EXHIBIT A

RYSAVY RESEARCH

Declaration of Peter Rysavy

July 17, 2017

Table of Contents

Introduction & Summary

1. This declaration responds to the FCC's Notice of Proposed Rulemaking (NPRM) on *Restoring Internet Freedom*. It proceeds in three parts: Information Service Classification, Public Switched Network/Interconnected Service, and Evolving Mobile Networks and Differentiated Offerings. This introduction presents a view of how the internet has evolved and summarizes the topics covered in detail in this declaration.

2. The internet was originally conceived as enabling the robust delivery of packets between end points across multiple nodes, primarily using Transmission Control Protocol (TCP) and Internet Protocol (IP). Early applications included email using Simple Mail Transmission Protocol (SMTP) and File Transfer Protocol (FTP). Content locations were static and routes between end points seldom varied. Over the decades, and particularly since 1990, innovation has flourished on the internet, resulting not only in a vast array of new applications, but a fundamental change in the nature of the internet itself. Internet service, which began as a communications offering with limited intelligence, has evolved into a highly intelligent platform that processes and transforms information in multiple ways and at multiple nodes to both enhance the user experience and enable applications that would not otherwise be possible. Some key elements in this near-constant transformation are how internet service providers (ISPs) and other nodes adapt, process, and optimize user content and how ISPs and other nodes dynamically optimize delivery paths for speed and efficiency. Further, content that used to be located centrally is now widely distributed, including within ISP networks, so much so that new internet architectures under investigation, such as Information Centric Networking (ICN) and Named Data Networking (NDN),[1] do not rely on routing based on IP addresses but instead focus retrieval based on the content desired.

3. Subscribers of broadband internet access service make use of a variety of applications over their broadband connections, including social networking, instant messaging, email, web browsing, and video streaming, all of which offer some combination of generating, acquiring, storing, transforming, processing, retrieving, utilizing, and making information available – the characteristics of an information service.

4. Furthermore, this information is not static. It is processed and often altered at multiple points by the ISP, in the transmission of the information (*i.e.,* in parts of the path over which packets

[1] See summary of IETF work on Information-Centric Networking at IRTF, "Information-Centric Networking Research Group (ICNRG)," available at https://trac.ietf.org/trac/irtf/wiki/icnrg. For further background, see also https://named-data.net/project/, https://blogs.cisco.com/sp/cisco-announces-important-steps-toward-adoption-of-information-centric-networking, and https://www.nsf.gov/pubs/2016/nsf16586/nsf16586.htm.

are routed), by third parties, and by content providers. Transmission of data has become intertwined with other services that provide value to users. The very transmission of data in the internet involves processing of information, in some cases transforming packets. Differentiated services, network address translation, congestion mitigation, and IPv4-to-IPv6 integration are all examples. Another important function ISPs provide is caching, which stores information and provides local retrieval, improving the user experience.

5. And beyond transmission, ISPs bundle or offer multiple other services that store, transform, process, and retrieve information including opt-in filtering for family safety, video optimization, and security functions.

6. All of these capabilities differentiate the internet from the Public Switched Telephone Network (PSTN). The two networks use dramatically different protocols, different architectures, different approaches in switching (packet versus circuit), different nodes within the networks, and they provide very different capabilities. Voice over Internet Protocol (VoIP) service providers can interconnect the two networks, but only in a limited fashion, and only with specialized gateway equipment and software. For example, telephones cannot be used to place calls to the billions of IP addresses on the internet.

7. The popularity of IP-based services such as video streaming has contributed to the explosion in the amount of data traveling through the mobile broadband network, which can experience congestion to a greater and more sudden degree than other networks. To meet user expectations, traffic prioritization and quality-of-service (QoS) management are essential functions. Furthermore, as networks move to 5G, QoS will play a crucial role for a capability called network slicing. 5G use cases include mission-critical applications such as advanced industry automation, telemedicine, and drone control, all of which will require intelligent traffic management. Another fundamental capability of 5G will be Multi-access Edge Computing (MEC), which will further intensify information processing within the network, enabling applications such as augmented reality (AR).

8. All of the above leads to the inescapable conclusion that broadband internet access service is dynamic and evolving, and provides far more than mere transmission. Mobile broadband is not an element of the PSTN. And mobile broadband will increasingly offer differentiated capabilities that enable QoS enhancements for emerging services and applications.

Broadband Internet Access Service Involves Many Elements of Information Service

"Core" Broadband Internet Access Functionalities Are Information Services and Not Mere "Network Management"

9. The *Title II Order* takes the general stance that internet access is a transmission technology implemented by TCP/IP protocols. The order classifies any other related capability as either a network management function (*e.g.*, DNS, caching), or a separable service (*e.g.,* email). Users, however, do not subscribe to internet service with the mindset of sending packets to an IP address. Users want to engage with the world in multiple ways, such as driving with turn-by-turn navigation or streaming a new show. The functionalities described in this section enable this form of engagement because they allow ISPs to manage their networks in a manner that contributes to what consumers value and seek out when they subscribe to a broadband internet access service. These offerings do not merely facilitate use of the basic network without changing the nature of the basic transmission, but rather add functionality that enhances the consumer's experience, expanding the network's capabilities beyond the mere transmission of data from one point to another.

Routing

10. The routing of Internet Protocol (IP) packets alone involves examination and processing of the packet at every router the packet traverses, including the routers managed by the ISP. Such examination and processing by the ISP is necessary to know which route to use *and* to implement policies, such as integrated or differentiated services. This information processing is inextricably intertwined with the transmission itself. As an example, documentation for a Juniper router lists 15 steps that the packet forwarding engine must perform to process each packet.[2] These routers are not just located in the core of the internet but are used by ISPs to communicate information to and from subscribers, to the internet, and to information servers they may provide, such as web servers, DNS servers, and email servers. Routing functions are integrated into current generation network equipment that is the next hop from an end user, such as a consumer-owned 4G wireless router,[3] Digital Line Subscriber Line Access Multiplexer

[2] See Juniper, "Packet Forwarding Engine Architecture for T Series Routers," available at https://www.juniper.net/documentation/en_US/release-independent/junos/topics/concept/packet-forwarding-engine-t320-t640-t1600-architecture.html (viewed May 24, 2017).

[3] See for example, Verizon Jetpack MiFi 7730L, described at https://www.verizonwireless.com/internet-devices/verizon-jetpack-mifi-7730l/.

(DSLAM), or Cable Modem Termination System (CMTS). Most home network equipment installed by ISPs also has routing, packet processing, and NAT functions.

11. Routing is not merely transmission, as routing offers services beyond just simply getting packets from one node to another. For example, the router may also enforce different policies, such as QoS, implemented through protocols such as Differentiated Services. The Internet Engineering Task Force's (IETF's) specification for Differentiated Services states: "This architecture is composed of a number of functional elements implemented in network nodes, including a small set of per-hop forwarding behaviors, packet classification functions, and traffic conditioning functions including metering, marking, shaping, and policing."[4] 4G wireless operators also implement QoS mechanisms for traffic differentiation. By way of example, the unlimited data service plans offered by some operators may deprioritize traffic for users that have exceeded a defined amount of data in circumstances involving network congestion.[5] This technique allows all subscribers to enjoy the benefits of the unlimited data plan; furthermore, subscribers are not adversely affected by users whose consumption of data could exceed the capacity of the cell. Providing users such additional value transcends network management. ISPs also provide a reliable and consistent customer experience by using methods such as Random Early Detection (RED) and Active Queue Management (AQM)[6], which selectively drop packets, forcing TCP transmitters to reduce the packet transmission rate. Analyzing traffic flows, implementing traffic policies, and acting upon the traffic flows involves acquiring, processing, and transforming information (for example, reordering or dropping packets). This functionality does more than facilitate mere transmission: Customers receive additional capabilities. In particular, their internet service works more reliably and more consistently, which makes a variety of applications possible that in the absence of such techniques would otherwise work sluggishly, or not at all.

---

https://ss7.vzw.com/is/content/VerizonWireless/Devices/Mifi/userguide/verizon-jetpack-mifi-7730l-ug.pdf. This device has features such as a firewall, port filtering, port forwarding, and customized lists of allowed applications.

[4] Internet Engineering Task Force, *An Architecture for Differentiated Services*, Request for Comments (RFC) 2475, available at https://tools.ietf.org/html/rfc2475.

[5] For example, see Verizon, "The new Verizon Plan Unlimited FAQs," available at https://www.verizonwireless.com/support/new-verizon-plan-unlimited-faqs/ (viewed July 8, 2017) ("To ensure a quality experience for all customers, after 22 GB of data usage on a line during any billing cycle we may prioritize usage behind other customers during network congestion. This means your data connection could slow down.").

[6] IETF, "IETF Recommendations Regarding Active Queue Management," RFC 7567, available at https://tools.ietf.org/html/rfc7567.

12. Cable internet access also can prioritize traffic using CableLabs' PacketCable Multimedia Specification (PCMM).[7] As described by CableLabs, this specification "support[s] the deployment of general Multimedia services by providing a technical definition of several IP-based signaling interfaces that leverage core QoS and policy management capabilities native to DOCSIS Versions 1.1 and greater." This capability acquires, processes, and transforms information. Comcast explains its recent open-source software implementation of PCMM as follows:

> For the past several months Comcast [has] been building a new policy engine for orchestrating Quality of Service (QoS) on our network and now we're excited to begin contributing key parts of that engine available to the open source community. QoS is a critical function for network operators. On our DOCSIS network, QoS technology is how we ensure that essential functions are allocated enough bandwidth to perform at the highest level. A good example is a voice call, which needs a certain amount of dedicated bandwidth to be crystal clear and without jitter.[8]

Consumers benefit from this technology because certain applications, such as the voice call mentioned in the Comcast example, operate in a dependable fashion and are not adversely affected by other traffic.

13. In addition, many ISPs allocate private addresses to users and must then perform network address translation (NAT) between the private and externally-facing, public IP addresses.[9] NAT, which acquires, stores, processes, and transforms packets, benefits customers in a couple of ways. Without it, ISPs would not have a sufficient number of Internet Protocol version 4 (IPv4) addresses for all of their customers, forcing customers to either use Internet

[7] CableLabs, *PacketCable Multimedia Specification*, available at https://apps.cablelabs.com/specification/packetcable-multimedia-specification.

[8] Comcast, "Introducing An Open Source Network Policy Engine," September 20, 2016, available at http://labs.comcast.com/introducing-an-open-source-network-policy-engine (viewed July 3, 2017). See also IETF RFC 6057, "Comcast's Protocol-Agnostic Congestion Management System," available at https://tools.ietf.org/html/rfc6057. The RFC states: "If the software determines that a particular subscriber or subscribers have been the source of high volumes of network traffic during a recent period of minutes, traffic originating from that subscriber or those subscribers temporarily will be assigned a lower priority status."

[9] For example, for non-routable IPv4 addresses, see IETF, *Address Allocation for Private Internets*, RFC 1918, available at https://tools.ietf.org/html/rfc1918.

Protocol version 6 (IPv6), which has many more addresses but is not supported by all internet nodes, or to restrict service to just the IPv4 addresses the ISP can allocate, possibly denying service to customers. NAT also provides a security function because the internal private addresses of customer devices are obscured, thus restricting unsolicited and potentially harmful internet traffic.

14. ISPs also provide IPv4-to-IPv6 gateway functions, interconnecting between IPv4 and IPv6 networks. Further, IPv6 also performs extensive packet processing. For example, the IETF specification RFC 7045, *Transmission and Processing of Ipv6 Extension Headers*,[10] explains how IPv6 network nodes, including ISPs' nodes, need to process what are called extension headers, resulting in different routing functions depending on the contents of the header. This extent of processing in IPv6 networks is significantly greater than in IPv4 networks. This function in IPv6 – which acquires, stores, processes, and transforms the packets – enables connections that would not otherwise be possible (for example, an IPv4 node communicating with an IPv6 node), or with more efficient routing, decreases latency and increases throughput, enabling real-time applications such as video conferencing and gaming. Network management concerns itself with delivering packets from one node to another. Functions that change the packets themselves, such as encapsulating an IPv6 packet within an IPv4 packet, such that the header data of the IPv6 packet is now the content information of the IPv4 packet, are information processing and transformation steps beyond mere transmission.

Caching

15. Many ISPs cache content using caching servers located within the ISP network. Because the cache stores and retrieves information, it is an information service. Moreover, it also provides functionalities that go well beyond merely facilitating transmission; rather, it affords the customer additional capabilities, taking it outside the scope of network management. With caching, the ISP's DNS servers direct an end user's request for specific content to different cache servers, depending upon the proximity of the end user and/or congestion at a given cache. Thus, content that would normally be delivered from a distant server can simply traverse the ISP-to-user connection. This eliminates internet bottlenecks, thereby improving users' quality of experience and adding value to their broadband internet access service by providing faster and more dependable service.

16. In some cases, the ISP owns and operates the cache. In other cases, the cache hardware can be provided by a third party, but is still operated at the ISP location.[11] In either case, the cache

[10] Available at https://tools.ietf.org/html/rfc7045.

[11] For example, see https://openconnect.netflix.com/en/.

is a part of the broadband internet access service offered by the ISP. The cache is not a service that users can opt out of—internet content requested by the user that is stored in the cache will be delivered from there to the user. Thus, the caching of information and transmission are inextricably linked.

17. At ¶ 37 of the NPRM, the FCC asks whether broadband internet users would experience incidental changes or more fundamental changes absent caching. Put simply, today's high-quality streaming content relies heavily on caching. Increasingly, internet content is bulking up. Streaming has already transitioned from standard definition to high definition, and the industry is currently providing an increasing amount of content in ultra-high definition. Virtual reality will impose even greater bandwidth demands on network operators.[12] Caching substantial portions of the internet's massive and growing content is essential to ensure that users do not have a degraded experience.

18. Moreover, companies such as Akamai operate Content Delivery Networks outside and inside ISPs. As the IETF has summarized:

> Content Delivery Networks (CDNs) provide numerous benefits for cacheable content: reduced delivery cost, improved quality of experience for End Users, and increased robustness of delivery. For these reasons, they are frequently used for large-scale content delivery. As a result, existing CDN Providers are scaling up their infrastructure, and many Network Service Providers (NSPs) are deploying their own CDNs.[13]

Inexplicably, at ¶ 372 in the *Title II Order*, the FCC states: "We observe that this caching function provided by broadband providers as part of a broadband Internet service, is distinct from third party caching services provided by parties other than the provider of Internet access service (including content delivery networks, such as Akamai), which are separate information services." From a technical perspective, however, the cache that an ISP operates is indistinguishable from such third-party services.

[12] For a discussion of the enormous bandwidth requirements of virtual reality, see ABI Research/Qualcomm, *Augmented and Virtual Reality: the First Wave of 5G Killer Apps*, 2017, available at https://www.qualcomm.com/documents/augmented-and-virtual-reality-first-wave-5g-killer-apps.

[13] Internet Engineering Task Force (IETF), *Request for Comments: 6707, Content Distribution Network Interconnection (CDNI) Problem Statement,* 2012.

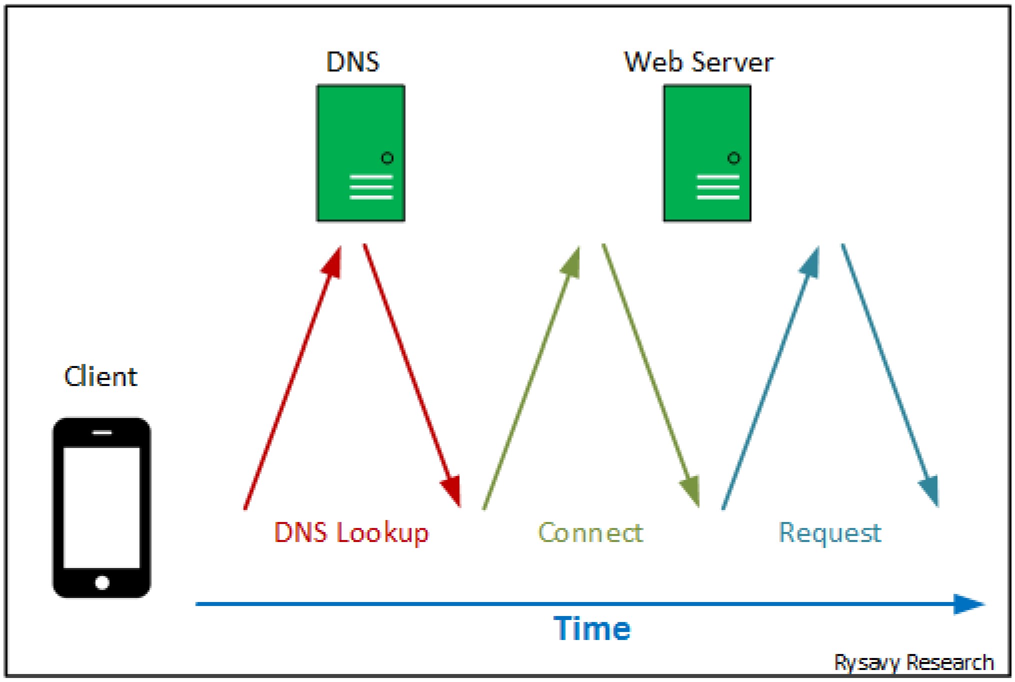
Domain Name System (DNS)

19. DNS provides the processing capabilities that allow subscribers to visit a website without inputting an IP address. When a subscriber types a domain name into a browser, the browser typically queries the ISP's DNS service for the proper IP address to send that information. DNS also provides a wide range of other services. For example, DNS can also be used for reverse lookups, with which a user queries DNS with an IP address to determine the domain name associated with the IP address. DNS operates in a similar mode when it provides an error-page-assist function for a user who has supplied an invalid address and DNS suggests similar pages the user may have been intending to reach.

20. In each of these cases, DNS service exhibits all of the hallmarks of an information service. A DNS server processes information when it receives DNS queries; it generates information when it delivers a response to an end user or queries an authoritative server; it stores domain name information in its cache; it transforms information when it takes a query from a user and sends it upstream (for information not in its cache); it retrieves information when it obtains domain name data from the internet; it utilizes information that it has stored in its cache; and it makes information available when it responds to DNS queries.

21. The *Title II Order* incorrectly characterized DNS as a network management function. For example, at ¶ 370 of the order, the FCC analogized DNS to a 411 telephone lookup service. But the two services are profoundly different. Using a 411 service, a user has a mindset of connecting to a phone number and knows only the name of person that she intends to call. The user then obtains a phone number through a separate call to the 411 service, and then makes a phone call using that number. In contrast, with DNS, the process happens inline, automatically and as part of the internet query. A user entering a search term into a web page, for example, does not think about needing to get an IP address first. He or she enters the term and the client software, if it does not already have the IP address of the search engine, performs a DNS query. Then, after obtaining the IP address, the client software connects to the desired server. Furthermore, as shown in Figure 1, the DNS query is one step in a multi-step communications process. Across time, a request to a DNS server is followed by a response from the DNS server; which is then followed by a connection request to and a response from the web server; which is then followed by a request for information from the web server.

Figure 1: DNS as an Integrated Step in Network Access



22. The DNS query is not an "adjunct-to-basic" function, as the *Title II Order* found in ¶ 367. The order states that an adjunct-to-basic function must be incidental to the underlying telecommunications service. The only perspective that warrants DNS being "incidental" is one in which users view themselves as communicating with IP addresses. But users seek answers to questions, to communicate with their loved ones, and to engage in myriads of other activities, none of which include wanting to know the IP addresses of the services with which they are communicating. Indeed, if IP addresses were so important, wouldn't business cards, in addition to listing the telephone numbers of a user, also include the IP address of their organization?

23. Finally, although third-party DNS servers are available, using an ISP-provided DNS service offers advantages to subscribers, including faster response to queries by being closer to the user and local knowledge needed for load balancing, as discussed in paragraphs 15 to 18.

Many Bundled Offerings Are Inherently Intertwined With Broadband Internet Access

24. ISPs offer numerous services that are part and parcel of the broadband internet access service. Many include one or more characteristics of information service and do not merely facilitate transmission. Nor are they stand-alone offerings. A few examples follow.

25. ISPs may provide user-directed content filtering as part of their broadband internet access offering. These services do not merely facilitate transmission. Rather, they involve the processing of information that results in the change of form and content of information sent over networks. One example of user-directed filtering is Web Guard, which is a free service that T-Mobile makes available to its broadband customers to help restrict adult content from being seen or accessed by family members under 18 years old.[14] This is a service a subscriber opts into for particular access lines, such as for his or her children. Because the filter processes information sent by the user in accessing web sites and because the user does not necessarily receive the requested page, the filtering is an information service. And because network management concerns itself with enabling transmission, a service that selectively makes information available (or, in other words, prevents certain transmissions), is not a network management function. Moreover, all of these services add value to the customer experience beyond mere transmission by making the internet safer for families.

26. Another form of content modification that mobile broadband providers employ is video optimization. To reduce the demand of high-resolution video on mobile devices with small screens, mobile operators optimize the content so as to consume less bandwidth. Such functionality benefits customers on usage-based plans, allowing them to consume more video for the same amount of data consumption. One example is AT&T's "Stream Saver" service, "which allows you to save data on content it recognizes as video by streaming higher definition video at Standard Definition quality on compatible devices (unless the video provider has opted out)."[15] Another is T-Mobile's "Binge On" service, whereby "[a]ll detectable video streaming is optimized for your mobile device so you can watch up to 3 times more video using the same amount of high-speed data."[16] Verizon also engages in video optimization.[17] Optimization of video resolution, particularly if done by video transcoding, is a

---

[14] T-Mobile, "Web Guard," available at https://support.t-mobile.com/docs/DOC-2144 (viewed July 1, 2017). AT&T offers a similar service called "Parental Controls," which can also restrict access to particular web sites. AT&T, "Parental Controls," available at http://www.att.net/parentalcontrols (viewed July 1, 2017). Other examples include Comcast xFi and Cox Parental Controls. See Comcast, "Personalizing and Controlling Your Home Network with XFINITY xFi," available at https://www.xfinity.com/support/internet/personalize-customize-hnetwork-xfi/ (viewed July 3, 2017); Cox, "Parental Controls," available at https://www.cox.com/aboutus/take-charge/parental-controls.html (viewed July 1, 2017).

[15] AT&T, "Stream Saver," available at https://www.att.com/offers/streamsaver.html (viewed May 30, 2017).

[16] T-Mobile, "Binge On," https://www.t-mobile.com/offer/binge-on-streaming-video.html, viewed May 30, 2017.

[17] Verizon, "Explanation of Video Optimization Deployment," https://www.verizonwireless.com/support/video-optimization/ (viewed June 13, 2017).

complex algorithmic process that processes and transforms the content, making it more than transmission.

27. Many ISPs also provide malware detection and alerting services for their customers in accordance with recommendations developed by the FCC's CSRIC III, Working Group 7[18] on Botnet Remediation, including the Anti-Bot Code of Conduct,[19] which typically covers all customers on a network rather than just those that have opted into a service. ISPs, using their routers or other security nodes, can also perform additional security functions, such as protecting web servers and end users against denial of service, detecting viruses, and distributing virus signatures to client systems. All such security functions relate to an information service that processes information that is beyond transmission. Simple transmission would mean that all traffic addressed to a user would be delivered. But instead, the ISP's security system processes the traffic addressed to a user and transforms it by delivering only a subset of the traffic that it deems safe, making the internet a safer place for subscribers.

28. Despite the popularity of email services from companies such as Google, many ISPs provide email service, which is an information service that acquires, stores, processes, and retrieves information. For many ISPs, this email service is bundled with internet access. ISPs that offer email generally also provide an option for a web interface so users can interact with their email without needing an email client program and many also offer an app for smart phones and tablets. Using a web interface or an app adds the functions of generating and transforming information. ISPs that offer email generally also offer spam filtering. This additional offering is an information service, because the spam filter must: (1) retrieve spam-processing criteria; (2) store this information; (3) process the user email by applying it against the criteria; and (4) then transform the content by marking spam messages as spam. Additional information processing associated with email accounts includes blocking email addresses, blocking email domains, white-listing email addresses, white-listing email domains, and forwarding emails to another email address.[20] These ISP email accounts may also have the ability for users to store contact information. Again, these capabilities are not simple transmission. Nor do they facilitate transmission.

---

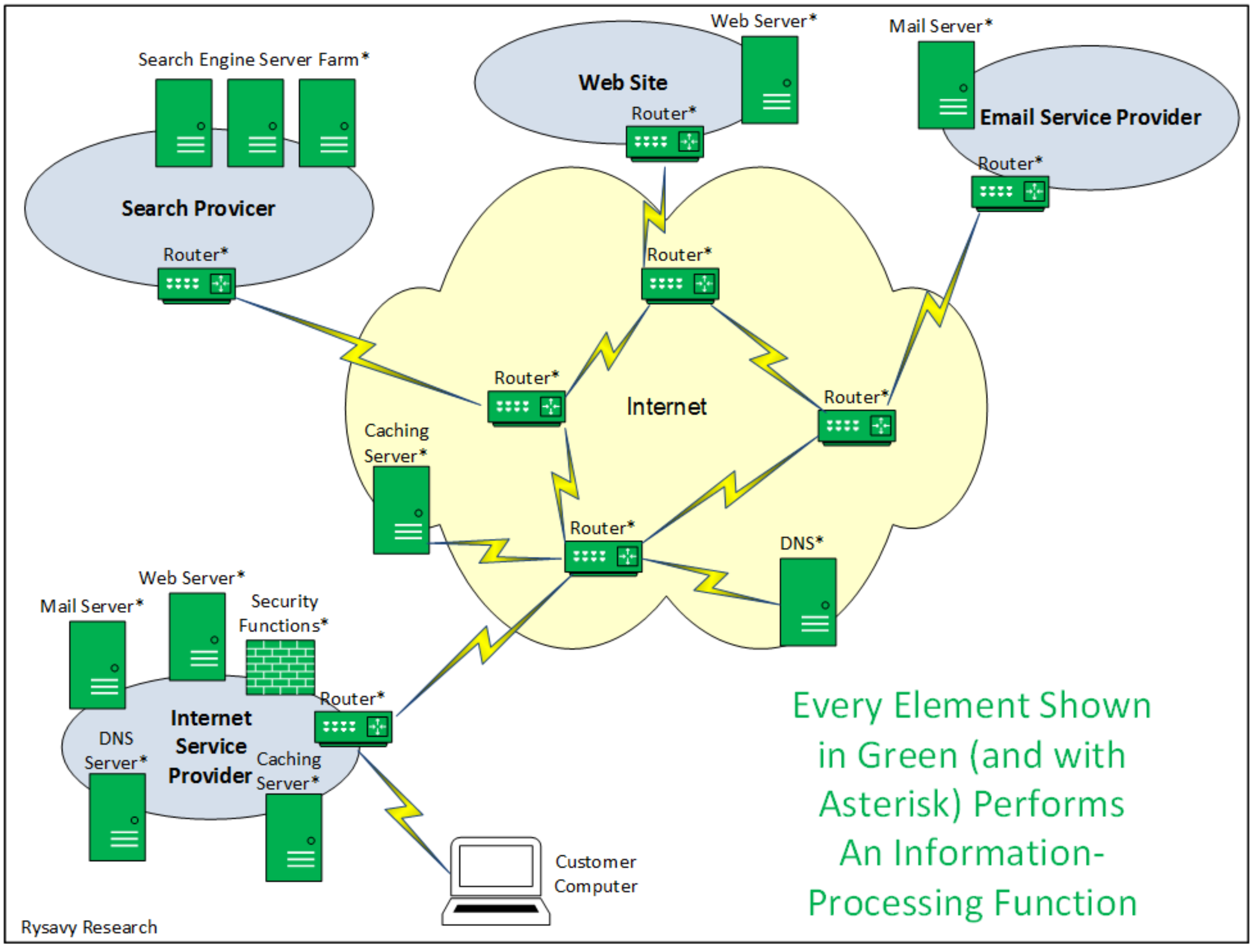
[18] See https://transition.fcc.gov/bureaus/pshs/advisory/csric3/WG%207.pdf.

[19] See https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf and https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.

[20] For example, see Charter, "Email Security," available at http://www.spectrum.net/support/internet/email-security/.

29. The following figure depicts the elements of the Internet discussed above, including routing, mail servers, web servers, DNS, routing, search engine, and the customer's computer. Every element in this diagram shown in green performs an information processing function.

Figure 2: Information Service Nature of the Internet



The Internet and the PSTN are Distinct Platforms

The Internet and PSTN are Separate Networks

30. The internet and the PSTN are two fundamentally different networks, using different architectures and protocols, and providing different capabilities. At the very heart of the PSTN is circuit-switching. On an end-to-end basis (telephone on one end to telephone at the other end), multiple circuits must be set up in series across different nodes before the phone call can occur. The purpose of the PSTN has always been the transmission of telephone calls, using a set of protocols called Signaling System 7 (SS7). The International Telecommunication Union

(ITU), which maintains the SS7 standards, states: "Signaling System No. 7 (SS7) is a set of telephony signaling protocols developed by ITU-T since 1970s, which is used to set up and tear down most of the world's telephone calls."[21]

31. This contrasts with the internet, which was developed for general purpose data-networking and uses packet-switching instead of circuit-switching. With packet-switching, individual packets traverse from node to node to reach their destination, with no connection setup beforehand. Each router that receives the packet makes a decision on how to forward the packet based on the IP address and other information contained in the header. At the end points, TCP handles items such as retransmission of packets and the pace at which it transmits packets so as to reduce network congestion. In contrast, with circuit-switching, the network creates an end-to-end connection using SS7 protocols, potentially across multiple paths, before any telephone communication can ensue. By way of analogy, packet switching is like traveling from one place to the next and not making arrangements for the next leg of the journey until arriving at a destination. In contrast, circuit-switching is like making reservations in advance for every leg of a journey before embarking on the trip.

32. The two approaches could not be more different. The PSTN uses a control architecture that employs the SS7 protocol stack, which is fundamentally different than the TCP/IP protocol stack. Table 1 shows the corresponding protocols relative to the International Organization for Standardization (ISO) Open System Interconnection (OSI) model.[22] The OSI model provides a methodology for characterizing networks. Because the set of protocols differs at every single networking layer, the two networks are completely incompatible with each other and cannot directly interoperate.

---

[21] ITU, "ITU Workshop on SS7 Security," 2016, available at https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx (viewed June 9, 2017).

[22] International Organization for Standardization, *Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model*, ISO/IEC 7498-1:1994, available at https://www.iso.org/standard/20269.html. This model provides a methodology for characterizing networks.

Table 1: TCP/IP Protocol Layers Versus SS7[23]

OSI Layer and Name	Internet: Transmission Control Protocol/Internet Protocol	PSTN: Signaling System 7 Protocol
7: Application	Application	Transactions Capabilities (TC), TUP, ISDN-UP. Also Mobile Application Part (MAP) for cellular networks.
6: Presentation		TUP, ISDN-UP
5: Session		TUP, ISDN-UP.
4: Transport	Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)	Signaling Connection Control Part (SCCP). Also Telephone User Part (TUP) and Integrated Services Digital Network (ISDN) User Part (ISDN-UP).
3: Network	Internet Protocol (IP)	MTP-3
2: Data Link	For example, Ethernet or LTE	MTP-2
1: Physical	For example, Ethernet or LTE	Message Transfer Part-1 (MTP-1)

33. Beyond protocols, the nodes in these networks also differ. In the internet, the interconnecting nodes are routers, which process IP packets and determine which routes to use. In contrast, the telephony network uses the following nodes: Service Control Point (SCP), Signal Transfer Point (STP), and Service Switching Point (SSP).[24] An SCP controls the service in telephone systems, originating and terminating control (signaling) messages; an STP routes SS7 control messages; and SSPs are switches that originate and terminate calls. These nodes are all fundamentally different from the routers used in the internet and perform different functions for a different purpose (as explained above).

[23] SS7 layering source: Figure 2/Q.700, International Telecommunication Union, *Specifications of Signalling System No. 7, Introduction to CCITT Signalling System No. 7 No. 7*, ITU-T Recommendation Q.700, 3/93, available at http://www.itu.int/rec/T-REC-Q.700-199303-I/e.

[24] For a further description, refer to Performance Technologies, *Tutorial on Signaling System 7 (SS7),* available at http://www.eurecom.fr/~dacier/Teaching/Eurecom/Intro_computer_nets/Recommended/ss7.pdf.

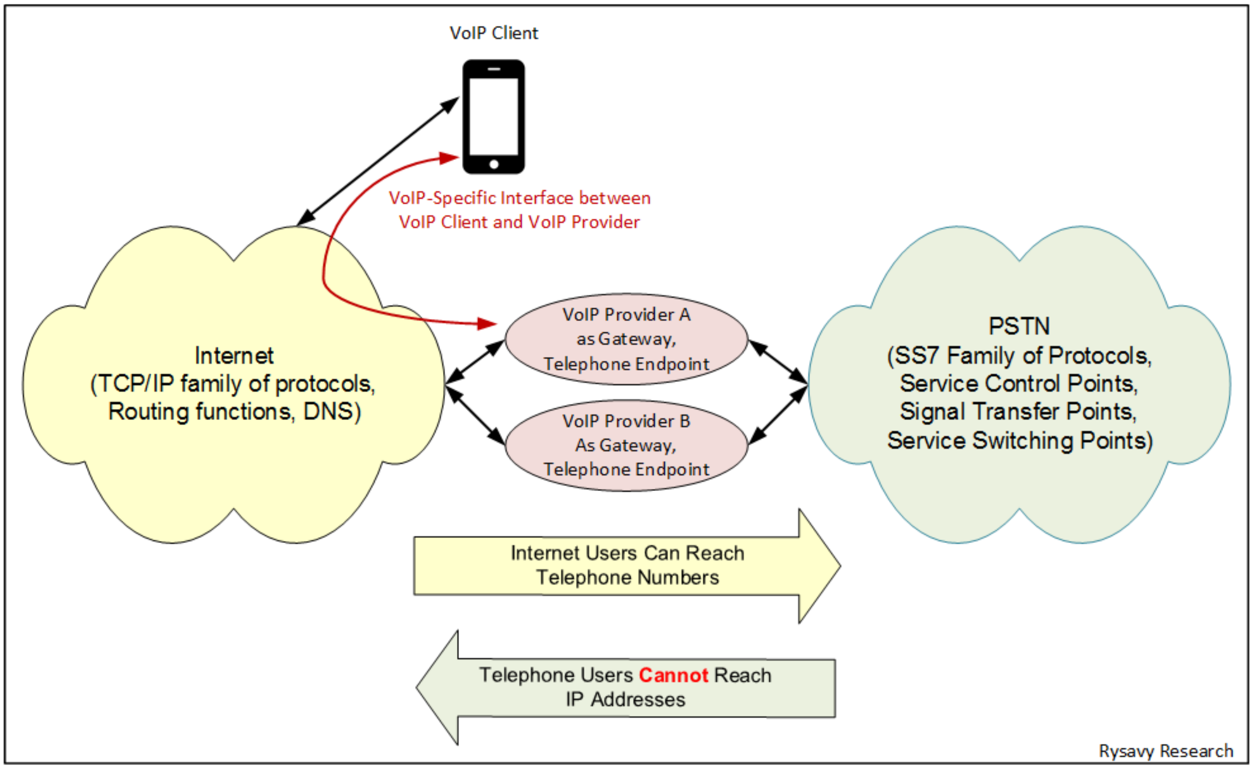
Interconnection of Internet and PSTN

34. The internet and the PSTN, as discussed in the preceding paragraphs, are separate networks that are operated in fundamentally different ways. While it is true that third-party VoIP applications and services enable a limited form of interconnection, these services do not create an integrated network between the internet and PSTN. With a VoIP service, such as from Vonage or a cable operator, a user can make a telephone call from the internet to a phone number on the PSTN, as shown in Figure 3. Such capability, however, is achieved by the VoIP provider (or a service provider on behalf of the VoIP provider) acting as a gateway to translate the different protocols. To the telephone network, the VoIP provider appears as a telephone network node. To the internet, the VoIP provider appears as an internet node. Without the gateway and protocol conversion functions of the VoIP provider, the two networks would not able to communicate with each other. This protocol conversion is not trivial and includes interfaces to the VoIP application (or VoIP gateway device) and PSTN signaling (control) capability. In addition, because internet nodes do not have telephone numbers, the VoIP provider must act as a telephone-number proxy on behalf of the internet node. Customers of these VoIP services may use a telephone number, but the VoIP provider acts as the end point for the voice calls and relays the call through its data (non-telephone) interfaces to the VoIP application, as shown in Figure 3. Over the internet, the call is carried as TCP/IP data traffic, not as a telephone call.

35. An analogy is transporting an automobile on a train car, which allows the passenger and the automobile to travel over the rail system.[25] Such capability does not transform the rail system and road system a single network. Nor does it permit perfect interoperability: Even though this system allows cars to reach any location that trains can go, it doesn't allow trains to go to places that cars can go by road. The same is true of the telephone network and the internet.

[25] For example, see Amtrak, "Auto Train," https://www.amtrak.com/auto-train.

Figure 3: VoIP Operators Providing Gateway Function between the PSTN and the Internet



36. Although internet users, with a subscription to a VoIP service, can make telephone calls to telephone numbers, the reverse is not true, as depicted in Figure 3. Telephone users cannot make connections to IP addresses, nor even to Session Initiation Protocol (SIP) Uniform Resource Identifiers (URIs), which is the most typical form of addressing for VoIP. The concept does not even make sense. Telephones are designed to connect with other telephones using the telephone number. A telephone, for example, cannot send an email or browse a web site. This inability further demonstrates how the existence of VoIP providers does not create an integrated network between internet and PSTN.

37. *The Title II Order's* assertion that mobile voice and data networks have converged is simply not correct. Even within the infrastructure of a modern mobile network, such as a Long-Term Evolution (LTE) network, different infrastructure handles voice than data, and separate gateways handle the interconnections to the internet and the PSTN. Voice in an LTE network is transported over IP packets within the operator infrastructure, but it remains a voice service designed to interconnect with the PSTN. When a user is on a voice call, that voice call does not provide the user any avenue to reach internet end points.

38. For these reasons, mobile broadband internet service and mobile telephony are distinct services that use different infrastructure, different protocols, and different interconnections.

Evolving Mobile Networks and Differentiated Offerings

39. 4G LTE networks implement a sophisticated QoS architecture to manage data flows. Traffic-flow parameters include whether bit rates are guaranteed, their priority relative to other traffic flows, the maximum amount of packet delay that can be tolerated, and the extent of permissible packet loss. LTE specifications define thirteen quality-class identifiers, each with unique parameters.[26] Voice over LTE (VoLTE), based on voice-over-IP protocols, uses these QoS mechanisms to provide carrier-grade voice service. Without this control, an LTE voice call would disintegrate if surrounding users were consuming large amounts of data. The network prioritizes voice as higher priority than data. The same prioritization of voice over data also occurs in 2G and 3G networks.

40. Many other applications could benefit from prioritization. Certain applications work better with network management, including live streaming, gaming, telemedicine, video conferencing (in which video and voice have different requirements[27]). Different applications, however, have different QoS requirements. Streaming music and video for example, requires high throughput but can tolerate delay and some packet loss. A health-monitoring device might consume only small amounts of data but requires high reliability and minimal delay. And, background processes such as application or operating system updates can run at lower priority.

41. A common misconception about traffic prioritization is that prioritizing one traffic stream will harm another. The *Title II Order* perpetuated this misconception by wrongfully concluding that the availability of priority treatment will degrade the experience of other users. The truth of the matter is that traffic differentiation is not a zero-sum game, because selective application of QoS can increase the quality-of-experience across the entire subscriber base.[28] In addition, QoS markings are not simply used to ensure performance of one traffic type over another at

[26] For details about LTE QoS, refer to 3GPP TS 23.203, *Technical Specification Group Services and System Aspects; Policy and charging control architecture*, available at http://www.3gpp.org/DynaReport/23203.htm. Specifically, see Table 6.1.7, "Standardized QCI characteristics."

[27] For instance, users can tolerate momentary video degradation, but voice must remain intelligible.

[28] For an analysis of this topic, see Rysavy Research, *How "Title II" Net Neutrality Undermines 5G*, April 19, 2017, available at http://www.rysavy.com/Articles/2017-04-How-Title-II-Net-Neutrality-Undermines-5G.pdf.

times of congestion. QoS can also be used simply to classify certain traffic types differently so that a particular routing or security policy can be applied to particular traffic types.

42. In the coming 5G world, QoS could play an even more important role than it plays today. The ITU 5G use-case model anticipates three main usage categories of 5G: (1) enhanced mobile broadband; (2) massive-machine type communications; and (3) ultra-reliable and low-latency (URLLC) communications.[29] While 4G networks can handle the first two categories, URLLC , also referred to as mission critical, opens cellular networks to capabilities never before possible, such as advanced industry automation, telemedicine, and drone control. Mission-critical communications will depend on traffic prioritization. The standardization work occurring in 3GPP has already begun addressing the 5G QoS architecture.[30]

43. 5G needs QoS management, not only for traffic prioritization to support mission-critical applications, but also to enable a fundamental capability in its architecture: network slicing. Network slicing, implemented through virtualization, will allow an operator to provide different services with different performance characteristics to address specific use cases. Each network slice operates as an independent, virtualized version of the network.[31] Critical health-care monitoring is an example of a use-case that could benefit from prioritization, in order to address issues such as a congested cell causing communications protocols to time out. Video teleconferencing is another example. 5G QoS management in general, and network slicing in particular, will enable thousands of new types of applications, facilitating entirely new businesses that use wireless connections.

44. 5G networks will offer enhancements to the capabilities of current 4G networks, so the capabilities discussed previously, such as user-directed filtering and video optimization, will also function in 5G networks. 5G networks, however, will process information to an even

---

[29] ITU, *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*, Recommendation M.2083-0, available at http://www.itu.int/rec/R-REC-M.2083-0-201509-I.

[30] 3GPP, Study on New Radio (NR) access technology (Release 14), 3GPP TR 38.912 V14.0.0 (2017-03), available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3059. See Section 11, "QoS," and section 11.1, "QoS architecture in NR and NetGen Core."

[31] For details, refer to 5G Americas, *Network Slicing for 5G Networks & Services*, November 2016, available at http://www.5gamericas.org/files/3214/7975/0104/5G_Americas_Network_Slicing_11.21_Final.pdf. The paper states: "Each slice is defined to meet different service/application requirements, which are represented in a certain QoS level. A QoS level can be defined by certain performance descriptors such as delay, jitter, packet loss and throughput."

greater extent. One example is Multi-access Edge Computing (MEC)[32], a technology that provides a programmable application environment within the radio access network. This approach, being standardized by the European Telecommunications Standards Institute (ETSI)[33], will process information to support applications such as augmented reality, connected cars, and intelligent video processing. Although it is being targeted for 5G, MEC will also be compatible with current cellular technologies. MEC is premised on the fact that simply transporting packets between users and centralized sites does not address all use cases. Consider augmented reality (AR), a new application category with tremendous upside that many large computer companies are now pursuing,[34] thanks in part to the resounding success of Pokémon Go. AR depends on the superposition of computer data on images that the user is viewing on his or her mobile device; thus, the user experience is vastly improved by minimizing the delay of the computer data. MEC, a capability provided by the ISP, will provide the processing at the edge that enhances the AR experience.[35]

[32] Previously called Mobile Edge Computing.

[33] For further details, see ETSI, "Multi-access Edge Computing," available at http://www.etsi.org/technologies-clusters/technologies/multi-access-edge-computing (last visited May 31, 2017). See also the ETSI white paper, "Mobile-Edge Computing," September 2014, available at https://portal.etsi.org/portals/0/tbpages/mec/docs/mobile-edge_computing_-_introductory_technical_white_paper_v1%2018-09-14.pdf.

[34] Global Market Insights anticipates the global market for AR products to reach $165 billion by 2024. See Mark Gurman, *Apple's Next Big Thing: Augmented Reality*, Bloomberg Technology, March 20, 2017, available at https://www.bloomberg.com/news/articles/2017-03-20/apple-s-next-big-thing.

[35] For additional information, see Monica Alleven, "Nokia tests MEC-based applications at University of Notre Dame venue," Fierce Wireless, June 6, 2017, available at http://www.fiercewireless.com/wireless/nokia-tests-mec-based-applications-at-university-notre-dame-venue. For market research on MEC, see iGillotResearch, *The Business Case for MEC in Retail: A TCO Analysis and its Implications in the 5G Era*, 2017, available at https://pages.questexweb.com/rs/294-MQF-056/images/the-business-case-for-mec-in-retail-a-tco-analysis-and-its-implications-in-the-5g-era.pdf.

Appendix: Summary of Technical Specifications

This declaration refers to a number of standards and specifications that relate to internet access being an information service. Table 2 summarizes these standards.

Table 2: Summary of Standards and Other Documents That Relate to Internet Access As an Information Service

Technical Standards Impacting Internet	Description
IETF RFC 1034, Domain Names – Concepts and Facilities, 1987.[36]	An introduction to the Domain Name System.
IETF RFC 1988, Address Allocation for Private Internets.	Use of private addresses to extend the range of internet addresses.
IETF RFC 2475, An Architecture for Differentiated Services.	Means for differentiating traffic flows to enable QoS management.
IETF RFC 6057, Comcast's Protocol-Agnostic Congestion Management System	Application of QoS to prioritize (acquire, process, transform) packets based on the information they contain.)
IETF RFC 7045, Transmission and Processing of IPv6 Extension Headers.[37]	How routers process extension headers in IPv6 for complex routing functions.
IETF RFC 7234, Hypertext Transfer Protocol (HTTP/1.1): Caching, 2014.[38]	Standardizes internet content caching.
IETF RFC 7567, IETF Recommendations Regarding Active Queue Management.	Congestion mitigation methods for the internet.
IETF RFC 7754, Technical Considerations for Internet Service Blocking and Filtering, 2016.[39]	Informational purposes document that "examines several technical approaches to Internet blocking and filtering in terms of their alignment with the overall Internet architecture."

[36] Available at https://www.ietf.org/rfc/rfc1034.txt.

[37] Available at https://tools.ietf.org/html/rfc7045.

[38] Standard available at https://tools.ietf.org/html/rfc7234.

[39] Available at https://tools.ietf.org/html/rfc7754.

Technical Standards Impacting Internet	Description
Named Data Networking (NDN) and Information Centric Networking (ICN)[40]	Not yet standardized, but multiple entities, including the Internet Engineering Task Force, are studying approaches for a new internet architecture in which addressing and routing is based directly on the requested information.
Multi-Access Edge Computing (MEC)[41]	MEC adds information processing at the edge of the network, within the ISP realm, to better support applications such as augmented reality. Applicable to 4G and 5G mobile networks. Being standardized by the European Telecommunications Standards Institute (ETSI).

About Rysavy Research

Peter Rysavy is the president of Rysavy Research LLC, a consulting firm that has specialized in wireless technology since 1993. Projects include analysis of spectrum requirements for mobile broadband, reports on the evolution of wireless technology, evaluation of wireless technology capabilities, strategic consultations, system design, articles, courses and webcasts, network performance measurement, test reports, and acting as an expert in patent-litigation cases. Clients include more than ninety-five organizations.

Peter is a broadly published expert on the capabilities and evolution of wireless technology. He has written more than 160 articles, reports, and white papers, and has taught more than forty public wireless courses and webcasts. He has also performed technical evaluations of many wireless technologies, including cellular-data services, municipal/mesh Wi-Fi networks, Wi-Fi hotspot networks, mobile browser technologies, wireless e-mail systems, and social networking applications.

From 1988 to 1993, Peter was vice-president of engineering and technology at Traveling Software (later renamed LapLink); projects included LapLink, LapLink Wireless, and connectivity solutions for a wide variety of mobile platforms. Prior to Traveling Software, he spent seven years at Fluke Corporation, where he worked on data-acquisition products and touch-screen technology.

[40] See for example, Information-Centric Networking Research Group (ICNRG), which lists various IETF RFCs analyzing information-centric networking approaches. Available at https://trac.ietf.org/trac/irtf/wiki/icnrg.

[41] Standards available at http://www.etsi.org/technologies-clusters/technologies/multi-access-edge-computing.

From 2000 to 2016, Peter was also the executive director of the Wireless Technology Association, an industry organization that evaluates wireless technologies, investigates mobile communications architectures, and promotes wireless-data interoperability. Peter Rysavy graduated with BSEE and MSEE degrees from Stanford University in 1979. More information is available at http://www.rysavy.com.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge and belief.

Executed on July 14, 2017.

Peter Rysavy

Peter Rysavy