Spectrum and Receiver Performance Work Group

Preliminary Thoughts on Enforcement:

Background, Questions and Proposed Deliverables

Dale N. Hatfield

April 10, 2013

Objective

To assist the Commission in developing new or revised technical strategies for responding more efficiently and effectively to the fundamental technological, operational, and economic trends that are creating an increasingly complex radio interference resolution and enforcement environment

Background

- Definitions
  - Interference Definition
  - Interference as Distinguished from Noise
    - Interference: coherent emission
    - Noise: incoherent emission
      - Natural sources such as lightening
      - Manmade sources such as rotating electrical equipment
    - Manmade Interference/Noise
      - Intentional radiators
      - Unintentional radiators (Part 15)
      - Incidental radiators (Part 18)

Background

- Definitions (Cont'd)
  - Intentional Interference (including jamming and spoofing)
    - Malicious
    - Intentional but not malicious
  - Notes

    (a) In modern broadband systems the interference may appear more like an incoherent emission than a coherent emission

    (b) An example of intentional but not malicious interference might be a school which unwittingly purchases an illegal jammer to prevent students from disrupting classes using their cell phones

Background

- Definitions (Cont'd)
  - Notes

    (c) Interference can be produced by radiation, conduction and induction

    (d) Need to distinguish between interference resolution and enforcement

    (e) Related to (c) and (d) above, need to discuss where Commission involvement should start and stop (e.g., in terms of RFI and co-site interference situations)

Background

- Traditional System Architectures and Characteristics
  - High power/high antenna sites
  - Large coverage areas
  - Noise limited
  - Predominantly analog
  - Single or limited waveforms (in a given service or band)
  - “Permanent” or longer term channel assignments (static vs dynamic spectrum access)
  - “Dumb” end user devices

Background

- Traditional Enforcement Tools
  - Call signs and related identifiers
  - Station licenses
  - Operator licenses
  - Technician licensing
  - Equipment type approval/type acceptance
  - Equipment labeling
  - Monitoring and inspections
  - Educational efforts/outreach/advisories
  - Self-enforcement

Background

- Traditional Resolution/Enforcement Steps
  - Detect interference
  - Locate interference source(s)
  - Indentify interference source(s)
  - Voluntary/facilitated interference resolution
  - Formal enforcement action

Evolving System Architectures and Characteristics

- Evolving System Architectures and Characteristics
  - Low power/low antenna sites
  - Small coverage area from individual sites
  - Interference limited
  - Predominantly digital, often broadband, noise-like
  - Multiple waveforms (in a given service or band)
  - Dynamic (versus static) spectrum access
  - “Smart” end user devices

Risks/Challenges Associated with Evolving Technology

- Examples
  - Despite intelligence at the edge or in the end user device, centralized control and timing (GPS) produce risks
  - Likewise, increased ability to build and deploy sophisticated jamming equipment (SDR/RF Amps) produce risks
  - More noise-like broadband signals make it harder to detect, decipher, identify, locate and isolate interference sources

Risks/Challenges Associated with Evolving Technology

- Examples (Cont'd)
  - With millions of devices in close proximity, aggregate interference from multiple sources may increase the ambient noise floor
  - Proliferation of devices producing unintended radiation in close proximity to communications systems/devices may also increase the ambient noise floor
  - Deployment of systems/equipment by minimally trained technicians in lieu of professional installation

Adequacy of Traditional Enforcement Tools/Processes

- Example Questions
  - Are the FCC's fixed and mobile spectrum monitoring resources adequate to deal with the evolving technologies described earlier?
  - To minimize the prospects of interference caused by improperly deployed systems/ equipment, should the FCC strengthen its role in ensuring professionalism in such deployments? Should there be more uniformity in the definition of "professional installation" across bands/services

Adequacy of Traditional Enforcement Tools/Processes

- Example Questions (Cont'd)
  - Given the proliferation of devices and other technological developments described earlier, should more emphasis be placed on electronically identifying and labeling the manufacturers, installers, owners/operators of devices and should there be more uniformity in such across bands/services?

Opportunities for Changes in Enforcement Paradigms

- Examples
  - Given the proliferation of "intelligent" end user devices (or the potential for a selected number of specially enhanced devices), can they be used in a crowd sourcing type of arrangement to assist in detecting, indentifying and locating malfunctioning devices or devices being used for the deliberate jamming or spoofing of critical systems?

Opportunities for Changes in Enforcement Paradigms

- Examples (Cont'd)
  - Similarly, given the "intelligence" (including storage capacity) in such end user devices, can they be used to make routine measurements of interference and noise in order to provide information that can be used to "calibrate" propagation models that are, for instance, used to establish exclusion zones or detect potential interference limit violations?

Opportunities for Changes in Enforcement Paradigms

- Examples (Cont'd)
  - Given the capabilities of end user devices, it has been suggested that they could be used to record on a loop basis, information on system/device performance and the interference/noise environment in order to later identify the cause and source of any harmful interference (i.e., forensic analyses); what are the advantages and disadvantages of having such a "black box" capability?

Opportunities for Changes in Enforcement Paradigms

- Examples (Cont'd)
  - If regular end user devices (or specially enhanced devices) are used to detect, identify and locate a malfunctioning or jamming/ spoofing device causing harmful interference, how is the information best conveyed to the SAS data base operator and the FCC so that a decision can be made as to whether or not to disable the offending device? How should the threshold for deciding to deactivate the device be established?

Private Sector Role in Enforcement

- Questions
  - Given the changes in technology outlined herein, what should the role of the private sector actors (such as traditional frequency coordinators, antenna site owners, and commercial vendors as well as the network operators themselves) be in resolving interference issues both intra-service and inter-service?

Proposed Deliverables

- June TAC Meeting
  - Deliver a presentation providing background on enforcement and identifying issues that will be subsequently addressed
- September TAC Meeting
  - Deliver preliminary recommendations regarding interference resolution (“de-confliction”) and enforcement programs and strategies
- December TAC Meeting
  - Deliver draft of final report with specific recommendations regarding new or revised enforcement strategies

Contact Information

Dale N. Hatfield
Senior Fellow
Silicon Flatirons Center for Law, Technology, and Entrepreneurship
Adjunct Professor
Interdisciplinary Telecommunications Program
University of Colorado at Boulder
401 UCB - Office 481A Wolf Law Building
Boulder, CO 80309
Office: +1 303 492 6648
Email: dale.hatfield@colorado.edu or dale.hatfield@ieee.org