

APPENDIX 2

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

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

DECLARATION OF PHILLIP BRONSDON

I. QUALIFICATIONS

1. My name is Phillip Bronsdon and I am currently Senior Vice President of Product Development for CenturyLink. I have held that position since December, 2015, and in that position I am responsible for CenturyLink's reliable and scalable delivery of product and technology launches. Prior to that time, I was responsible for duties as CTO at IntelePeer, Inc. The organizations I have led have been responsible for voice network architecture, voice network capacity planning, new technology identification, and data network architecture. The matters recited in this Declaration are based on my personal knowledge, information and belief, and if called to testify, I could and would testify competently to the same effect.

2. CenturyLink offers mass-market Broadband Internet Access (BIA) service to consumers and small businesses across the 37 states where CenturyLink is the ILEC. We also offer BIA service to small business customers in a limited number of markets outside our ILEC serving area.

3. The purpose of this declaration is to describe the technical characteristics of BIA service and, particularly, how BIA service clearly qualifies as an information service as defined in the Telecommunications Act and under the Federal Communications Commission's past precedents. As described below, BIA service providers are expected to do more than just

transport packets. They are expected to provide a comprehensive, integrated service that includes telecommunications and information service functionality (i.e. acquiring, generating, storing, transforming, processing and retrieving information). And, as described below in greater detail, the ever evolving and dynamic characteristics of this Internet connectivity of BIA service is fundamentally different from the largely static one dimensional, transmission-oriented TDM voice network.

II. BROADBAND INTERNET ACCESS SERVICE OFFERS CONSUMERS THE CAPABILITY TO ACQUIRE, GENERATE, STORE, TRANSFORM, PROCESS, AND RETRIEVE INFORMATION

A. Internet capabilities offered via BIA Service

4. **Even before considering the underlying network functionality that enables it, it is important to note that the fundamental purpose and function of BIA service is to offer customers the capability of acquiring, generating, storing, transforming, processing, and retrieving information – because Internet Service Providers (ISP), like CenturyLink, in BIA service, offer customers an integrated information service solution that provides them with the capability of using content and applications that rely on the Internet.** Customer use of the Internet has evolved over time. Early on, this activity consisted largely of downloading small data files and applications or accessing email. Increasingly, it consists of high-band-width applications like video and gaming, and of customers themselves generating content (information) by serving or uploading to websites videos, blogs, videos, pictures, and other content. BIA service is also fundamental to information processing, retrieval, and storage associated with cloud services. BIA service provides customers with the ability to acquire and retrieve content through online applications including streaming video, online gaming, web browsing, and social networking. BIA service also provides customers access to remote storage and processing capabilities such as cloud based file-sharing, online data storage solutions, and

virtualized computing platforms. *See* pages 20 through 24 of CenturyLink's Comments for a more detailed discussion of the capabilities of BIA service.

B. Information processing, etc. within network functionality enabling these Internet capabilities

5. **Of course, to enable this capability described above, the underlying ISP network functionality to BIA service itself integrates a range of information processing, retrieval, storage, and other functions that make up the functionality that is information service functionality.**

6. At a high level, the World Wide Web (WWW) is an implementation of Internet protocols that link together information resources residing on the Internet. An information resource is linked to another resource using a Uniform Resource Locator (URL). The URL is a format that is used to identify the protocol used to access the information resource (e.g. http, ftp, etc.), the hostname¹ of the server that contains the information resource, and the path to that information resource located on the server. The WWW depends on the DNS to resolve hostnames within URLs to Internet Protocol (IP) addresses where information resource is located. It also depends on the ongoing operation of multiple Internet protocols and routing to access the information resource. This combination of IP, routing, and DNS, is essential to distributing, storing, and retrieving information on the Internet. Without this arrangement, it would be impossible to locate, access, or distribute information on the Internet. An Internet service provider must maintain all three functions and supporting infrastructures in their network in order to provide useable Internet services.

7. Digging down to an additional layer of granularity, this overall process of communicating information on the Internet involves an assemblage of many protocols and

¹ Technically, an IP address can be used in place of the hostname, but this is rare.

methods. These protocols and technologies are defined by an *open* set of technical documents known as Requests For Comments (RFC), of which there are over 8200 and growing. It is an ever-changing set of normative and informative documents maintained by members of the Internet Engineering Task Force (IETF). For official standards, anyone can contribute subject to peer review, thus there is no single organization or group that controls the Internet standards. It is an open forum where non-members can contribute informational RFCs *suggesting* protocols and methods that could be, or have already been, implemented with little peer review. Furthermore, there are no restrictions on inventing and implementing new protocols and methods outside of these technical documents. This is an international convention that is similar to the publishing processes of academic and scientific journals.

8. **Consistent with the Commission's discussion of BIAS in its 2002 *Cable Modem Order*² CenturyLink's BIA service enables the Internet capabilities described above through network functionality that, itself, integrates a range of information processing, retrieval, storage, and other information service functionalities that go far beyond mere transmission. This includes at least seven broad categories of ISP network functionality that creates the BIA service Internet connectivity described above:**

(a) **Practical operational and customer service functions that must be installed in order to make BIA service usable to subscribers.** The host of information service features and capabilities that are included as part of BIA service includes the installation of hardware (MODEM) and software (e.g. Norton anti-virus software), along with simple and

² *Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities*, GN Docket No. 00-185, CS Docket No. 02-52, Declaratory Ruling and Notice of Proposed Rulemaking, 17 FCC Rcd 4798 (2002) (*Cable Modem Order*). See also Comments of CenturyLink, *Restoring Internet Freedom*, WC Docket No. 17-108 (July 17, 2017), at 12-25.

complex customer services and technical support – all of which are provided when customers purchase CenturyLink’s BIA service. To qualify for CenturyLink’s BIA service a customer must live in a CenturyLink qualified area, have a computer system, and acquire a MODEM or gateway. The MODEM must be connected to their computer via WiFi or an Ethernet or USB interface to establish their high speed Internet connection with CenturyLink. Customers have the option of purchasing or leasing a MODEM or gateway from CenturyLink, or they may attach any MODEM of their choice to their CenturyLink High-Speed Internet service, provided that the MODEM supports the technology on which the customer is provisioned. Customers can find a list of approved MODEMs in CenturyLink’s Internet Management disclosure found at <http://www.centurylink.com/aboutus/legal/internetservicedisclosure.html>. But, in all cases, the MODEM is responsible for, among other things: (i) translating the private IP address assigned to the user’s device (usually by the MODEM) to a public IP address that ISPs like CenturyLink assign to the outside interface of the MODEM; (ii) maintaining a data table that keeps track of connections between internal private addresses and external public addresses, translating and delivering each packet between the public and private address spaces;³ and (iii) providing NAT and firewall security services to protect the subscriber’s network and device(s) from threats on the public Internet and protect the ISP network from threats that may otherwise be easily exposed on subscriber networks and devices. Thus, the MODEM and its complex information processing capabilities that facilitate the subscriber’s connectivity to BIA service.

³ Commonly, a subscriber has a private network on their premise. The IETF has reserved specific ranges of IP addresses to use for addressing interfaces on private networks. These reserved addresses are not publicly routable on the Internet. For these cases, the MODEM performs Network Address Translation (NAT), transforming the packets on the private network from private addresses to the public IP address assigned to the outside interface of the MODEM.

(b) IP addressing functionality and domain name resolution through a

Domain Name System (DNS): The information processing, etc. inherent to BIA service Internet connectivity is also demonstrated in the IP addressing functionality, including DNS, that is an integral part of the service. In order for BIA service to work, CenturyLink must also provide a network configuration to the customer's MODEM connecting the customer premise BIA service functionality to the Internet capability that the customer seeks. This service configuration consists of an integrated IP addressing, routing, and DNS functionality that is also fundamental to BIA service. The customer MODEM is a gateway/router on the customer premise network that is assigned a publicly routable IP Address and contains a table of one or more routes that lead to the Internet and the IP Addresses of the CenturyLink DNS service, which are distributed to devices on the customer network. DNS is an application layer protocol that, in turn, binds names to addresses and other information necessary to establish and maintain communication with resource servers on the Internet. It is defined by the Internet Engineering Task Force (IETF) as a hierarchical, distributed, and autonomous system implemented by a diversity of community-maintained, authoritative and caching servers.⁴

It works, at a high level, as follows: Consider a BIA user seeking to access CenturyLink's Customer Support Website at www.centurylinkservices.net via their CenturyLink BIA service. In this example, the user finds the link via a search service and clicks on it. Then the browser application on the customer's computer initiates a request to a preconfigured DNS server, provided through the set-up of the BIA service connection. This is a request for the addresses associated with the link. And, the DNS server is a *resolver* or caching name server.

⁴ See Mockapetris, P. "RFC 1034 - DOMAIN NAMES - CONCEPTS AND FACILITIES" and "RFC 1035 - DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION." IETF.org. IETF, November 1987, available at: <https://tools.ietf.org/html/rfc1034> and <https://tools.ietf.org/html/rfc1035>.

When the request is received by the DNS resolver, it first looks in its cache for an answer. If found that answer is returned immediately. Otherwise, the resolver must search other authoritative DNS servers distributed around the world, beginning with one of the root servers from a preconfigured list. It then follows a series of referrals (*aka* delegations) to eventually reach the authoritative server that has the answer. For the example, `www.centurylinkservices.net`, the resolver queries a root server, which responds with a referral to the `.net` Top Level Domain (TLD) servers.⁵ The resolver then queries a TLD server, which responds with a referral to the `centurylinkservices.net` servers. The resolver then queries a `centurylinkservices.net` server, which finally responds with the address, `209.26.88.23`, as the authoritative answer. This process is known as recursion. The resolver stores each answer it receives in its own memory/storage (i.e. cache) for future reference, and is refreshed frequently through the same recursive process. Thus, if a subsequent request asks for `mail.centurylinkservices.net` (for example), the resolver already knows of the `centurylinkservices.net` authoritative servers to query and can skip the rest of the referrals. The user's computer is then able to send a Hypertext Transfer Protocol (HTTP) request over the CenturyLink network, or if necessary over the Internet, to the correct CenturyLink web server. This is a very simple example and often this critical functionality of Internet connectivity provided by DNS is more complex.

And, DNS performs far more information processing than that described above. DNS also includes a variety of underlying network functionality information associated with names such as with name service (NS), mail exchange (MX) and service (SRV) records. It provides mechanisms, such as canonical name (CNAME), delegation name (DNAME), and

⁵ TLD Servers are at the highest levels of hierarchy of the DNS system, just below the root servers. The Top Level Domain is the last part of the domain name, following the dot, e.g. `.net`.

pointer (PTR) records for selecting alternative routes to information as well as facilitating information distribution or content delivery systems. DNS also stores various types of security information, including sender policy framework (SPF) records to verify email sources and DNS Security (DNSSEC) credentials and signatures to authenticate domain names and services on the Internet. Domain names are regularly analyzed and categorized to facilitate web filters on firewalls and for parental controls. When a name is not found, the DNS can be used to redirect browsers to a web service that can correct typos or provide search assistance. The ways in which DNS is used to store, distribute, and process information is continually evolving in the IETF RFC technical documents.

As the Internet directory, the DNS is the source of authority for both the domain names that identify organizations and individuals on the Internet, and the IP addresses required to establish Internet communication. The DNS has a reverse namespace that records how IP addresses are allocated (i.e. it identifies names associated with an address) in conjunction with the Shared Whois Project (SWIP).⁶ Finally, DNS is integral to the operation of a network, as networks themselves use hostnames and URLs to identify service endpoints and management interfaces within the network.

(c) Transmission Control Protocol (TCP)/Internet Protocol (IP) processing, including routing, packet fragmentation & re-assembly, and transport layer delivery between application endpoints. Also critical to the Internet connectivity of BIA service, and also demonstrating the information processing, etc. inherent to the service, is the ongoing implementation of protocols that enables the “internetworking” of networks that is inherent to the service.

⁶ **SWIP** is a process for providing information about which organization is using a specific IP address or block of IP addresses.

This is based on what is “officially named the TCP/IP Internet Protocol Suite and commonly referred to as TCP/IP (after the names of its two main standards).”⁷ The TCP/IP Internet Protocol suite is actually a collection of layered protocols, of which there are four layer abstractions defined by the TCP/IP specification: 1) the network interface or link layer, which binds the upper layers to an underlying physical transport device but does not specify the networking mechanisms; 2) the Internet layer, which handles communication between elements on the network; 3) the transport layer, which facilitates the delivery of payloads between application endpoints; and 4) the application layer, which processes the payload according to an implementation of a particular application.

These Internet Protocols are, themselves, layered on top of the physical transport network, which, in the more comprehensive Open Systems Interconnection (OSI) model, itself comprises layers: 1) the physical layer, and 2) the data link layer – as well as the Internet protocols which cover OSI layers three (3) through seven (7), with a subset of addressing protocols that coordinate with layer two (2).

These Internet protocols define an information service that relies on an underlying transport network and are all enabled by BIA service. Even though the Internet depends on the transport network, by implementing an IP network as a service to consumers, a BIA service provider is offering an integrated worldwide information service that includes the transport network service needed to physically transmit the information, encoded as multiplexed signals on a transport medium, between geographically distinct locations. Note that there is a *transport layer* defined in both the TCP/IP layer model (at layer three (3)) and the OSI model (at layer four (4)) that has a different meaning from the concept of a *transport network*. A *transport network*

⁷ Comer, Douglas E. Internetworking With TCP/IP Vol 1: Principles, Protocols, and Architecture – 3rd ed. Englewood Cliffs: Prentice-Hall, 1995.

consists of the physical infrastructure and codecs required to transmit data from one geographic point to another (OSI layers one (1) and two (2)). Whereas, the *transport layer* (OSI layer four (4)) is a specification for establishing a data communication channel across a logical network, defined by the network layer (OSI layer three (3)), to connect two or more applications (at OSI layer seven (7)). This may be in separate geographic locations, or may be in the same location and even running within the same central processing unit (CPU) where the data never traverses a physical network.

These internetworking protocols provide a means of communicating between applications on disparate networks. These applications may reside on separate Local Area Networks (LANs), belonging to anything from a large organization to an individual, that are interconnected by Wide Area Networks (WANs) operated by various other organizations, including Internet Service Providers.

IP packets may traverse a variety of transport networks, such as Digital Subscriber Line (DSL), Digital Service level 1 & 3 (DS1,DS3), Synchronized Optical NETWORK (SONET) Optical Carrier level 3 & 12 (OC-3,OC12...), Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM), frame relay, dial-up MODEM, Ethernet, token-ring, wireless fidelity (Wi-Fi), cellular, satellite, etc., utilizing various media such as copper twisted pair, radio frequencies, coaxial cable, and fiber optics. The TCP/IP protocol suite does not cover the physical transport layer of networking, which is layers 1 and 2 in the OSI model. The underlying physical transport network is an assumed dependency, the details of which, through the abstraction of layering, are a separate concern from Internet technology. A BIA service provider may implement and operate their own transport network, or they may focus on Internet technologies and lease circuits from a transport provider.

Further demonstrating the information processing, etc. functionality of BIA service, is the IP header and functionality. This is the core of the protocol suite that specifies the information necessary to deliver a packet across networks, including the source and destination addresses (IP addresses) as well as the fragmentation and reassembly of packets as they traverse diverse network devices with various frame-size limitations. An IP packet has a header that provides the information for handling the packet. This includes: protocol information, header and packet lengths, fragmentation information, a time-to-live to keep packets from routing around infinitely, the protocol of the next layer up (the transport layer) that determines how the packet is handled at the destination, a checksum to verify the integrity of the header, the destination IP addresses, the source IP address, and other options. The source typically does not have a direct network connection to the destination, and so sends the packet to a known gateway, which is a specialized server called a router, that is connected to two or more networks. A router inspects its connections with other network devices in comparison to the address information in the packet header to determine which connection is the best path to the destination address. The router then forwards the packet to an IP Address at the other end of the selected connection. The device at the other end of the connection could be the destination, a router connected to the destination network, or a router on an intermediate network. Each router in the path does the same, inspecting the header and determining the next connection in the route, until the packet is delivered to the destination address. With the transmission of information, packets may take numerous paths between a source address and a particular destination address.

Notably, the TCP/IP suite actually relies on several routing protocols to deliver packets. Routing protocols, such as Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol

(RIP), specify the algorithms for identifying and selecting from several potential paths that packets may take across multiple networks and the exchange of dynamic routing information. In other words, using these protocols, routers are regularly communicating and processing dynamic, real-time changes to the multitude of routes across the various networks.

The IP protocol also specifies the process of packet fragmentation and reassembly. Fragmentation may be done by the source or an intermediate router. Reassembly is normally left up to the destination. Routes are limited in the size of packet they can transmit based on the Maximum Transmission Unit (MTU) of the underlying transport device. This is determined at the link layer based on the type of physical transport media. If a router determines that the MTU of the link to the next router in the path is not sufficient to carry the complete packet, then it will perform packet fragmentation to break apart the packet into two or more smaller segments that are within the MTU limit of the link. All packets, including fragments, are carried over the Internet in a distributed manner following the most efficient path as determined by the routers. Fragmented packets are reassembled at the destination and only then are the combined packets passed up to the next layer of processing.⁸

TCP, in turn, is a transport layer protocol that offers a logical “connection oriented byte stream” that ensures packets are delivered to their destination complete and in order.⁹ The TCP header includes sequence numbers and acknowledgements to keep packets in the correct order and ensure delivery. A TCP connection is established with what is known as a three-way handshake, involving a Synchronize (SYN) packet from the client to the server, a SYN+Acknowledge (ACK) packet from the server back to the client, and an ACK from the

⁸ Firewalls and other security services may reassemble packets prior to arriving at the destination.

⁹ RCF 1180 A TCP/IP Tutorial.

client to the server that completes the negotiation. From there, as each packet arrives at its destination intact with a sequence number, the destination will include an acknowledgment of that sequence number in a corresponding response to the source. If the source does not receive that acknowledgement within a given window, then it will resend the packet. Additionally, TCP specifies a virtual destination port and virtual source port, which are used to map the transaction to an application. TCP allows the source and destination to create a virtual circuit that is full duplex, meaning it can simultaneously send and receive data packets.

Other transport layer protocols also exist, the most prominent being the User Datagram Protocol (UDP), which is a connectionless protocol. With UDP, each packet is delivered independently on a best effort basis and, like TCP, the UDP header specifies the source and destination ports used to identify the application layer processing. Unlike TCP, UDP has less overhead; there are only four fields in the header, the source and destination port numbers, the UDP message length, and a checksum for message integrity, as opposed to the nine or more fields in the TCP header. Plus, there is no handshake negotiation. A request must fit within a single packet. If a requester does not receive an expected response within a specified timeout, then it retries and will continue to retry up to some preconfigured retry limit. Generally, the response must also fit within a single packet. DNS is one example of an application layer service that primarily uses UDP for its transport layer.

(d) Network Topology and Evolution: The topology of BIA service provider networks, and the evolution thereof over time, also illustrates to fundamental information processing, etc. characteristics inherent to BIA service Internet connectivity. In the beginning, the Internet was built from general purpose computers (servers) interconnected with various telecommunications circuits. These servers were often multipurpose, running many

services such as DNS, RIP, HTTP, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Network Time Protocol (NTP) and so on, while also performing the basic routing function of the Internet protocol.

Over time, the ever increasing complexity and processing demand of BIA services required that this equipment be split out onto separate servers. In some cases these became highly specialized servers, such as routers that manage the delivery of packets between network connections. Yet they remain information processing systems built primarily from general purpose computer operating systems, and the specialized functions remained a collection of protocols and algorithms implemented as software. These functions can still be implemented on general purpose computing platforms and these functions are often moved around from one type of specialized server to another type with a different combination of features. For example, next generation firewalls combine services such as packet inspection and filtering, routing, DNS caching, network monitoring, email processing, encryption and decryption, web redirection for errors and exceptions, and so on. Conversely, many modern routers are now incorporating firewall features to provide advanced security capabilities during the routing process.

Today, much of the network is implemented in large data centers, facilitating a combination of general computing and storage platforms as well as specialized hardware appliances. At CenturyLink, these data centers are called TeraPOPs. They are located and operated separately from data centers that host customer information systems, yet they are data centers housing a fundamental information system that is a network service.

The ISP industry is also proceeding towards the adoption of Software Defined Networking (SDN) and Network Function Virtualization (NFV). SDN, which is still in its infancy, describes the management automation (*aka* orchestration) of network assets and

services. Typically this includes the coupling of big data frameworks which leverage advanced analytics and machine learning to serve as feedback loops for these SDN driven networks to predict, recommend, and prescribe orchestrated actions in an effort to improve the responsiveness, adaptability, and resilience of the network.

NFV involves the implementation of the normally physical network functions on virtualization platforms, with the goal of hosting many of these virtual network elements on massive multiprocessor general purpose computing platforms. Each element is implemented as software running on these platforms, yet behaves as the physical appliance would. NFV is further along in the deployment of operational applications than SDN. This is the next technological frontier in the evolution of the industry, and the development of the network as software and data, i.e. information, further substantiates the concept that BIA services are themselves information services.

In the past, present, and future, it is apparent that an Internet service provider's network is an evolving, fluid information processing system that relies on physical data transport technologies. Yet the Internet protocol functions independently from those telecommunication technologies, operating at a higher computing layer, which integrally involves generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications.

(e) **Integrated Network Security:** The information processing, etc. inherent to BIA service Internet connectivity is also demonstrated in the ongoing, integrated network security that is essential to BIA service. Behind the scenes, but fundamental to every activity of a BIA service user is the 24/7 management activity of CenturyLink engineers – managing the CenturyLink network to ensure that all customers receive secure and uninterrupted Internet

connectivity. These tools and practices must constantly evolve to keep up with the new and innovative ways that customers use the network and to keep up with changing network technologies. When malicious behavior is identified on CenturyLink's network, CenturyLink engineers employ various techniques to help provide a positive customer experience. These techniques are separate and unique from the optional security packages that a consumer or small business customer can purchase such as virus software or firewall services. CenturyLink's integrated network security management techniques include ongoing monitoring and management practices to ensure that customer systems are not propagating viruses, distributing spam email, or engaging in other malicious behavior. For example, CenturyLink uses industry best practices to prevent virus/spam delivery to customer email accounts. CenturyLink also automatically detects and mitigates DoS (Denial of Service) attacks and Distributed DoS (DDoS) attacks that may impact CenturyLink's High-Speed Internet customers and deploys network management activity to prevent border gateway protocol (BGP) hijacking.¹⁰ CenturyLink may also block malicious sites and phishing sites to prevent fraud against its customers and to prevent CenturyLink customers from becoming infected, using techniques such as DNS blackholing and IP address blackholing.¹¹ These techniques may require CenturyLink to acquire malicious traffic reports from trusted third parties. CenturyLink generates internal reports using data collected from routers on its network. CenturyLink uses algorithms that allow CenturyLink to process the data collected to verify the accuracy of the information received from trusted third party source(s). This process accurately identifies customers whose computers may be infected with a virus or malicious software (malware) and trigger the Customer Internet Protection Program

¹⁰ **BGP hijacking** means the take-over of groups of IP addresses by advertising illegitimate routes using the Border Gateway Protocol.

¹¹ **Blackholing** refers to situations where data [traffic](#) is discarded (*aka* dropped).

(CIPP). CIPP is integrated network security designed to help curtail the spread of viruses and malware, including botnets,¹² and assist its customers whose computers are infected with viruses and malware. The CIPP is available to CenturyLink residential and small business BIA service customers. Once infections have been detected, CIPP assists with the mitigation of virus and malware infections, including botnets. CenturyLink proactively provides virus and malware notification, mitigation and security education for its BIA service customers.

Focusing at a more granular level on just a few of these network security activities, the information processing that defines each comes into clear view:

Denial of Service (DoS) and Distributed DoS (DDoS) attacks.

CenturyLink uses filters that have been installed in certain routers on its network to process data that flows through these routers in order to detect and mitigate Denial of Service (DoS) and Distributed DoS (DDoS) attacks. This involves the collection, processing, and storage of packet header and traffic flow (netflow) information.

Border gateway protocol (BGP) hijacking. To prevent border gateway protocol (BGP) hijacking, CenturyLink routinely communicates with route registries, which are information services that store and distribute data about network addresses, autonomous systems, and route delegations (*aka* Classless Inter-Domain Routing (CIDR) block ownership). CenturyLink uses this information with an algorithm to generate route filters that confirm whether an IP address advertised to CenturyLink by a customer is in fact owned by that customer.

¹² **Botnet** refers to a network of computers infected with malicious software and controlled as a group without the owners' knowledge, e.g., to send spam messages.

Anti-spoofing. CenturyLink has implemented Best Current Practices (BCP) for anti-spoofing¹³ widely within its network. This technique examines packets that enter CenturyLink's network to ensure the packets originate from the correct interface. When a match is not detected, the filter blocks these "spoofed" packets to prevent DDoS attacks. Together, these techniques provide robust anti-spoofing features within the CenturyLink network.

Firewalls. Firewalls provide a particularly important role in CenturyLink's Internet services. Customers reasonably expect their ISP to provide services to secure their network from the Internet access that is being provided. This may be implemented within a residential customer's MODEM, with a firewall appliance on the customer premise, or within the CenturyLink network between a customer's service and the Internet. A firewall processes packet headers and the application payload data on an ongoing basis to inspect for threats as well as to meet contractual compliance in the case of businesses and government agencies. They transform packets by translating the packet addressing between internal private addresses and public Internet addresses, i.e. Network Address Translation (NAT). Furthermore, in order to inspect even encrypted packets, portions of the Security Sockets Layer (SSL) and Transport Layer Security (TLS) headers and messages are transformed in the process of decrypting and re-encrypting packets. Customers that require protection from data leaks may require the firewall to modify or omit data within the packet payload. Customers with security concerns or in compliance with laws require the ISP to provide security services to capture and store packets and firewall logs for analysis and reporting.

These security features, all of which involves the information processing, etc. activities indicative of an information service, are all fundamental to ensuring the reliability and

¹³ This is done according to IETF standards documents, BCP-38 and BCP-84: <https://tools.ietf.org/pdf/bcp38.pdf>, <https://tools.ietf.org/pdf/bcp84.pdf> .

availability of Internet access to CenturyLink customers as well as to protect the confidentiality and integrity of customer information communicated via the Internet. Additional information about CenturyLink's integrated security solutions is available in CenturyLink's Internet Management Disclosure, which can be found at: <http://www.centurylink.com/aboutus/legal/internetservicedisclosurefull.html>.

(f) **Caching.** Caching is another network management technique utilized by BIA service providers that is both fundamental to the operation of the service and fundamentally constitutes information storage, processing, etc. functionality. Content such as documents, web pages, images, gaming technology, IP addresses, live and on-demand videos, rich media content (including audio) and software updates may be cached or stored to reduce bandwidth usage, remove potential peering constraints, reduce server load, reduce latency and to provide a better overall experience for the online user. As described in detail above, network providers have DNS servers that cache IP addresses and other data to reduce the load on the DNS hierarchy and to reduce latency by responding directly to redundant DNS queries for the same hostnames or references in the hierarchy. Similarly, application and content providers often maintain copies of their content in multiple Content Delivery Network (CDN) servers distributed in geographically diverse data centers. Network providers also market the distribution of CDNs within their network infrastructure at locations close to end users, which can reduce latency and potential network congestion.

In addition to the fundamental storage characteristics of these practices, they rely upon a variety of BIA service provider network features that also fundamentally consist of information processing, etc. For example, DNS is used to distribute URLs to content servers that are nearest to the consumer. DNS is used along with the content provider's route advertisements

in order to route content specific URLs to the nearest edge caching nodes. The use of HTTP redirect¹⁴ is also common to complete the transaction with a service having optimal delivery capabilities. Anycast routing¹⁵ may further enhance this type of distribution mechanism. Service providers may support multicast routing¹⁶ on their managed networks, which reduces network congestion by distributing a single stream and replicating of data to multiple locations. These types of enhancements are facilitated by the information processing and storage capabilities of the Internet service provider's network infrastructure.

(g) Network monitoring, capacity engineering and management, fault management, and troubleshooting. Also underlying BIA service are a variety of network management functions such as network monitoring, capacity engineering and management, fault management, and troubleshooting that also fundamentally consist of information processing, etc. These are generally performed at CenturyLink's Network Operations Center (NOC) or back office and serve to provide a steady and accurate flow of information between the cable plant system of which is essential to BIA service Internet connectivity. CenturyLink actively manages its BIA service network by deploying enhancements to these various network management tools. In these activities, CenturyLink provides 24/7 customer service support in an effort to provide its customers with uninterrupted and secure service. CenturyLink also follows industry-leading network security standards to ensure the integrity, availability and confidentiality of our customers' network information.

¹⁴ When a web browser attempts to open a URL that has been redirected, a page with a different URL is opened.

¹⁵ Anycast routing is a technique where many servers announce their own address as the route to a single, common address, known as the anycast address, such that traffic will be routed to the nearest such instance of the service.

¹⁶ Distributing data such as, audio/video streaming broadcasts to multiple recipients.

C. Other information service functionalities sold with BIA service

9. In addition to these information service functionalities described above that enable BIA service Internet connectivity, customer are able to purchase a variety of additional information service functionalities with their service. These include:

(a) ***CenturyLink Email service.*** While customers are able to use third party email service with their BIA service, all CenturyLink BIA service customers are also able to use CenturyLink email service – and many do.¹⁷ And, although a customer can choose an alternative, the customer’s ISP is expected to provide email service in order for the customer to have a functional Internet service. Unlike DNS, email is not a real-time service where any delay in the service will cause a corresponding degradation in the Internet service or customer experience. Therefore, this service is more suitable to outsourcing where it makes technical and financial sense. Moreover, regardless of whether a CenturyLink BIA service customer utilizes CenturyLink email or a third party email functionality, CenturyLink network functionality inherent to its BIA service enable email. Among other things, the ISP must enable email processing (and the IP protocols necessary to it) in regard to security and email-related storage/caching functions.

(b) ***CenturyLink landing page.*** Customers purchasing CenturyLink’s BIA service are automatically provided a landing page at www.centurylink.net where they can access their CenturyLink provided email, news, sports, entertainment and games.

¹⁷ CenturyLink’s Email service is provided by a third party called Synacor. However, this arrangement is transparent to our customers since the email service they receive from CenturyLink includes a Centurylink.com domain, is branded as a CenturyLink service, and is only available via the online landing page that CenturyLink provides customers at www.centurylink.net.

(c) *Geolocation Based Advertising, Web Helper and speed test servers.*

Geolocation Based Advertising, Web Helper and speed test servers are also included in CenturyLink BIA service services. Geolocation location-based advertising is advertising which can be based on a geographic attribute, such as address, zip code or neighborhood. Targeting advertising by location is a common practice with television, direct mail, mobile phones and the Internet. Geolocation location-based advertising utilizes information processing, etc. to essentially accomplish the same thing – to target advertising to customers at the address, zip code or neighborhood associated with their High Speed Internet service to improve the location accuracy and relevance of advertisements and a customer's overall Internet experience. Customers can learn more and exercise their options regarding participation in this service at <http://locationbasedadvertising.centurylink.com>. The CenturyLink Web Helper service provides helpful search results to our customers when they would otherwise encounter DNS errors. Customers see search results offered by the CenturyLink Web Helper service when they click on an invalid link or enter an invalid Web address into the address bar of their browser. Misspellings and typing errors frequently cause these errors. In instances where the site they were looking for is clear, they may not see this page at all. Instead, the service may take them directly to the site. Customers can learn more and exercise their options regarding participation in this service at <http://webhelper.centurylink.com/faq.php>. Customers may also test the speed of their BIA service connection using third party speed servers that may be accessed on our website at <http://internethelp.centurylink.com/internethelp/zam-speed-test.html>.

(d) *CenturyLink @Ease[®] and CenturyLink[®] Stream.* Additional

CenturyLink services that are available to BIA service subscribers for an additional fee include CenturyLink @Ease and CenturyLink[®] Stream.

With CenturyLink @Ease[®] customers can choose a package that fits their security, backup needs and support services. Packages include Identify Guard[®] Basic Protection[®], 24/7 technical support or automatic online back-up from Norton[™]. CenturyLink @Ease is available via three package offerings including a Standard package, an Advanced package, and an Ultra package. Details regarding these solutions are available at <http://www.centurylink.com/home/Internet/>.

CenturyLink also recently launched a market trial of our over the top video stream service called CenturyLink Stream the four markets of Albuquerque, New Mexico; Boise, Idaho; Des Moines, Iowa; and Tucson, Arizona. CenturyLink Stream is available to customers over a qualifying mobile or internet capable device without a set-top box. CenturyLink Stream is also available for online purchase on a national basis to customers purchasing a high-speed internet connection from any broadband provider at speeds between 5-25 Mbps. Additional information about CenturyLink Stream is available at: www.centurylinkstream.com.

D. Distinguishing the legacy voice network

10. The dynamic network functionality enabling the Internet connectivity provided by BIA service is fundamentally different from the largely static one dimensional, transmission-oriented Time Division Multiplexing (TDM) voice network. To begin with, as described above, the Internet is an open, dynamic system that includes an unrestricted community of providers, organizations and individuals that can evolve the functionality of the Internet quickly. In contrast, the TDM network is a static, generally closed system operated securely within the confines of each telecommunications provider based on stable, relatively mature and unchanging standards. Additionally, Internet protocols that control the functionality of the Internet, such as

routing protocols, are themselves communicated in-band via the TCP/IP suite¹⁸ and create a dynamic, interactive network functionality that is essential to creating the dynamic and interactive characteristics inherent to BIA service usage. In contrast, the TDM network generally separates the signaling protocols from the information that is being transported, such that the control protocols are out-of-band on isolated secure networks within the control of each telecommunications provider. And, this signaling protocol serves functions based solely upon the set up and tear down of calls.

But, the fundamental differences between BIA service networks and TDM networks do not end there. As compared to the great diversity of capabilities described above that is provided via BIA service, TDM technology, itself, was designed solely to accomplish the efficient transmission of basic types of communications - telegraph and voice communications – in a single point-to-point transmission. And, in contrast to the multitude of underlying information processing, etc. characteristics entailed in BIA service and the underlying ISP networks that enable it, described above, the telecommunications switching network or Public Switched Telephone Network (PSTN) leverages this TDM transmission technology solely to establish dedicated end-to-end connections to enable voice conversations between voice service subscribers. The telecommunications switch provides two types of interfaces. Line interfaces that connect loops to the voice service subscribers and trunk interfaces used to connect switches. The purpose of a switch is to connect lines to lines, lines to trunks, trunks to lines, and trunks to trunks. As calls are placed between voice-service subscribers that have connections to the same switch, the switch will establish a line to line nailed-up or dedicated end to end connection for

¹⁸ Albeit, subnet isolation and security are commonly used to separate some internal control traffic from the service data traffic. However, some protocols required to establish communications and interdomain routing, such as DNS and BGP, cannot be effectively separated from the service data traffic.

the duration of the call. As calls are placed between voice-service subscribers that are connected to different switches, the originating switch will establish a line to trunk connection and the terminating switch will establish a trunk to line connection. In some arrangements when there is a tandem switch involved in the call path, the tandem switch will establish a trunk to trunk connection between the trunk side of the originating and terminating switch. This is also a nailed-up or dedicated end to end connection for the duration of a call as described above with a line to line connection. This dedicated connection establishes a path for the real time unaltered voice communication to take place. This is fundamentally different from the dynamic point to multi point application driven information service capabilities of BIA service.

E. A note on third party DNS

11. **One final note:** In the past, it has been suggested that the fact that DNS functionality can be obtained from third parties means that it is not an integral part of BIA service. This is not the case. The availability of third party DNS service does not change its integral nature within BIA service. To begin with, because most customers will not seek third party DNS services, a BIA service provider has an obligation to service DNS queries. The service provider must provide their customers with a reliable and efficient means of querying the DNS. Without this, customers cannot navigate the Internet, or if it's inefficient, then customers will experience service degradation. Therefore, DNS is a necessary component of BIA service from the customer's perspective. Additionally, whether provided via CenturyLink or a third party, the above discussion makes plain that DNS is an essential component of BIA service. Finally, the BIA service provider's DNS functionality tends to provide performance and security benefits not available via third party DNS services. For example, CenturyLink is a leader in deploying DNSSEC in its DNS recursive servers. This security processing capability assures

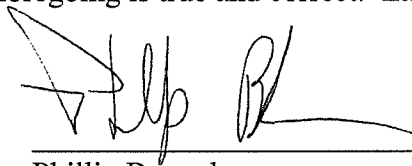
CenturyLink's customers that the DNS answers for domains authenticated with DNSSEC have been properly validated as originating from the authentic source. DNSSEC is integral to the functionality of CenturyLink's backbone infrastructure, and thereby a key requirement to ensure the availability of Internet services. Furthermore, CenturyLink has implemented best practices in its DNS configuration often not included in third party DNS services, including an "anycast" design using dynamic routing and a distributed topology, along with other techniques to mitigate Cache Poisoning.¹⁹ Anycast is a method by which many servers announce themselves as the route for the same set of IP addresses for an appropriate²⁰ application layer service, such as DNS. These servers replicate the information resources for the service. Thus, a request sent to a service address will be routed to the nearest information source announcing that address. If the nearest server goes down or is impaired, it automatically withdraws its route announcement and requests are rerouted to the next nearest server in near real time. This method has proven to be extremely resilient over the last couple decades, and is a best practice used by many large authoritative DNS service providers. CenturyLink uses this technique to protect the entire DNS infrastructure, authoritative services and the resolver/caching infrastructure, which is not a common practice. The resiliency of this solution mitigates DoS attacks by localizing the effects so that they have minimal impact and can be countered quickly; and by disbursing DDoS attacks across a much larger infrastructure that can handle the load, likely keeping some elements completely unaffected. By employing other configuration techniques and maintaining current software versions it is possible to further mitigate Cache Poisoning attempts. The DNS provided by CenturyLink also uniquely assures network reliability for those customers who use its DNS.

¹⁹ Cache poisoning is when corrupt DNS data is introduced into a DNS resolver's cache potentially resulting in an incorrect IP address or other forged data in the answer.

²⁰ In general, for an application service to be appropriate for anycast, it must be unaffected by asymmetric routing, which normally requires UDP as the transport layer.

In addition to implementing the many network management techniques described above and in its online Internet Network Management disclosure, CenturyLink also ensures that the software within its DNS is current and optimized to minimize delays and latency in DNS responses. When BIA service customers experience online delays or disruptions they can call the CenturyLink repair department who will conduct troubleshooting on behalf of the customer. When the customer is using CenturyLink's DNS resolvers, CenturyLink is able to identify if the latency or disruption they are experiencing is from a problem on CenturyLink's network, including whether there is an issue with CenturyLink's DNS resolver, or an external problem that may be affecting name resolution. In many cases, such problems can be corrected using tools to reset portions of the cache for particular domain names without impacting the service overall. Furthermore, the CenturyLink DNS is used to improve the robustness of the customer's online experience through CenturyLink's Web Helper service.

I declare under penalty of perjury that the foregoing is true and correct. Executed on
July 17, 2017.

A handwritten signature in black ink, appearing to read 'Phillip Bronsdon', written over a horizontal line.

Phillip Bronsdon
Senior Vice President of Product Development for
CenturyLink