Silicon Flatirons

KNOW WHAT'S NEXT.

Dale N. Hatfield – Opening Remarks
Spectrum Conference:
Next Generation Interference Resolution and Enforcement
Thursday, September 15, 2016

Dale N. Hatfield – Opening Remarks
Spectrum: Next Generation Interference Resolution and Enforcement
A Silicon Flatirons conference, Thursday, September 15, 2016

- Thank you Pierre and let me add my own welcome to you all of you
- What I would like to do in the next few minutes is provide some context for the balance of the conference and highlight a few of my own <u>personal</u> concerns (which may not reflect the view of institutions with which I am affiliated)

- At the highest level, I regard the FCC as having two fundamental or foundational roles – one of which is the management and protection of the radio spectrum environment upon which all of us are increasingly dependent
- Said another way for emphasis, management and protection of the radio spectrum environment is not some small, obscure part of the agency's responsibilities, it is the guts of it
- Stepping down one level from that highest level, managing the spectrum environment consists of four basic activities:
    - Allocating spectrum for various uses such as radio or television broadcasting, cellular radio, or military radar
    - Establishing technical and service rules to govern the use of the spectrum
    - Distributing the rights to operate within an allocation to particular individuals or entities (sometimes referred to as the assignment step) and, fourth and finally,
    - Enforcing the technical and service rules established in the second step – of course many of those rules are aimed at controlling interference
- Too often, in my opinion, the critical importance of the interference resolution and enforcement step in managing the spectrum environment is underappreciated or, worse yet, overlooked; and so is the failure to fully appreciate its rapidly changing nature

- Just as failing to enforce speed limits in a school zone endangers children, failing to enforce spectrum rules endangers not only services that are critical to the Nation's economic and social wellbeing, but to public safety, homeland security and national defense

- Having provided that background, let me proceed by laying out a series of hypotheses that I believe are true but need to be scrutinized by experts in fora such as this conference and then, as I indicated before, touching on two threats that I find particularly troubling

- My *first* hypothesis or premise is that United States is experiencing explosive growth in wireless devices and systems that must successfully operate not only in increasingly close proximity to one another in the frequency, space and time dimensions but also to other electrical and electronic devices that unintentionally or incidentally emit (or are susceptible to) electromagnetic radiation; this increased densification of often disparate devices and systems increases the risk of disruptive and harmful interference.
- *Second*, many of the technological changes being made in radio systems to capture increased spectral efficiencies and generate additional spectrum capacity present challenges to traditional systems and techniques used to detect, identify, locate, mitigate, report and, where necessary, prosecute those responsible for causing harmful interference (example DSA); moreover the underlying technological developments can enable deliberate, malicious and potentially widely disruptive attacks on the Nation's critical infrastructure – a point I will return to in a few moments
- *Third*, while these technological developments present spectrum measurement, direction finding and other enforcement related challenges, these same (and related) technological developments hold the promise of increasing the efficiency and efficacy of interference resolution and

enforcement activities, especially when combined with notions such as crowd sourcing and the big data paradigm (parenthetical comment)

- *Fourth*, budgetary constraints on public entities and cost minimization pressures on commercial entities suggests the need for new models of public – private cooperation in interference resolution and enforcement to avoid unnecessary duplication of facilities and functions and to speed up responses to serious interference incidents; those same budgetary pressures also suggest the importance of carefully balancing ex ante and ex post enforcement activities (example)

- In the few minutes I have remaining and in an attempt to be as provocative as I can within that time, I am going to focus my attention on one relatively narrow area of enforcement broadly defined – jamming and spoofing:
    - Jamming refers to intentionally sending a signal that disrupts the operation of a receiving device
    - Spoofing refers to intentionally sending a fake signal meant to masquerade as an actual or legitimate signal
- Within that relatively narrow area, I am going to focus on malicious jamming and spoofing where the intent is disrupt authorized wireless communications for nefarious purposes; it is perhaps obvious, but wireless systems inherently have a degree of openness or and hence vulnerability – otherwise they wouldn't work
- Malicious jamming and spoofing exploit that inherent openness
- Technically, jamming is pretty easy to understand but spoofing is more subtle; in brute force jamming you just send an interfering signal that is more powerful and hence obscures the desired signal
- For example,
    - A fake GPS signal could lead a navigation device in a vehicle to think that it is one place when it is really at another with potentially disastrous results;
    - A fake telemetry signal could be used to tell a valve in a flood control system to open when it should really be closed – again with potentially disastrous results

    - A fake command and control signal could be used to divert the drone-delivered pizza you ordered and have it sent instead to the smart young hacker down the street – just kidding
- Spoofing is particularly pernicious because, unlike jamming, the signal looks and acts like a normal, legitimate signal so you don't sense its effects (example – navigation)
- Especially concerning would be the use of spamming and/or spoofing by really bad guys such as non-state actors who actively seek to inflict harm, perhaps in conjunction with other activities aimed at major transportation hubs or large public gatherings

- Continuing in my role as provocateur, I will provide a laundry list of developments that I believe increases the risk of intentional jamming both malicious and non-malicious
    - 1. Widespread adoption of Software Defined Radio technology based upon low cost hardware platforms and open source software libraries that facilitate the creation of sophisticated jammers and spoofers
    - 2. A rapidly increasing pool of people – both professional and amateur/hobbyists who are proficient in the creation of such devices SDRs (anecdote here at CU)
    - 3. The falling costs of such devices due to low cost hardware platforms I mentioned, widening availability of reusable software and a reduction in the associated programming skills necessary to create the devices (1-3 a perfect storm)
    - 4. Forgive me for being a little more technical for a moment, but another development that is changing the risk is the trend toward separating the control plane in a network from content or data plane as in Software Defined Networking; the command and control plane or subnetwork is the nervous system of a network; while the change has many operational and economic benefits, it creates a particularly critical attack surface
    - 5. Related to all of the preceding developments is the progress being made in the direction of protocol aware jamming which allows the

jamming signal to be sent not continuously but at particularly critical moments when the desired signal is most vulnerable; this can significantly reduce the amount of transmitting power needed to produce a disruption and make jamming harder to locate from a distance

- 6. Deploying defenses against deliberate jamming and spoofing attacks are certainly possible but outside the national defense and homeland security arena, they may conflict with the desire – indeed the necessity – of producing, for example, low cost IoT devices and systems
- 7. Is the scaling back of spectrum enforcement activities at the FCC – particularly in terms of reducing field activities; this is a sensitive area but I have a strong personal belief that the long term erosion of field resources has the potential to wear away the nation's ability to both prevent (ex ante) and adequately respond to (ex post) the kinds of jamming and spoofing attacks I just described

- I will stop there and just say that I am looking forward the remainder of the conference and learning more about these and other issues from the incredible group of experts that we have assembled here this afternoon.