alarm providers' and their customers' ability to access and use reliable broadband connections in a non-discriminatory and prioritized basis. Alarm data and event notifications must be received and transmitted by broadband providers without discrimination or deprioritization.

#### **I. ADT IS COMMITTED TO INNOVATION IN THE ALARM AND SECURITY SERVICE SECTOR**

ADT operates on the technological cutting edge in the home and business safety business, deploying state-of-the-art technology that improves user access to emergency alert services, and enhances the speed, accuracy, and content of alert data delivered to first responders and customers. As customer provided broadband connections are a vital part of these innovations, safeguards are needed to ensure that alarm data and related information will be transmitted over broadband connections quickly, accurately and on a prioritized basis all the way from the customer's premises to alarm monitoring centers and on to emergency responders.

Alarm data used by ADT and similar providers generally consists of smaller and less frequent data transmissions that are wholly distinct from the consistently higher volume of data consumed by the typical users of broadband networks such as online video distributors (“OVDs,” such as Netflix) or e-commerce providers that have much higher data and bandwidth, but less urgent, transmission requirements.<sup>2</sup> Unlike video entertainment or e-commerce communications, alarm data communications save lives and protect the well-being of individuals and families by alerting emergency service responders to a fire, carbon monoxide poisoning, home break-in, or medical emergency. Vital information communicated from a customer to an alarm monitoring center to an emergency service responder can save lives. Emergency service responders rely upon the critical, first-in-time messaging provided by alarm services to initiate, update and sometimes cancel emergency dispatch requests. For all these reasons, alarm data transmitted between the customer’s premises and alarm monitoring centers, including alarm alerts, medical alerts, equipment status updates, surveillance footage and video verification, absolutely requires secure, timely and reliable communications.

---

<sup>2</sup> Compared to the costs of the underlying technology or ongoing transmissions, the carrying costs of such low volume alarm data are *de minimis*. Alarm event, video, and other life safety data must be transmitted from the customer’s alarm location, across the network(s), to the monitoring center in a matter of seconds. The *de minimis* nature of this alarm data combined with its life and death impact necessitates regulatory protection to ensure the highest available QoS prioritization is assigned to alarm safety data on any, and all, broadband transmission networks.

## **II. STATE AND LOCAL GOVERNMENT REGULATION OF ALARM INDUSTRY**

### **A. VIDEO VERIFICATION OF ALARMS REQUIRED FOR DISPATCH**

As alarm technology has advanced, a number of cities, including Detroit, Las Vegas, Milwaukee and Salt Lake City, have adopted alarm verification ordinances<sup>3</sup> that require visual verification of an alarm event, either in person or through surveillance video, before emergency services will be dispatched. Other municipalities have enacted policies that prioritize response to alarm signals when accompanied by video or in-person verification. To comply with these ordinances and help ensure the best use of first responder resources for customers, many alarm providers, including ADT, offer surveillance video cameras connected to the overall alarm system that are capable of capturing a video clip, or providing access to live streaming video for a limited time, when motion is detected. This intermittent, low-volume video can be shared with first responders when requested. Blocking, throttling or de-prioritizing these types of data transmissions could slow emergency assistance, or deny it entirely. The Commission must be aware of, and protect such communications from discrimination or deprioritization.

### **B. BUILDING CODES MANDATE ALARM SIGNAL TRANSMISSION SPEED**

To ensure that alarm data is transmitted in a timely fashion, many municipalities around the country have also incorporated industry codes like the National Electric Code's NFPA 72 (the National Fire Protection Association's Fire Alarm and Signaling Code) or Underwriters Laboratories 827 into their own building codes. Among other things, NFPA 72 (2013 Edition<sup>4</sup>) mandates a 90-second maximum transmission time for an alarm signal to travel from the

---

<sup>3</sup> <http://www.siacinc.org/docs/STANDARDS/List%20AHJ%20Req.pdf>

<sup>4</sup> National Electric Code's National Fire Protection Association (NFPA) National Fire Alarm and Signaling Code, NFPA 72 (2013 Edition) 26.6.3.1.10.: <https://www.nfpa.org/Assets/files/AboutTheCodes/72/72-13ROPDraft.pdf>

premises to the central monitoring station. Underwriters Laboratory (UL) has similar requirements (UL 827<sup>5</sup>) that require adherence to NFPA 72. Data transmission over wirelines, and now over broadband subject to Title II regulation, has traditionally been so highly regulated that meeting a 90-second standard was never in doubt. If data blocking or throttling over broadband were to occur however, central monitoring stations could lose their UL certification and fall out of compliance with NFPA 72, and subsequently, an untold number of building codes around the nation.

### **III. ADT REQUIRES PRIORITIZED ACCESS TO END-USER CUSTOMERS AND FIRST-RESPONDERS**

#### **A. ADT SUPPORTS NO-BLOCKING AND NO PAID PRIORITIZATION FOR LIFE-SAFETY SERVICES**

ADT supports a “light touch regulatory approach” that allows alarm service providers to protect their prioritized use of broadband networks, including challenging, if necessary, ISP practices that harm such use. Alarm and emergency services are particularly vulnerable if services are in any way slowed or blocked.<sup>6</sup> Absent protections, broadband providers would be free to block a particular alarm service provider’s messaging content and to discriminate amongst competing alarm service providers.

The alarm industry is highly fragmented and includes more than ten thousand small businesses. The overwhelming majority of alarm and emergency service providers are small businesses without the capacity to challenge the activities of large broadband access providers, or withstand a multi-year review of allegations. Blocking also could impede the development of innovative alarm and emergency services offering increased consumer protection that

---

<sup>5</sup> [https://standardscatalog.ul.com/standards/en/standard\\_827\\_8](https://standardscatalog.ul.com/standards/en/standard_827_8)

increasingly rely on broadband networks, including networks being converted from traditional, copper-based, common carrier regimes to IP-based broadband networks.<sup>7</sup>

Paid for priority schemes should not be permitted, and it should be clear that emergency service data should never be degraded. BIAS providers should never be able to prohibit, limit or slow access to alarm and other emergency services.

**B. ADT SUPPORTS NON-DISCRIMINATION AND NO UNREASONABLE PRACTICES**

Non-discrimination principles preventing deprioritization of data is particularly important for life safety services relying on broadband customer access. A regulatory framework that prevents discrimination against alarm emergency and life-saving services, applications, products or providers, and supports interoperability, security, and privacy, is in consumers' and the nation's best interest.

**C. MOBILE BROADBAND PROVIDERS SHOULD ALSO PRIORITIZE ALARM AND EMERGENCY DATA**

Many of ADT's current features and future innovations rely upon mobile technologies to maintain a high level of security and protection for consumers when they are outside a protected premise. Alarm and emergencies services are increasingly reliant on access to customers with wireless devices, such as smartphones, and the use of mobile networks. ADT urges the Commission to prohibit mobile broadband providers from blocking or throttling web content and mobile applications related to alarm and emergency services that compete with the mobile broadband providers' own voice or telephony services, subject to reasonable network management. ADT asks the Commission to provide a means for a quick resolution of issues potentially arising from discrimination involving a mobile carrier that impedes the functioning of

---

<sup>7</sup> See, e.g., Technology Transitions, et al., GN Docket No. 13-5 et al., *Order, Report and Order and Further Notice of Proposed Rulemaking, Report and Order, Order and Further Notice of Proposed Rulemaking, Proposal for Ongoing Data Initiative*, FCC 14-5 (rel. Jan. 31, 2014).

alarm and emergency services through such technology. ADT believes competitive, affordable, and accessible wireless broadband connectivity will aid in delivering a cohesive platform to protect consumers' digital and physical identities while enabling traditional and innovative alarm and emergency services.

#### **IV. ADT SUPPORTS DATA PRIVACY AND PREVENTION OF ANTI-COMPETITIVE PRACTICES**

Any adopted framework affecting alarm service providers' access to their customers should include protections against the broadband provider's use of this same customer information, obtained through network management technical analysis or otherwise, for its own marketing or competitive purposes.

Many of the large broadband and high-speed access providers have their own alarm and emergency products supported on their own broadband platforms. ADT supports initiatives of the Commission that prohibit the ISP from usurping the privacy and QoS expectations of consumers by using the proprietary account information of alarm service providers for their own competitive purposes, or the sale of such information to third parties. Through Business Intelligence practices, i.e., deep packet inspection technologies for network traffic classification which includes network demographics, analysis, and record generation, ISPs possess the technical capability to identify customers of non-ISP alarm and security providers, to block or discriminate against the non-ISP alarm and security providers, to block or discriminate against the non-ISP alarm providers' data on the network, and to engage in further anti-competitive practices to encourage these consumers to utilize the ISPs' own security systems.

Regulatory protections are needed that limit the use of these technologies to ISP network management purposes, and expressly forbid the identification of existing alarm customers for the

purpose of service conversion, marketing, and communication, and purposeful service degradation strategies designed to create dissatisfaction with the legacy provider in order to induce service provider changes. Such practices should be expressly forbidden and non-ISP alarm service providers should have a direct recourse should their customer information be misused by an incumbent ISP.

## **V. ADT SUPPORTS EXPEDITED CONSIDERATION OF COMPLAINTS**

The Commission asks “should we consider another general rule and framework (such as Commission adjudication of non-discrimination complaints)”<sup>8</sup> and “If we restore the broadband Internet access service classification to an information service, should that alter our complaint and enforcement process in this context?”<sup>9</sup> ADT supports procedures requiring the Commission to quickly review complaints alleging blocking, throttling, or other unfair practices by broadband Internet access providers, as well as mobile Internet access providers, similar to the process put forward in Section 275 for ILECs and later, some BIAS providers. A bifurcated complaint procedure where alarm service providers are required to file some complaints with the Commission and receive a ruling within 120 days, while filing others with the FTC, where rulings can take years, is confusing and disincentivizes potential victims of unfair practices to pursue corrective action. Smaller alarm companies (the vast majority of the industry) are unlikely to be able to withstand a lengthy review process and could go out of business waiting for their complaints to be heard.

---

<sup>8</sup> Notice at para. 75.

<sup>9</sup> Notice at para. 95.



## CONCLUSION

Tomorrow's public safety and lifesaving services such as home alarm systems, school and business security, and disaster alert data will certainly depend on access to reliable broadband networks. To ensure the health and safety of consumers, alarm data must travel across broadband networks without the threat of blocking or deprioritization. As the largest provider of home and business automation and alarm monitoring services in the United States and Canada, ADT asks the Commission to adopt rules consistent with its concerns.

Respectfully Submitted,

THE ADT CORPORATION

Holly Borgmann  
Head of Government Affairs  
The ADT Corporation  
1501 Yamato Road  
Boca Raton, FL 33431

/s/ Frank Cona  
Frank Cona  
Vice President, Chief IP Counsel and Chief  
Privacy Officer  
The ADT Corporation  
1501 Yamato Road  
Boca Raton, FL 33431

July 17, 2017