Open Access License Notice

Best Paper Award for 2015

Impact of Net Neutrality and the Open Internet Order on Security and Privacy in Education

Lorie M. Liebrock
liebrock@cs.nmt.edu

Judy Holcomb
judy@cs.nmt.edu

Kaley Goatcher
kgoatcher@cs.nmt.edu

Jesse B. Crawford
jcrawford@cs.nmt.edu

Tyler Cecil
tcecil@cs.nmt.edu

New Mexico Institute of Mining and Technology
801 Leroy Place
Socorro, NM 87801
1-575-835-5481

Abstract - The Open Internet Order is the result of a multi-year Federal Communications Commission (FCC) effort to address the challenge of net neutrality. This paper analyzes the impact of the Open Internet Order on universities in terms of standard operating procedures, costs, security, privacy, and quality of education. This paper only considers the US regulations that affect Internet access and their implications on universities. These regulations may also have wide-ranging international implications, which are not considered here.

Categories and Subject Descriptors

K.5.2 [Legal Aspects of Computing]: *Governmental Issues – Regulation*

***General Terms**:* Legal Aspects, Security

***Keywords**: Education, FCC, Internet, Net Neutrality, Open Internet Order, Privacy, Regulation, Section 706, Security, Title II, University*

1. THE WINDING PATH TO NET NEUTRALITY AND THE OPEN INTERNET ORDER

Net neutrality has received extensive media coverage over the past several years. To gain perspective on the history of net neutrality, consider the New York Times listing of stories on this topic. Beginning with a story on January 15, 2006 entitled Hey, Baby Bells: Information Still Wants to be Free, we see early articles on enhancing broadband service and protecting "the anyone-can-publish anything culture of the Internet," showing that net neutrality is not just a recent concern [24]. The mere words "net neutrality" and "open Internet" convey the promotion of free expression and the opportunities for innovation against which few would argue. The Federal Communications Commission (FCC) proceeding, *In the Matter of Protecting and Promoting the Open Internet, GN Docket No. 14-28, Notice of Proposed Rulemaking (NPRM)* [10] has generally been discussed in terms of preserving net neutrality. This requires a brief review of the recent history of attempts to promulgate Internet regulation; it is important to understand the process that has brought Internet regulation to this point. The impending changes in regulatory structure have the potential to impact technology development as well as deployment. The complexities of compliance with a new regulatory framework may have unintended consequences that will become more apparent as end users see changes in their services and costs. This paper presents a historical review and considers impacts on students and universities, with focus on privacy and security.

2. UNFETTERED INTERNET DEVELOPMENT AND DEPLOYMENT

Internet usage and application has expanded exponentially over the past ten years. For context, consider Internet usage penetration. Internet World Stats shows that by 2014, 87.7% of the North American population were Internet users [18]. According to the US Census Bureau, the penetration in the US has gone from 73.5% in 2009 to 88.4% in 2013 [5]. This growth has had tremendous impact on retail; in 2014 alone online retail grew by 15.4% with web sales totaling more than $304B [17, 16].

In addition to this overall growth in Internet use, the Internet has dramatically impacted education. With the advent of Massive Open Online Courses (MOOCs), courses can reach many thousands of students, with one study showing an average of 43,000 students per course [14]. Given the low completion rate of such courses, approximately 6.5%, it is perhaps more appropriate to focus on more traditional educational delivery. In the fall of 2012, for the first time, the Integrated Postsecondary Education Data System (IPEDS) collected data on the number of courses delivered exclusively via distance education [2]. This data shows that approximately 22% of graduate students and 11% of undergraduate students are exclusively taking distance education courses. With the addition of students taking some courses via distance, the report shows that approximately 25% of undergraduate and 30% of graduate students take at least some of their courses via distance education. These statistics provide an indication of the pervasive use of the Internet in education, without even considering use of the Internet by students for research purposes, which happens on a daily basis for many students in higher education.

3. TOWARDS PROTECTION OF AN OPEN INTERNET

The FCC attempted to comprehensively address the need for regulatory support for concepts of net neutrality and an open Internet in the 2010 Open Internet Order, [1], which was overturned by the federal district court in 2014 following an appeal by Verizon [26]. In its decision, the D.C. Circuit Court proposed the FCC rely on section 706 of the Telecommunications Act of 1996 for the legal authority to

impose additional regulation of the Internet on the Broadband Internet access service (BIAS) providers.

In response, the FCC initiated the present proceeding, *In the Matter of Protecting and Promoting the Open Internet, GN Docket No.14-28, with a Notice of Proposed Rulemaking (NPRM)* adopted and released on May 15, 2014 [10]. The NPRM in this matter was intended to solicit comments from a broad cross section of interested parties, including broadband Internet service providers, technology developers, and end users. The NPRM asked for comments to determine the future FCC regulatory alternatives that would maintain Internet openness, while promoting innovation and technology deployment. At the same time, the NPRM requested consideration of the application of Section 706. The Commission also stated in the NPRM they were soliciting comments on the possible application of Title II of the Communications Act as a basis for legal authority to determine the appropriate methodology to ensure ubiquitous Internet access, while spurring technology development and deployment. Section 706 and Title II are discussed further below.

4. SCOPE OF RESPONSE TO NOTICE OF PROPOSED RULEMAKING

The fundamental question posed in the NPRM was "What is the right public policy to ensure the Internet remains open?" [10] It is significant that the FCC received over four million comments, representing a broad cross section of interests.

Figure 1: Word cloud of comments on the NPRM.

The word cloud in Figure 1 provides an indication of the focus of those comments, with each word's size proportional to the percentage of comments including that word. Included in those comments was a filing by the American Association of State Colleges and Universities et al., which focused on the potential impact of the NPRM on universities [4]. It is interesting to note that the very technology under consideration provided the means for the record response to the NPRM.

5. TITLE II, SECTION 706, AND FORBEARANCE

The Internet was developed in a business environment, generally unfettered by government regulation. The "Open Internet Order reclassifies broadband Internet as a 'telecommunications service' under Title II of the Communications Act while simultaneously foregoing utility-style, burdensome regulation that would harm investment ... (the) Order will also use the significant powers of Section 706 not as a substitute but as a complement" [12].

Title II of the Communications Act of 1934, 47 U.S.C. 151 §151 et seq., consists of seven major titles. Title I, General Provisions, had been the basis for the FCC regulation of broadband Internet access service (BIAS) as an information service. In the Open Internet Order, by reclassifying BIAS as a telecommunications service, the FCC asserted the right to regulate under Title II, the common carrier provision. Title II is comprised of 31 sections.

The Telecommunications Act of 1996, Pub. L. No. 104-104, §706(a), 110 Stat. 56, 153, Section 706 addresses advanced telecommunications incentives. The general provisions provide that the FCC and each state commission "with regulatory jurisdiction over telecommunications services shall encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans (including, in particular, elementary and secondary schools and classrooms) by utilizing, in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment" [6].

Universities and other institutes of higher education are not included in Section 706. Commissions were mandated to have initiated a notice of inquiry within 30 months after the passage of the Act, to determine "whether advanced telecommunications capability (were) being deployed to all Americans in a reasonable and timely fashion" [6]. Advanced telecommunications capability "is defined, without regard to any transmission media or technology, as high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology" [6]. If the services were not being reasonably deployed, the commissions were authorized to "take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition in the telecommunications market" [6].

In a series of Section 706 proceedings, various parties petitioned the FCC to take action to stimulate deployment of advanced services. The FCC ultimately determined it had authority to act under Section 706, but that such authority did not permit the agency to treat ISPs as common carriers.

In the Open Internet Order, the FCC opted to forbear from application most of the Title II regulations to BIAS and mobile broadband. Forbearance is the concept of refraining from doing something that one has a legal right to do. In this case, the FCC has refrained from applying full common carrier regulations to Internet services.

6. FORBEARANCE – TITLE II "LIGHT TOUCH"

The Open Internet Order continues the "light-touch" regulatory framework that has resulted in the development of the Internet to date by forbearance of most sections of Title II. The FCC exercised its authority to forbear from application most provisions of Title II as well as over 700 agency rules and regulations. The major provisions of Title II, with the core being Section 201 and 202, that will apply are:

- Section 201, establishing service requirements

- Section 202, preventing discriminatory practices
- Section 208, addressing investigation of consumer complaints and related enforcement
- Sections 206, 207, 209, 216, and 217, enforcing related provisions
- Section 222, protecting consumer privacy
- Section 224, concerning fair access to poles and conduits
- Sections 225 and 255, protecting people with disabilities
- Section 254, increasing universal service support for broadband service through partial section application;

The major provisions subject to forbearance include tariffs and other forms of rate approval, unbundling or other forms of utility regulation. The Open Internet Order is consistent with the theory that the Internet technology and deployment has successfully evolved in the absence of traditional industry-wide rate regulation. The Open Internet Order blends application of both Title II and Section 706 [11].

7. THE OPEN INTERNET ORDER: A NEW PARADIGM

The *Report and Order on Remand, Declaratory Ruling, and Order*, (the Open Internet Order) was adopted on February 26, 2015, and released on March 12, 2015. The Open Internet Order relies on the use of both Title II and Section 706. Tom Wheeler, Chairman of the FCC concisely stated "The Open Internet Order reclassifies broadband Internet access as a 'telecommunication service' under Title II of the Telecommunications Act while simultaneously foregoing utility-style burdensome regulation... and will also use significant powers in Section 706" [12]. Chairman Wheeler stated that "the Open Internet Order will: Ban Paid Prioritization: 'Fast lanes' will not divide the Internet into 'haves' and 'have-nots'. Ban Blocking: Consumers must get what they pay for – unfettered access to any lawful content on the Internet. Ban Throttling: Degrading access to legal content and services can have the same effect as blocking and will not be permitted." He also stated "open Internet protections would – for the first time – apply equally to both fixed and mobile networks" [12]. The adoption of Title II regulation along

with the application of Section 706 for broadband Internet service providers (ISPs) is a significant change in the level of government involvement, which will impact both Internet service providers and end users. Issues raised by the Comments of American Association of State Colleges and Universities et al. [4] addressed the need for an expanded definition of end users to include higher education institutions and libraries. Following this recommendation, those institutions would not be constrained in determining how they used the broadband services they had purchased from public broadband Internet access service providers. This flexibility was adopted in the Open Internet Order such that colleges and universities will continue to be able to provide user services in an academic setting based on individually determined policies, procedures and cost. The implications of this new regulatory structure on the relationships that educational institutions have with broadband Internet access service (BIAS) providers is more difficult to predict; this is one of the inherent results of the transition to Title II. Under the Open Internet Order, colleges and universities, as premise operators, will maintain the ability to negotiate individual contracts with BIAS providers to deliver the bandwidth that the educational institution requires. Alternatively, colleges and universities may file to become ISPs. University options are discussed in more detail below.

8. A BLUEPRINT FOR UNCERTAINTY

The Final Rule in the Open Internet Order was published in the Federal Register on April 13, 2015 [11]. The rule was scheduled to become effective June 12, 2015. Interested parties had 60 days to file to a petition for judicial review.

The Federal Register publication begins the 60-day countdown to the effectiveness of most, but not all, of the new net neutrality rules. The modified information collection requirements in paragraphs 164, 166, 167, 169, 173, 174, 179, 180, and 181 of this document are not applicable until approved by the Office of Management and Budget (OMB). The Federal Communications Commission will publish a separate document in the Federal Register announcing such approval and the relevant effective date(s).

On April 13, 2015, United States Telecom Association filed a Supplemental Petition for Review in the United States Court of Appeals for the District of Columbia in Case No. 15-1083. On April 14, 2015, CTIA – The Wireless Association filed a Petition for Review in the United States District Court of Appeals for the District of Columbia Circuit in Case No. 15-1091. On the same day, AT&T also filed a Petition for Review in the same court in Case No. 15-1092.

At the time of submission of this paper, within one day of publication of the Open Internet Order in the Federal Register, the above referenced three petitions for review were filed. Additional petitions were filed challenging the reclassification of BIAS as a Title II telecommunications service. In addition, the concept of applying forbearance from most provisions of Title II for an entire industry is a novel approach, which will likely provoke a barrage of appeals. As Commissioner Michael O'Rielly stated in his dissenting comment, "all of Title II applied through the backdoor of sections 201 and 202 of the Act, and section 706 of the 1996 Act" [27].

The D.C. Circuit Court declined to stay the Open Internet Order in United States Telecom Association v. FCC. Thus the Open Internet Order became effective on June 12, 2015 [28].

9. EDUCATIONAL IMPLICATIONS

The future implications of the Open Internet Order are not yet clear. The potential impact on students and universities from the perspective of cost, education, privacy, and security is considered below. There are at least two possible interpretations for the treatment of universities under the Open Internet Order that could have substantially different impacts. These possibilities are: universities may be classified as premises operators (POs) or BIAS/ISPs[1].

The university PO classification is currently explicit due to the forbearance that the FCC exercised in classifying universities as premise operators; the FCC declined to apply the open Internet rules and said explicitly "the premise operator would not

[1] Following the Open Internet Order language, BIAS and ISP are used interchangeably.

itself be considered a broadband Internet access service unless it was offered to patrons as a retail mass market service" [11, p149]. ISP classification of universities will come about if universities file for such classification or if and when the FCC forbearance is reversed and the current default classification of universities as POs reverts to the requirement for universities to meet all Title II regulations for ISPs.

One of the impacts of university classification that must be considered is related to the ability to shape (network) traffic. Throttling or traffic shaping allocates bandwidth based on organizational priorities. Historically, universities have used traffic shaping to give high priority to traffic for courses and lower priority to consumer content such as Netflix or social media; this addresses university educational and research missions, while controlling costs.

9.1 Universities as Premise Operators (POs)

Under the Open Internet Order, universities are currently classified as POs. With PO classification, universities are not subject to Title II regulations and can continue to optimize traffic based on the organizational mission. This will allow universities to continue to prioritize access to support their primary student education function, without increasing costs to directly support non-educational functions. For example, courses can be streamed using high priority and optimum bandwidth, while recreational materials may be given lower priority, reduced bandwidth, or may even be blocked.

9.1.1 Possible Impacts on Students

When a student lives in on-campus housing and pays for Internet access as part of their residential fees, the university provides service, but may still throttle to optimize performance for education. In this case, as an individual, the student's access could be restricted dependent on what they are doing. If the student is playing online games or streaming Netflix movies, he/she may have reduced bandwidth, whereas his/her access to course and/or research materials may have higher priority and bandwidth. Ultimately, this is advantageous for students' education – their primary reason for being on campus is given priority.

9.2 Universities as Internet Service Providers (ISPs) or Broadband Internet Access Services (BIAS)

If universities are classified as ISPs, then they will not be able to follow the typical practices that restrict flow based on the type of service being provided. Traffic shaping is often used to shrink the potential for illegal or inappropriate activity coming from universities. This may be done by restricting or blocking the traffic for protocols that are being used on incorrect ports. Traffic shaping has been effective for years on campuses in managing network costs and focusing university resources on the education and research mission, however, this will not be allowable for ISP universities.

9.2.1 Possible Impacts on Students

When a student lives in on-campus housing and pays for Internet access as part of their residential fees, the university acts as the ISP. In this case, as an individual, the student's access would be protected independently of what he/she is doing – from social networking to taking a course using distance infrastructure. At first blush, this is an advantage for students as they can do whatever they want and expect to have the same priority as every other Internet use on campus. However, it is likely that the cost of Internet access would increase to meet the requirements of Title II ISPs and for some students Internet access can be more of a distraction that an educational resource.

9.3 Overall Impact of University Classification

The classification of universities as POs and the associated ability to use blocking, throttling, and prioritization will allow continued control of the cost of education and the quality of educational delivery.

If universities are to be classified as ISPs, they will not be allowed to shape or throttle their campus infrastructure traffic. Therefore, to effectively support their educational and research missions, they will likely be required to pay higher infrastructure costs. The higher costs will be necessary to increase the overall bandwidth to compensate for the requirement to eliminate prioritization of traffic

by application type. This increase in infrastructure costs will have to be passed on to students in the form or increased tuition or fees. Additional costs will be necessary to insure Title II compliance. The classification of universities as ISPs and the associated requirement to eliminate blocking, throttling, and prioritization will likely have a negative impact on the cost and focus of education and research.

University ISPs will have few choices for dealing with the consequences. They could: 1) eliminate Internet access in private spaces, 2) outsource all ISP services in dorms, which will likely increase the cost to students, 3) increase the cost of Internet access in dorms to ensure sufficient bandwidth to compensate for not using traffic shaping and to cover the cost of the extra regulatory mandates incurred by Title II compliance, or 4) eliminate direct charging and increase the general cost of education to provide sufficient bandwidth for all uses, which may be found legally unacceptable.

Each of the ISP options are likely to increase the cost of education, which may then increase student debt and negatively impact higher education.

10. IMPACTS ON PRIVACY AND CONCERNS

Privacy and security are fundamental to universities, regardless of classification as PO or ISP. While the Open Internet Order, for the most part, does not directly address privacy and security concerns, there are several possible impacts on privacy and security. Open Internet Order regulations may directly restrict the ability of BIAS providers to quickly respond to security threats. Simultaneously, the Open Internet Order may prevent some violations of consumer privacy while disincentivizing others.

10.1 Privacy

End-user privacy has been a significant ongoing concern in Internet regulation. Advocates of privacy regulation have focused on the push for net neutrality as a way to advance their agendas. In Europe, a 2011 press release of the organization charged with oversight of privacy regulation stated that "a serious policy debate on net neutrality must effectively address users' confidentiality of communication" [7]. US

law provides significantly fewer protections for consumer privacy than those of the European Union [22], creating even greater demand for increased protection of consumer privacy on the Internet. This is especially important in the case of ISPs, who occupy a privileged position on the network that allows them to capture an immense amount of information about consumers. That data can be highly valuable to advertisers and other commercial users. ISPs can readily determine the websites visited and applications used by consumers; in many cases they can even see the contents of messages sent. This information can be collected without the user's knowledge.

The Open Internet Order does not directly address privacy with new rules, leading some organizations to consider it a partial loss [8]. However, the Order specifically refrained from forbearing on Section 222: Protecting Consumer Privacy, which has historically protected the privacy of telephone consumers. Privacy advocates view the Section 222 protections as unusually strong relative to typical US privacy protection and feel that the FCC has historically been effective in enforcing them [25]. This is a promising improvement over the previous lack of clear regulation preventing disclosure of consumer web usage behavior, if it is interpreted as preventing this kind of use of consumer data.

However, these regulations may be too weak in their application to the Internet. Section 222 protects information about the "quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service" [19], preventing disclosure for most purposes besides provision of service and publication of subscriber lists (as in a phone directory). The exact application of this statute to Internet service remains to be determined, but protections on "type, destination, ... and amount of use" [19] would appear to prevent the disclosure of Internet usage data. However, these terms were written with telephone service providers in mind and their exact application to Internet service is a matter of speculation.

Officials of the Federal Trade Commission (FTC), which generally advocates for consumers on matters including privacy, have observed that the FTC is not able to bring action against Title II common carriers [23]. As such, the Open Internet Order precludes FTC action against ISPs. The FTC has been the primary federal

agency responsible for privacy protection and has been involved in a number of enforcement and policy actions involving ISPs [13]. FTC officials are concerned that FCC privacy enforcement will prove ineffective, leaving consumers with little protection from unauthorized release of their usage data. FCC officials are particularly concerned that Internet regulation significantly expands the scope and complexity of privacy concerns, potentially stretching the limits of FCC enforcement mechanisms [23].

Privacy regulation in the Internet space is complicated by new types of data collection and analysis that are practical with computer technology. In the case of telephone networks, up until recently, and even now, it is not practical for telephone providers to collect and analyze the full contents of all phone calls. Because Internet traffic is in a digital format at all points, mass collection and analysis of data for purposes such as advertising is very practical. This potential is not hypothetical, as this type of tracking has been attempted on a large scale at least once [3].

Internet service providers also have the ability to modify traffic travelling over their networks to enable third-parties to more effectively track their customers, significantly compromising customer privacy in the process. Customer tracking presents a serious concern as several mobile Internet service providers have already experimented with this technique [20, 15].

It is unclear how existing Section 222 privacy protection will apply to these practices, and what, if anything, the FCC will do to address these very real privacy concerns. This is especially true in the case where ISPs modify web traffic in order to enable tracking by third parties—a concern with no clear analogy to Title II's origin as regulation of telephone networks.

The Open Internet Order may have some indirect beneficial privacy effects as it changes the value proposition surrounding collection of consumer data. The Open Internet Order bars many of the reasons ISPs might use information about the nature of consumer data, such as throttling and prioritization based on destination or the service in use. This may eliminate or at least reduce the value

proposition in installing and maintaining expensive deep packet inspection equipment to analyze customer usage.

Finally, the Open Internet Order applies a set of transparency requirements that require disclosure of certain information about services and commercial terms, including a privacy policy. Disclosure of a privacy policy has already been required in most cases, but the Open Internet Order ensures its application to all BIAS providers. Unfortunately, existing privacy policies are often very long and it is impractical for consumers to be fully aware of advertising and tracking practices that may be disclosed deep inside of them [21]. If the Open Internet Order is not interpreted as preventing this type of inspection of consumer data, these practices will likely continue with little consumer awareness.

Overall, the Open Internet Order privacy regulations are not likely to significantly impact universities, as the prohibited behavior is generally inconsistent with university practices. In consideration of their general obligation to protect the privacy of their students and staff, universities may be benefited by these changes being applied to their upstream Internet service if the FCC effectively protects consumer privacy. The final impact on privacy is heavily dependent on FCC interpretation and enforcement of Section 222 rules, a question still to be resolved.

10.2 Security

Because the Open Internet Order regulations significantly restrict the ability of ISPs to block or throttle traffic, there is concern that they will unintentionally restrict the ability of ISPs to manage traffic for security purposes. This will either prevent necessary aggressive responses to evolving security threats or introduce a regulatory burden that creates an unacceptable delay in responding to rapidly spreading threats. Even policies that require security personnel to have security management actions reviewed by legal counsel or receive other vetting before implementation could prevent action during the critical period immediately after detection of a new major threat (such as a virus epidemic or distributed denial of service attack).

ISPs have used several network management techniques to control the spread of malware and other types of security exposures. For example, it is common for residential ISPs to block outgoing simple mail transfer protocol (SMTP) on port 25 because of its frequent use by botnets to send spam email. ISPs have also targeted protocols including Internet Relay Chat (IRC) and NetBIOS to slow specific malware epidemics. ISPs may also entirely disable service to customers with infected computers that may pose a threat to other users. Such action is often a result of compromise by a botnet that may send spam or participate in a distributed denial of service attack.

The situation is more dramatic in universities, which have historically taken a much more aggressive stance to prevent the spread of malware. Most, if not all, universities have a policy of disconnecting any network device that has a known malware infection. Some universities go so far as to require a centrally managed antivirus agent be installed on all devices—including personally owned devices in residence halls—and enforce this by automatically disabling network access for non-compliant devices. This type of network access control is especially important in universities where network architecture and user behavior otherwise often allow malware to spread quickly, which potentially interferes with university operations.

The recently released Open Internet Order regulations provide a broad exception to restrictions for any type of "reasonable network management," which is defined as such [11]:

> *"A network management practice is a practice that has a primarily technical network management justification, but does not include other business practices. A network management practice is reasonable if it is primarily used for and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service."*

Determining the exact limitations of reasonable network management will be critical to establishing the overall impact of the Open Internet Order regulations on

network security operations. To what extent is early control of a potential security concern a legitimate network management purpose?

The Open Internet Order specifically clarifies network security as a motivator for reasonable network management actions, however, these questions remain a major concern as the Open Internet Order explicitly states that reasonable network management will be evaluated on a case-by-case basis. Evolving security threats, such as phishing and social engineering, will likely motivate security practices that are technically sound but push the limits of reasonable network management as currently accepted.

Universities, as premise operators, are currently exempt from these regulations. If, however, universities become subject to regulation as ISPs, they will face significant questions about their ability to continue effective but aggressive security policies such as mandatory host-based security software.

More problematically, universities usually control liability and expenses by throttling or blocking peer-to-peer file transfer protocols and other types of network activity frequently associated with activity of questionable legality. Should universities continue to be exempt as premise operators, they will be free to \ block network traffic of which they do not approve. However, should universities become fully subject to the Open Internet Order as ISPs, they will almost certainly not be able to continue this practice.

Recent enforcement action by the FCC to prevent Comcast's throttling of BitTorrent traffic confirms the FCC's intent to prohibit blocking of services on the basis that they may be used primarily for illegal applications. The action states that blocking services with significant illegal uses does not qualify as reasonable network management under regulation at the time [9].

Loss of the ability to block services that result in frequent complaints of copyright infringement could be a significant added legal liability expenses for universities. Additionally, universities can be more financially effective by refusing to carry network traffic that does not align with the university mission.

11. CONCLUSIONS

Although the FCC has published the Open Internet Order that classifies universities as premise operators unless they petition to be considered Internet service providers, within a single day three petitions for review were filed. This provides an indication of how unsettled the issues surround net neutrality and the Open Internet Order are. Changes in this legislation and its application to universities may affect privacy, security, cost, and standard operating procedures on campuses across the nation. Universities are admonished to watch carefully the evolution of this legislation to protect the privacy, security, and education of students.

REFERENCES

[1] FCC. Preserving the Open Internet Broadband Industry Practices, GN Docket No. 09-191, WC Docket No. 07-52, Report and Order, 25 FCC Rcd 17905 (2010).

[2] National Center for Education Statistics, U.S. Department of Education, "Enrollment in Distance Education Courses, by State: Fall 2012", 23rd Edition, NCES 2014-023, 2014.

[3] N. Anderson. "NebuAD CEO defends web tracking, tells Congress it's legal", Ars Technica, July 9, 2008.

[4] American Association of State Colleges and Universities, American Council on Education, American Library Association, Association of American Universities, Association of College & Research Libraries, Association of Public and Land-grant Universities, Association of Research Libraries, Chief Officers of State Library Agencies, Council of Independent Colleges, EDUCAUSE, and Modern Language Association, Comments of, Apps.fcc.gov, July 18, 2014.

[5] U.S. Census Bureau, "Computer and Internet use", http://www.census.gov/hhes/computer/, accessed 2015.

[6] 47 U.S.C. §1302, "Advanced Telecommunications Incentives", 2015.

[7] European Data Protection Supervisor, "A serious policy debate on net neutrality must effectively address users' confidentiality of communication", Press Release, October 7, 2011.

[8] K. Walsh, "Today's Net Neutrality Order is a Win, with a Few Blemishes", Electronic Frontier Foundation, March 12, 2015.

[9] In the matter of formal complaint of Free Press and Public Knowledge against Comcast Corporation for secretly degrading peer-to-peer applications and broadband industry practices petition of Free Press et al. for declaratory ruling that degrading an internet application violates the FCC's internet policy statement and does not meet an exception for "reasonable network management", Federal Communications Commission, File No. EB-08-IH-1518, WC Docket No. 07-52, Memorandum Opinion and Order, August 1, 2008.

[10] In the Matter of Protecting and Promoting the Open Internet, Federal Communications Commission, GN Docket No. 14-28, Notice of Proposed Rulemaking, May 15, 2014.

[11] In the Matter of Protecting and Promoting the Open Internet, Federal Communications Commission, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, March 12, 2015.

[12] T. Wheeler, "Statement of Chairman Tom Wheeler, Re: Protecting and Promoting the Open Internet, GN Docket No. 14-28", FCC-15-24a2, DOC-332260A2, March 10, 2015.

[13] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers", March, 2012.

[14] G. Ferenstein. "Study: Massive Online Courses Enroll an Average of 43,000 Students, 10% Completion", TechCrunch, March 3, 2014.

[15] K. Hill. "AT&T Says it's 'Testing' Unique Tracker on Customers' Smartphones", Forbes, October 28, 2014.

[16] A. Enright, "U.S. Annual e-retail Sales Surpass $300 Billion for the First Time", Internet Retailer, February 17, 2015.

[17] Internet Retailer, "The All-New 2015 Top 500 Guide", 2015.

[18] Internet World Stats, "World Internet Users Statistics and 2014 Population Stats", June 30, 2014.

[19] 47 U.S.C. §222, Privacy of Customer Information, 2015.

[20] J. Mayer. "How Verizon's Advertising Header Works", Webpolicy.org, October 24, 2014.

[21] A. M. McDonald and L. F. Cranor. "Cost of Reading Privacy Policies", I/S A Journal of Law and Policy for the Information Society, 4:543, 2008.

[22] L. B. Movius and N. Krup, "US and EU Privacy Policy: Comparison of Regulatory Approaches", International Journal of Communication, 3:19, 2009.

[23] J. Bracy, "FTC Officials Concerned about Jurisdiction after FCC Net Neutrality Order", The Privacy Advisor, March 10, 2015.

[24] The New York Times, "Net Neutrality", http://topics.nytimes.com/top/reference/timestopics/subjects/n/net_neutrality/index.html, accessed 2015.

[25] A. Peterson, "The FCC's Net Neutrality Decision Could Mean Stronger Privacy Rules for Internet Service Providers", Washington Post, February 17, 2015.

[26] "Verizon v. FCC", 740 F.3d 623 (D.C. Cir. 2014).

[27] M. O'Rielly. "Dissenting Statement of Commissioner Michael O'Rielly Re: Protecting and Promoting the Open Internet, GN Docket No. 14-28", FCC-15-24a6, DOC-332260A6, March 10, 2015.

[28] L. Beck. "Open Internet Order Unstayed & Effective", Federal Regulation Advisor, June 15, 2015.