# Mobile Device Theft Prevention WG
# Report to the FCC TAC

June 11, 2015

## Contents

- Mission
- FCC Request for Further Advice
- Interim Findings for On-Device Anti-Theft Features
- Interim Findings for Device Identifier Hardening
- Next Steps

# WG Participants

- Co-Chairs:
  - Brian Daly, AT&T
  - Rob Kubik, Samsung
- FCC Liaisons:
  - Walter Johnston
  - Charles Mathias
  - Chad Breckinridge
  - Elizabeth Mumaw
- Dennis Roberson, FCC TAC Chair

- Asaf Askenazi, Qualcomm
- Jay Barbour, Blackberry
- Alan Bersin, DHS
- Brad Blanken, CCA
- Jeff Brannigan, DHS
- Matthew Bromeland, Metropolitan DC Police Department
- Craig Boswell, Hobi
- Eric Feldman, ICE/Homeland Security Investigations
- Thomas Fitzgerald, New York City Police Department
- Les Gray, Recipero
- Shelley Gu, Microsoft
- Joseph Hansen, Motorola
- Jamie Hastings,  CTIA
- Joe Heaps, National Institute of Justice
- Gary Jones, T-Mobile
- Sang Kim, LG
- Jake Laperruque, Center for Democracy and Technology
- Irene Liu, Lookout

- John Marinho, CTIA
- Samuel Messinger, U.S. Secret Service
- James Moran, GSMA
- Jason Novak, Apple
- Kirthika Parmeswaran, iconectiv
- Greg Post, Recipero
- Deepti Rohatgi, Lookout
- Mark Romer, Asurion
- Mike Rou, eBay
- Matt Rowe, Gazelle
- Christian Schorle, FBI
- DeWayne Sennett, Editor  (AT&T)
- David Strumwasser, Verizon
- Maxwell Szabo, City and County of San Francisco
- Ron Schneirson, Sprint
- Samir Vaidya, Verizon Wireless

# MDTP WG Mission

- Emphasis will be on longer term initiatives that will combat more sophisticated theft scenarios
  - Developing recommendations on next generation anti-theft features
  - Processes including recommendations for hardening of existing device identifiers and the possible need for new, more secure identifiers
  - Security mechanisms with higher consumer acceptance (e.g. biometrics)
  - More focused analysis of analysis overall theft ecosystem including how stolen devices are re-entered into the marketplace (e.g. recycling industry)
  - Further recommendations on improved reporting mechanisms

- Consideration will also be given to the efficacy of extending theft prevention mechanisms to other classes of devices.

- Provide an assessment of progress made in the area of device theft prevention as some of these recommendations have been applied

# FCC Requests for Further Advice

At the initial 2015 meeting of the TAC, the FCC Chairman requested the MDTP WG consider the following tasks (details as provided by the FCC are in the backup material), :

- Task 1 – On-Device Theft Prevention Features Template
- Task 2 – Hardened Device Identifiers
- Task 3 – Database

Tasks 1 and 2 - an interim report was provided May 1

Task 3 feedback is scheduled for October 1

## Interim Findings - On-Device Theft Prevention Features

- CTIA national mobile security and privacy survey (April 30, 2015)
  - 61 percent of Americans who own smartphones and tablets use PINs and passwords
  - Up more than 20 percent from 2012
  - CTIA cites one of the reasons for this increase is a result of the collective wireless industry's consumer education activities as well as the initiatives developed by individual companies
  - Planned recurring survey effort for continued monitoring of improvements

- Progress to prevent mobile device theft is being made
  - New Data Reveal Thefts Down 40% In London; 22 % In San Francisco; And 16% In New York City
    - http://www.ag.ny.gov/press-release/ag-schneiderman-london-mayor-johnson-and-da-gasc%C3%B3n-welcome-dramatic-global-drop
  - MDTP working group should attempt to obtain data from other jurisdictions

# Efforts Already in Progress

- Mobile OS providers and manufacturers are in various stages of deploying anti-theft solutions to comply with the voluntary commitments and state laws
  - California requires any smartphone that is manufactured on or after July 1, 2015, and sold in California after that date, to include:
    - Technological solution at the time of sale, to be provided by the manufacturer or operating system provider, that, once initiated and successfully communicated to the smartphone, can render the essential features of the smartphone inoperable to an unauthorized user when the smartphone is not in the possession of an authorized user
  - The smartphone shall, during the initial device setup process, prompt an authorized user to enable the technological solution

- While the California law mandates technological solutions, it is important to note these solutions will be deployed nationwide under the CTIA Voluntary Commitment

| Anti-Theft Tool: | CTIA Commitment | California Law (SB962) | Minnesota Law | Working Group View |
|---|---|---|---|---|
| **Date: July 2015** | Required | Required | Required | Required |
| **Smartphones** | Required | Required | Required | Required |
| **No Cost to Consumer for devices sold at retail** | Required | Silent | Required | Required |
| **For retail sale, preloaded** | Required if not Downloadable | Silent | Required if not Downloadable | Required if not downloadable with no additional purchase |
| **For retail sale, downloadable** | Required if not Preloaded | Allows technological solutions in addition to those provided in the device or OS. | Required if not Preloaded | Required if not preloaded with no additional purchase |
| **“shall include a technological solution at the time of sale”…….. “once initiated and successfully communicated to the smartphone” - SB962 Sec 2 (b) (1)** | Required | Required | Required (“sold or purchased in MN” S.F. No. 1740, 2014) | Required |
| **Remote Wipe** | Required | Silent | Silent | Required |
| **Allow the Authorized User to Render Essential Features Inoperable to Unauthorized Users Once Communicated** | Required | Required | Silent | Required |

| Anti-Theft Tool: | CTIA Commitment | California Law (SB962) | Minnesota Law | Working Group View |
|---|---|---|---|---|
| **Continue to function for 911 calls** | Required | Not incompatible with 911 | Silent | Required |
| **Continue to function for emergency numbers programmed by the user.** | Optional | Unclear | Silent | Optional |
| **Prevent reactivation by unauthorized user including factory reset** | Required to the extent technologically feasible | Required | Silent | Required to the extent technologically feasible |
| **Restore user data to the extent feasible** | Required | Silent | Silent | Required |
| **Reverse inoperability if recovered by authorized user** | Required | Required | Silent | Required |
| **Initial Setup “prompt an authorized user to enable the technological solution” - SB962, Sec 2 (b) (1)** | Silent | Required | Silent | Required |
| **Opt-Out by Authorized User or Authorized User Designee, at any time SB962 Sec 2  (b) (2)** | Silent | Required | Silent | Required |
| **In addition, permit use of additional solutions if available - SB962 Sec 2 (3) (f)** | Required, if available for users’ smartphone | Allows, but does not require | Silent | Allowed but not required |

# “Automatic On” Device Set-up California Law Requirement

- Consumers:
  - During device setup authorized user is prompted to enable the anti-theft technological solution

- Consumer choice required
  - Consumers should have the option to affirmatively elect to disable this protection, but it must be clear to the consumer that the function the consumer is electing to disable is intended to prevent the unauthorized use of the device
  - An authorized user of a smartphone may affirmatively elect to disable or opt-out of enabling the technological solution at any time.
    - Physical acts necessary to disable or opt-out of enabling the technological solution may only be performed by the authorized user or a person specifically selected by the authorized user to disable or opt-out of enabling the technological solution

## Consumer Use of Solutions

- Availability of on-device anti-theft features on all smartphones is expected to increase after the effective date of the CTIA Voluntary Commitment and the California and Minnesota laws
  - MDTP Working Group recommends the industry perform a study, after July 1, 2015, to gather data on consumer usage, and trends
  - In particular, the study should aim to determine when users are prompted to activate it, whether uptake for these features continues to improve

- CTIA report is evidence that consumers are increasing usage of anti-theft features on smartphones

# Efforts Cited by CTIA to Increase Consumer Use of Solutions

- Smartphone Anti-Theft Voluntary Commitment, signed by major network operators, device manufacturers and operating system companies, helps protect consumers while recognizing the companies' need to retain flexibility so they may constantly innovate and adapt, which is key to stopping smartphone theft

- Implementation of international databases to help prevent reactivating reported stolen devices

- Smartphone manufacturers notify or prompt users via new smartphones upon activation or soon after of its capability of being locked and secured from unauthorized access by setting a PIN/password

- Smartphone manufacturers provide information on how to secure/lock new smartphones in-box and/or through online "Quick Start" or user guides

- Developed and promote a listing of apps for various mobile operating systems that would remote lock, erase or track devices; and

- Created video public service announcements and social media outreach efforts directing users to anti-theft resources

# Consumer Education

- MDTP Working Group encourages the FCC to create a website/consumer education portal that informs users about the anti-theft initiatives and legislation industry is committing to support, that includes links to each of the carrier, smartphone manufacturer, and OS provider webpages that describe their anti-theft features (after July 2015) and consumer response actions in the event their device is lost or stolen
    - If was a result of a criminal act, consumers should first contact local law enforcement (e.g., 911) to report the crime
    - Consumer should contact their carrier to cancel service and blacklist the device
    - Smartphone manufacturer/OS provider may be contacted regarding their solutions

- Working with industry, the FCC should look towards additional consumer education opportunities

# Hardening of the IMEI

- IMEI reprogramming does not appear to be the significant issue today that it once was
  - Improvement in overall IMEI security levels was acknowledged by the European Commission
  - 2009-2010: 58% decrease in allegations of IMEI tampering; 45% decrease in impacted manufacturers; 83% of compromised device models pertain to just two manufacturers with whom GSMA worked with
  - Need to look at more recent data to confirm the trend

- Industry does not recommend a replacement hardware identifier
  - Changing the identifier could be drastic in terms of global standards and best practices impacts, development & deployment with impacts to the entire network, handsets, fraud and operations systems, and roaming
  - IMEI defined in global 3GPP standards, provides capabilities needed and further enhancements are being explored
  - GSM Association Handset Security Technical Principles contain detailed technical measures designed to increase the security of the IMEI against unauthorized change
  - Increasing security of IMEI implementations has been an area of focus for GSMA for over 10 years

# Hardening of the IMEI

- Centralized reporting and correction of newly identified IMEI security weaknesses to improve device security levels during the manufacturing lifecycle of current and future device products
  - GSMA and the world's leading mobile device manufacturers established a formal process
  - Reports are referred to the relevant manufacturers, investigated, and responded to within 42 days
  - Contain details of proposed remedial action and dates from which equipment with new security measures will be introduced

- Most of the world's largest handset manufacturers formally signed up to support GSMA initiatives
  - The practical coverage of the GSMA solution still needs to be validated

- GSMA Device Security Group will revisit the entire IMEI security topic in 2015 as it has already identified this topic as being a priority for next year and the work will, at a minimum, involve a review of the technical design principles and reporting and correction process
  - GSMA's North American Regional Interest Group will provide North American-specific concerns
  - As a result of the study, ATIS and/or 3GPP may be involved if standardization efforts are required.

# Preliminary Recommendations

- The FCC TAC recommends a deeper investigation by industry into the causal factors for the increase in consumer use of on-device solutions that could be used for determining how to optimize further efforts to incentivize greater consumer use of anti-theft features, if necessary
  - Recommend completion by EOY2015

- The FCC TAC recommends an industry-led investigation into whether the increased availability of anti-theft functionality on new smartphones, as well as the upcoming initial device setup prompts that will be required by California legislation after July 2015, have the effect of further increasing consumer use of these features.
  - Such a study should be undertaken after the July 1, 2015 date to allow for a sufficient number of devices with these features to have been placed into circulation

## Anticipated Recommendations to the FCC Chairman

- Continued studies to determine whether implementations post July have the desired affect on mobile device theft
  - Refers to the planned recurring survey effort for continued monitoring of improvements
  - Better tracking of actual phones stolen – investigate as part of the MDTP working group task 3 deliverable

- FCC voluntary framework for a set of on-device capabilities to guide industry
  - Based on the “working group view” column of the Best Practices Template: Comparison of Anti-Theft Tools

- FCC to work with industry on developing effective outreach initiatives to educate the consumer

- Identify key technological areas where the FCC should seek further information from industry
  - IMEI
  - Requirements and Use of databases
  - Future theft prevention opportunities

## MDTP Plan for 2H2015 - Make Additional Progress

- Further explore tasks 1 & 2
  - deeper investigation by industry into the causal factors for the increase in consumer use of these features

- Address Task 3 - Database

- Continue with the 2015 mission including:
  - Explore Next Generation Anti-theft Features
  - More focused analysis of analysis overall theft ecosystem including how stolen devices are re-entered into the marketplace (e.g. recycling industry)
  - Further recommendations on improved reporting mechanisms
  - Law enforcement engagement

# BACKUP

# Task 1 - On-Device Theft Prevention Features Template

- Password protection, Remote lock/wipe/restore functionality
- Most effective only if they are part of a package of practical solutions that consumers actually use, and today the majority of U.S. consumers don't
- WG asked to explore developing a proposed template approach that would ensure wider and easier use
- The template should cover:
  - A relatively uniform approach to these features (from the end user perspective) so that consumers do not need to re-educate themselves whenever they change devices
  - An "automatic on" approach, or something similar, under which consumers can set up a new device only if they select a screen-saver password (whether digits, biometric, or something else) and activate lock/wipe/restore features
  - A feature making it easier for consumers to report thefts to providers and/or police, including reporting the device's IMEI
  - General consideration of the implications of Wi-Fi only connectivity.

# Task 2 - Hardened Device Identifiers (IMEI)

- Reliable IMEIs are critical not only for theft prevention, but also for improving the integrity of the wider provisioning system that uses the identifiers
- GSMA and 3GPP have begun discussions in this area, we need more urgency
- The WG was asked to assess rapidly whether there are any constraints that would prevent 3GPP and/or GSMA from developing a standard for a hardened IMEI by the end of this year
  - Note it is recommended that the WG work through ATIS as the North American 3GPP Organizational Partner

# Task 3 - Database

- The WG is asked to study database systems that effectively track stolen items (phones, cars, funds) and develop a spec sheet for an effective stolen phone database that might be focus on North America

- GSMA already hosts a configurable stolen phone database which is facilitating pan operator blocking and information distribution. There is an opportunity for ecosystem participants to make greater use of this resource through optimized configuration and adoption

- The WG should finalize the proposed spec sheet by October 1

# Cybersecurity Working Group

FCC TAC Meeting

June 11, 2015

# Agenda

**Executive Summary All Subworking groups**

Smartphone Security Subworking group detailed slides

Consumner IOT Subworking group detailed slides

Securing SDN Subworking group detailed slides

Appendix

# Working Group Members

- WG Chair: Shanid Ahmed, Accenture / Paul Steinberg, Motorola Solutions
- Vice Chair: Ramani Pandurangan, XO Communications
- FCC Liaisons: Jeffery Goldthorp, Ahmed Lahjouji
- Members:
  - John Barnhill, Genband
  - Mark Bayliss, Visualink
  - Nomi Bergman, Brighthouse
  - Mike Bergman, CEA
  - John Brzozowski, Comcast
  - Ken Countway, Comcast
  - Brian Daly, AT&T
  - Renato Delatorre, Verizon Wireless
  - John Dobbins, Earthlink
  - Martin Dolly, AT&T
  - Dale Drew, Level 3 Communications
  - Adam Drobot, Open Tech Works
  - Amit Ganjoo, Oceusnetworks
  - Dick Green, Liberty Global
  - Craig Greer, Samsung
  - Russ Gyurek, Cisco
  - Theresa Hennesy, Comcast
  - Farooq Kahn, Samsung
  - Dr. Prakash Kolan, Samsung
  - Tom McGarry, Neustar
  - Paul Misener, Amazon
  - Jack Nasielski, Qualcomm
  - George Popovich, Motorola Solutions
  - Katrin Reitsma, Motorola Solutions
  - Christoph Schuba, Ericsson
  - S Rao Vasireddy, Alcatel Lucent
  - Jack Waters, Level 3 Communications
  - Brian Witten, Symantec
  - David Young, Verizon Wireless
  - Lim Youngkwon, Samsung

# Smartphone Security Sub-WG Summary

**(Chair: Martin Dolly – AT&T)**

- **Scope/direction**
  - Develop platform agnostic baseline security controls, recommended settings and common vernacular for reporting on device security and application permissions.
- **Key actionable deliverables**
  - Step 1: Looking at some option (low hanging fruit) to connect the published security questions (CAC) published online into the mobile experience (not automation)
  - Step 2: A 'wizard' approach to facilitation of mobile device security configuration for users - output planned are requirements for such a utility
  - Step 3: A set of generic requirements for an 'active' on-board security checker (application)

# Smartphone Security Sub-WG Summary

- **Deliverables**
  - Deliverable 1: Connecting Security Recommendations to Mobile Experience
    - Draft: Ongoing
    - Final: September 2015
  - Deliverable 2: Wizard approach to configure/secure Mobile Device
    - Draft: June 11, 2015
    - Final: September 2015
  - Deliverable 3: Generic Requirements for Active Security Checker
    - Draft: August 2015
    - Final: December 2015

# Consumer IOT  Security Sub-WG Summary

**(Chair: George Popovich - Motorola / Tom McGarry – Neustar)**

- **Scope/direction**
  - Examine the cyber security challenges posed by the IoT space, and suggest actionable recommendations with particular focus on the security of IoT consumer products
  - Investigate how stakeholders are addressing security challenges today, identify the gaps, and understand the potential impact of these challenges to the future of the IoT industry
- **Key actionable deliverables**
  - June 2015: Industry landscape survey
  - September 2015: Communicate the current security gaps in the IoT space
  - December 2015: Recommendations for facilitating positive changes in the security, privacy and resiliency of IoT devices and systems
    - Develop platform agnostic baseline security controls, recommended settings and common vernacular for reporting on device security and application permissions.

# Consumer IOT  Security Sub-WG Summary

- **Deliverables**
  - Deliverable 1: Industry Landscape Survey
    - Draft: May 2015
    - Final:  June 2015
  - Deliverable 2: Prioritized Gap Assessment
    - Draft: September 2015
    - Final: End September 2015
  - Deliverable 3: Recommendations
    - Draft: November 2015
    - Final: December 2015

# Securing Software Defined NW Sub-WG Summary

**(Chair: Ramani Pandurangan – XO Communications)**

- **Scope/direction**
  - This WG aims to define SDN / NFV for the context of FCC TAC and describe architectures and sample use cases.
  - As the industry's adoption is still evolving there may not be a set of established practices but the White Paper will describe how industry is handling these evolving architectures, specifically with respect to security challenges and how the industry is leveraging the architectures to mitigate risks.
- **Key actionable deliverables**
  - White Paper review lessons learned from other control plane protocols such as BGP and DNS.
  - White Paper expects to provide actionable recommendations to TAC primarily with a view to increase user awareness of the challenges and opportunities of these architectures in the area of security.

# Securing Software Defined NW Sub-WG Summary

- **Deliverables**
  - Deliverable 1: June 2015 to September 2015
    - Consult industry practitioners
    - Determine security challenges and opportunities
    - Identify lessons learned from other protocols
    - Capture industry practices
  - Deliverable 2: September 2015 to December 2015
    - Explore FCC role
    - Develop actionable recommendations to TAC
    - Deliver White Paper

# Agenda

Executive Summary-All Subworking groups

**Smartphone Security Subworking group detailed slides**

Consumner IOT Subworking group detailed slides

Securing SDN Subworking group detailed slides

Appendix

# Definition: Topic 1 - Simplifying Smartphone Security

Today, configuring a device to minimize security and privacy risks can be can be confusing and requires consumer education so that the impacts are not well understood by most consumers. Last year, the Commission asked the Consumer Advisory Committee to recommend a series of questions that could be presented to consumers by way of their smartphones. The answers to these questions would be used by an app resident on the device to configure the device's security and privacy settings to the user's liking. We originally had in mind that the Smartphone Security Checker could be a platform for presenting the questions to users, but we have turned our attention to apps produced and on the market. We recommend that the TAC be asked to provide us with a set of recommended generic requirements that we could seek comment on, thereby promoting the availability of features in such apps that converge on a set of common security and privacy concerns.

# Simplifying Smartphone Security Sub Working Group Members

- Brian Daly, AT&T
- Martin Dolly, AT&T (Lead)
- Renato Delatorre, Verizon
- Amit Ganjoo, Oceusnetworks
- Dr. Prakash Kolan, Samsung
- Katrin Reitsma, Motorola Solutions
- Lim Youngkwon, Samsung

# Scope: Simplifying Smartphone Security

- **Proposed scope/direction**
  - Develop platform agnostic baseline security controls, recommended settings and common vernacular for reporting on device security and application permissions.
- **Key actionable deliverables**
  - Step 1: Looking at some option (low hanging fruit) to connect the published security questions (CAC) published online into the mobile experience (not automation)
  - Step 2: A 'wizard' approach to facilitation of mobile device security configuration for users - output planned are requirements for such a utility
  - Step 3: A set of generic requirements for an 'active' on-board security checker (application)

# Work Plan: Simplifying Smartphone Security

- Deliverable 1
  - Draft: Ongoing
  - Final: September 2015
- Deliverable 2
  - Draft: June 11, 2015
  - Final: September 2015
- Deliverable 3
  - Draft: August 2015
  - Final: December 2015

# Work Plan: Simplifying Smartphone Security Cont.

- Potential key sources of input – *preliminary list*
  - Device Vendors – Samsung, Sony, HTC, Apple, LG, etc.
  - Platform representation – Google / Android, Apple / iOS, RIM / Blackberry, Microsoft / Windows Phone, alternative mobile OSs – e.g. FireOS, Sailfish, Firefox OS, Ubuntu, Tizen
  - Carriers – AT&T, Verizon
  - Security Solution providers – Lookout, NQMobile, Symantec, Intel
  - Device OEMs– Broadcomm, AMD, Qualcomm, TI, Freescale, Marvell

## Status: Simplifying Smartphone Security

- Accomplishment 1
  - Draft Requirements
- Accomplishment 2
  - Initiated reach out to Security Solution application providers

# Issues: Simplifying Smartphone Security

- Issue/Concern 1:
  - Request:  Additional Expertise in order fill representation from the entire ecosystem identified in potential key sources of input slide

# Agenda

Executive Summary-All Subworking groups

Smartphone Security Subworking group detailed slides

**Consumner IOT Subworking group detailed slides**

Securing SDN Subworking group detailed slides

Appendix

# Definition: Topic 2 - Applying Security to Consumer IoT

The WG will examine the special cybersecurity challenges posed by the emerging Internet of Things, and suggest actionable recommendations to the FCC with particular focus on the security and protection of IoT consumer products.

Questions:

- What are the underlying technologies (e.g., WiFi, ZigBee, GPRS, LTE) that dominate the IoT space? and what security vulnerabilities and challenges do they present in the IoT environment?
- What other security challenges face IoT consumer products?
  - For example, to what extent does lack of physical security pose a threat to unsupervised IoT devices? Explain.
- What is the industry doing to secure and protect battery-operated and resource- constrained (i.e., minimum computing power and memory) M2M devices, which cannot encrypt its data?
- How are the IoT/M2M stakeholders addressing those security challenges and vulnerabilities, and what are the gaps?
- What is the potential impact of these security challenges on the future of IoT/M2M industry, the end user and the economy, especially when IoT devices become fully integrated in all of our systems, including our critical infrastructures?
- What role could the FCC play in facilitating positive changes in the security, privacy and resiliency of M2M/IoT devices and systems?

# Consumer IoT Security Sub Working Group Members

- Co-chairs: Tom McGarry, Neustar, George Popovich, Motorola Solutions
- Members:
  - Mike Bergman, CEA
  - John Brzozowski, Comcast
  - Brian Daly, AT&T
  - Renato Delatorre, Verizon
  - Martin Dolly, AT&T
  - Craig Greer, Samsung
  - Russ Gyurek, Cisco
  - Christoph Shuba, Ericsson
  - Brian Witten, Symantec

# Scope: Applying Security to Consumer IoT

- **Proposed scope/direction**
  - Examine the cyber security challenges posed by the IoT space, and suggest actionable recommendations with particular focus on the security of IoT consumer products, including the securing of unsupervised and resource constrained devices
  - Investigate how stakeholders are addressing security challenges today, identify the gaps, and understand the potential impact of these challenges to the future of the IoT industry where IoT devices become fully integrated in all of our systems, including our critical infrastructures
- **Key actionable deliverables**
  - **June 2015:** Industry landscape survey
  - **September 2015:** Communicate the current security gaps in the IoT space
  - **December 2015:** Recommendations for facilitating positive changes in the security, privacy and resiliency of IoT devices and systems

# WorkPlan: Applying Security to Consumer IoT

- **June Deliverable - Industry landscape survey**
  - Provide a snapshot of our ongoing industry landscape survey, which will include existing best practices, standards, consortium efforts, and leading technology solutions
  - **Draft: 5/29/15; Final: 6/11/15**
- **September Deliverable– Gap analysis**
  - Communicate the current security gaps in the IoT space per our industry landscape study, and discuss how technology advancements may address these gaps
  - **Draft: 9/11/15; Final: 9/24/15**
- **December Deliverable – Recommendations to address the gaps**
  - Propose a FCC role in facilitating positive changes in the security, privacy and resiliency of IoT devices and systems, with recommendations focused around addressing the gaps identified earlier in the year
  - **Draft: 11/30/15; Final: 12/9/15**

# Status: Applying Security to Consumer IoT

- **Accomplishment – Snapshot of industry scan delivered on June 11th**
  - **We will continue to learn from industry throughout the year, but this deliverable serves as a snapshot of our efforts over the past 3 months**
  - **June deliverable executive summary:**
    - Many IoT consortiums in existence; we are considering the appropriate means of engagement with major ones now
    - Real improvement will only come with time. Industry experts suggest process improvements (e.g. Security Maturity Models like BSIMM) over short-term fixes.
    - IoT security best practices are emerging (e.g. CSA Mobile Working Group, CEA)
    - We have decided to begin studying technology trends to analyze how to secure low cost and resource constrained IoT devices in the future

# Issues: Applying Security to Consumer IoT

- **Issue/Concern:**
  - – Consumer vs. industrial vs. Critical Infrastructure IoT scope
    - Help us better understand the requested focus on the *consumer* IoT space
    - Each market space calls for different levels of cybersecurity protections
    - Should our focus remain on consumer regardless of the severity of gaps discovered?
  - – We believe our scope does not include consumer privacy concerns. We assume this is accurate. Looking for any clarifications on this.
  - – Some consortia seem to prefer more formal interaction. We may need guidance on how to approach some consortia.

# Agenda

Executive Summary-All Subworking groups

Smartphone Security Subworking group detailed slides

Consumner IOT Subworking group detailed slides

**Securing SDN Subworking group detailed slides**

Appendix

# Definition: Topic 3 – Securing SDN

There are clear signs that the telecommunications market is standing at the cusp of a significant paradigm shift in how computer networks of the future will be designed, controlled, and managed. One of the key technologies at the heart of this transformation is called Software Defined Networking (SDN) architecture. According to ONF, this new approach to designing, building, and managing networks make it possible for enterprises and carriers to gain unprecedented programmability, automation, and network control, enabling them to build highly scalable, flexible networks that readily adapt to changing business needs. The way this is accomplished is by decoupling the control and data planes, logically centralizing network intelligence and state, and abstracting the underlying network infrastructure from the applications.

SDN is sometimes considered to carry significantly more cyber risk than traditional network architectures. Therefore, the need to secure both SDN's centralized network's control plane and distributed dataplane seem essential. It would be worthwhile considering how to build in security as opposed to retrofitting it, and seeking to apply lessons learned from the long running efforts to secure existing control plane protocols such as BGP, and DNS.

# **Definition**: Topic 3 – Securing SDN

Questions:

- What are the key security challenges that SDN architectures present? And how is the telecom industry addressing them?
- What measures could be employed to make networks deploying SDN applications resilient and secure?
- What is the trust model that should be applied between devices and controllers, and between controllers?
- What, if any, high-assurance approaches may apply to SDN?
- What specific lessons can we extract from the long running efforts to secure existing control plane protocols -- such as BGP and DNS – to benefit SDN-based networks?
- What are the pros and cons of embedding security within the network, as opposed to embedding it in servers, storage and other computing devices?
- What are the strengths and weaknesses of Software Defined Security (SDSEC)?
- What role could the FCC play in facilitating positive changes in the security, privacy and resiliency of SDN?

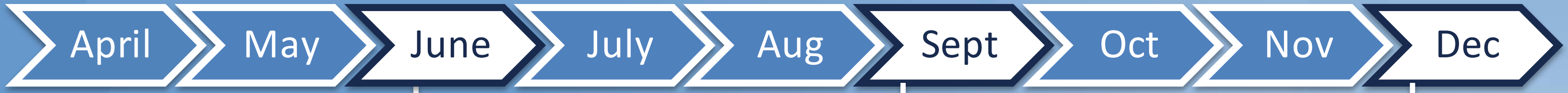
# Securing SDN Sub Working Group Members

- Ken Countway, Comcast
- Brian Daly, AT&T
- Martin Dolly, AT&T
- Dr. Prakash Kolan, Samsung
- Ramani Pandurangan, XO Communications (Lead)
- Christoph Schuba, Ericsson
- S Rao Vasireddy, Alcatel Lucent (Co-lead)

# Scope: Topic 3 – Securing SDN

This WG aims to define SDN / NFV for the context of FCC TAC and describe architectures and sample use cases. As the industry's adoption is still evolving there may not be a set of established practices but the WP will describe how industry is handling these evolving architectures, specifically with respect to security challenges and how the industry is leveraging the architectures to mitigate risks.  The WP will also review lessons learned from other control plane protocols such as BGP and DNS. The WP expects to provide actionable recommendations to TAC primarily with a view to increase user awareness of the challenges and opportunities of these architectures in the area of security.

# 2015 Securing SDN Sub Working Group (SWG) Plan



April May June July Aug Sept Oct Nov Dec

- Form team
- Develop scope
- Determine deliverables
- Develop deliverable outline
- Determine deliverables for TAC quarterly meetings

- Identify input resources
- Consult industry practitioners
- Determine security challenges and opportunities
- Identify lessons learned from other protocols
- Capture industry practices

- Explore FCC role
- Develop actionable recommendations to TAC
- Deliver WP

# Status: Topic 3 – Securing SDN

- Team formed
- Scope and outline for the deliverable (White Paper) identified
- Plan of work leading up to each TAC meeting is developed
- Initial information collected on
  - SDN definition, principles, architecture, security challenges and opportunities
  - NFV objectives, framework, some aspects of security challenges
- Consulted with one industry practitioner; another one to be scheduled for the week of 6/8

# Deliverable (White Paper) Outline

1. Purpose and scope of the White Paper (WP)
2. SDN / NFV definition, objectives, architecture and use cases
3. Security challenges
4. Security opportunities engendered by the architectures
5. Industry handling
6. Lessons from BGP DNS and other control plane protocols
7. Strengths and weaknesses of Software Defined Security (SDSEC)
8. FCC Roles
9. Actionable Recommendations
10. References
11. Appendix – Security in Network vs. in Servers etc., Trusted Computing
12. Input from industry practitioners

# Agenda

Executive Summary-All Subworking groups

Smartphone Security Subworking group detailed slides

Consumner IOT Subworking group detailed slides

Securing SDN Subworking group detailed slides

**Appendix**

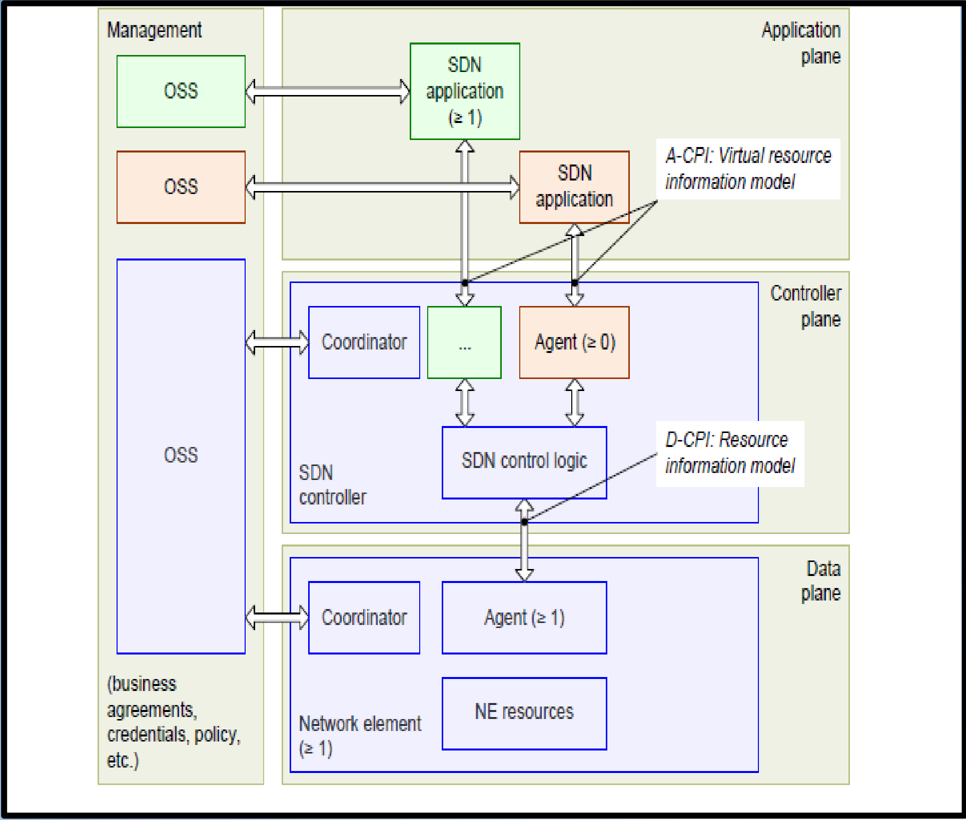
# Appendix

# SDN

To provide open interfaces that enable the development of software that can control the connectivity provided by a set of network resources and the flow of network traffic though them, along with possible inspection and modification of traffic that may be performed in the network

# SDN Principles And Architecture

- Principles
  - Decoupling of control and data planes
  - Logically centralized control
  - Exposure of abstract network resources and state to external applications, programmability of the network
- The architecture makes no statement about the physical realization of the components
- Multiple trust domains (Customer, Partner, Service Provider) are shown. Each with its own management functionality



SDN Components with Management

# SDN Security Challenges

- Centralized control may expose a single high-value asset to attackers, as distinct from a larger number of autonomous assets in a distributed control domain
- New types of threats arise due to the explicit programmatic access SDN offers to clients that are typically separate organizational or business entities
- In an SDN context, there are expected to be more components that could affect isolation, interacting more dynamically than in non-SDN networks
- Given the interconnection of different companies and organizations encouraged by SDN, the architecture is strongly driven by notions of trust domains with well-defined boundaries
- The architecture therefore requires strong authentication and robust security at all interfaces
- Not unique to SDN is the fact that insiders represent a significant security threat, and that operator error threatens system integrity
- Architecture should include strong identity and credential management functions that secure all entities and their associated state

# Security Opportunities

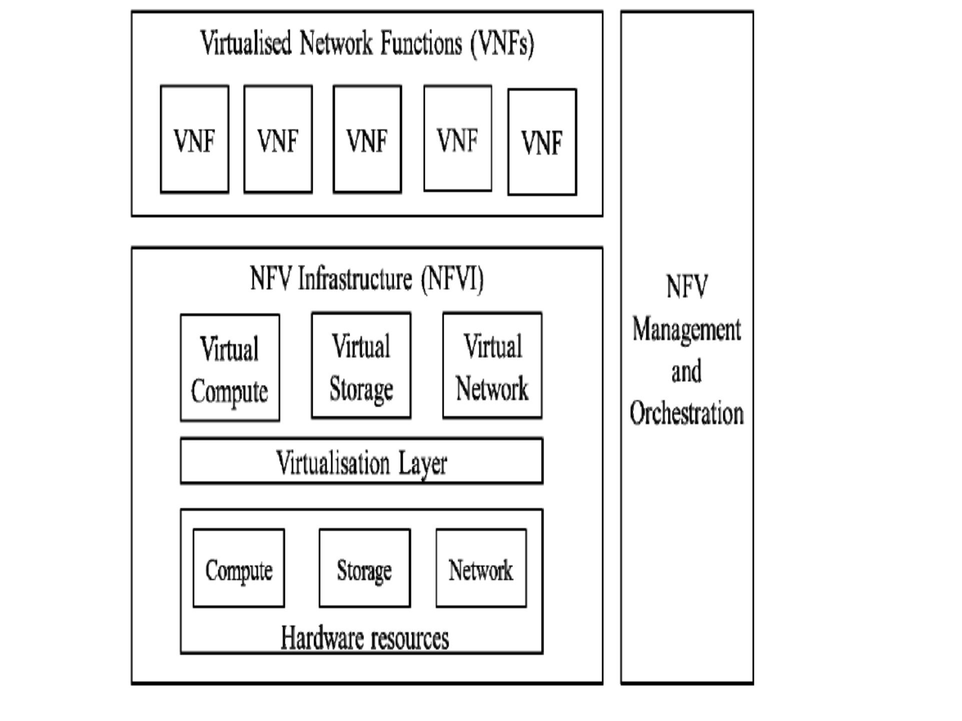
- The programmability feature also provides opportunities to enhance the security posture of networks
- Use SDN techniques to construct a data plane security solution that is able to coordinate both network and security devices to detect and react to attacks in a more flexible way

# NFV Objectives

- Improved capital efficiencies compared with dedicated hardware implementation
- Improved flexibility in assigning virtual network functions compared with dedicated hardware
- Rapid service innovation through software-based service deployments
- Improved operational efficiencies resulting from common automation and operational procedures
- Standardized and open interfaces between virtualized network functions and the infrastructure and associated management entities so that such decoupled elements can be provided by different vendors
- Reduced power usage by migrating workloads and powering down unused hardware

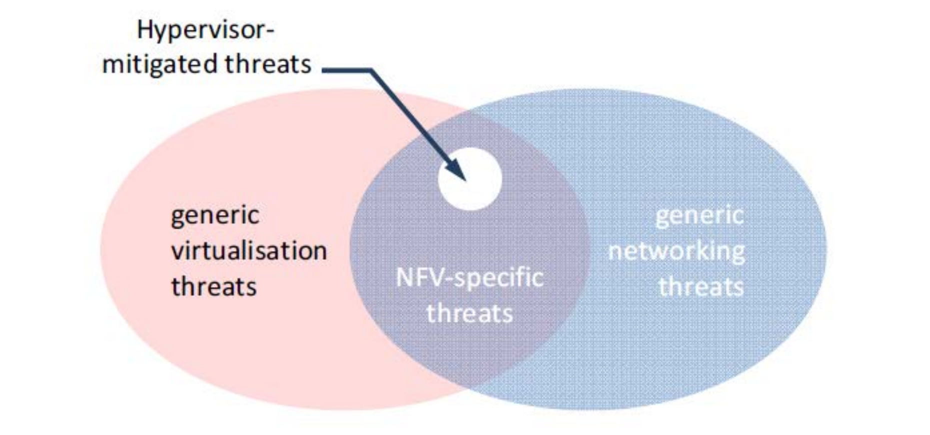
# High Level NFV Framework

- Network Functions (NF) as software-only entities
- NFs run over the NFV Infrastructure (NFVI)
- Virtualized Network Function (VNF), the software implementation of a network function capable of running over the NFVI
- NFVI includes the diversity of physical resources and how these can be virtualized. NFVI supports the execution of the VNFs
- NFV Management and Orchestration covers the orchestration and lifecycle management of physical and/or software resources that support the infrastructure virtualization, and the lifecycle management of VNFs



# NFV - Threat Surface

- Since a VNF is but a network function running on a virtual machine, the set of all the security threats to a network
- comprising VNFs, at the first approximation, is a union of:
  - all the generic virtualization threats
  - the threats specific to the system of physical network functions prior to virtualization
  - new threats due to combining virtualization technology with networking



# References

- ETSI GS NFV-SEC 001 V1.1.1 (2014-10) Network Functions Virtualization (NFV); NFV Security; Problem Statement
- ETSI GS NFV-SEC 003 V1.1.1 (2014-12) Network Functions Virtualization (NFV); NFV Security; Security and Trust Guidance
- SDN architecture Issue 1 June, 2014 ONF TR-502
- Principles and Practices for Securing Software-Defined Networks January 2015 ONF TR-511

# Consulted Industry Practitioners

- Torsten Dinsing, Ericsson, “Virtualizing the Network”

# Technological Advisory Council

## Spectrum and Receiver Performance

## Working Group

## June 11 , 2015

# 2015 Mission

- Make recommendations in areas focused on improving access to and making efficient use of the radio spectrum from a system and receiver perspective
- Provide support as the Commission considers TAC recommendations related to the statistical aspects of interference
- Conduct analysis and make recommendations related to enforcement issues in a rapidly changing RF environment

# Working Group

- **Chair:**
  - Lynn Claudy, NAB
  - Greg Lapin, ARRL

- **FCC Liaisons:**
  - Julius Knapp
  - Uri Livnat
  - Bob Pavlak
  - Matthew Hussey

- **Participants / Contributors:**
  - Dale Hatfield, University of Colorado
  - Pierre de Vries, Silicon Flatirons
  - Brian Markwalter, CEA
  - David Gurney, Motorola Solutions
  - Steve Kuffner, Motorola Solutions
  - Geoff Mendenhall, GatesAir
  - Robert Dalgleish, Ericsson
  - Kumar Balachandran, Ericsson
  - Robert Miller, incNetworks
  - Patrick Welsh, Verizon
  - Bruce Judson, Qualcomm
  - Mark Richer, ATSC

# Working Group Areas of Focus

- Develop recommendations about statistics of interference and risk-informed decision making
- Recommend strategies for interference resolution and enforcement in a changing RF environment
- Propose methods for characterizing the operational impact to receiver performance from interference

# Risk-Informed Interference Assessment

- **Goal** : Find quantitative ways to reason about the risks of harmful interference due to changes in radio service rules, e.g. new allocations, rule changes, and waivers
- **Status**
  - Provided FCC staff with detailed list of potential speakers and courses on quantitative risk assessment
  - Briefed WSRD Steering Committee and CSMAC on this work; lively engagement, especially from the CSMAC
  - There's interest from academic research groups; working to convert this to student projects and funding applications

# Risk-Informed Interference Assessment

- **Status** (Cont'd)
  - **Defined a Work Plan**
    - Medium term: risk analysis for a simplified case
    - Short term: for specific historical cases(s), identify (1) data required to do a risk-informed assessment, (2) mappings of RF metrics to service-level metrics
    - Gathering data on interference to MetSat in 1695-1710 (aka CSMAC WG1, AWS-3 blocks A1 & B1)

# Risk-Informed Interference Assessment

- **Challenges**
  - Finding cases that are relevant to WG members and the FCC but that do not trigger ex parte requirements; the hot topics are open proceedings but thus out-of-bounds
  - Recruiting TAC members who are able to invest time in this work
  - Expertise: tools and skills to do this analysis exist, but still rare in the spectrum community

# Interference Resolution and Enforcement

- **Goal**: Recommend strategies for interference resolution and enforcement to address changing RF environment
- **Significant Developments**:
  - Straw-man proposal considered and adopted at CSMAC meeting on May 12, 2015
  - Some details of the FCC's Enforcement Modernization program were made public on April 2, 2015
  - Release of R&O and 2nd NPRM in 3.5 GHz Band on April 21, 2015
  - Continued technological advances e.g., SDR radios capable of tuning an extremely wide range of frequencies, low cost computer processors and mass storage devices that make feasible I/Q measurements for immediate or forensic analyses, and economical UAV/drone platforms
  - Changing threat vectors for both malicious and non-malicious intentional interference enabled by similar technological advances

# Interference Resolution and Enforcement

- **Challenges/Issues in Refining and Extending the Straw-man Proposal**
  - Not intended to address the situation where interference is causing an immediate threat the safety of life and property
  - Did not contemplate bi-lateral sharing and hence interference from federal government systems into commercial systems
  - Learning from, but not violating ex parte rules associated with, on-going FCC proceedings (e.g., 3.5 GHz)
  - Existing and future societal resources for interference resolution and enforcement in a dynamic shared spectrum environment spread (a) over multiple entities, private and public and (b) within the public sector, between the FCC, the NTIA and individual government agencies (e.g., the FAA)

# Interference Resolution and Enforcement

- **Need for a System Engineering Approach (Motivation)**
  - Fact that existing and future resources for interference detection, classification/identification, location, resolution, reporting and enforcement are and will continue to be scattered across multiple entities both public and private
  - Budgetary constraints on public entities and competitive cost minimization pressures on commercial entities suggesting the need, for example, to avoid unnecessary duplication of facilities or functions
  - Changing threat vectors for both malicious and non-malicious intentional interference and the potential for vastly improved interference resolution and enforcement equipment and processes including “big data” and crowd sourcing techniques
  - Need to automate interference resolution and enforcement systems in order to speed responses and reduce costs
  - Proposed changes in FCC enforcement strategies as reflected in its Enforcement Modernization program

# Interference Resolution and Enforcement

- **Deliverables for TAC meeting on December 7, 2015:**
  - Updated straw-man proposal incorporating *inter alia* work on transmitter identifiers, emission designators, and Passive Intermodulation (PIM)
  - Preliminary recommendations for immediate, specific actions to be taken by the FCC (and, indirectly, NTIA) to initiate the system engineering approach/study
  - Detailed recommendations for a research plan for the system engineering study to be carried out in 2016

# Receiver Characteristics Subgroup

- **Goal : To provide the FCC with metrics and procedures to aid in the decision-making process when assigning different services to adjacent frequency bands**

# Receiver Characteristics Subgroup

- **Past Results**
  - Surveys of incumbent services
    - Frequency allocations in FCC regulations.
    - Receiver design standards
  - Conclusions
    - There is a wide variation in the quality of receiver standards that are publicly available
    - For many services it is not possible to predict adjacent channel interference from new services due to insufficient codification of receiver performance

# Receiver Characteristics Subgroup

- **Current Trends**
  - Develop a common set of parameters to describe receiver performance from among the following:
    - 3GPP has a comprehensive set of parameters; tests to certify behavior in the presence of potential interferers
    - ETSI (TR 101854) endorses Net Filter Discrimination to predict compatibility between adjacent systems
    - NTIA Interference Protection Criteria
    - CEPT European Communications Committee performs predictive coexistence studies

# Receiver Characteristics Subgroup

- **Proposed Course**
  - For new services that want to obtain frequency allocations:
    - The FCC should require analysis of the impact on incumbents based on a common set of operational parameters
  - For December 2015, develop a white paper outlining recommended procedures and guidelines for the Commission

# Receiver Characteristics Subgroup

- **Potential Challenges**
  - The Analysis
    - Who should perform it?
    - Can the FCC trust the results?
  - If incumbent receivers not designed to strict standards
    - How to characterize all receiver designs within a service?
  - Incumbent's confidential/proprietary information
    - Is it in the incumbent's best interest to share information?
    - Can this process be misused by either party?

THANK YOU

# Future Game Changing Technologies Working Group

Chairs: Nomi Bergman, Adam Drobot

FCC Liaisons: John Leibovitz, Nnake Nweke, Walter Johnston

11-June-2015

# Working Group Members

- WG Chair: Nomi Bergman, Bright House Networks
  Adam Drobot, OpenTechWorks

- FCC Liaisons: John Leibovitz, Nnake Nweke, Walter Johnston

- Members:
  - Kumar Balachandran, Ericsson
  - John Barnhill, Genband
  - Mark Bayliss, Visualink
  - John Chapin, SGE
  - Lynn Claudy , NAB
  - Brian Daly, AT&T
  - John Dobbins, Earthlink
  - Jeffrey Foerster, Intel
  - Dick Green, Liberty Global
  - Ramani Panduragan, XO Communications
  - Thyagarajan Nandagopal, NSF
  - Jack Nasielski, Qualcomm

# Working Group Members Cont'd

- Members:
  - Mark Gorenberg, Zetta Ventures
  - Russ Gyurek, Cisco
  - Farooq Kahn, Samsung
  - Gregory Lapin, ARRL
  - Brian Markwalter, CEA
  - Tom McGarry, Neustar
  - Paul Misener, Amazon
  - Bruce Oberlies, Motorola Solutions
  - Lynn Merrill, NTCA
  - Mark Richer, ATSC
  - Marvin Sirbu, SGE
  - Paul Steinberg, Motorola Solutions
  - Hans-Jurgen Schmidke, Juniper Networks
  - Kevin Sparks, Alcatel-Lucent
  - Sanjay Udani and David Young, Verizon

# Future Game Changing Technologies Working Group

1. Ideas for FGCT gathered from WG and TAC
2. Formation of Sub-Working Groups
   - Demand – Brian Markwalter
     - New Functionality
     - Business Models and Impacts
   - Capacity – Jack Nasielski
   - Architectures – Kevin Sparks
   - Basic Technology Building Blocks – WG
3. Sorting and Selection of most impactful technologies for the SWGs to focus on – in progress
4. Today's presentations are work in process

# Future Game Changing Technologies Working Group

Products for year end:

1. Short write-ups for technologies and ideas gathered
2. In depth write-ups for prioritized technologies
3. In depth presentation for “basic” technology building blocks
4. Actionable recommendations
5. Informational briefing

# FGCT Demand Sub-Working Group Discussion

**Brian Markwalter**

# FGCT Demand Sub-Working Group

## Uncategorized Demand List

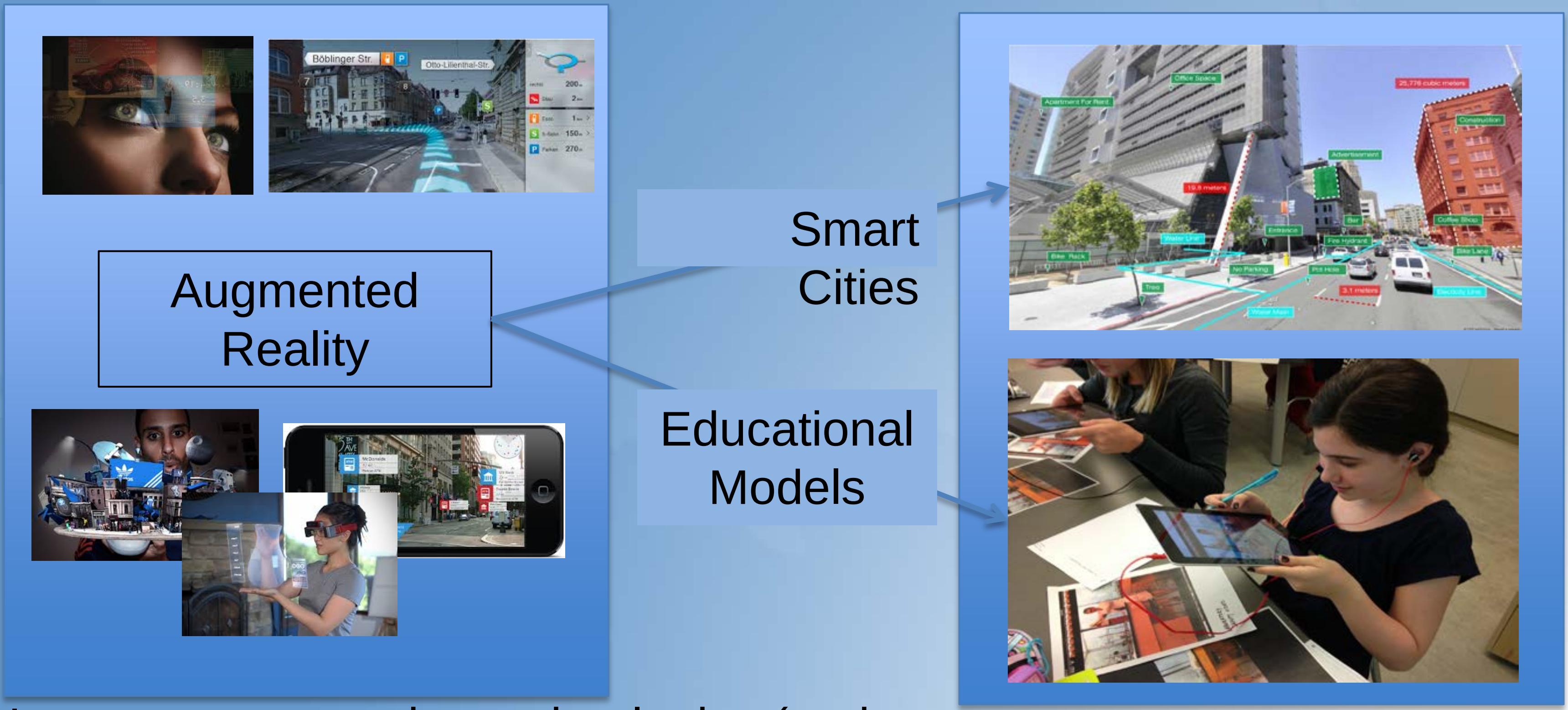
- Smart Cities
- Personalized Medicine
- New Educational Models
- Augmented Reality
- Self Driving Cars
- Commercial UAVs
- Uniform National Public Safety Network
- Pervasive Video
- Device-device communications

Contains overlapping mix of applications and technologies.

# FGCT Demand Sub-Working Group

Technology

Applications



Augmented Reality

Smart Cities

Educational Models

In process separating technologies (and requirements, like latency) from applications

**FGCT Demand Sub-Working Group**

# Technology Impacting Our Lives and Changing Network Demand

# FGCT Capacity Sub-Working Group Discussion

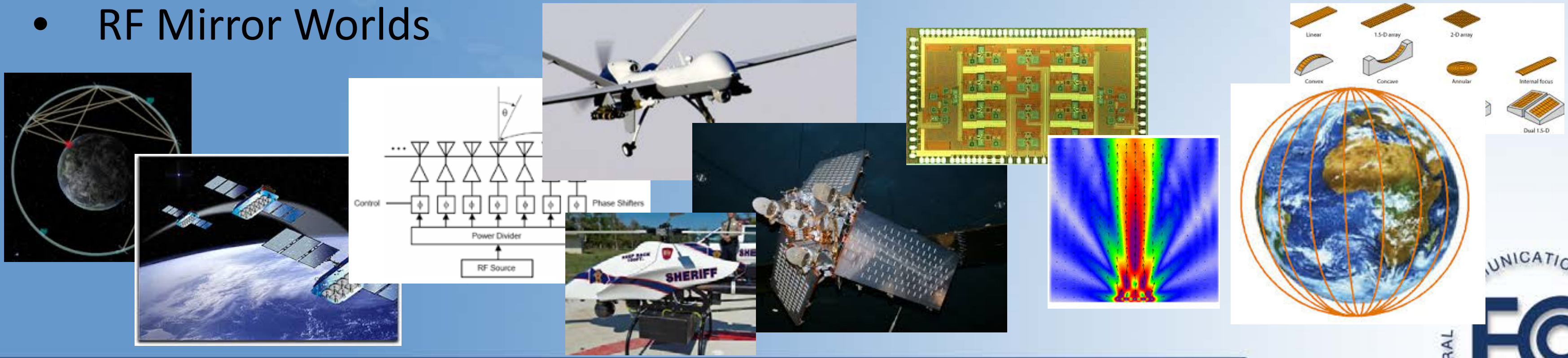
Jack Nasielski

# FGCT Capacity Sub-Working Group

## Capacity and Coverage Impacting Game Changing Technologies

- Carrier aggregation
- Network efficiencies for IoT/M2M
- Drones and Airborne Transmitters
- High capacity Geo Sat MEO LEO
- Hybrid 4G/5G/Geo Sat
- RF Mirror Worlds

- National Public Safety Network
- Distributed intelligent network edge
- Micro antenna arrays
- ATSC 3.0 - NG Broadcast TV std
- Full Duplex radio

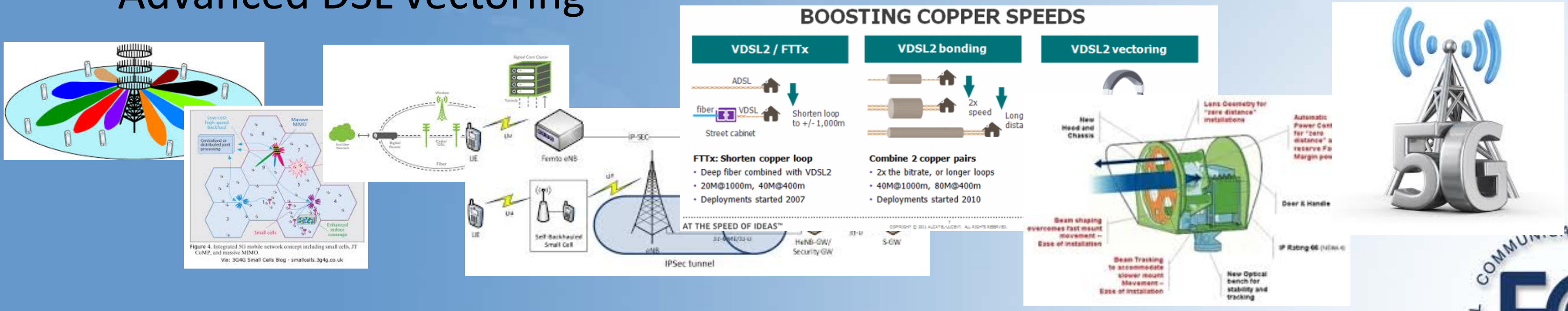


# FGCT Capacity Sub-Working Group

## Capacity and Coverage Impacting Game Changing Technologies

- Massive MIMO
- Virtual RAN/Cloud RAN
- UF-OFDM waveform
- Small cells w/LTE-U and w/mmWave
- Intelligent Multi-RAN/RAT Access
- Advanced DSL vectoring

- NG PON
- Free Space Optical Comms
- 5G (as a whole)
- Self-backhauling & Self-discoverable
- Defining new 3D channel models



BOOSTING COPPER SPEEDS

VDSL2 / FTTx

FTTx: Shorten copper loop
- Deep fiber combined with VDSL2
- 20M@1000m, 40M@400m
- Deployments started 2007

VDSL2 bonding

Combine 2 copper pairs
- 2x the bitrate, or longer loops
- 40M@1000m, 80M@400m
- Deployments started 2010

VDSL2 vectoring

AT THE SPEED OF IDEAS™

ADSL
fiber
VDSL
Street cabinet
Shorten loop to +/- 1,000m
2x speed
Long dista
Figure 4. Integrated 5G mobile network concept including small cells, JT CoMP, and massive MIMO.
Via: 3G4G Small Cells Blog - smallcells.3g4g.co.uk
Small cells
Massive MIMO
Femto eNB
Self-Backhauled Small Cell
UE
IPSec tunnel
HeNB-GW/ Security GW
S-GW
New Head and Chassis
Lens Geometry for "zero distance" installations
Automatic Power Cont for "zero distance" a reserve Fa Margin pow
Door & Handle
IP Rating 66
New Optical bench for stability and tracking
Beam Tracking to accommodate slower mount Movement – Ease of installation
Beam shaping overcomes fast mount movement – Ease of installation
5G

# FGCT Capacity Sub-Working Group

## Capacity and Coverage Impacting Game Changing Technologies

- Invited presentations on the suggested topics.
- So far have had 2 meetings, with presentations on:
  - Massive MIMO, reviewed principles of design for increased spectral efficiency with spatial diversity
  - 5G , reviewed existing industry whitepapers for 5G radio, network, and service technologies.

Will continue to examine topics with an eye towards actionable recommendations.

# FGCT Architecture Sub-Working Group Discussion

Kevin Sparks

## FGCT Capacity Sub-Working Group

# Architecture Impacting Game Changing Technologies

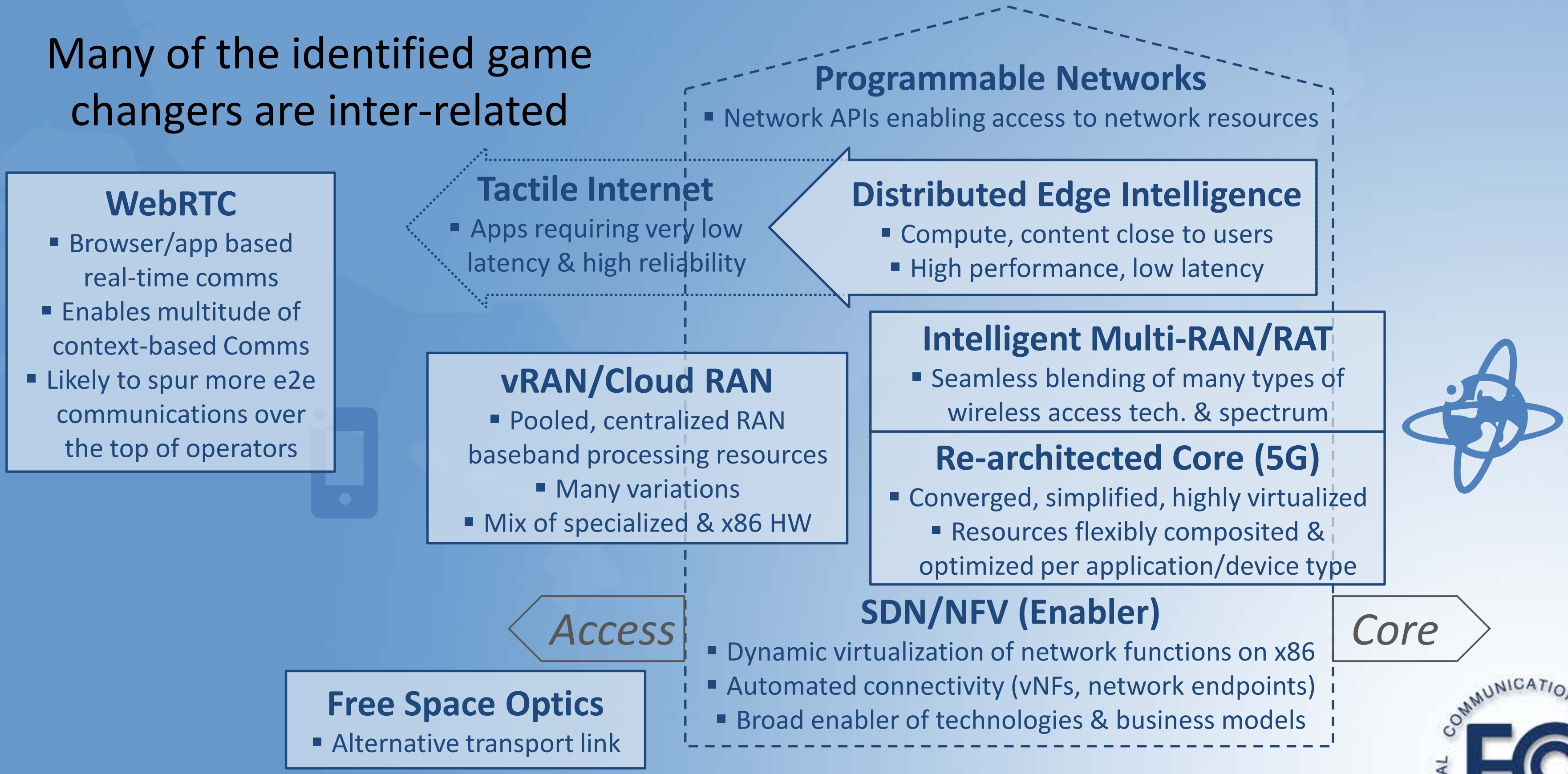
- Several game changers with significant architectural impact identified
- Preliminary exploration & prioritization for focused evaluation in progress
- Technologies rated across 5 dimensions
- Next step: deeper dive sessions to better assess impacts and FCC relevance

**Initial Rating Summary** (Averages)

| Technologies | | Impacts Network Structure | Drives New/Changed Business Models | Spurs Innovation & Competition | Impact to FCC Responsibilities | Potential to be Actionable | |
|---|---|---|---|---|---|---|---|
| SDN/NFV | 1 | 4.4 | 3.8 | 3.8 | 2.9 | 3.1 | 18.0 |
| vRAN/ Cloud RAN | 2 | 3.8 | 2.7 | 3.8 | 2.2 | 2.0 | 14.5 |
| Free Space Optical Comms | 3 | 2.3 | 2.8 | 2.8 | 2.3 | 1.8 | 12.0 |
| 5G/Multi-RAT Core Re-Arch. | 1 | 4.3 | 3.4 | 4.0 | 2.9 | 3.1 | 17.7 |
| Distributed Edge Intelligence/ Tactile Internet | 1 | 4.0 | 4.1 | 4.3 | 3.1 | 3.4 | 18.9 |
| WebRTC | 2 | 2.6 | 3.7 | 3.6 | 2.5 | 2.8 | 15.2 |

## FGCT Capacity Sub-Working Group

# Architecture Impacting Game Changing Technologies



Many of the identified game changers are inter-related

### Programmable Networks

- Network APIs enabling access to network resources

### WebRTC

- Browser/app based real-time comms
- Enables multitude of context-based Comms
- Likely to spur more e2e communications over the top of operators

### Tactile Internet

- Apps requiring very low latency & high reliability

### Distributed Edge Intelligence

- Compute, content close to users
- High performance, low latency

### Intelligent Multi-RAN/RAT

- Seamless blending of many types of wireless access tech. & spectrum

### vRAN/Cloud RAN

- Pooled, centralized RAN baseband processing resources
- Many variations
- Mix of specialized & x86 HW

### Re-architected Core (5G)

- Converged, simplified, highly virtualized
- Resources flexibly composited & optimized per application/device type

### SDN/NFV (Enabler)

- Dynamic virtualization of network functions on x86
- Automated connectivity (vNFs, network endpoints)
- Broad enabler of technologies & business models

### Free Space Optics

- Alternative transport link

# Future Game Changing Technologies Working Group

## Thank You!

# Future Game Changing Technologies Working Group

# Appendix and Backup

# Future Game Changing Technologies Working Group Charter

- The workgroup will seek to identify technologies with the potential to radically change communication infrastructure and business models across a broad range of fronts. The intent is to identify seminal technologies and concepts that the Commission should understand and possibly include in its considerations. The workgroup will seek to identify these catalysts and assess their potential impact. The group will be charted to scan across a wide breadth of technical areas, identify areas of potential promise, and organize them in the context of synergies and potential impacts.

# Future Game Changing Technologies Working Group Charter

- Examples of areas that could be examined include 5G, Massive MIMO, millimeter wave devices, bidirectional channel sharing, interference cancellation technology, space-based free space optical systems, cube-satellites, low earth orbit satellites, fiber enhancements, the use of crowd sourced measurement techniques, software defined networks, radar/radio spectrum sharing, etc.

# Future Game Changing Technologies Working Group

Basic Technologies

- Computing
- Storage
- Communications
- Sensors
- Actuators
- Interfaces
- Software
- Power

Important Enablers

- Cloud Computing
- Mobility
- Analytics
- Artificial Intelligence
- Autonomy
- Software Defied Functionality

# Next Generation (NG) Internet Service Characteristics & Features Working Group

Chairs: Russ Gyurek, Cisco
John Barnhill, GENBAND

FCC Liaisons: Walter Johnston, Scott Jordan, Daniel Kahn,
Padma Krishnaswamy

FCC On-Site Meeting, Washington DC
June 11, 2015

# Working Group Members

- **Members**
  - Mark Bayliss, Visualink
  - Nomi Bergman, Bright House
  - KC Claffy, CAIDA
  - John Dobbins, Earthlink
  - Adam Drobot, OpenTechWorks
  - Andrew Dugan, Level3
  - Stephen Hayes, Ericsson
  - Theresa Hennesy, Comcast
  - Scott Jordan, FCC
  - Farooq Kahn, Samsung
  - Thyaga Nandagopal, NSF
  - Tom McGarry, Neustar
  - Milo Medin, Google
  - Lynn Merrill, NTCA
  - Jack Nasielski, Qualcomm
  - Ramani Pandurangan, XO Comm
  - Mark Richer, ATSC
  - Marvin Sirbu, Carnegie Mellon
  - Kevin Sparks,  ALU
  - Sanjay Udani, Verizon
  - David Young, Verizon

# NG Internet Service Characteristics & Features Charter

- The Internet has and will continue to evolve:
  - Driven by the transition to all IP
  - From simple backbone/access network to a complex environment of dedicated links, Content Delivery Networks (CDNs), specialized routing/peering arrangements, etc.
  - Supporting : Remote terminal access/ email -> Web browsing/ media transfer -> Video streaming

*Commission Hypothesis:*

- A ‘best effort’ network is evolving towards one where Quality of Service (QoS) is a growing concern
- Need for benchmarks to measure QoE and the support of rich services
- The Internet will transition to a role of critical infrastructure

# Constant Evolution – User Driven, Technology Enabled

Devices, Capacities, Bandwidth, Content

## Yesterday's Internet

- Limited Devices
- Wired Access
- Stationary Devices
- Human Driven Usage
- Email, Web Browsing
- Downloaded Content

## Today's Internet

- Wired or Wireless Access
- Many Mobile Devices
- Human Driven Usage
- Entertainment Content
- Content Delivered at Backbone and Metro
- Streaming Content

## Tomorrow's Internet

- Wired or Wireless Access
- Fixed & Mobile Devices
- Built-in Sensors with Data Collection
- Content Delivered at the Metro/ Edge
- "Thing" Driven Usage
- Public Safety

# Commission Asks Workgroup to Comment on:

- Critical infrastructure services
- PSTN Services Transition
  - Work last Several TACs.
  - Record Largely Complete
- Internet of Things
  - 2013 & 2014 TAC Work
  - 2015 Security IoT Sub-WG
- Cybersecurity
  - 2014, 2015 TAC Work Group
- Public Safety

- Governance
  - Relevant standards and governance bodies/ Models
- Metrics
  - QoS/QoE: End to end network and Network to Network
  - Health and Performance benchmarks
- New technologies (e.g. 5G, SDN/NFV, NDN, Caching)
  - Game Changing Tech. WG
  - Caching & edge compute

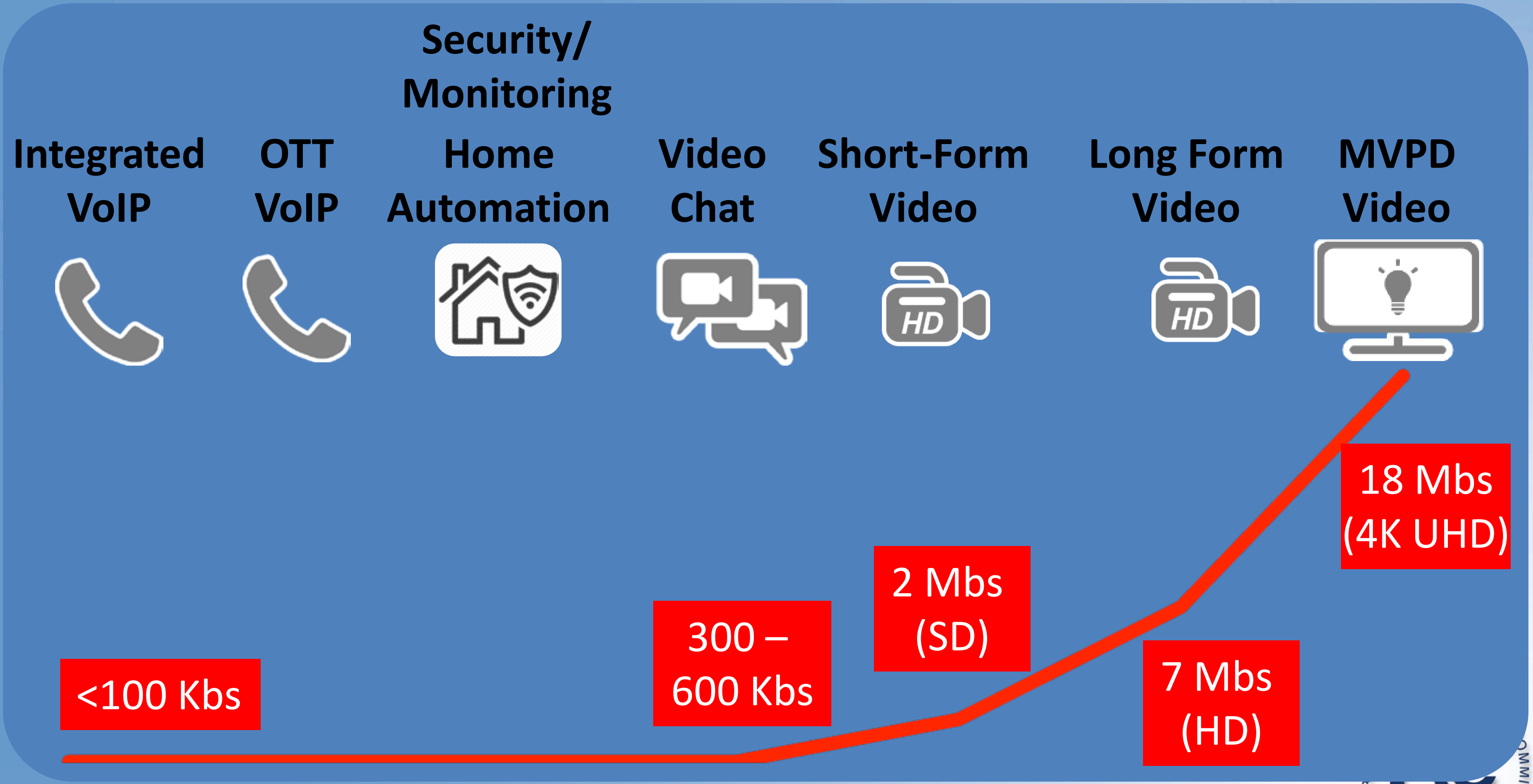
# Tenets of NG Internet

- Open to all to offer and access information & services, with maximal "networking effect"
- Offers efficient, reasonable cost access with ample capacity for a broad range of uses
- Provides the means to support real-time and other latency- sensitive, bandwidth-demanding applications with acceptable QoE, subject to the limits of the subscribed access service (SLA)
- The Internet has adapted over time, policy should continue to promote innovation and development, supporting the maximum span of service characteristics
- Access to any legal content or site
- Strongly protects users' confidentiality and privacy, while retaining effective capability for Lawful Intercept

Key Drivers

# WHERE WE ARE TODAY, AND EXPECTED GROWTH

# Consumer Broadband Access Consumption



Security/ Monitoring

Integrated VoIP

OTT VoIP

Home Automation

Video Chat

Short-Form Video

Long Form Video

MVPD Video

<100 Kbs

300 – 600 Kbs

2 Mbs (SD)

7 Mbs (HD)

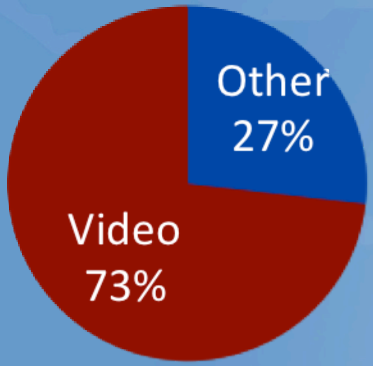
18 Mbs (4K UHD)

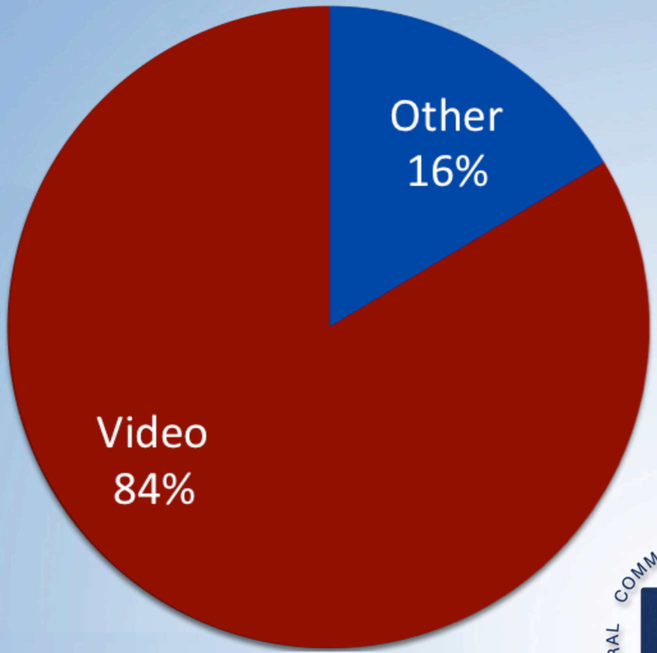
Source for video stream sizes: Cisco VNI – 2014 -2019

# Consumer Internet Traffic Growth - USA

**2014 - 98.3 EBs**

**2019 – 314.6 EBs**





Source: Source Cisco VNI – 2014 -2019

# Evolution Trends

| Factor | Trend | 2014 | 2019 |
|---|---|---|---|
| Devices | Smart Phones and IoT | 2.0B | 3.9B |
| Speeds | Both Fixed (W+) and Mobile (W-) speeds growing rapidly | 22.2Mbs W+<br>2.6Mbs W- | 45Mbs W+<br>6.1Mbs W- |
| Traffic Volume | Consumer Internet Traffic | 98.3EB | 314.6EB |
| Traffic Mix | Video Growth is dominant driver of consumer Internet consumption | 73% | 84% |
| Access Mix | Wireless data growth but fixed still dominant (All Internet Traffic) | 6.4EB W-<br>115.4 W+ | 43.2EB W-<br>343.3 W+ |
| Metro/ Long Haul Changes | Virtualization/ Dynamic Mgmt<br>CDN I/C Shifting from Core to Metro | 165 vs 52 EB<br>(76% of all IP) | 499 vs 49 EB<br>(91% of all IP) |

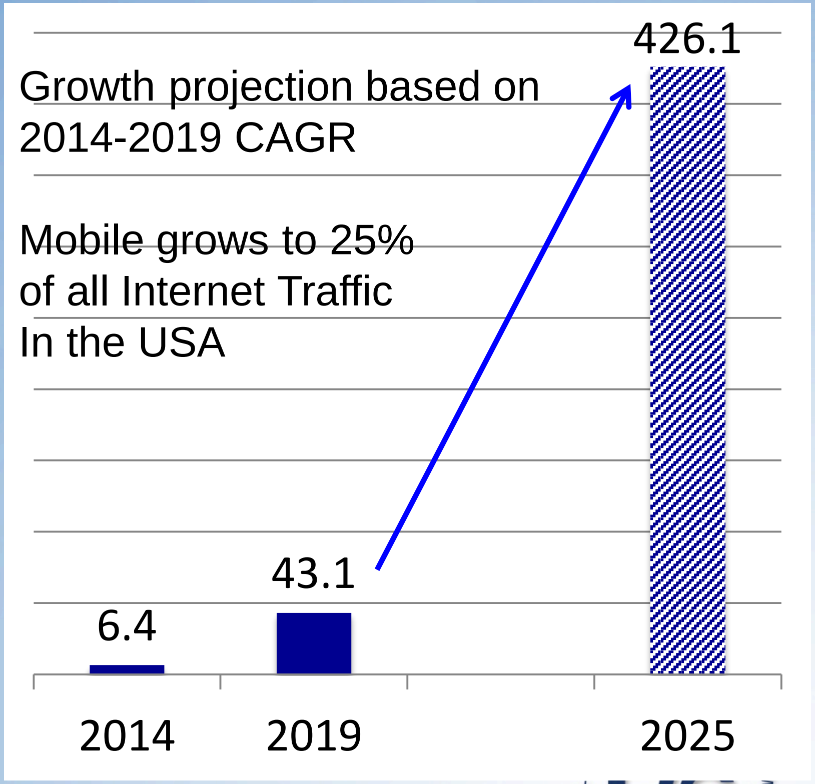
Source: Source Cisco VNI – 2014 -2019

# NG Internet Drivers

- Compute & Content Centric Distributed Edge:
  - Potential for content and compute to be integrated into NG routers
  - Compute edge moves into SP/BIAS network
  - Content becomes front edge of cloud to include compute resource, not just caching
  - CDN and BIAS boundaries become fuzzy and virtual
  - Less inter-domain traffic, less inter-domain issues
  - Content providers and BIAS networks vertically integrate CDN capabilities
  - Interconnect moves from centralized to more local level

# NG Internet Drivers

- Mobility Growth Drives New Hierarchy
  - Mobile devices will become more opportunistic / User behavior changing
  - Flexibility to go “down-market” to support new low requirement needs (IoT)
  - Wireless LTE may compete with fixed wire-line
  - Land line capability must scale to support the continuing wireless boom…it’s a fiber world



Growth projection based on 2014-2019 CAGR

Mobile grows to 25% of all Internet Traffic In the USA

*Source: Cisco VNI report May 2015*

# NG Internet Drivers

- Societal changes
  - Mobility, access everywhere
  - Encryption is new rule
  - Many devices connected per user
  - Forecast: Peak traffic growing faster than non-peak traffic
- Devices outnumber people (IoT)
  - Constant data streams from billions of devices
- More Enterprises shifting to public Internet
  - Impacts Internet load during day (peak time)
- Pervasive Services: Video, Medical, Home monitoring, Automotive, etc
- Programmability
  - Replacing non-automated processes [provisioning] infrastructure layer impact
  - Not realistic to cross AS boundaries,
  - Used to control aggregate flows, not individual
- BIAS is critical component of End-to-end infrastructure

Major Factors For Consideration

# BANDWIDTH, QOS/QOE

# Main Questions

The working group will study the following questions related to the tenets

1. Does the NG Internet require QoS?
2. What are driving factors which would require QoS?
3. What are consumer QoE expectations?

*What new technologies may have positive or negative impact?*

# Major Factors affecting Internet QoE

- Inter-domain: Interconnect, Peering
- Network Design practices (CDN, Routing, …)
- Encryption/Encapsulation
- Limited/lack of Bandwidth
- Traffic Shaping
- Congestion

# Bandwidth & QoE

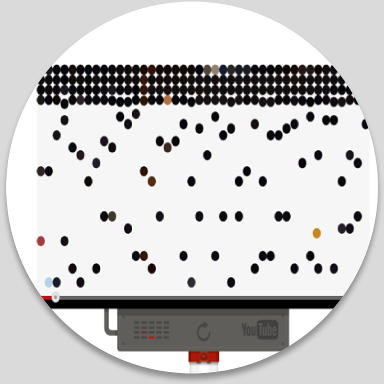
- Bandwidth is one of many factors in delivering QoE
  - IE, increasing BW does not always equate to greater QoE
- Each party independently enacts, manages, and applies QoS
  - QoS does not really span across multiple networks and/or devices
- Differential treatment of traffic in forwarding plane
- Metrics & Measurement of QoS
  - Jitter, Latency, Delay, P-loss; may not be meaningful due to multiple networks involved in service delivery

# QoS and QoE Definition

- *QoS attempts to objectively measure the service delivered by the vendor, It is typically measured by the service terms of a contract and measures performance relative to pre-agreed quality parameters.*

- *QoE in the context of telecommunications networks is a purely subjective measure from the user's perspective of the overall value of the service provided. QoE must take into consideration every factor that contributes to overall user value such as suitableness, flexibility, mobility, security, cost, personalization and choice.*

# Quality of Experience (QoE) “Levers"



## Server/ Content Capacity

**Edge Providers Control**

- Quality of content
- CDN/Servers/Location
- First mile
- Content owner footprint emerging

## Transit Capacity

**Edge Providers Control**

- Transit selection
- Path performance in real time

**ISPs Control**

- Number of paths
- Interconnect path capacity planning

## Broadband Capacity

**Edge Providers Control**

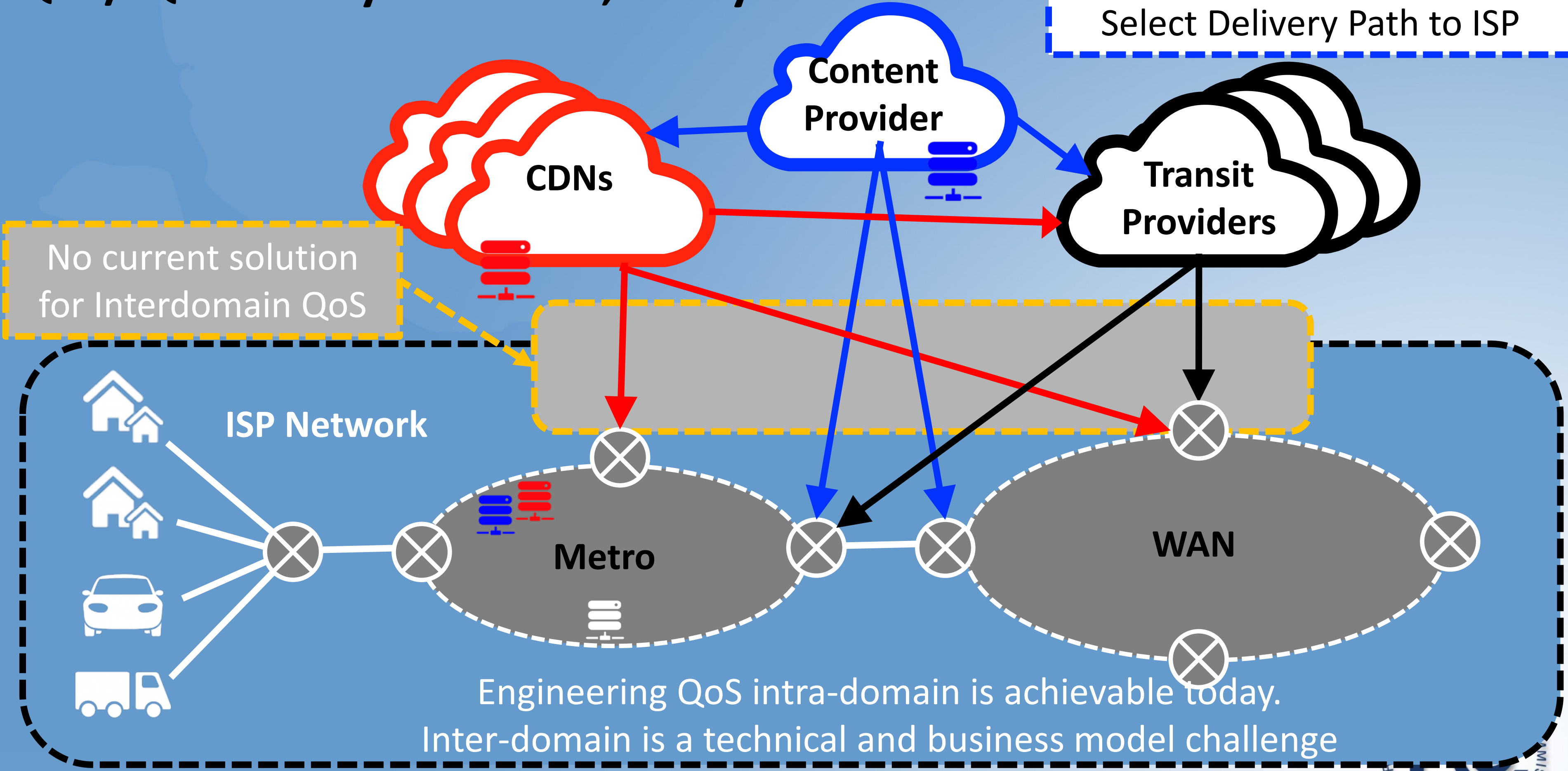
- Client Decisions

**ISPs Control**

- Broadband capacity

## QoS/ QoE: Many Providers, Many Boundaries

Content/ Service Providers Select Delivery Path to ISP



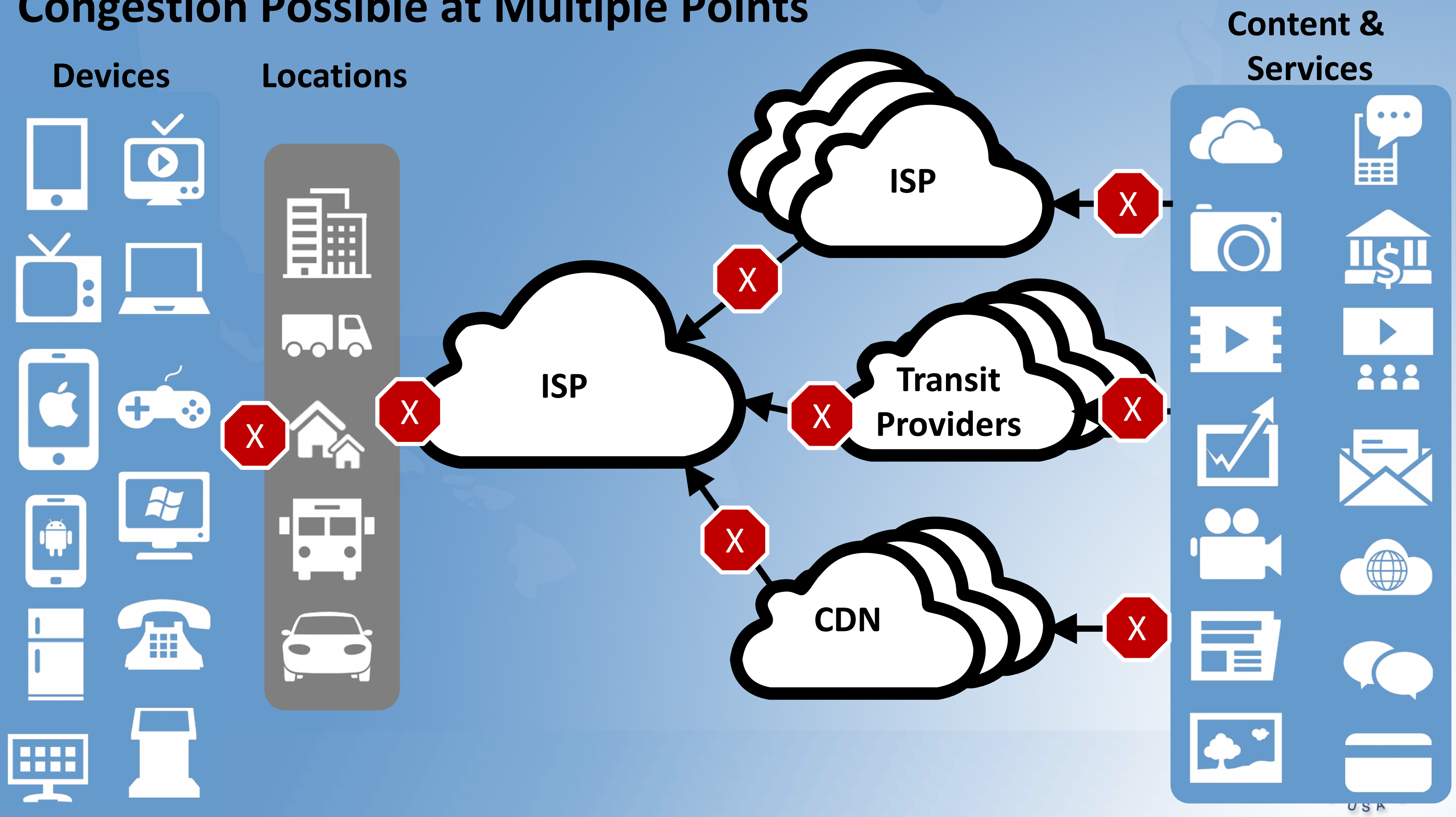
No current solution for Interdomain QoS

Engineering QoS intra-domain is achievable today.
Inter-domain is a technical and business model challenge

# Congestion Mgmt/Traffic Shaping

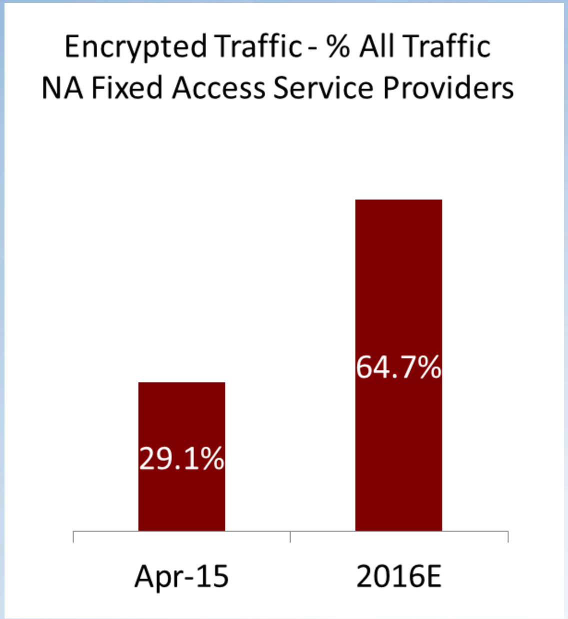
- Congestion Management - A collection of techniques used to prevent and handle network congestion
  - Necessary to manage the network
  - Always possible to misuse to discriminate inappropriately, but that is not the intention
- Techniques: *packet marking, admission control, caching, rate control, routing algorithms, packets scheduling, etc*
- *Trends:*
  - *Encryption: Most techniques still possible, but with less granularity since networks knows less, especially with respect to content.*
  - *Traffic Increase: Most of the congestion management and traffic shaping will continue to occur at the network edge*
- http://www.bitag.org/report-congestion-management.php

## Congestion Possible at Multiple Points



# Encryption: From Exception to Rule

- Multiple drivers pushing encryption everywhere
  - Browsers now more aggressive about warnings
  - Google now using SSL by default as ranking signal for search
  - Major email operators implementing peer TLS encryption
- North American Internet traffic rapidly growing "darker"
  - Netflix and YouTube streams will be SSL encrypted by the end of the year
  - Accelerated growth in SSL by default since Google ranking announcement
  - Ad networks are all working on SSL enablement as well



*Source: Sandvine*

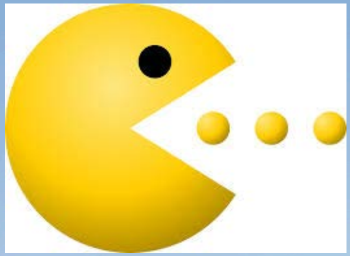
# Encryption: From Exception to Rule

- Impacts to Service Providers
  - DPI, transparent caching, and some firewalling all break
  - Less ability to track evolution of traffic types and services
  - May complicate traffic management and QoS implementations in limited number of SPs
  - Payload compression, often used on microwave backhaul links, fails, reducing the effective capacity delivered
  - TCP compression and optimization techniques used in SATCOM systems become ineffective, potentially seriously affecting user performance
- Other impacts
  - Significantly improves resiliency to man-in-the-middle attacks that inject malware
  - Much more complicated task for Law Enforcement interception
  - Improves user privacy and prevents ISP tracking and analysis (DPI, "supercookies"), website redirection, etc…

Working Towards Actionable Recommendations

# SUMMARY, WHAT'S NEXT

# Summary & Focus Ahead



- Video is eating the Internet, and aggressive
- CDN and Compute → edge, continual evolution of efficiency (thru ISP or CDN provider) - Greater exploration of impact
- Encryption: As network goes dark, impact on all parties
- QoS Metrics and reporting: Access options
- QoE: Determine expectations, and ways to measure
- SDN and programmability, impact on AS’s, then cross-domain
- Technology game changers (service characteristics drivers)
- ISP (BIAS) heterogeneity – disparity in architectures

# Feedback, Questions, Input

***Any sufficiently advanced technology is indistinguishable from magic***

- Arthur C. Clark

# BACKUP

# NG Internet Service Characteristics & Features Charter

The Internet continues to evolve: from a network that originally supported remote terminal access and email, later to web browsing and media transfer, now to the present environment where video streaming has become a dominant service. A 'best effort' network is evolving towards one where Quality of Service (QOS) is a growing concern and where the Internet assumes the role of critical infrastructure. The architecture of the Internet has adapted to better support these issues morphing from relatively simple backbone/access network architecture to a more complex environment of dedicated links, Content Delivery Networks (CDNs), specialized routing/peering arrangements, etc. The transition to IP ('the death of the PSTN') will further hasten this evolution to an environment wherein IPv6 is the underlying addressing scheme. This work group will seek to ***assess future service requirements*** for the Internet driven by the need to provide critical infrastructure services, the transition of services from the PSTN to an IP based platform, the expected impact of IOT, cybersecurity needs, governance models and other factors. The work will examine efforts within relevant standards and governance bodies to frame these issues as well as look at potential architectural changes driven by these ***service needs*** for public safety, ***QOS metrics for end/end and network/network interfaces*** and new technologies such as 5G. The work group will also seek to make recommendations on benchmarks that could serve to better inform policy makers on the health and status of the Internet.

# Roadmap for Future Unlicensed Services Working Group

Chairs: Mark Bayliss, Milind Buddhikot

Vice Chair: John Barnhill

FCC Liaisons: Michael Ha

June 11, 2015

# Working Group Members

- WG Co Chairs:  Mark Bayliss, Milind Buddhikot

- Vice Chair, John Barnhill
- FCC Liaisons: Michael Ha, Karen Rackley

- Members:
  - John Barnhill, GENBAND
  - Mark Bayliss, Visualink
  - Nomi Bergman, Brighthouse
  - Milind Buddhikot, Bell Labs
  - Adam Drobot, Open Techworks
  - Dick Green, Liberty Global
  - Russ Gyurek, Cisco
  - Jeff Foerster, Intel
  - Theresa Hennesy, Comcast
  - Farooq Kahn, Samsung
  - Jack Nasielski, Qualcomm
  - George  Lapin
  - Mark Racek, Ericsson
  - Brian Markwalter CE.org

## Roadmap for Future Unlicensed Services

Unlicensed services have played an unexpectedly vital role in the evolution of communication capabilities and in providing a ‘wireless commons’ for innovation. It is critically  important for the Commission to understand both the potential pathways for continued evolution of unlicensed services as well as potential threats to the continued viability of the ‘commons’.

# Work Group Focus

(1) Evolving and novel applications

- (e.g. low power WANS, internet-of-things (IOT), unlicensed LTE).

(2) New business models

- (e.g. managed vs. unmanaged vs. private, indoor-only services).

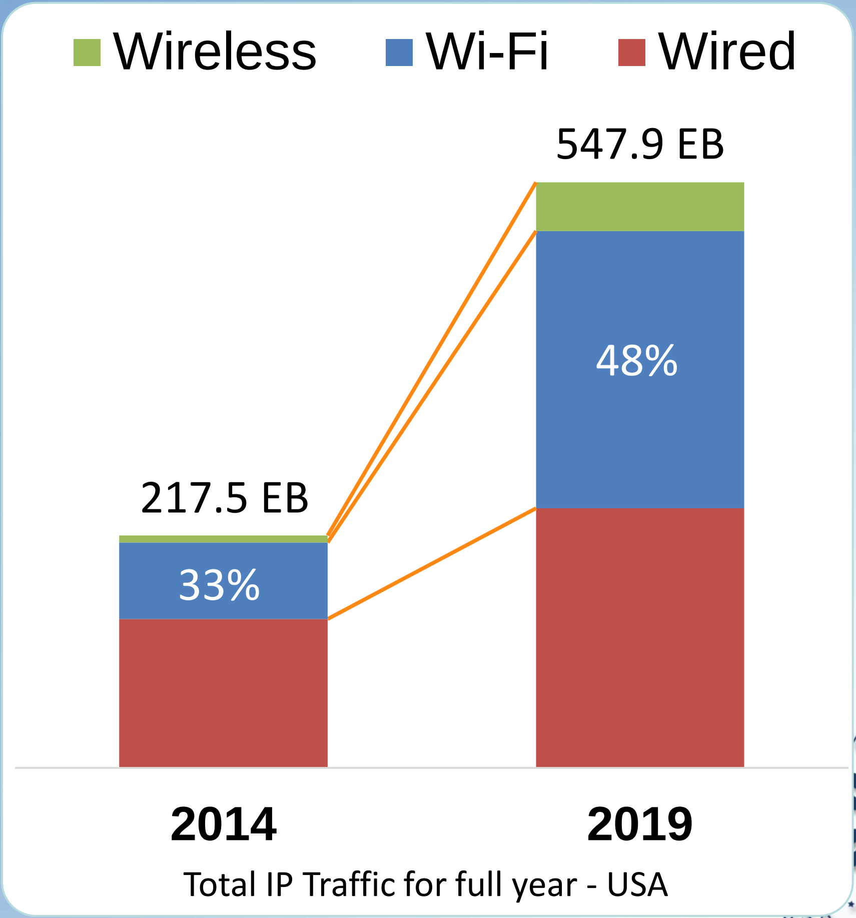
(3) New candidate spectrum bands to increase available spectrum.

(4) Voluntary etiquettes for unlicensed service applications that will help protect the commons model

(5) The potential impact of present EMC limits for consumer and industrial devices on the continued growth and vibrancy of unlicensed services.

# United States IP Traffic Growth

- Wi-Fi Already Important to US Economy and Usage
  - $62B annual incremental retail sales value - USA*
- Mobile data traffic offload is high-value consumer use case
  - 57% mobile data traffic offloaded in 2014 growing to 66% in 2019
  - Impact on traffic grow CAGR is 7%
- 33% - 2014 portion of Total IP Traffic accessed over Wi-Fi
- 48% - 2019 estimate of Total IP Traffic accessed over Wi-Fi



Total IP Traffic for full year - USA

Source: Source Cisco VNI – 2014 -2019

*UNLICENSED SPECTRUM AND THE U.S. ECONOMY, June, 2014, ce.org

# Unlicensed Spectrum Usage

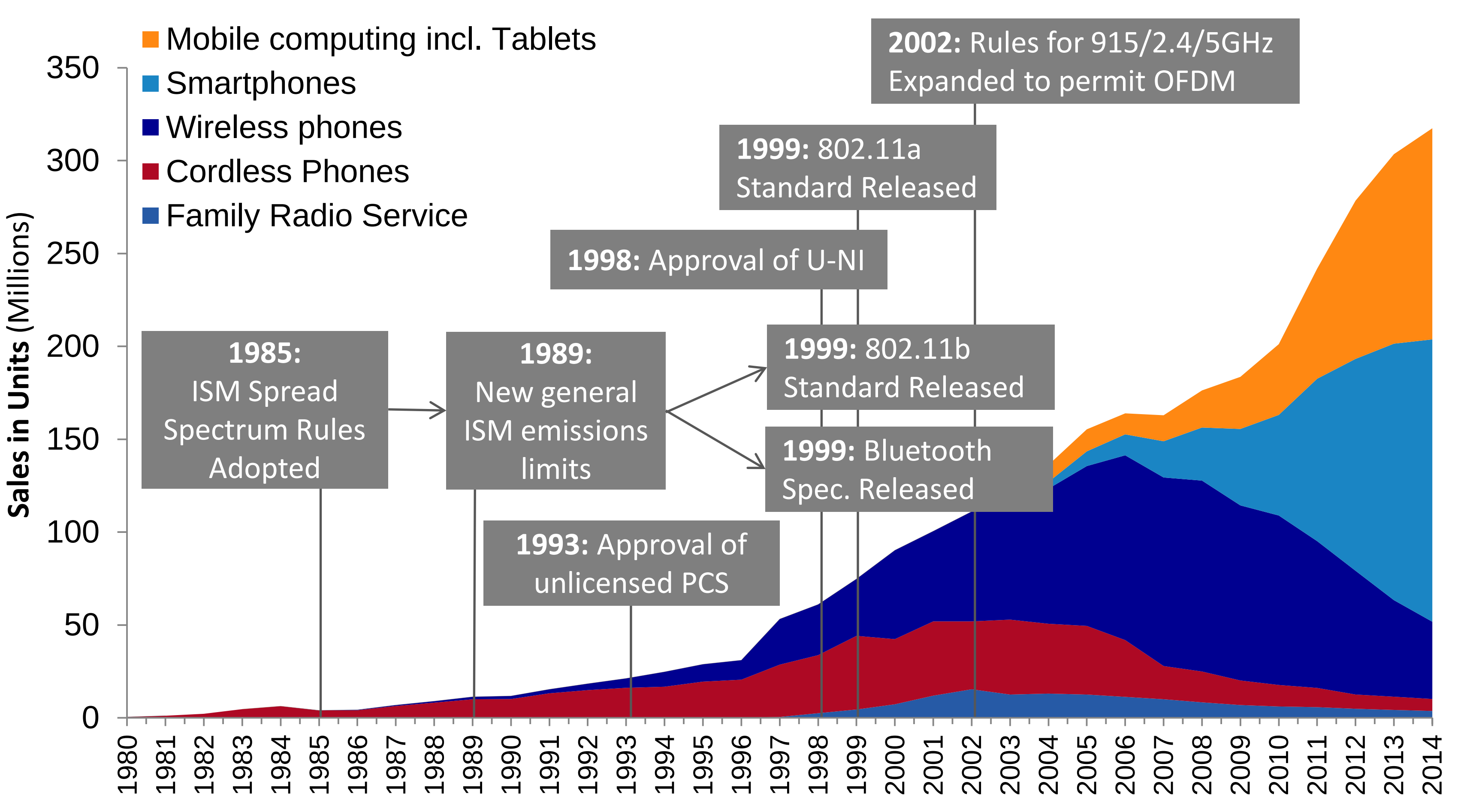
- Key Use Cases
  - Cellular Offloading to Wi-Fi
  - Residential Wi-Fi
  - Wi-Fi Internet Service Providers
  - Wireless Personal Area Networks
    - Bluetooth, Zigbee, WirelessHart, etc
  - RFID
  - Medical Pans
  - Cordless phones, remote controllers

- Bandwidth/ throughput increase through policy actions and emerging technologies
  - More spectrum allocation, TV white spaces, spectrum sharing
  - MIMO, Beam forming, LTE-U, mmWave

Graphic Courtesy NCTA.org

*Source: UNLICENSED SPECTRUM AND THE U.S. ECONOMY, June, 2014, ce.org

# Unlicensed Spectrum Growth - Selected Categories



**1985:** ISM Spread Spectrum Rules Adopted

**1989:** New general ISM emissions limits

**1993:** Approval of unlicensed PCS

**1998:** Approval of U-NI

**1999:** 802.11a Standard Released

**1999:** 802.11b Standard Released

**1999:** Bluetooth Spec. Released

**2002:** Rules for 915/2.4/5GHz Expanded to permit OFDM

Source: http://www.ce.org/CorporateSite/media/gla/CEAUnlicensedSpectrumWhitePaper-FINAL-052814.pdf

# Spectrum Available for Unlicensed Broadband Under 6 GHz

| Band | Current | Pipeline | Comments |
|---|---|---|---|
| TV White Spaces | 0-150 | + | Future TV White Space availability subject to results Incentive Auction |
| 902-928 MHz | 26 | - | |
| 2400-2483.5 MHz | 83.5 | - | |
| 3550-3700 MHz | 150 | - | Licensed-by-rule under Part 96 - April 2015 |
| 5150-5350 and 5470-5825 MHz | 555 | | |
| 5350-5470 and 5850-5925 MHz | | 195 | Proposed U-NII-2B and U-NII-4 bands are under discussion |

+ Represents where multiple initiatives are underway but additions aren’t quantified

Please note that this is for unlicensed broadband use and there are more spectrum available for other unlicensed applications

## 3Q Work Activity

- Industry Engagement to obtain input for possible future recommendations.
  - Meetings with unlicensed spectrum equipment manufactures.
  - Unlicensed spectrum groups and organizations.

**New Item:**

- Looking for TAC input and support to assess the noise environment impact on spectrum usage.
  - Assess the current state of noise environment.
  - Review Current rules for intentional and unintentional incidental radiators.

## Q32015 Industry Engagement– Sample Questions

1. What applications and services, both new and future, do you expect to drive demand for the future use of unlicensed spectrum?
   a. Any quantifiable projections on the potential value of these applications and services?
2. Are you aware of any data or market projections on the relative growth of narrow v. wide channels (e.g., white space v. 802.11ac/ad) to better understand future unlicensed spectrum needs?
3. Are you aware of, experiencing, or anticipating heavy congestion in the use of the existing unlicensed spectrum bands which is currently impacting services in those bands or will impact services in those bands in the near future?

## Q32015 Industry Engagement – Sample Questions

4. Are there any existing FCC rules governing the use of the unlicensed bands that are impacting the deployment of existing or future new services? If so, which rules should be revisited and why?
5. If the FCC were to open up new spectrum for unlicensed use, which frequency bands would be the highest priority?
6. Are there new applications and services which could use unlicensed spectrum but which may not fit into the existing rules as currently governed by the FCC Part 15?
7. Do you have any data to suggest that some unlicensed bands are underutilized? Are you aware of any causes?

# FCC TAC: 477 Testing

# 477 Testing WG

June 11, 2015

- Steve Lanning (WG Chair)
- Tom Wilson
- Chris Feathers
- Chelsea Fallon (FCC)
- Kenneth Lynch (FCC)
- Others

# Update

- Some TAC recommendations from 2014 work are expected to appear in the next filing window
  - Streamlined upload process
  - Comprehensive filing summary and receipt
- Funding for client side application yet to be approved
- Expect development of client side application in FY16
- Client side application would
  - Ease process of compiling data
  - Support smaller geographic reporting
  - Support additional reporting variables

# Work Program

- Review requirements for the application
- Survey platforms used to make current 477 submissions
- Survey platforms available to run new 477 software
- Provide input on security and confidentiality issues
- Develop recommendations on how to collect subscribership data beyond counts by data rates
- *Develop maps and charts to highlight need for more detailed data collection and maps*

# Comments and Feedback