Enforcement Subcommittee

15 August 2017

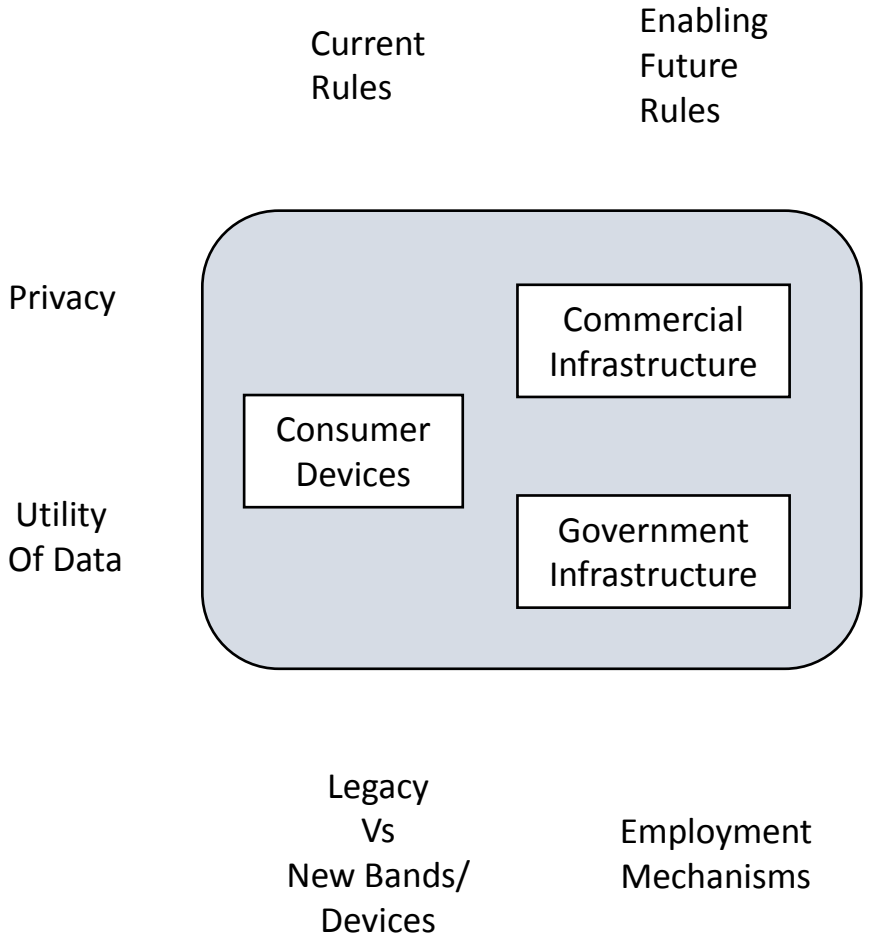
Enforcement

1. What options do you see for making enforcement more robust, including by increasing automation to prevent interference, and to identify and respond to interference when it does occur in the near or longer term?
2. What are the principal technical and operational options for enabling automated enforcement, at both the network and device levels, and how would you address cybersecurity and privacy requirements? Please consider, among others, options related to: station IDs; data cloud/fog architectures; and crowd-sourcing.
3. What options for automated enforcement are unique to the development and deployment of 5G technologies/applications?
4. What steps do you recommend the Federal Government, specifically NTIA, take to implement automated enforcement processes? What steps will the private sector need to take? Please consider steps relating to technical, process and policy issues, including potential operator-to- operator coordination approaches?

    - Co-Chairs: Mark Crosby and Paul Kolodzy
    - Members: Mary Brown, Dale Hatfield, Mark McHenry, Janice Obuchowski, Rick Reaser, Dennis Roberson, Mariam Sorond, Bryan Tramont, Bob Weller

Automated Enforcement

- GROUP 1: Background
  - Status of enforcement operations?
  - Current Policy Framework
  - Previous Work in Automated Enforcement
- GROUP 2: Options for more robust enforcement
  - Automated Prevention
  - Automated Response
  - Legal/Policy/Technology Ramifications
- GROUP 3: Technical / Operational Options
  - What is possible technically?
  - What are the limits in policy?
  - What is the impact (pro and con) for any option?
- GROUP 4: 5G-specific Impact
  - Unique technical aspects?
  - Legacy vs Green-Field deployments?
  - Fixed vs Mobile uniqueness?
- ALL: Recommendations?
  - Policy Changes?
  - Demonstrations and/or Investments?
  - Coordination Approaches for Sharing?



Status

- Still formulating precise recommendations … Presenting preliminary findings today
- Recommendations provided in this briefing represent “raw” material that has not been vetted nor approved by the full enforcement subcommittee

Activities

- Multiple Subcommittee Group Meetings
- Developed bibliography of prior work
- List of references and contacts
- Spoken with a number of interference hunters and equipment manufacturers.

Preliminary Findings

- Most companies hire consultants to locate and identify interference. Some larger companies (*e.g.*, wireless carriers) have internal teams
- Interference broadly divides into three types:
  - Intra-system (self) interference
  - Proximate (nearby) interference, affecting just one site/user
  - Widespread interference, affecting multiple sites/users
- Current framework limits the ability of consultants to precisely locate and identify sources due to privacy and access issues
- "Automated" systems are relatively primitive or limited to specific standards-compliant systems (cellular PCIs, WiFi SSIDs/MAC addresses, etc.)

Preliminary Findings

- Evolving Challenges
  - Networks of small cells, even down to the size of home routers
  - Towers or antennas that are relatively close together
  - Massive capacity (20 Gbps) and Low latency (1ms latency)
- New Challenges
  - Device to device communications: Autonomous and direct radio connection between devices; not controlled by infrastructure after setup.
  - Adaptive antenna arrays: mobile Beamforming and FD-MIMO
  - Dynamic framing: Traffic adaptive uplink and downlink frame duration can present transient interference.
- New Capabilities
  - Large processing bandwidth that could support high quality spectrum measurements

Preliminary Recommendations

- Establish an information sharing program/database to help enable automated identification of interference sources. NTIA should investigate who would pay for and who would operate the 5G enforcement activity
- Study the bounds of impact based on transient interference to ascertain levels that can cause performance impact to victim receivers
- Develop a machine readable report standard for interference detection results (e.g, time, location), classification results (bandwidth), and logging
- Mandate that remote ‘kill switch’ , ‘pause transmission’, ‘beacon-ID’, or ‘band blocking’ software be installed in 5G equipment to aid in machine-machine interference diagnostics and/or to shutdown errant devices
- Analyze the different enforcement process ‘stages’ to determine the automation approaches and the costs/benefits of automation at each stage
- Develop an automated enforcement architecture design