Silicon Flatirons
A Center for Law, Technology, and Entrepreneurship at the University of Colorado

*Roundtable Series on Entrepreneurship, Innovation,
and Public Policy*[*]

New Times, New Methods: Upgrading Spectrum Enforcement

Laura Littman and Brad Revare[†]

February 2014

COLORADO LAW
UNIVERSITY OF COLORADO BOULDER

[*] The Silicon Flatirons Roundtable Series on Entrepreneurship, Innovation, and Public Policy is sponsored by Brad Feld, Managing Director of the Foundry Group. This is the 34th Flatirons Report. More Reports – on topics including private equity, internet governance, cloud computing, angel investing, and modern pedagogy – can be found at http://www.siliconflatirons.com/publications.php?id=report. Roundtable and Summit discussions further the Silicon Flatiron Center's goal of elevating the debate around technology policy issues

[†] Laura Littman is a Research Fellow at Silicon Flatirons and Brad Revare is a 2015 J.D. Candidate at the University of Colorado Law School

Highlights

- The group came to a rough consensus that the Federal Communications Commission (FCC) Enforcement Bureau is under resourced to adequately address radio spectrum issues, more resources must be committed to interference enforcement, and better distinctions need to be made about jurisdiction.
- Participants agreed that there must be a greater role of private actors in enforcement; however, it still remains unclear what that role should be.
- Participants highlighted the importance of transparency and monitoring, specifically asking what information is available, how that information is being used, and how to better collect data about interference events and organize it in a usable way.
- Participants agreed that spectrum interference has become more complicated and that there is a need for a taxonomy of spectrum interference to guide the development of regulation.

1. Introduction

The increasingly complex radio spectrum environment is changing the sources and nature of interference threats to an increasingly important resource. At the same time, new and evolving technologies and processes hold great promise for mitigating these threats to the critical spectrum resource and the systems that rely on it.

On November 14, 2013, the Silicon Flatirons Center convened a group of about two-dozen spectrum experts with a wide variety of backgrounds and expertise (list of participants in Appendix A). This group considered the threats and potential solutions for improved spectrum enforcement and developed associated findings and framed recommendations for the Federal Communications Commission (FCC), the National Telecommunications and Information Administration (NTIA), the White House, Congress, and other policymaking groups.

A webpage with links to resources prepared for the meeting is available at: http://www.siliconflatirons.com/initiatives.php?id=SpectrumEnforce. Resources include a reading list and an agenda for the discussion. After the roundtable, the Silicon Flatirons hosted the conference, *Radio Spectrum Pollution: Facing the Challenge of a Threatened Resource*—a report from the conference is available on the conference webpage at: http://www.silicon-flatirons.org/events.php?id=1365.

1.1. Goals

The aim of the roundtable was to use the collective expertise of participants to map the changing technical, economic, and legal/regulatory landscape in spectrum management and to explore new or revised approaches to interference detection, identification, location, mitigation, and enforcement. Additionally, the conference participants provided guidance and recommendations about governmental and private sector activities to reform, as necessary, the enforcement of spectrum rights and obligations.

1.2. Context

The U.S. is experiencing expansive growth in wireless communications devices and systems. Both must successfully operate not only in close proximity to one another in frequency, space, and time but also in the presence of other electrical and electronic devices that unintentionally emit or are susceptible to electromagnetic waves. Moreover, because of this growth and the limits on usable frequencies, there is increased emphasis on sharing spectrum among often disparate users on a dynamic rather than static basis. Dynamic sharing coupled with the increased mobility of end user wireless devices increases the risk of interference that is more intermittent and difficult to identify and locate. This presents new challenges in institutional relationships and interagency processes for detecting, identifying, locating, reporting, and mitigating unintentional and intentional interference or jamming.

The value of spectrum allocations—especially dynamically shared spectrum ones—to commercial entities depends on the processes and resources spectrum managers have available to reduce the incidence of harmful interference and to resolve it quickly and effectively when it does arise. Similarly, the willingness of federal government agencies to share larger amounts of spectrum in more dynamic ways with non-government actors (and vice versa) depends on their confidence that the applicable rules and regulations regarding such sharing will be enforced so that the impact of disruptive or harmful interference is reduced to acceptable levels.

In the past, the FCC has used a plethora of both longer-term techniques (such as system, operator, and technician licensing and equipment authorization) and shorter-term techniques (such as advisories, field investigations, and enforcement actions) to reduce the number of interference conflicts and to resolve them when they arose. However, today's wireless systems and devices are increasingly capable of:

- Operating with virtually unlimited numbers of waveforms (i.e. types of signals);
- Utilizing more dynamic rather than more static channel assignment methods;
- Taking advantage of software defined radio and related techniques to operate across multiple bands;
- Making concurrent use of overlaid macro-, micro-, and pico-cell architectures (so called HetNets); and
- Producing more "noise-like" broadband digital signals that are often harder to detect, decipher, identify, and locate at a distance.

Moreover, today's transmitting/receiving systems could potentially be installed and configured by individuals with little or no technical training, working for entities that are not held responsible for doing a job correctly. Finally, the wider availability of low cost, very small, intelligent transmitting devices increases the interference threat from “pirate radio” operators and from the intentional jamming of services critical to the safety of life and property.

On a brighter note, these increasingly intelligent, flexible, and often networked devices and systems have a greater potential to detect, identify, locate, report on, and mitigate interference that they encounter. Such information could be used to facilitate informal interference mitigation steps or as evidence in formal enforcement actions. For example:

- Radios with the types of capabilities listed above can change their mode of operation (e.g., the waveform that they are employing) or the channel or band on which they are operating to avoid interference (or to mitigate interference that they may be producing in another device or system).
- Radios with increased sensing, processing power, and data storage capabilities (i.e., distributed intelligence) can use that power in “real time” to contribute locally gathered information to a central controller to resolve severe interference cases associated with the safety of life and property.
- On a longer-term basis, the locally-gathered information, with appropriate privacy protection, can be used forensically to troubleshoot interference events after the fact and, more routinely, to “calibrate” propagation models used to predict coverage and establish exclusion zones.

1.3. Report Content

In order to foster debate, statements made during the roundtable are not attributed to participants in this report, though a list of attendees is provided in Appendix A. Participants were invited to speak as individuals and to express views that may not be those of their organizations. Facts or opinions that are reported are those of individual participants and unless otherwise noted, they are not consensus positions.

This report is organized around the themes that emerged from the discussion and proceeds as follows: Part 2 examines the FCC’s enforcement capabilities, Part 3 suggests an increased role for private actors in enforcement, Part 4 explores the possibility of interference mitigation through transparency and monitoring, Part 5 offers a categorization of interference and identifies key interference issues today, and Part 6 concludes.

2. FCC enforcement capabilities and the role of private actors in enforcement

The roundtable participants discussed the FCC’s enforcement capabilities and the role of private actors in enforcement, highlighting three main points (1) the need for clear interference mitigation rules, (2) The FCC’s enforcement capabilities in spectrum interference, (3) the role of radio frequency device certification, (4) the lack of resources for effective enforcement, and (5) issues in interference enforcement litigation.

2.1. The need for clear interference mitigation rules

The discussion of regulatory schemes began with a presentation highlighting the importance of a clear enforcement framework. Successful enforcement requires clear rules and standards for emitting parties. Enforceable rules require knowledge of law and engineering. Whether it is a statutory provision that prohibits someone from operating under Section 301 of the Act,[1] Part 15 rules,[2] or any other rule, there must be clear requirements. An example of an unclear requirement (here, a statutory provision) is that common carriers cannot engage in unreasonable and unjust practices. The requirement is unclear without case law—and even with case law, the definition of "unreasonable and unjust practices" is debatable.

Even sophisticated consumers get confused about emission standards, contributing to the increasing problem of spectrum interference. For example, today, there are approximately 40 emission standards for digital and GPS devices.[3] Likewise, many operators do not fully understand what emission designators represent,[4] making it difficult for them to comply with rules and expectations. As new and emerging technologies and products continue to be introduced in the marketplace, operator/consumer confusion will continue to grow as well.

A common problem identified was that no useful definition of harmful interference exists. Further, while the group agreed that defining harmful interference is difficult, there was disagreement about whether harmful interference should be defined. Many participants said that the inability to define harmful interference makes enforcement of interference extremely difficult; and thus, the industry needs to come up with a definition. Specifically, one participant said that since "the key to having good enforcement is to have very clear rules," the "you know it when you see it" definition of harmful interference is not sufficient to support effective enforcement. On the other hand, other participants argued that there will never be an appropriate definition of harmful interference because of the complexity and every-changing nature of the industry. For example, one participant noted that the FCC often focuses its limited spectrum enforcement resources on public safety, so when faced with non-public safety related interference, the FCC might find the source and prompt voluntary resolution by the operator, but it often will not go as far as saying the interference is harmful or issue fines and forfeitures for interference. Rather, the FCC's forfeitures in cases involving alleged interference tend to be based on violations of clear and specific technical rules.

[1] License for radio communication or transmission of energy, 47 U.S.C. § 301, *available at* http://www.law.cornell.edu/uscode/text/47/301.

[2] Radio Frequency Devices, 47 C.F.R. § 15, *available at* http://www.law.cornell.edu/cfr/text/47/part-15.

[3] *See* Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Transmission Systems, Report and Order FCC 02-48 60-77 (2002), http://transition.fcc.gov/Bureaus/Engineering_Technology/Orders/2002/fcc02048.pdf.

[4] Emission Designator, Wikipedia, http://wiki.radioreference.com/index.php/Emission_Designator (last visited January 31, 2014).

Defining harmful interference is a recurring issue in the industry[5] and could be the topic of a whole other roundtable meeting or conference. For this reason, the participants were instructed not to focus on the definition of harmful interference but to focus on the enforcement issues.

Finally, adding to the difficulty of making clear rules is the fact that technology is evolving rapidly and rules promulgated fifteen to twenty years ago may no longer be relevant or cannot be interpreted. For example, we are now using some bands that are of much higher frequencies and the propagation is fundamentally different than in the lower bands in use when the rules were adopted—hence, the rationale is lost.

2.2. The FCC's enforcement capabilities in spectrum interference

One participant provided a background on the FCC's enforcement capabilities in spectrum interference. The participant explained that the FCC's enforcement capabilities include issuing warnings (citations and notices of violations) and, more commonly, instigating monetary forfeiture proceedings (punishment is used to both remedy harms and to deter others from acting unlawfully). Further, if the actor does not pay the fine, the case is given to the Department of Justice (DOJ) in a long, elaborate process. However, the FCC has the ability to enforce harsh punishments for violations. For example, the FCC can issue cease and desist orders (but it must do so in administrative law proceedings). The participant pointed out that the FCC has the ability to seize illegal equipment (using US marshals) and obtain court injunctions (through the DOJ).[6]

One participant said that unless the FCC provides "good old fashioned enforcement, businesses are compelled to cheat or get right up to the line of the rules." The participant explained that new entrants in wireless are adjacent neighbors or are sharing spectrum with current wireless users, and their goal is to produce a profit. If these players can push the edge of what is legal and not get caught, then that behavior gets "enshrined" in everyday practice. Thus, the only way to stop some interference is by FCC boots-on-the-ground enforcement.

[5] *See* Clarifying Harmful Interference Will Facilitate Wireless Innovation, White Paper, IEEE-USA's Committee on Communications Policy (July 31, 2012), http://www.ieeeusa.org/policy/whitepapers/IEEEUSAWP-HarmfulInterference0712.pdf (The FCC and NTIA have six sub issues to clarify about harmful interference).

[6] "FCC's enforcement efforts are generally accomplished through an administrative process whereby FCC first issues citations against entities not otherwise regulated by FCC for violations of laws it enforces. For subsequent violations by such entities, or for initial violations by FCC regulated entities (such as common carriers, broadcasters, or other licensees), FCC may impose a civil penalty through forfeiture proceedings or take additional enforcement actions that include, for example, cease and desist proceedings, injunctions, and revocation of common carrier license operating authority for violations of the requirements of the national registry. Enforcement of a forfeiture order is done in federal court through the Department of Justice, which handles violations of statutes that FCC enforces." Telemarketing: Implementation of the National Do-Not-Call Registry, U.S. GEN. ACCOUNTING OFFICE, GAO-05-113, at 16 (2005), *available at* http://books.google.com/books?id=dnBlbdAW7pEC&pg=PA16&lpg=PA16&dq=fcc+court+injunction+through+the+doj&source=bl&ots=lDFwLrmsBG&sig=DP_qo0megkXO6r4PF_PWVIgxIS4&hl=en&sa=X&ei=CaXAUuzhJ8f4yAHs-YHACw&ved=0CCsQ6AEwAA#v=onepage&q=doj&f=false.

Another participant proposed that if more boots-on-the-ground enforcement is the solution, there simply needs to be more financial support. Accordingly, that participant suggested that all licensed spectrum holders should pay a tax to the FCC enforcement department, and that the enforcement department should use the additional revenue to invest in collecting maps of interference and then make and enforce its rules based on the findings from those maps.

Finally, another participant analogized spectrum enforcement to traffic enforcement. The participant explained that in the beginning there were speedometers in cars to inform drivers of their speed and tracking motorcycles used for enforcement. Next, enforcers introduced radar guns (but, the participant pointed out, there were jammers, and the participant asked whether this meant that there should never have been radar guns—and answered, probably not). The participant noted that more recently, technology for enforcement and monitoring has evolved, including red light photo tickets, insurance companies installing monitoring devices in cars, and flashing signs on the road that inform a driver that he or she is going too fast. The participant analogized that in spectrum enforcement, we are in the stage of introducing speedometers and radar guns. Importantly, the participant urged that we must ask whether we are being most efficient and using technology to do the "easy tasks" and using people for the "hard stuff."

2.3. The role of radio frequency device certification

Certification of devices is critical to effectively mitigate interference.[7] However, one participant pointed out that there is a gap between certification and how products are used. The participant explained that when certifications are made, the FCC uses a clear legal framework, but the equipment is often deployed several years later for different uses and the certifications become outdated. Thus, the problem is that the FCC is unable to move quickly enough on certification of devices.

One participant highlighted the importance of the relationship between the Office of Engineering and Technology (OET) and its lab. Specifically, when working with innovative radios and other products, the participants said that devices must be flexible so they do not run afoul of the rules. Thus, if someone else takes advantage of the same knowledge database (KDB),[8] the device can be applied in different contexts in an enforcement action. Accordingly, there is a tension between not wanting to discourage the flexibility of OET uses and a need for clear rules.

Importantly, one participant pointed out that certified devices can cause interference and an operator of a certified device that causes interference can be fined for

[7] *See* Commissioner Susan Ness, Re: Amendment of Pars 2, 15, 18 and Other Parts of the Commission's Rules to Simplify and Streamline Frequency Equipment, FCC (April 2, 1998), http://transition.fcc.gov/Speeches/Ness/States/stsn810.html; Unlicensed RF Devices, FCC Part-15 Rules, *available at* http://www.arrl.org/part-15-radio-frequency-devices#FCC.

[8] Reference to the FCC Knowledge Database, https://apps.fcc.gov/oetcf/kdb/index.cfm, which "publishes equipment authorization procedures and measurement guidance in the form of FCC Public Notices and Knowledge Database (KDB) publications."

causing interference. Similarly, another participant explained that there can be post-certification and post-manufacturing issues that cause interference. If there are post-certification or post-manufacturing issues that cause interference, the device will not be compliant although the manufacturer or user may not be aware that the device is not compliant. Thus, the question arises about what is the most effective time period for enforcement—*ex ante* or *ex post*? Given that FCC enforcement teams are shrinking, *ex post* may be a more viable option. Further, one participant stressed that the question remains, who are the cops?

2.4. Insufficient resources for effective enforcement

Most participants voiced that the FCC does not have sufficient resources for effective enforcement; thus, the FCC is not able to address the damage interference causes. One participant suggested that while the FCC Chairman and Commissioners focus on the big policy issues, the rulemaking is often done "deep in the bowels of the FCC," and there is very little review of those rules. Specifically, at the leadership level, less than half of the personnel are devoted to spectrum issues. Further, the number of personnel dedicated to spectrum enforcement is diminishing. The group agreed that these issues must be addressed.

The participant noted that at the Enforcement Bureau's peak, there were about 350 people working in enforcement; today, there are about 265 people[9]—about 100 of these workers work in the field and about 20 are in the spectrum enforcement division.[10] Instead of just enforcing rules related to spectrum interference, the participant said that FCC field resources are also focused on issues such as tower lighting and broadcast inspections, and only a portion of fieldwork focuses on interference-related issues. Finally, the participant observed that there does not appear to be political or budget support for hiring new spectrum enforcement staff to replace retiring staff. Likewise, another participant noted that there is a brain drain from the FCC just when "the FCC needs smart people to keep up with the innovations" in sophisticated technology that uses spectrum.

Because the FCC's spectrum enforcement division and the field team are so short-staffed, the question becomes whether the market will police itself. Particularly, will actors complain if they cannot get something through because of interference? One participant suggested that actors will police and complain if something does not get through, making auditing important (as opposed to non-routine application). Thus, the participant said that limited resources will be focused on actual problems. Accordingly, another participant suggested that with its limited resources, the FCC should assume an auditing role and leave the primary role of interference enforcement to a third party.

For example, one participant pointed out that the FCC has an active role in non-routine device certification issues. The participant said that if the FCC audits certification

[9] Fiscal Year 2014 Budget Estimates Submitted to Congress, FCC, at 6 (April 2013), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-320096A1.pdf.
[10] Id. at 8.

bodies for unusual patterns to review their effectiveness, the FCC's limited resources will be better utilized. However, it is a multi-part solution that also requires private bodies like Telecommunication Certification Bodies (TCBs)[11] that answer in the process quickly and are more reformed. Today, TCBs have a 90-day process for non-routine certifications because the FCC asks a lot of questions to the TCB, which is a very interactive process that slows everything down. In conclusion, the participant said that the focus should be on allowing the TCBs to do their job independently and quickly and the FCC's resources should focus on an auditing functionality rather than a permissive functionality.

2.5. Issues in interference enforcement litigation

Participants discussed issues in interference enforcement litigation. Some participants agreed that the current system lacks a process for adjudication and the entire field lacks available case law.

First, one participants asked who would be responsible for resolving interference disputes (FCC v. NTIA, federal government v. state government, courts v. administrative law judges)?

Next, participants posed the following questions: "Would a court refuse to hear a case determining the definition of harmful interference and refer it exclusively to the FCC?" "What would it take for a party to bring a case for harmful interference—a record of fighting a fine from the FCC?" "What are the due process requirements if a device is causing interference to the DoD?

One participant suggested that parties must bring cases involving individuals, such as the mom and pop stores using security cameras and LED lights that are causing interference. However, the participant recognized that this requires someone to stand up and bring the case, which is not likely. Thus, the participant suggested that perhaps an entity like a law school clinic could bring such a case.

Using Coase's theory of externalities, a participant observed that harm is reciprocal. Specifically, one actor's use is another actor's interference, raising the issue of rights—who has the right to continue to act? Another participant asked how a dispute where a LED light bulb interferes with a large wireless carrier's network should be resolved. That participant argued that there must be a mechanism for rights enforcement and there must be transparent definitions of spectrum rights for coordination. Further, a participant pointed out that when commercial parties are involved, outcomes will have significant economic impact. The participant asked, what should be done with organizational and due process concerns?

[11] "The Commission may designate a Telecommunications Certification Body (TCB) to approve equipment under the Certification procedure based on an application with all the specified information. The TCB shall process the application to determine whether the product meets the Commission's requirements and shall issue a written grant of equipment authorization. The grant shall identify the TCB and the source of authority for issuing it." Equipment Authorization, FCC, http://transition.fcc.gov/oet/ea/procedures.html#sec4 (last updated March 22, 2013).

3. Privatizing enforcement: a greater role for private actors

There was a rough consensus that there should be more privatization of enforcement. Participants agreed that the FCC should promulgate rules and have a part in enforcing rules, but there is also a role for third-party actors and industry organizations. The FCC has limited resources, and assuming most actors are incentivized to do the right thing, privatization provides more capable and efficient enforcement. Privatization could take the form of voluntary policing, where stakeholders resolve issues without taking them to the FCC. However, issues arise in three scenarios: (1) cooperation within privatization, (2) public institutional challenges after privatization, and (3) special issues in enforcement such as the importance of infrastructure and public safety.

Several participants expressed that privatization requires cooperation; once a player no longer cooperates, there may not be success in enforcing agreements between parties. An example is the complicated medical device agreements with airplane manufacturers—here, the private parties attempted to come to an agreement without FCC involvement.[12]

Additionally, another participant identified that because interference is hard to track in the digital and mobile environment, where social norms were once helpful in preventing interference, there are now institutional challenges in privatized enforcement. Although there was some hesitation, the group agreed that the FCC should encourage the private sector to play a greater role in enforcement and let another party administer a third party database. Specifically, one participant articulated that the government should promulgate and enforce rules; but there can be, and needs to be, a role for the private sector to help with enforcement.

Finally, one participant stressed that privatization of enforcement of interference mitigation must be done carefully. With privatization, the participant said, enforcement operations related to critical infrastructure and public safety must not be forgotten. Thus, a model incorporating privatization must still concentrate on the important areas of critical infrastructure[13] and public safety. Specifically, with interfering technologies increasing and in more places (from card readers to security cameras), there is and needs to continue to be cooperation from private citizens to promote infrastructure and public safety.

[12] Referring to the MBAN rulemaking in 2.3 GHz. *See* Neil Grace, FCC Dedicates Spectrum Enabling Medical Body Area Networks to Transform Patient Care, Lower Health Care Costs, and Spur Wireless Medical Innovation, FCC News, 202-418-0506 (May 24, 2012), http://www.fcc.gov/document/fcc-dedicates-spectrum-enabling-medical-body-area-networks, Medical Body Area Networks, First Report and Order, FCC 12-54 (May24, 2012), http://www.fcc.gov/document/medical-body-area-networks-first-report-and-order.

[13] The term "critical infrastructure" refers to infrastructure (often these days privately owned) that utilizes RF (often for control and monitoring and internal system communications) such as pipelines, railroads, and public transportation, water filtration and sewage systems, etc.– infrastructure that if it fails can have devastating public safety consequences. Some people may include wireless networks (cellular/PCS) in the list of critical infrastructure.

4. Interference mitigation through transparency and monitoring

Next, the discussion turned to the role of transparency and monitoring to improve interference mitigation through enforcement. First, the participants discussed information transparency as an incentive not to interfere. Second, the participants identified the utilization of bettering monitoring as a way to improve enforcement. Third, One participant suggested the solution of a third party RF emission data clearing house to alleviate interference problems.

4.1. Information transparency as an incentive to not interfere

Many participants highlighted the need for improved transparency in order to improve enforcement. One participant called for licensed operations to be documented publicly. Specifically, with better information transparency, users will be more aware of where there is interference at a given time and area. This participant suggested that the information could be automated and would not require very many manpowered resources.

For example, in the case of Terminal Doppler Weather Radar (TWDR),[14] teams of people volunteered to find out who was interfering. It ended up that there were security cameras running across the town that interfered with the radar. A participant said that this improvement in information transparency is workable because people will be incentivized to use it—"Most people want to do things the correct way," the participant said, "and if people can easily check to see if they will interfere with other applications, people would follow that."

4.2. Utilizing better monitoring to improve enforcement

One participant called for "a complete change in enforcement" that utilizes collaboration to find deviant behavior. The participant suggested that this would involve developing an "ingenious sensor network," which may go as far as including drones in spectrum enforcement. Another participant stated that there must be continuous monitoring of wide geographic areas of spectrum. A third participant suggested that there must be an effort to gather useful data and integrate of that data into chips that can operate in the spectrum.

However, other participants were quick to point out several issues with data monitoring. First, data monitoring will be expensive (in the tens of millions of dollars

[14] "The Terminal Doppler Weather Radar (TDWR) systems serve the critical function of providing the FAA with quantitative measurements for gust fronts, windshear, microbursts, and other weather hazards. The FAA uses this information to improve flight safety at major airports. Weather Radar Interference Enforcement, FCC Encyclopedia, https://www.fcc.gov/encyclopedia/weather-radar-interference-enforcement; Illegal Marketing of Unauthorized Radio Frequency Devices, Citation and Order, FCC DA 12-52 (January 17, 2013), http://transition.fcc.gov/eb/Orders/2013/DA-13-52A1.html. This case was one instance where the source of the interference was traced to a security camera. Most TDWR interference is due to WISP operators operating UNII devices and failing to enable DFS as required by section 15.407(h)(2) of the FCC Rules.

annually for a nationwide network of sensors). Second, finding bad actors is hard (especially in today's digital and mobile world). And third, there will undoubtedly be privacy issues with the data monitoring techniques suggested.

Because the FCC does not have the necessary resources for ubiquitous monitoring, the participants once again discussed the role of the private sector—in this case for privatized monitoring. In some form, there is a need to use a third party database[15] for enforcement because, as several participants agreed, "there is a tremendous incentive to cheat." Improving data prompts the question of rights, but before enforcing rights, the data must be available. Thus, improved data collection must be paramount, said one participant.

One participant noted that the current Government Master File (GMF)[16] is not situated to help solve the challenge of database enforcement. Importantly, another participant noted that the Environmental Protection Agency has a nation-wide network of sensors, and, the participant said, there is no reason the same cannot be done in spectrum enforcement. There is research and development going on for enforcement in spectrum monitoring and databases, which, participants agreed, should be a top priority going forward.

4.3. A Third Party RF Emission Data Clearing House

A proposed solution to improve enforcement was the creation of a neutral, third party clearing house for interference reporting. Ideally, this would include crowd sourcing and big data collection to collect data and use the data to create an interference map. However, when interference incidents are resolved without FCC Enforcement Bureau intervention, the agency and the engineering and research community are unaware of those incidents. One participant said that third party clearing houses will continue to cause the problem of information not getting to academics and others interested in the information. Additionally, several participants said that there will surely be significant data processing and privacy challenges. Nonetheless, some participants saw a third party clearinghouse as a "productive way to increase enforcement for bad actors."[17]

[15] There could be several third party databases, including spectrum monitoring information, frequency coordination data, FCC-authorized third party databases, or new databases that could be developed to support the task.

[16] "The GMF is a data source containing records of the frequency assigned to all U.S. Federal Government agencies in the United States and its possession. Data is obtained from NTIA." See Joint Spectrum Data Repository, Defense Information Systems Agency, Department of Defense, http://www.disa.mil/Services/Spectrum/Enterprise-Services/Joint-Spectrum-Data-Repository.

[17] *See infra* Appendix A for a note on third party clearing houses written by Dale Hatfield as a response to this roundtable discussion.

5. Causes of interference

Looming over the discussion was the question of defining interference. There was a broad consensus that radio interference has become more complicated. Some participants were frustrated that there is no clear framework for discussing the issue.[18] One participant said that in defining solutions, the first step is to define the problem, and that right now, the problem is that there are dozens of types of interference. While the participants did not come up with a specific taxonomy for interference, the participants observed several causes of spectrum pollution that result from device innovation, social norms, and incentives.

First, this section provides a list of distinctions that came up in the conversation about interference. Second, this section identifies the following three main causes of interference discussed: (1) tinkering, (2) jammers, and (3) aggregation.

5.1. Distinctions in interference

Participants suggested that a taxonomy of interference would require separating issues into buckets. Once issues are separated, the goal is to address the issues in those buckets separately to drive solutions. Some buckets might have readily identifiable problems and solutions while others might not. Additionally, some attributes might be nested; for example, intentional interference can be malicious or not malicious.

The table below lists a collection of distinctions that came up in conversation during the roundtable. Going forward, this list can be used as the starting point to create a taxonomy of interference.

Noise (*incoherent*)	Interference (*coherent*)
Natural (*Lightning*)	Manmade (*Rotating electrical equipment*)
Intentional (*Spoofing & Jamming*)	Unintentional
Malicious (*jamming public safety)*	Not malicious (*School cell phone jammers*)
Sophisticated	Simple
Aggregated devices (*LED car headlights)*	A single device (*security camera)*
High power	Low Power
Harmful	Not harmful
Signal level	Noise level
Incumbent	New entrant
New device	Old device
Subtle (*Software defined radio*)	Obvious
Certified device	Uncertified device
Manufacturing issue	Post-manufacturing issue (*Tinkering*)
Government device	Non-government device

[18] *See* discussion *supra* Part 2.1 "The need for clear interference mitigation rules."

5.2. Specific interference issues today: tinkering, jamming, and aggregation

The participants identified tinkering, jammers, and aggregation as three main issues causing interference problems today.

5.2.1. Spectrum pollution due to RF device tinkering[19]

One participant stated that a significant number of enforcement actions by the Spectrum Enforcement Division has to do with unauthorized equipment or authorized equipment that has been modified from the terms of the authorization (i.e., has been the result of tinkering). This is opposed to interference caused by the proper use of authorized equipment. Another participant added that today, most radios can be tinkered with in many different ways, so interference cases involving tinkering are hard to group together. Specifically, radios used today are very different than the traditional crystal radios.[20] Most radios made in the last ten years contain microprocessors that make changing the frequency or power possible in software. Further, while the FCC made rules to prevent users from making changes to software-defined radios, almost all radios today operate in a loophole[21] so they are not governed as software-defined radios. A participant observed that the FCC has proposed tightening security rules for 5 GHz UNI radios because they have observed the problem there, but the participant said that the problem will surely persist in other places that are not yet observed.

Further, manufacturers today have no control over what a person does with a radio once it is out of the manufacturer's control. One participant observed that many users are experimenting with different frequencies—and the participant said those these users either disregard the rules or do not know the rules. That participant noted that the

[19] For the purposes of this section, "tinkering" is defined as modifying a piece of equipment for an alternate or improved functionality beyond the manufacturer/inventor's original purpose.

[20] A major advancement in radio technology was the development and use of the piezoelectric effect in quartz crystals to more precisely control the frequency of a radio transmitter. Before that invention, radio transmitters drifted around widely in frequency and you had to provide very wide channels to prevent the emissions in one channel from moving into or very close to an adjacent channel and causing interference there. While this was a major breakthrough and allowed narrower (more spectrally efficient) channel spacing, the quartz crystals themselves were very expensive, even for major users. (One reason is that they often had to be installed in special ovens to keep their temperature constant.) This drastically restricted the frequency agility of radio transmitters. Later, with the onset of digital techniques, frequency synthesizers were developed that could generate an almost unlimited number of transmitter frequencies on demand and, in doing so, they used just a single quartz crystal as a reference. This provided the much needed frequency agility that allows cellular radios, for example, to operate on hundreds of narrow channels within one or more bands. The radio transmitter itself can be either a traditional hardware defined radio or a software defined radio but the ability to generate any transmit frequency that you want is a critical part of dynamic spectrum access that is typically associated with SDR.

[21] *Ex Parte* Statement of Marcus Spectrum Solutions, In the Matter of Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies, 3 ET Docket No. 03-108 (2005), http://apps.fcc.gov/ecfs/document/view;jsessionid=VwWrPzmTSTpWDg3N4Hqc8vrYDHyp7TDXLlp2xJm3GjwnQyNnNfdQ!-1969853125!NONE?id=6518174313.

question then arises, who should enforcers go after—the manufacturers or the tinkerers?

Another participant added that manufacturers lose control because people installing devices may not install the devices properly or may disable certain features. That participant said that in the old days, manufacturers could control technicians, but today, installations are done in haste and a priority is placed on what works best for the consumer—if necessary, an installer will disable an important feature.[22] Additionally, one participant suggested that although it is the FCC's job, it is extremely difficult for the FCC to go after individuals who purchase and operate devices that cause interference unless they interfere with public safety operations. For example, in the 1970s, the citizen's band (CB) radio enforcement actions were a complete failure.[23]

One participant raised the point that enforcement against tinkerers exposes the problem of unintended consequences. The participant argued that trying to control tinkering can limit the operator, manufacturer, and consumer, potentially in harmful ways (e.g. discouraging innovation).[24] Accordingly, another participant observed that, especially in software defined radios, there is a disconnect between the real world and the policy world—"it is really hard to contain tinkerers or open source software and enforcement cannot account for or enforce all of the potential interference." Instead, the participant said that there is a need to adapt a flexible policy standard that takes into account the tinkering problem and also the unintended consequences of enforcement that may limit the innovations or other beneficial results.

5.2.2. Interference from jammers

There is now a proliferation of sophisticated jamming devices that are increasing the noise floor.[25] Although some jammers may not be malicious, some participants voiced that there must be enforcement against jammers.

One participant noted the important point that even non-malicious jammers can cause harmful interference. For example, jammers in teens' cars minimize distracted driving but could also block a 911 call from an adjacent car.

Another participant argued that enforcement staffers need to focus both on the supply side and demand side of jammers, and the problem is that current enforcement only focuses on the supply side.

[22] For example, impairing Dynamic Frequency Selection in a device, which normally auto-selects the frequency with the lowest interference levels.

[23] Philip J. Weiser & Dale N. Hatfield, *Policing the Spectrum Commons*, 74 FORD. L. REV. 663, 682 (2005), http://ir.lawnet.fordham.edu/flr/vol174/iss2/12.

[24] For example, open source software is successful largely because anyone can modify and experiment with the source code, unlike closed systems that remain with the original inventor.

[25] Christian Sandvig, *Spectrum Miscreants, Vigilantes, and Kangaroo Courts: The Return of the Wireless Wars*, 63 FED. COMM. L.J. 481, 498 (2011), http://www.repository.law.indiana.edu/fclj/vol63/iss2/7/.

5.2.3. The issue of aggregate interference

Several participants observed that interference is commonly caused by the aggregation of more and more devices that are used closer and closer together.[26] Specifically, there are aggregate interference issues where shutting down a single device or enforcing certification standards will not solve the problem. Instead, aggregate interference changes the landscape of interference, and where there are billions of dollars invested in the spectrum industry, any small effect caused by aggregate interference becomes significant. Thus, one participant posed the important question—how can we counter the effects of aggregate interference? There was group consensus that aggregation changes the environment of spectrum use and requires increased and more dynamic sharing.

6. Conclusion

Two important notions came from the discussion. First, there are more devices today than ever before. However all participants agreed that this is a very good problem to have—one participant articulated, "If the choice is less devices and less use of spectrum, I would take more devices and greater interference problems." The second notion is the issue of balance. While the FCC may not have a clear understanding of what harmful interference is, rules and enforcement must strive for an acceptable balance between utility and interference. Specifically, the issue comes up of how to treat incumbents versus innovators. In all new bands, there will be an opportunity to attempt attrition, and split the baby type of solutions can provide important implications in the quest to create a system that works for all parties involved.

From these two notions arise the themes discussed in the roundtable and in this report. These themes can be posed as the following questions. These questions require more attention by the industry.

- What is the role of the FCC, what is the FCC's ability to enforce given its resources, and how can the FCC and other enforcers' jurisdictional reach be better defined?
- What is the role of private actors and how can that role be increasingly utilized to take the weight off of the resource-scarce FCC?
- How can improved transparency and monitoring help mitigate interference issues and improve enforcement?
- What are the categorizations of types of interference and how can they be used to create a taxonomy of interference?

[26] Nada Golmie et al, *Interference Evaluation of Bluetooth and IEEE 802.11b Systems*, 9 WIRELESS NETWORKS 201, 201 (2003), http://morse.colorado.edu/~tlen5520/Papers/GolmieBluetooth.pdf.

APPENDIX A

Roundtable Participants

List of attendees

Lynn Claudy, Senior Vice President, Technology, National Association of Broadcasters
Mark Crosby, President and CEO, Enterprise Wireless Alliance
Pierre de Vries, Co-Director, Spectrum Policy Initiative and Senior Adjunct Fellow, Silicon Flatirons Center
Thomas Dombrowsky, Senior Engineering Advisor, Wiley Rein LLP
Rebecca Dorch, Director, Western Region, Enforcement Bureau, FCC
Ari Fitzgerald, Partner, Hogan Lovells US LLP
Mark Gibson, Senior Director, Business Development, Comsearch
Chris Guttman-McCabe, Executive Vice President, CTIA – The Wireless Association
Dale Hatfield, Co-Director, Spectrum Policy Initiative and Senior Fellow, Silicon Flatirons Center; Adjunct Professor, University of Colorado
Ben Kapnik, Law Clerk to the Hon. Carlos Lucero, United States Court of Appeals, Tenth Circuit
Matt Larsen, Owner, Vistabeam
Peter Manetti, Former President, US West Wireless
Michael Marcus, Marcus Spectrum Solutions LLC
Paul Margie, Partner, Wiltshire & Grannis LLP
Mark McHenry, Founder, Shared Spectrum Company
Robert McKenzie, Director, Crown Castle USA
Jay Monroe, Chairman and CEO, Globalstar
Jeffrey Reed, Willis G. Worcester Professor in the Bradley Department of Electrical and Computer Engineering and the Director of Wireless@Virginia Tech, Virginia Tech.
Blake Reid, Clinical Professor, University of Colorado Law School; Director of Fellowships and Special Projects, Silicon Flatirons Center
Frank Sanders, Chief, Telecommunications Theory Division, U.S. Department of Commerce, NTIA/ITS
Steve Sharkey, Chief of Engineering and Technology Policy, T-Mobile USA
Douglas Sicker, DBC Endowed Professor, Computer Science, Director, Interdisciplinary Telecommunications Program, University of Colorado
David Solomon, Partner, Wilkinson Barker Knauer, LLP
Peter Tenhula, Senior Advisor, U.S. Department of Commerce, NTIA
Phil Weiser, Dean, University of Colorado Law School; Executive Director, Silicon Flatirons Center
Jeff Wepman, Engineer, Spectrum and Propagation Measurement Division, NTIA/ITS

Rapporteurs

Laura Littman, Silicon Flatirons, Research Fellow, JD Colorado Law 2013
Brad Revare, Colorado Law, JD Candidate 2015

APPENDIX B

Third Party Clearinghouses
Roundtable Response Note
By: Dale Hatfield

Dale Hatfield wrote the following note in response to the November 14, 2013, Silicon Flatiron Roundtable, *New times, New Methods: Upgrading Spectrum Enforcement*. He identified the topic of the note, third party data clearinghouses, as an actionable item that came out of the discussions during the formal events of the roundtable and conference and at the reception and dinner afterward.

NOTE:

There is a dearth of reasonably detailed and searchable information on actual interference incidents and, since many interference incidents are frequently resolved <u>without</u> FCC Enforcement Bureau intervention, the agency and the engineering/research community are unaware of them. Moreover, even when the Commission gets a complaint, the issue may be resolved without any formal action and, to my knowledge, based upon discussions with Commission staff, there is generally no information made public about the incident. While information on the small number of cases that result in formal enforcement actions (e.g., a consent decree) is made public, complete technical and other details are typically not available. Thus, it is very difficult to ascertain what particular devices or classes of devices are causing interference incidents and what the associated trends are.

Before now, we were aware that cellular carriers have engineering teams in the field whose job it is to fix technical problems at the local level, including resolving interference issues. However, in the past at least, carriers seemed to be unable or at least reluctant to publicly release information on interference incidents. Based upon my own experience that has been at partially confirmed by conversations with knowledgeable industry folks (including some attendees at the conference), the barriers to the release of such information stem from some combination of the following: (a) lack of communications between technical people in the field and centrally located policy/regulatory personnel who are in a better position to see the value of the information in improving interference mitigation, (b) a perhaps unfounded concern that if they approach FCC enforcement people when it is not absolutely necessary due to the severity of the situation, they may reveal some inadvertent rule violation on their own part, and (c) competitive concerns between and among carriers.

There were three developments at the roundtable/workshop that changed my own thinking (and I think others as well) about the value of gathering and publicly releasing information on interference incidents. First, I think there was increased recognition that policymakers and regulators need more information on the nature, frequency and severity of such incidents in order to ascertain the significance of the interference threat as spectrum becomes increasingly valuable and increasingly complex to manage. Second, strong statements made by a senior technical person from a major carrier expressing a strong interest – indeed a strong desire – in making such information available to the engineering community and others who might be in a position to help reduce the number and severity of costly-to-resolve interference incidents. Three, that the carriers and their vendors might be in a better position to develop interference avoidance techniques if more information was known about the characteristics of the systems and devices that are most apt to cause interference now or in the future.

The admittedly sketchy idea that emerged from these developments was that carriers would be encouraged to release, perhaps on monthly basis, information on interference incidents – information that is now known to be collected by carriers on a routine basis. The information would be released to a neutral, independent third party. The information might include somewhat detailed descriptions of the type of device causing the interference, the name and model number of the device, the name of the manufacturer and FCC ID Number that indicates that the device has received a grant of authorization (if applicable), the geographic location and environment within the interference occurred (e.g., in a shopping mall, office building, manufacturing plant or urban street corner), etc. It might also include information on how the interference was resolved – e.g., by the manufacturer voluntarily supplying an added filter or the owner voluntarily replacing a malfunctioning device. It would be the responsibility of the neutral third party to aggregate, "anonymize," appropriately summarize, and then publicly release a report of the results.

The public report would allow carriers to benefit from the experience of other carriers in terms of how they detected and resolved certain interference issues. It would also facilitate carriers and the manufacturers of frequently interfering devices to voluntarily work out longer term solutions and thereby avoid direct Commission regulation. It would also facilitate initiatives by equipment vendors and standards making groups to develop technological solutions to mitigate or avoid interference. It would allow the Commission to get an early warning of specific types of devices or particular models of devices that are generating greater numbers of interference complaints. Such warnings would allow the Commission to initiate an appropriate investigation – e.g., into whether a particular model of a device is actually in compliance with the rules or whether the governing rules and regulations should be changed through a rulemaking proceeding. It would also give the Commission factual information on which to establish its internal priorities for its enforcement activities and to justify the enforcement portion of its budget. I believe these benefits are significant and justify further effort on our part.