
The Federal Communications Commission ("FCC" or "Commission") released a Memorandum Opinion and Order ("Order") on July 24, 2012, with regard to the dispute between Tennis Channel, Inc. ("Tennis Channel") and Comcast Cable Communications, LLC ("Comcast"). The Order, a 3-2 decision, affirms the following conclusions made by an Administrative Law Judge ("ALJ"): (1) Comcast, a multichannel video programming distributor ("MVPD"), violated the FCC’s program carriage rules through its preferential treatment of Comcast-affiliated programming networks over those networks which were similarly-situated and unaffiliated with Comcast; (2) Comcast effectively restrained the Tennis Channel’s ability to compete fairly in violation of section 616 of the Communications Act and 47 C.F.R. § 76.1301(c) of the Commission’s rules through its carriage discrimination against Tennis Channel, a non-affiliated video programming vendor or network; and (3) Comcast must pay Tennis Channel a forfeiture of $375,000 and carry Tennis Channel at the same level of distribution as Golf Channel and Versus (now NBC Sports Network), similarly-situated and Comcast-affiliated networks. The Order significantly marks the first time that an MVPD has been found in violation of the FCC’s federal anti-discrimination program carriage rules since the statute’s adoption in 1993.

The dispute originated in 2010, when Tennis Channel filed a complaint against Comcast under section 616 of the Communications Act, 47 U.S.C. § 536, which pertains to discrimination in carriage agreements. Initially, the ALJ issued a decision in favor of Tennis Channel, concluding that Comcast violated the program carriage rules, prompting Comcast to appeal the decision to the Commission. Following a de novo review of the ALJ’s decision, the Commission supported the ALJ’s overall conclusion that Comcast discriminated with regard to carriage against Tennis Channel and in favor of Golf Channel and Versus on the basis of affiliation in violation of section 616 of the Act and section 76.1301(c) of the Commission’s rules. As to remedies, however, Comcast retains “full discretion in determining the level of penetration it chooses to carry the free channels” and the Commission rejected the ALJ’s ordered channel placement remedy.
Congress added section 616 to the Communications Act through the Cable Television Consumer Protection and Competition Act of 1992, in effect governing the carriage requirements between MVPDs and video programming vendors. These regulations aim to prevent MVPDs from engaging in discriminatory conduct or that which unreasonably restrains video programming vendors through video programming distribution that is based on whether or not the network is affiliated with the MVPD. According to the Act, an "affiliate" means another person or company who is owned or controlled or owns and controls another, or has the same ownership. The FCC implemented section 616 in an administrative regulation at 47 C.F.R. § 76.1301.

In its July ruling on Comcast’s appeal from the decision of the ALJ, the Commission affirmed the ALJ’s fine and equal distribution determination. The equal distribution remedy means that Tennis Channel has to be carried on the same distribution tier as Golf Channel and NBC Sports Network. But the Commission vacated the ALJ’s decision to grant the equitable channel placement remedy because “the record does not sufficiently establish that Tennis Channel’s ability to compete fairly was unreasonably restrained by its channel placement.” The equitable channel placement remedy would have required Comcast to place Tennis Channel close to Golf Channel and NBC Sports Network in its channel listings.

The majority of FCC commissioners determined that Tennis Channel is similarly situated to Golf Channel and NBC Sports Network because they carry similar sports programming, appeal to similar viewer demographics, solicit similar advertisers, and have almost identical ratings. The majority concluded that Comcast’s position as the largest MVPD with 23 million subscribers created a “ripple effect,” such that “one MVPD’s decision to carry a network at a specific level of distribution increases the likelihood that another MVPD will carry that network at the same level of distribution.” Therefore, the majority of commissioners reasoned, the fact that other MVPDs carried the Tennis Channel at a similar or worse tier than Comcast was the result of Comcast’s decision and direction and could not be used as objective evidence of where the market would carry the Tennis Channel but for Comcast’s choice. The majority also gave no weight to Comcast’s claim that it conducted a cost-benefit analysis in determining Tennis Channel’s placement because a Comcast executive admitted that it did not provide a complete analysis by failing to quantify “what Comcast might have gained by moving The Tennis Channel to a more widely-distributed tier.”

Two of the five FCC Commissioners, McDowell and Pai, disagreed with the majority decision, writing that the majority’s analysis relied on the incorrect assumption that Comcast treated Tennis Channel differently than every other major MVPD (those with 2 million subscribers or more) in the United States.
However, not one major MVPD found Tennis Channel to be "similarly situated" to Golf Channel and Versus when making carriage decisions. No meaningful difference exists between Comcast's distribution of Tennis Channel to that of other major MVPDs with no ownership interest in Tennis Channel. Thus, McDowell and Pai found that the majority's statistical analysis was fundamentally flawed.

Finally, the dissent said the majority's decision will have a broader, negative impact on consumers. Arguably, Comcast and other MVPDs will be incentivized to carry networks they do not want on tiers with broader penetration, and at higher prices than ever before, simply out of fear of discrimination suits. Furthermore, the MVPDs' additional programming costs "will come out of the pockets of consumers, not from MVPDs' bottom lines."

The Order does not mark the end of the program carriage dispute between Comcast and Tennis Channel. Comcast has appealed the FCC's decision in the United States Court of Appeals for the District of Columbia on the ground that the decision is "arbitrary, capricious, and an abuse of discretion." Though the Commission denied Comcast's petition to stay the Order pending the federal court's decision, the circuit court granted a stay of the Order pending appeal. The Court of Appeals has slated oral arguments for February 2013.

Summarized by Abbi Hutcherson

_In re Applications of Cellco Partnership d/b/a Verizon Wireless and SpectrumCo LLC and Cox TMI, LLC For Consent To Assign AWS-1 Licenses; Applications of Verizon Wireless and Leap for Consent To Exchange Lower 700 MHz, AWS-1, and PCS Licenses; Applications of T-Mobile License LLC and Cellco Partnership d/b/a Verizon Wireless for Consent to Assign Licenses, Memorandum Opinion and Order and Declaratory Ruling, 27 F.C.C.R. 10698 (Aug. 21, 2012)._
these concerns.

I. PROPOSED TRANSACTIONS

Three series of applications were addressed in the Opinion and Order. The first was an application between Verizon Wireless ("Verizon") and Leap Wireless International Inc. ("Leap") that included (1) assignment from Verizon Wireless to Leap of a lower 700 MHZ Band Block A license for the Chicago Basic Economic Area ("BEA"); (2) assignment from Leap to Verizon of twenty-three PCS licenses and thirteen AWS-1 licenses, disaggregated portions of one Personal Communication Services (PCS) license and one AWS-1 license, and partitioned portions of three AWS-1 licenses; and (3) assignment of partitioned portions of Leap's AWS-1 licenses to Verizon Wireless. As proposed, Verizon would acquire an additional ten to twenty megahertz of PCS spectrum and 10-30 megahertz of AWS-1 spectrum in 202 CMAs. Leap would gain an additional twelve megahertz of Lower 700 MHZ spectrum in thirteen Cellular Market Areas ("CMAs") in the Chicago BEA in the transaction.

In a second series of applications, Verizon Wireless sought AWS-1 licenses from numerous cable companies, via SpectrumCo, LLC and Cox TMI, LLC. This transaction sought to assign 122 of SpectrumCo's AWS-1 licenses and thirty of Cox's AWS-1 licenses to Verizon (hereinafter "SpectrumCo-Cox Assignments"). The licenses included 121 BEA licenses and one Regional Economic Area ("REA") license from SpectrumCo, and thirty BEA licenses from Cox. Approval of the SpectrumCo and Cox assignments would provide Verizon near nationwide coverage, with an additional twenty to thirty megahertz of AWS-1 spectrum in 630 out of 734 CMAs nationwide. As part of a larger transaction tied to this series of applications, Verizon had also entered into commercial agreements ("Commercial Agreements") with the cable companies that provided: (1) Verizon, SpectrumCo, and Cox the right to act as sales agents of one another's services; (2) each company the option to become resellers of Verizon's services after four years; and (3) a joint venture among Verizon, Comcast, Time Warner Cable, and Bright House to develop ways to integrate wireline and wireless services.

In response to initial Commission and DOJ staff concern over spectrum aggregation, Verizon initiated negotiations in a third series of applications to divest certain AWS-1 licenses it would acquire as a result of the transactions initially proposed. Verizon Wireless and T-Mobile License LLC ("T-Mobile") sought Commission consent for the full and partial assignments of AWS-1 licenses by and between T-Mobile and Verizon Wireless. These assignments were contingent upon the Commission's approval of the SpectrumCo and Cox assignments, as well as the Leap assignments. Under this transaction, T-Mobile
would hold an additional ten to twenty megahertz of AWS-1 spectrum in 125 CMAs, and Verizon Wireless would hold an additional ten to twenty megahertz of AWS-1 spectrum in seventeen CMAs.

II. PUBLIC INTEREST CONSIDERATIONS

The FCC addressed concerns regarding these transactions and their potential effects on public interest. The Communications Act requires the Commission to closely examine the impact of spectrum aggregation on competition, innovation, and efficiency of spectrum use. This review consists of an examination of potential harms to the public interest, along with any verifiable, transaction-specific benefits that would further the public interest. Moreover, the Commission may impose additional remedial conditions to address these benefits.

In the Opinion and Order, the Commission acknowledged applicant claims that their proposed transactions would result in a more efficient use of spectrum. The additional spectrum would provide Verizon Wireless with the means to meet growing consumer demand for better broadband services, which will enable it to better serve its customers. In considering the potential effects of the proposed Leap assignments of twelve megahertz of lower 700 MHz A-block spectrum from Verizon Wireless in thirteen CMAs, the Commission found that the transaction is unlikely to result in competitive harms. In addition, the Commission found that competitive harms were unlikely to result from the T-Mobile Verizon Wireless assignments. Because they were unlikely to result in competitive harms in local markets, the T-Mobile Verizon assignments were also unlikely to result in nationwide price increases.

However, the Commission expressed concern over a potential for public harm under the proposed SpectrumCo and Cox assignments, in markets where Verizon Wireless would hold twenty to forty megahertz of the AWS-1 spectrum. Specifically, if Verizon does not quickly deploy all of the spectrum it would acquire, the transaction could cause a ripple-effect that would result in a loss of competition and nationwide effects on prices in various local markets.

III. CONSENT DECREE

To allow the transactions to move forward, the Commission and the Department of Justice Antitrust Division negotiated a proposed consent decree, requiring Verizon Wireless, SpectrumCo, and Cox to amend the Commercial Agreements. An amendment to the Commercial Agreements will ensure that there is no restriction on Verizon Wireless's sale of any Verizon service; to ensure there is no restriction on Verizon Wireless's ability to authorize, permit, or enable Verizon to sell in combination with any broadband, telephone, or
video programming distribution services; and to ensure that consumers have options to receive service packages from multiple competitors.

IV. CONCLUSION

With the conditions proposed in the Consent Decree, the FCC concluded that the approval of these transactions will serve the public interest. Furthermore, the transactions will allow the service providers to put the spectrum to use that will provide better service to their customers.

*Summarized by Talon Hurst*

*In re Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions, Notice of Proposed Rulemaking, 27 F.C.C.R. 12,357 (Sept. 28, 2012).*

On September 28, 2012, the Federal Communications Commission ("FCC" or "Commission") adopted a *Notice of Proposed Rulemaking ("NPRM")* launching the incentive auction process contemplated in the Middle Class Tax Relief and Job Creation Act of 2012 ("Spectrum Act"). According to the FCC, these auctions are market-based tools to repurpose broadcast television spectrum for mobile broadband by offering unique financial opportunities to broadcasters, including a portion of the auction proceeds for participants.

The broadcast spectrum incentive auction will be the first such auction attempted worldwide and will serve as a model for other countries facing similar spectrum squeezes. Demand for the finite broadcast spectrum has soared with the rise of sophisticated mobile devices like smartphones and tablets that require much more spectrum than traditional cell phones. As a result, the U.S. faces a major challenge to ensure that wireless networks keep pace with these demands in the years ahead. According to the FCC, "meeting this challenge is essential to continuing U.S. leadership in technological innovation, growing our economy, and maintaining our global competitiveness."

I. THREE-PART AUCTION PROCESS

The *NPRM* outlines a three-part auction process that includes: (1) a “reverse auction” in which current broadcast licensees submit bids to relinquish their spectrum in return for payment; (2) a “repacking” or repurposing of the reclaimed spectrum to accommodate mobile broadband and other uses; and (3) a more conventional “forward auction” to license the reclaimed and repurposed
spectrum.

The first component, the reverse auction, involves the collection of bids from current television broadcast licensees who, if selected, would agree to voluntarily relinquish their rights in exchange for payment. Among the issues left unclear and upon which the Commission now seeks comment are details of how to collect bids and how to determine the winners as well as the amount of the winner’s payments.

The second major component of the incentive auction outlined by the Commission in the *NPRM* is the repacking process. This process includes reorganizing the broadcast television bands in a way that allows television stations to continue being broadcast while using less of the highly sought-after UHF band. This would be accomplished by repacking or shifting the broadcasts to the VHF band. However, this proposal raises several issues, as certain VHF channels are particularly susceptible to interference and both the Spectrum Act and treaties require coordination with Canada and Mexico when dealing with spectrum authorization changes near their respective borders. The ultimate goal of repacking is to create contiguous blocks of spectrum from the UHF band that could then be used for flexible use, including Mobile TV and other mobile operations.

The Commission labels the third element of the incentive auction the “forward auction.” It is similar to a traditional competitive bidding auction, whereby bids are placed for flexible-use spectrum licenses. However, the quantity and specific frequencies of spectrum available for bidding will not be known in advance, but rather depend on the success of the repacking and reverse auction. With the forward auction, the Commission’s goal is to establish a framework that will accommodate different quantities and frequencies of newly available spectrum, as opposed to more traditional single band plans with fixed frequencies.

As the Commission details in the NPRM, the three major elements of the incentive auction are highly interdependent. For example, the process that is chosen for the repacking will directly affect the acceptance of broadcaster bids in the reverse auction, as broadcasters with rights to spectrum that is not part of any repacking will not be eligible to participate in the reverse auction. However, the Commission seeks comment on whether or not to expand participation in the reverse auction, and whether to establish reverse auction bid options that include “going off the air, switching from a UHF to VHF television channel, or sharing a channel.” The Commission also seeks comment on several other aspects of the proposed auction process as well. This includes the appropriate sequencing of the auction process, specifically whether the forward auction should take place before, after or at the same time as the repacking or the reverse auction. The Commission also seeks comments on procedures for col-
lecting bids and determining winners and payment amounts for the auctions.

II. PROPOSED ALLOCATION FOR NEW WHITE SPACE AND UNLICENSED USE SPECTRUM

In addition to the three major elements of the proposed incentive auction of broadband television spectrum, the NPRM proposes and seeks comment on a plan to alter the current allocation of the 600 megahertz band. The Commission proposes using five megahertz blocks rather than six megahertz blocks for reclaimed spectrum, while establishing six megahertz “guard bands” between mobile and broadcast operations to minimize or prevent interference.

As part of its overarching goal of repurposing “the maximum amount of UHF band spectrum for flexible licensed and unlicensed use,” the Commission also proposes measures that would make more spectrum available for unlicensed “white space” uses, including, for the first time, a portion of spectrum available on a uniform nationwide basis. In addition to making repacked spectrum available for unlicensed use, the proposed 600 megahertz band plan proposes moving the Radio Astronomy Service and wireless medical telemetry service (“WMTS”) from channel 37. Currently, channel 37 is reserved for receive-only, non-interfering radio astronomical scientific research, and for WMTS, which enables medical equipment to transmit critical patient data. The proposed plan would, in essence, make the 600 megahertz band available for unlicensed use.


The Middle Class Tax Relief and Job Creation Act of 2012 (Act), signed into law February 22, 2012, created the First Responder Network Authority (FirstNet). The Act requires that the Federal Communications Commission (“FCC”) reallocate and grant a license to FirstNet for the use of the 700 MHz D-block spectrum and the existing public safety broadband spectrum. FirstNet is an independent authority within the National Telecommunications and Information Administration (“NTIA”). FirstNet’s authority ends in 2027. The Act grants FirstNet the authority to hold a single nationwide public safety wireless license. With that broad authority, FirstNet can take all actions necessary to build, deploy, and operate the nationwide public safety broadband network. FirstNet’s license is an exclusive ten year license, renewable for a
maximum of ten years. The FirstNet Board of Directors ("Board") held its first meeting on September 25, 2012, thereby initiating the planning phase for the network.

The fifteen member Board has three permanent members: the Secretary of the Department of Homeland Security, the Attorney General, and the Director of the Office of Management and Budget. The remaining twelve members, appointed by the Secretary of Commerce, include individuals with extensive knowledge and expertise in telecommunications, public safety experience such as police officers and firefighters, and those representing the interests of the states and local government. The Board is charged with making strategic decisions regarding the execution of FirstNet operations. To assist in carrying out FirstNet's duties, the Act mandates the creation of an advisory committee. At its first meeting, FirstNet designated a subgroup of SAFECOM, an emergency communications program of the Department of Homeland Security's OEC and OIC, as its public safety advisory committee.

The purpose behind FirstNet is to designate a communications network completely dedicated to facilitating communication among public safety first responders. Currently, first responders use commercial broadband networks such as Verizon or Sprint, which is problematic as the network can slow or stall with traffic at a high volume. These broadband networks are unreliable, unstable, and cannot meet the specific needs of first responders.

This dedicated network will provide for better and faster communication among police, firefighters, emergency services personnel, and other first responders during emergencies through a nationwide wireless broadband network. By providing "dramatically" superior "communication and collaboration among multiple public safety agencies," Congress hopes to improve response time during emergencies, keep communities safe, and save lives. With a network dedicated to first responders and broad authority to build and operate the network, FirstNet has a great breadth of possible real world applications. The type of communication possible with FirstNet could include the following: a blueprint application for firefighters whereby they can map a burning building and assess the best point of entry; the ability to send live video feeds of natural disasters to a command center; lessened communication time between a police precinct and the dispatched officer; and unimpeded communication to officers at a sporting event where private networks are likely slowed by those in attendance. The hope is that FirstNet will evolve with technology to continue providing dramatically superior communication among first responders.

FirstNet is charged with creating and promoting the integration of the network with public safety answering points, or its equivalent. Where public safety communication infrastructure already exists, FirstNet will have to create partnerships to ensure cost effective use of the network and equipment.
FirstNet is responsible for establishing nationwide standards for use and access to the network. The network will require national and regional data centers that provide connectivity between a radio access network and a public Internet or switched network, or both.

To promote and acquire this integration, FirstNet must consult with state, tribal, and local authorities regarding the construction of the network and any radio access network build out, placement of towers, coverage areas, network maintenance, assignment and selection of entities seeking to access or use the network, and training needs of local users. FirstNet will ensure the safety, security, and resiliency of the network, address special considerations in areas and regions with unique homeland or national security needs, and guarantee substantial and fast rural coverage.

To fund FirstNet, Congress created a Public Safety Trust Fund and provided the FCC with authority to administer several spectrum auctions to fund it. First, the Act makes available several bands currently used by the federal government. Proceeds exceeding the cost of reallocating the current federal users of the designated spectrum will be made available to FirstNet. The Act also directs the FCC to initiate incentive auctions of spectrum currently used for broadcast television. Current licensees of this spectrum would relinquish control of their licensed spectrum in exchange for a share of the auction proceeds. The first $1.75 billion in proceeds from the incentive auction will fund the TV Broadcaster Relocation Fund; through 2022, funds in excess of that amount will go into the Public Safety Trust Fund. After 2022, the authorization for the trust expires, and any funds remaining are to be used for deficit reduction.

The Act allows FirstNet to charge a network user fee to all public safety entities, a lease fee to non-public safety entities wishing to access the network, and an equipment and infrastructure fee to any non-public safety entity wishing to access equipment such as towers or antennas. No dollar cap is specified, but FirstNet must charge a sufficient yet reasonable amount for access and use. FirstNet is estimated to raise $15 billion over the next 11 years.

At its first meeting, a preliminary network design was proposed and members discussed a general idea for developing public safety specific applications (e.g., a blueprint application for firefighters). During its open comment period on suggestions for a network design, FirstNet drew a wide array of responses including those from experts, private wireless companies, and state governments. In mid-November of 2012, the FCC officially granted FirstNet a single ten-year renewable license for the 700 MHz D-block spectrum, marking another important step toward the construction of this dedicated network.

Summarized by Adi Nunez

On July 19, 2012, the Chairman of the Senate Homeland Security and Governmental Affairs Committee, Senator Joseph Lieberman, and Senators Susan Collins, Jay Rockefeller, Diane Feinstein, and Tom Carper introduced the Cybersecurity Act of 2012 ("Act"). The Act amends a number of existing federal laws, coordinates activities between several key agencies, and creates the National Cybersecurity Council. The Act is split into seven titles. Despite the acknowledged need to improve cybersecurity coordination and information sharing, the Senate, after several attempts, could not overcome procedural hurdles within the chamber and the legislation died with the end of the 112th Congress. The legislation will have to be reintroduced in the 113th Congress.

I. TITLE I: PUBLIC-PRIVATE PARTNERSHIP TO PROTECT CRITICAL INFRASTRUCTURE

Title I would create a National Cybersecurity Council ("Council") comprised of members drawn from several agencies and appointed by the President. Led by the Secretary of the Department of Homeland Security ("Secretary"), the Council would be responsible for assessing risk to critical cyber infrastructure ("CI"). As defined, Critical CI includes those entities that, if destroyed, interrupted, or taken over by a hostile entity, could “reasonably result in . . . the interruption of life-sustaining services . . . a mass casualty event; or mass evacuations . . . [or] catastrophic economic damage to the United States.” In addition, critical CI covers systems that, if disrupted, would lead to “severe degradation of national security or national security capabilities.” Title I would require the Council, through one of its member-agencies, to assess and prioritize CI by order of importance within a Council-maintained inventory. The Council would coordinate the adoption of voluntary cybersecurity practices, which would be developed by the private sector. To encourage adoption of these voluntary standards, the Council would establish a certification program which would entitle certified entities to certain incentives, such as immunity from certain punitive damages in claims stemming from harm caused by a cyber attack and the expedited issuance of security clearances. Title I further requires the Council provide an annual comprehensive report to Congress, detailing both the Council’s actions and public and private activity related to remediation or mitigating threats to CI. Finally, Title I requires the Council to identify and coordinate international compliance through the Department of State.
II. TITLE II: FEDERAL INFORMATION SECURITY MANAGEMENT AND CONSOLIDATING RESOURCES

Title II amends the Federal Information Security Management Act (FISMA), which requires federal agencies to develop and implement comprehensive plans to protect sensitive data and information. The Act shifts FISMA authority from the Office of Management and Budget to the Department of Homeland Security ("DHS"), with exceptions for security agencies such as the Department of Defense. These security agencies will, like all other agencies, be required to report to the Secretary on information and data security practices, but may, at their discretion, withhold from DHS sensitive data and information. Non-security agencies, on the other hand, will not have such discretion.

III. TITLE III: RESEARCH AND DEVELOPMENT

Title III directs the White House Office of Science and Technology Policy ("OSTP"), through coordination with DHS, other relevant federal agencies and higher education institutions, to "build upon [existing] programs . . . to develop a national cybersecurity research and development plan." This comprehensive plan will be updated every two years and will focus on: design, testing, and verification of secure systems; ensuring data privacy for such systems; promoting data security on the Internet; authenticating messages and information obtained over the Internet; identifying and overcoming insider threats in secure systems; improving consumer and user literacy related to systems and Internet security; and other directives determined by OSTP and DHS. Under this title, OSTP would take the lead in coordinating federal cybersecurity research and development efforts while the National Science Foundation ("NSF") would be authorized to create a grant program for cybersecurity research and training.

IV. TITLE IV: EDUCATION WORKFORCE, AND AWARENESS

Title IV directs DHS, in coordination with other federal agencies, to develop a campaign to foster and promote cybersecurity education programs in higher education. Concurrently, NSF would evaluate and report to Congress the status and capabilities of cybersecurity education programs at institutes of higher education within the United States. Title IV would also create a public–private consortium tasked with developing cybersecurity awareness and training programs to prepare members of the community to respond to a cyberattack or threat. Furthermore, Title IV creates the National Cybersecurity Competition and Challenge ("Challenge"), to consist of "national and statewide competitions and challenges that seek to identify, develop, and recruit talented [stu-
dents and others] to . . . perform duties relating to the security of the Federal information infrastructure." A Federal Cyber Scholarship-for-Service program would be created to recruit the next generation of information technology professionals and train them to meet the cybersecurity needs of the federal government. Title IV also authorizes a cybersecurity review of the federal workforce and overhauls the government's technology acquisition process.

Title IV institutes requirements for a number of cybersecurity reports. These reports include a report produced by the Department of Justice that details investigation, prosecution, and sentencing related to cybercrime, as well as a report produced by DHS describing "impediments to appropriate public awareness," related to consumer-level cybersecurity threats, such as malware and phishing, and off-the-shelf technology to combat such threats.

TITLE V: FEDERAL ACQUISITION RISK MANAGEMENT STRATEGY

Title V reaffirms the original legislative principles contained in FISMA, and would specifically require the "development and periodic update of an acquisition risk management strategy designed to ensure, based on mission criticality and cost effectiveness, the security of the Federal information infrastructure." Title V would also amend agency information technology procurement processes to address information security requirements to ensure federal procurement officers are adequately trained to understand those security requirements.

TITLE VI: INTERNATIONAL COOPERATION

Title VI requires that the Secretary of State appoint a senior official in the State Department (Senior Official) to "provide strategic direction and coordination for United States Government policy and programs aimed at addressing and responding to cyber issues overseas," both within the State Department, such as with embassies and consulates, and externally, such as with other agencies and foreign governments. Title VI also requires that the Senior Official report on "global issues, trends, and actors considered to be significant with respect to cybercrime." Finally, Title VI authorizes the Senior Official to consider cybersecurity interests when prioritizing foreign aid allocations and interventions.

TITLE VII: INFORMATION SHARING

Title VII affirms a private right to take reasonable action to protect information security systems against adverse cybersecurity action. This includes a pri-
vate actor’s right to monitor and defend both their own information systems as well as a third-party’s system if they have obtained the third-party’s consent and use the third-party’s system to store, process, or transmit data.

Title VII also authorizes private actors to disclose related information so long as such disclosure is “solely for the purpose of protecting an information system,” and does not interfere with existing law. The Secretary, with the cooperation of security agencies, will create voluntary cybersecurity exchanges to “receive and distribute . . . cybersecurity threat indicators.” These exchanges would process “in as close to real time as possible, cybersecurity threat indicators,” therefore avoiding overlap and redundancies among agency data collection in this area. The Secretary, in consultation with privacy and civil liberties experts and security agencies, is charged with establishing and enforcing privacy guidelines controlling information gathered from the exchanges, and will, through coordination with Justice and other agencies, establish “a mandatory program to monitor and oversee compliance.” The Act would protect information shared by private sector entities with the exchanges from being disclosed pursuant to a Freedom of Information Act request. For purposes of privilege and trade secrets, information shared with an exchange would not be considered a waiver of those protections. The Act also restricts how law enforcement can use information obtained from the exchanges by limiting its use to protect information systems or to protect individuals from bodily harm. Title VII also contains language establishing the federal government’s liability for harm to a private actor resulting from data or information gathered through the exchanges and limits actions against the government resulting from similar action.

Expressing the Sense of Congress Regarding Actions to Preserve and Advance the Multistakeholder Governance Model under Which the Internet Has Thrived, S. Con. Res. 50, 112th Cong.

On May 30, 2012, Representative Mary Bono Mack, along with sixty-three cosponsors, introduced H. Con. Res. 127, a concurrent resolution, “[e]xpressing the sense of Congress regarding actions to preserve and advance the multistakeholder governance model under which the Internet has thrived” (“Resolution”). The multistakeholder model referred to is the current decentralized, bottom-up approach to Internet governance, where non-governmental institutions lead, relying on input from private- and public-actors. Likewise, on June 27, 2012, Senator Marco Rubio, along with forty cosponsors, introduced a
similar Resolution in the Senate as S. Con. Res. 50. On August 2, 2012, the Resolution passed the House of Representatives by a vote of 414, whereas the Senate unanimously agreed to its version of the Resolution on September 21, 2012. During the lame duck session of the 112th Congress, the House of Representatives unanimously agreed to H. Con. Res. 50, making it Congress' official position to support “a global Internet free from government control . . . .”

Through congressional findings, the Resolution emphasizes the Internet’s global importance, describes the risk of certain proposals to the Internet and its multistakeholder model, and identifies the U.S. as a proponent of a free Internet. Congress resolved that the U.S. should continue its defense of the Internet’s multistakeholder model and should challenge any attempts to subjugate the Internet to the regulatory ambit of a centralized governmental authority. Specifically, Congress urged the Executive Branch “to promote a global Internet free from government control,” and to preserve the multistakeholder model.

What cannot be overstated enough is the gravity that the Resolution gives to the Internet’s multistakeholder governance model. The Resolution’s impetus wholly stems from Congress’ fear that this multistakeholder model now faces an existential threat. Accordingly, this summary focuses on how, and where that threat has most recently manifested itself, and why the threat is so poignant.

I. THE IMPORTANCE OF A STABLE AND FREE INTERNET

The Resolution identifies several critical functions of the Internet, each of which depends upon the multistakeholder model. First, the global economy needs a stable Internet, free from government control. Next, the open nature of the Internet fosters the development of democratic self-government by providing access to “knowledge, services, commerce, and communication.” Third, the Internet has a vital role in market-competition, enabling self-expression, and facilitating access to information. Fourth, online access propagates the protection of human rights. Lastly, the Internet’s collaborative nature promotes innovation, development of technical-capacity, economic growth, and freedom of expression.

II. THE HISTORY OF THE INTERNATIONAL TELECOMMUNICATIONS REGULATIONS AND THE INTERNET

To best understand why the Resolution so emphatically calls for decentralized, private-sector led Internet, one must juxtapose the history of the Internet with the history of international-telephone-call regulation. In 1992, two signifi-
Significant events occurred: The ratification of the International Telecommunications Regulations ("ITRs"), which govern international phone calls, and the enactment of the Scientific and Advanced-Technology Act ("Technology Act" or "Act"), which enabled commercial participation with the then government- and research-only networks that became the Internet.

Due to the Technology Act, Internet use among the private-sector boomed, overwhelming the government, and prompting further minimization of the government’s control. By 1998, the government had delegated management of the Internet’s Domain Name System ("DNS") to multistakeholder organizations—the Internet Corporation for Assigned Names and Numbers ("ICANN") and the Internet Society. ICANN managed the DNS, and the Internet Society proposed voluntary regulations that were drafted with input from engineers, governments, academics, and interested corporations. In effect, the governance style of the Internet had transitioned from a top-down approach to a bottom-up one. As the U.S. House of Representatives’ Committee on Energy and Commerce ("Committee") noted in its report accompanying H. Con. Res. 127, by the late 20th-century, the Internet’s astronomical utility was realized due to private- and public-sector cooperation and to the absence of government control.

Alternatively, the 1992 ITRs used a top-down regulatory approach to address rates paid between telecommunication providers for international calls. The ITRs have had lackluster and unsatisfactory results. As the Committee noted, the ITRs resulted in a price-hike on international calls, where nationalized telecommunications providers reaped substantial payments. Comparing the effects of the 1992 ITRs on voice telephony and of pre-1992 government control on the Internet, the stifling potential of centralized, government regulation on technological development becomes readily apparent. As the Resolution emphasizes, the threat to the Internet is that it will fall under government control, and thereunder its robustness and appeal will wither.

III. THE CONCERN OVER CERTAIN COUNTRIES’ PROPOSALS

As the Resolution noted, in December 2012, the United Nations’ International Telecommunications Union ("ITU") met for the World Conference on International Telecommunications ("WCIT") in Dubai, UAE. At the WCIT, the ITU reviewed the current ITRs, and considered revisions proposed thereto by its Member States. Prior to the WCIT, the ITRs only encompass voice telephony. At the meeting, the ITU considered proposals that effectively brought the Internet under its jurisdiction by expanding the definition of "telecommunications" from voice telephony to include "data," or "processing."

A movement, led by certain influential ITU Member States, has been afoot
to rein in the multistakeholder governance model of the Internet. Russia proposed a modification of the ITRs’ definition of “telecommunication” to include “data,” in addition to a separate proposal giving the ITU authority to distribute IPv6 addresses, a task currently performed by ICANN through a contract with the U.S. Department of Commerce. Likewise, the Arab States—a regional group comprised of Bahrain, Saudi Arabia, Egypt, UAE, Iraq, Libya, Kuwait, Morocco, Oman, Qatar, Sudan, Tunisia, Jordan, Lebanon, Comoros, Djibouti, and Somali—proposes incorporating “processing” into “telecommunication.”

Also, in a September 12, 2011 letter to the U.N. General Assembly, China, Russia, Tajikistan, and Uzbekistan called for an “information security” regime with enhanced cyber-security measures. As the Committee noted, this “information security” regime may very well serve as a platform for Internet censorship, and for the creation of a centralized Internet control authority. If either the “processing,” “data,” IPv6, or “information security” proposals are incorporated into the ITRs, then the Internet will, to a degree, fall under the ITU’s purview—a top-down approach to Internet governance.

To summarize, Congress worries that the Internet’s open nature is threatened by proposals considered at the 2012 WCIT that call for an expansion of the ITU’s jurisdiction. To date, the Internet has thrived under the bottom-up, multistakeholder governance model. Alternatively, the ITU’s approach to the regulation of international calls has had subpar results, strongly indicating that a top-down regulatory regime would be ill-suited to the Internet. A further concern is that countries will use the proposed “information security” regime to engage in Internet censorship. Accordingly, Congress has called upon the U.S. government to promote the multistakeholder model and to defend it against the proposals to be considered at the 2012 WCIT, which challenge that model by calling for ITU oversight of the Internet.

At the conclusion of WCIT, the United States delegation ultimately refused to sign the final version of the treaty, stating concerns over how it would impact the Internet.

*Summarized by Andrew D. Getsinger*