# The Biggest Challenges Facing Enforcement

**Remarks of John Chapin**
**Presented at the panel on**
**The Use Of Technology to Improve Enforcement**
**During the Silicon Flatirons Workshop on**
**Next Generation Interference Resolution and Enforcement**
**15 September 2016**

**Feedback and discussion are encouraged.**
**The author may be reached by email: jchapin@cmu.edu**

Preface: We must distinguish enforcement by regulator vs enforcement among parties to a contractual agreement. This discussion focuses on enforcement by regulator

Summary of the 4 biggest challenges in one sentence:
Enforcement needs to become cheaper, more effective, and faster while preserving key freedoms.

## Challenge 1: Make enforcement cheaper so it can be more pervasive, without breaking the federal budget.

We observe the **Increased Role of RF devices** in all aspects of our lives. This drives the need for more pervasive enforcement in two ways.

1. Interference is increasingly harmful and/or costly
   ➜ **reliable mitigation** is increasingly important
   Example, Safety-critical communications:
   Used to be limited user base (public safety, aircraft, ships)
   or locations (medical equip in hospitals)
   Now becoming a broad user base and all locations:
   autonomous vehicles, body-worn medical devices

2. Spectrum demand is increasing ➜ **more spectrum sharing**
   a. increased opportunity for interference
   b. more complex spectrum access methods
      i. more likelihood of design error in the access method
      ii. more complex devices

1. more likelihood of implementation error
2. cost of certification test grows to the point that it stifles innovation ➜ increase reliance on enforcement to reduce required ex ante confidence level

Can't afford to do even as much enforcement as we need today, so how are we going to make it more pervasive? Need to find ways to make it much cheaper. This is big challenge #1.

# Challenge 2: Make enforcement more effective despite new technologies that make it harder.
# Challenge 3: Make enforcement much faster than it is today.

Unpack these challenges using the OODA loop formalism

**Observe - Collect data about the world**
Tech trend towards short range low power dense networks ➜ more difficult to observe transmissions from a distance ➜ more expensive to monitor.
Tech trend towards MIMO, Directional antennas ➜ cannot observe all nearby transmitters from a single spot.

**Orient - Understand what the data means**
The orient stage has two parts.

1. Determine which device/network the transmission came from.
   Tech trend towards flexible operation (changing frequencies and waveforms) ➜ can't look in a static database to map a signal back to a system
   Tech trend towards bursty spectrum use
   Tech trend towards noise-like waveforms

2. Attribute responsibility to an organization or individual.
   Analogy:
   You all own a PC or a laptop.
   How many of you are willing to take full legal responsibility for every transmission your computer makes on the internet?
   If it's not you, then who is responsible?

Specific cases of interest for the challenge of attibuting responsibility.

- vendor makes it too easy for end user to misconfigure the device (this has been a major ause of interference by 5 GHz Dynamic Frequency Selection WiFi devices)

- operator fails to upgrade device with OS provided by software vendor, and the security breach is exploited by attackers (android upgrade problem)
- a 3rd party Spectrum Access System is involved (upcoming 3.5 GHz band)
- one piece of radio equipment is virtualized and shared by multiple operators (expected in future Internet Of Things networks to reduce infrastructure costs)

**Decide - Select course of action**
**Act - Implement the decision**
Multiple steps involved in Decide&Act for interference mitigation

1. Determine whether harmful interference occurred
2. Determine whether there are protected rights
3. Determine who needs to change their behavior how much
4. Cause that entity to change their behavior as required.

Today decide&act is a case-by-case human-centric process:
the FCC enforcement bureau representative on the spot
the FCC administrative process
(eventually) a legal process.
Use of automation to speed this process up, while still protecting due process, is a major challenge.

Decide&Act is particularly difficult in some cases:

- Aggregate interference
- Political issues intervene (e.g. garage door problems)
- All parties involved are operating within the rules (e.g. T-Mobile / Sirius XM, Nextel / public safety)

# Challenge 4: Improve enforcement to overcome challenges 1-3 without losing key freedoms of our current system

Reminder of the overall challenge statement:
Enforcement needs to become cheaper, more effective, and faster while preserving key freedoms.

Preserve (& increase!) collaborative problem resolution
risk: regulator gets involved and people stop being good neighbors or trustworthy counterparties

Preserve privacy

risk: enforcement methods that result in pervasive collection of information about user behavior

Preserve permissionless innovation

risk: enforcement methods that require systems to use or avoid specific signals or behaviors

Preserve freedom from political meddling

risk: selective enforcement when resources and systems unable to keep up with demand

## Note: These freedoms are also at risk if we don't improve the way we do enforcement

In a world of greatly increased spectrum sharing, the alternative to pervasive, effective, fast enforcement is fine-grained regulatory control of spectrum access.

- A universal "prior restraint" regime at the second-by-second level
- Prior restraint harms freedoms in the first amendment context
- It would harm freedoms in spectrum management as well, for largely the same reasons.