WSRD Workshop VIII
Wireless Spectrum Sharing:
Enforcement Frameworks, Technology and R&D
May 5, 2016

Workshop Structure & Guidance

Workshop Goals:

- Outline the wireless spectrum sharing enforcement needs, scenarios and issues for the short-term and long-term, from multiple perspectives.
- Discuss the architectural, economic, regulatory and business frameworks that can deliver enforcement solutions.
- Identify innovative tools, techniques and database requirements for additional research.
- Develop ideas for advanced R&D to help inform WSRD recommendations to OSTP.

Framing the Day

This session will present a tutorial on the terminologies, current practices and one or two proposed enforcement frameworks to stimulate further exploration of enforcement in spectrum sharing. Key enforcement related ideas to be discussed include:

1. Compliance (ex ante): Rule definitions and certification;

2. Monitoring: observation and detection;

3. Adjudication: deciding whether an observation proves culpable interference; and,

4. Compliance (ex post): Remediation and/or punishment.

Session #1 (Panel): Enforcement Needs, Concerns, and Issues

This session will feature an interactive panel to help identify topics that will be addressed in more detail in the subsequent workshop sessions. Included in this discussion is a consideration of the practical as well as the more abstract issues involved in the enforcement of spectrum sharing agreements. With the continuation of existing sharing situations along with the emergence of new sharing scenarios, there may be a divergence between the near term needs, issues, and challenges and those in the long term. Panelists will address:

- How important is enforcement to spectrum sharing? What are the interpretations for enforcement?
- What compliance (*ex ante*, pre-deployment) mechanisms are needed? Can *ex ante* mechanisms reduce the need for compliance (*ex post)* mechanisms?
- What are the sharing scenarios, both traditional and new that challenge existing enforcement regimes.
- What are the enforcement needs for near-term efforts? Long-term exploration?

- What the enforcement perspectives and expectations from the government and industry for spectrum sharing?
- What are the tradeoffs between implementing successful enforcement mechanisms and user privacy?
- Are there legislative or regulatory changes needed to implement successful spectrum sharing enforcement?
- What specific R&D deliberations at the workshop will be useful?

Session #2 (Breakouts): Enforcement Scenarios, Architectures, and Responsibilities

Much remains to be learned about how to build a dependable environment for existing and new spectrum sharing scenarios. For example, new spectrum sharing scenarios will require a dependable sharing environment. Dependability means, among other things, that rights are enforced appropriately. Protection of rights includes protection from harmful interference, but in the broader sense addresses more than that. For example, it remains to be determined how principles of enforcement would apply to database driven mediation systems (such as SASs).

This session will separate the participants into three (3) groups to consider the needs and issues identified during Session #1. Each group will be tasked to approach their questions from three different perspectives. A summary session will follow to compare the outputs from the different groups: Are there common priorities and actions across the three perspectives? If not, why not? Hopefully, approaching the topic from different perspectives will reveal the most challenging issues and research needs.

Group 2A: Enforcement Scenarios

This group will approach the session's goal and questions through further refinement of the key sharing scenarios and the associated needs for enforcement within those scenarios. The group may wish to refine the scenarios and the associated enforcement needs using different dimensions such as users from different domains (e.g., federal and non-federal), different forms of systems (e.g., radars, communications, terrestrial v. space, etc.) and different licensing regimes (e.g., licensed, unlicensed, licensed by rule). More focused questions for this group may include:

- How do scenarios define enforcement needs and features?
- Do different scenarios require different enforcement frameworks and mechanisms or are there common approaches?
- How is harmful interference distinguished from simple intrusion?
- How should harmful interference or intrusion from incidental radiators (e.g., switching power supplies) be handled as an enforcement matter in a shared spectrum environment?

Group 2B: Enforcement Architecture

This group will approach the session's goal and questions through outlining one or more enforcement architectures and associated systems or processes. The group may wish to explicitly identify key elements for an enforcement architecture including systems for certification, monitoring, adjudication, compliance and review. More focused questions for this group may include:

- What are the other end-to-end technology needs for enforcement that are critical for different stakeholders?

- What is the current architecture and what are the major gaps in view of rapid changing technology
- What kind of an architectural network is useful – standalone overlay networks, organic integration, disparate dissemination, device centric, network centric, user feedback based, others?
- What role do databases (e.g., license, tower, and equipment databases) serve for enforcement? Band access systems?
- How can cloud sourcing be used?
- Why and how automation be used?
- What monitoring systems, if any, are needed?

Group2C: Enforcement Roles & Responsibilities

This group will approach the session's goal and questions through defining roles and responsibilities of the different stakeholders and systems whether regulatory agency, incumbent operator, band access manager/system, end device user and system, or others. More focused questions for this group may include:

- What current enforcement responsibility mechanisms are in place? Where do these mechanisms fall short especially in view of the rapid technological changes that are occurring?
- What are the appropriate roles and responsibilities of government agencies and the private sector in developing and managing automated enforcement systems?
- What technology toolsets are needed for the regulatory agencies?
- What role should "third party" systems (e.g., databases, access systems) play?
- Are "victim" systems responsible for identifying and reporting harmful interference?
- What mechanisms need to be put in place to provide an ability to audit systems?
- What data must be available to ensure an audit provides useful information?
- Who should be responsible for audits?
- How do differences between and among civil, criminal and administrative roles affect enforcement?
- What economic factors affect enforcement? Who will pay for any required interference monitoring systems?

Session #3: (Moderated Discussion) Innovative Architectures, Tools, and Techniques

Research and development will play an important role in enabling increased use and sharing of the spectrum. Recognizing the goal of the workshop, "identify innovative tools, techniques and database requirements for additional research," this session will explore what R&D can address for enforcement and identify key R&D actions. As an example technology area, it is widely anticipated that more intense sharing of spectrum will result in an increase in enforceable events, many of which may be of short duration. Thus, it would be worth exploring the appropriate automation of enforcement functions and what research and development is needed for such automation. Many issues may be addressed by technology development including:

- What R&D is needed to developing technology for monitoring and adjudication of interference?
- What, if any, new functionality must be incorporated into equipment to ensure successful spectrum sharing and enforcement?

- Does automation help? What can be automated?
- What technology R&D needed for auditing systems? What safeguards need to be put in place to ensure that national security requirements are not compromised?
- What enforcement technologies can be implemented short-term? What additional measures can be taken over a long-term?
- How is the concept of jamming evolving in the era of agile and software-defined radios, and what are the implications for enforcement?
- Similarly, how is the threat of spoofing evolving in an era of frequency agility and software-defined radios and what are the implications for detection and remediation?
- Can technology help resolve differences between and among civil, criminal and administrative roles for enforcement?
- How should technology be used to walk the fine line between privacy and enforcement?

Session #4: (Moderated Discussion) Transitioning to the Future

As with previous WSRD workshops, this one will undoubtedly identify a long list of challenges, opportunities, and candidate actions. This session will explore the topics discussed during the day, identify priorities, define key R&D needs, and consider how policymakers and research funders might reason about future possibilities. The outputs, as defined and prioritized during this closing session, will help inform WSRD recommendations to the OSTP and will be available for regulatory agencies and the overall community to consider and to use for inspiration and action.