Designing Automated Enforcement for Spectrum Regulation

Automating Enforcement at the Regulatory Authority Level

J. Stephanie Rose

JSR67@Pitt.edu

Department of Informatics & Networked Systems

School of Computing and Information

University of Pittsburgh

Abstract

Spectrum scarcity has been the foundation of several arguments as to why innovative spectrum management initiatives are needed. Subsequently, the resolutions for spectrum management in an attempt to circumvent "scarcity" has pointedly been centralized towards optimizing spectrum allocation. By approaching spectrum management in this linear manner, efforts to alleviate spectrum management issues at the regulatory authority level have been limited if not non-existent. Whilst focusing on spectrum allocation as an *ex-ante* enforcement measure – which typically encompasses actions such as Spectrum Access Systems, the infrastructure and legal framework of this enforcement are often overlooked.

There has been much discussion regarding whether it is best to take an *ex ante* or *ex post* approach to spectrum regulation and subsequent enforcement. However, we rarely delve into the *in eventus* (during an event) actions that would need to be implemented to ensure spectrum infractions aren't falling by the wayside. But how can we best accomplish this? Additionally, how are regulatory authorities supposed to maintain oversight of automated enforcement structures for incumbents, radio frequency interference, and/or schemes promoted for shared spectrum environments when the regulators do not have an automated enforcement structure capable of interfacing with those types of innovations? This research focuses on designing an automated enforcement scheme that strives to find a solution to implement a more *in eventus* enforcement framework for spectrum sharing at the regulatory authority level.

Introduction

In most cases, innovative spectrum management initiatives are focused on how to best allocate frequency bands. Other initiatives are centralized on interference. Currently, there is a limited amount of research being conducted on how we can innovate regulation at the regulatory authority level such as that of the Federal Communications Commission. When making considerations for regulation there needs to be clear rules of engagement for users to follow and concrete penalties for violations. Within spectrum policy, the timing of intervention and enforcement actions are described as *ex ante* or *ex post* policy initiatives. "The purpose of *ex ante* enforcement is to provide a prophylactic strategy for ensuring that unsafe technologies and processes, which may result in undesirable performance, are never applied" (Cui et al 2014). Conversely, *ex post* enforcement is a prescriptive measure used in order to remedy undesired behaviors after they have already occurred. However, what no research has advocated for is *in eventus* regulation. This is to mean that instead of attempting to implement policy for actions that have yet to occur or adjudicate violations after they have been made, there is a protocol for surveillance in order to catch violations while the act is in progress.

More recently, considerations for automating spectrum enforcement have been focused on frequencies where sharing may or will become more intensive. When considering automating enforcement for spectrum, more often than not the frameworks are concentrated on incumbents, radio frequency interference, and/or schemes to promote shared spectrum environments. Enforcement within the real world has legal frameworks, surveillance (patrols), and repercussions for infractions, otherwise known as enforcement. For the online environments, we are still working towards governance and digital enforcement best suited for an ever-expanding technological landscape. Due to the emerging intensity of interconnectedness, current approaches are at best nascent. For spectrum, this task becomes even more challenging as many devices, services, and users rely on efficiency and availability of frequencies without fear of interference. As spectrum reliant technologies continue to prevail, the policies, regulation, and enforcement for a more congested spectrum environment need to be developed in an attempt to streamline and optimize the law and order of spectrum regulation and enforcement in an automated manner from a regulatory authority perspective

The focal point of this research is to develop an automated enforcement structure that will not only focus on *ex ante* and *ex post* enforcement mechanisms, but also considers *in eventus* regulation. For enforcement to occur, there needs to be an enforceable regulation, protocol, mechanism, office of responsibility, and adjudication process. Evermore, for optimal enforcement to emerge, clarity needs to be determined for legal intervention at the regulatory authority level. In order to posit the necessary components for such a mechanism, I have investigated legal frameworks, automated enforcement, and other pertinent information to develop an enforcement scheme and conceptual framework suitable for automating spectrum enforcement.

This paper is comprised of six sections of content. In the first section entitled background, I will discuss the problem and how it relates to the current spectrum environment. Secondly, in the

related works section, I will discuss works that similar to my chosen research area of interest. Thirdly, in the methodology section, I will discuss which methods I selected and how they relate to the problem and solution. Fourth, I will explore the outcomes of my work. Fifth, I will examine the implications of my proposed mechanism utilizing documentation from the Deputy Assistant Secretary of Defense for Systems Engineering. Lastly, I will conclude by discussing the limitations and future work within the discussion portion.

Background

My research is focused on developing an *in eventus* regulation mechanism for spectrum policy enforcement. Currently, the Federal Communications Commission's Enforcement Bureau encompasses three regional offices which directly account for 13 states total. Typically, the Enforcement Bureau adjudicates spectrum violations in an ex post manner. The research questions I have selected include the following:

RQ1: How prevalent are interference issues within commercial spectrum management?
RQ2: How does the FCC adjudicate spectrum interference violations?
RQ3: Is there a more innovative way to regulate radio spectrum?

Regulation, automation, and enforcement when investigated separately aid in analyzing existing measures and help determine which attributes can best create a system for enforcement within a shared spectrum environment.

Regulation within the scheme of telecommunications rarely discusses in great detail the actual enforcement measures taken to dissuade violators from interfering with radio spectrum and/or violating the terms of their agreements. As we begin to conceptualize automated enforcement measures that include regulatory authority inputs, it becomes more imperative than ever to understand the fundamental infrastructure on how enforcement is handled within these spaces.
Automation is arguably one of the most hot button topics in the 21st Century. Due to its overuse and popularity, the intent of what is meant by automation when discussing telecommunications policy, regulation, and enforcement can become elusive because automation in this day and age can encompass a myriad of operations and procedures. This paper discusses automation in the context that current enforcement procedures that are performed by the Federal Communications Commission (FCC), National Telecommunications and Information Administration (NTIA), or even incumbents are taken "off the page" and adapted into a design that would be most optimal for computational purposes. This is to mean that in lieu of having physical agents using "directional sensing techniques" to find interference, a system has been designed to extrapolate data (whether through intermediary devices, crowdsourcing, or other technological means) and implement enforcement based on a set of rules and conditions that have been predefined by the regulatory authority.

The concept of enforcement in a telecommunications or cyber perspective has been nascent when compared to other ideologies and frameworks for regulation which has a well-defined construct

for arbitration such as the enforcement we see with law (whether municipal, state, or federal). However, a primary bottleneck for exerting or developing enforcement schemes for telecommunications is essentially the concept of harm. Yet, traditional law - especially that of traffic, road, and/or vehicle violations – incorporate the notion of perceived harm (whether intentional or unintentional), being a risk to others is a component for certain violations where an individual can be a danger to others and/or themselves.

Furthermore, the regulatory authority structure for enforcement as described in this paper will refer to the enforcement bureau as a subset of the Federal Communications Commission as shown in figure 1 below.

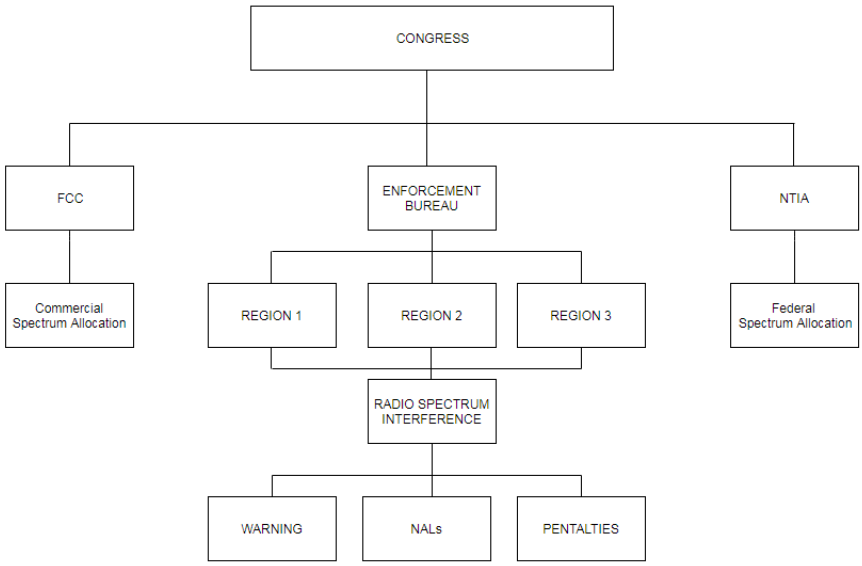

Figure 1: Spectrum Enforcement Regulatory Authority Hierarchy

While the majority of discussion and debate has centered on the ramifications for consumers and producers, little attention has been devoted to the regulators who enforce Congress' will (Coopman 1999). In order to enforce spectrum interference, the Federal Communications Commission Enforcement Bureau takes action through warnings, notices of apparent liability, and/ or penalties. Overall, there are three regions for the enforcement bureau that enforces spectrum for the United States. "However, the FCC has neither time nor resources to enforce current communications laws, let alone this new mandate from Congress" (Coopman 1999).

The radio spectrum enforcement process typically follows the pattern outlined in figure 2. A complaint is received, the respective enforcement bureau within the regional location will investigate (sometimes they are able to interview the offender and gain additional insight as to why they chose to operate without a license or that they may be purposefully interfering with radio

spectrum purposefully through other means). Next, a type of enforcement action will be imposed such as a warning, notice of apparent liability (NAL), forfeiture order, or a different category of document that may or may not impose a penalty (some also require a mandatory response to the FCC by mail). Lastly, the information is updated to the enforcement bureaus database which is currently housed on the FCC's transitional webpage (not the main FCC.gov URL).

Figure 2: Current Enforcement Protocol

The current approaches don't appear to be much a deterrent for individuals operating unlicensed radio stations, as many of them are multiple offenders, however, based on the data extracted from the enforcement bureau database, it doesn't appear that much is being done in order to heed would be offenders. Additionally, in some circumstances, entities are purposefully interfering with public safety frequency channels, however, again, the data does not show any deviation in the enforcement measure in order to deter tentative harmful disruptions. To this end, this is why is imperative that a more in eventus model for regulation and subsequent enforcement measures should be exerted by the FCC's enforcement bureau. Furthermore, additional clarity into the types of enforcement and a hierarchal structure for infractions, if adopted by the enforcement bureau, would allow an automated enforcement structure to be easily implemented and deployed.

Related Works

Considerations for enforcement for radio spectrum is not a new concept. Many others have posited solutions to spectrum interference and how regulatory agencies should respond accordingly. In 1989, Vicanni posited a spectrum enforcement measure where an automated monitoring system would surveil unassigned frequencies in an attempt to make spectrum enforcement more manageable. Furthermore, in 2009, Coopman analyzed the FCC's regulatory and enforcement strategies. Moreover, in Markovic et al 2009, they developed a tool that "supports formal specification of policies and rules and their automated enforcement on process models". During 2012, Tenhula's work sought to find an expedient resolution for harmful interference. In Altamaimi et al 2013, they examined "three enforcement approaches, exclusion zones, protection zones and pure *ex post* and consider their implications in terms of cost elements, opportunity cost, and their adaptability". Additionally, Cui et al 2014 discussed "rational choices about enforcement approaches and costs require analysis of rights, objectives, precision, etc." Conversely, Littman and Revare convened a roundtable in 2014 with a myriad of subject matter experts to collectively map the changing spectrum landscape. Furthermore, Park et al 2014 discuss the spectrum enforcement issue only in the *ex ante* and *ex post* approach. More recently, Miettinen et al 2017 approached enforcement through an IoT Sentinel.

Many of the scholarly works reviewed in relation to spectrum enforcement focus on enforcement from the perspective of access and restriction. "There are two distinct, but closely related problems with [spectrum usage rights] SURs today: the boundaries and the enforcement of the rights" (Tenhula 2012).

Another scholar, whose work is not focused on spectrum enforcement, does however, provide valuable insights regarding enforcement. In Steven Shavell's work on optimizing enforcement, he provides various at details and timing of enforcement. Within this article he discusses figure 3 below.

General Method of Enforcement	Dimensions of Enforcement		
	Stage of Intervention	Form of Sanction	Private versus Public
Tort law	Harm-based	Monetary	Private
Safety regulation	Prevention and act-based	Monetary	Public
Injunction	Prevention	. . .	Private
Criminal law	Prevention, act-based, and harm-based	Monetary and nonmonetary	Public
Corrective taxation	Act-based	Monetary	Public

Figure 3: Dimensions of Enforcement by Method

This table of dimensions, although not directly aligned with the enforcement power of the FCC, provides a good roadmap on how to best apply a hierarchal enforcement approach to the regulatory enforcement measures that the FCC currently deploys. Shavell explains how the enforcement actions are missing from the table above, however, in the methodology section, I provide a separate table which includes enforcement measures readily available at the FCC's disposal.

The research conducted in this paper, theorizes an infrastructure that would be adaptable for future transference to an automated framework. Specifically, by implementing a more *in eventus* approach to radio spectrum enforcement, identifying optimal enforcement, and providing a conceptual framework for regulatory authorities such as the FCC, regulatory oversight would be better prepared for more emerging technologies, whether it's 5G or the billions of devices promised with the advent of IoT.

Methodology

In order to address the problems of spectrum interference, enforcement adjudication, and transition of policy into an automation mechanism, I have utilized a multimethod approach. The methods were selected to specifically answer the problems I have stated such as prevalence of interference within spectrum environments, enforcement adjudication, and innovating regulation in an attempt to provide continuous oversight for emerging technologies.

These methods included a document analysis of 650 Federal Communications Commission Enforcement Bureau actions of various types of enforcement, however, the 217 infractions specifically pertaining to radio spectrum interference were used for this research. Additionally, in order to construct the conceptual framework and subsequent aids to articulate optimal enforcement

in an in eventus construct, a system requirements model was utilized. Finally, case studies investigating existing automated enforcement systems that have been deployed and are currently in use were assessed in order to determine what an automated enforcement system for the Federal Communications Commission would need to entail as a first step measure. Furthermore, considerations of the affordances and negative externalities these deployed systems incur were also deemed useful in order to gain a whole picture concept of what setbacks a system created on a large scale for enforcement uses may face.

Document Analysis

Each of the 650 cases were coded into an excel spreadsheet by extrapolating data from each html file for recorded enforcement actions between 2017 and 2014. Attributes captured included name (whether corporation or an individual person), case number, date of the violation, location (city and state), frequency band disrupted, enforcement type (e.g. warning, NAL, penalty, etc.), publication type (which may vary depending on the enforcement type), type of entity (such as a religious institution, business, individual/ dual actors, etc.), enforcement bureau department region, enforcement bureau department location (some of the more serious enforcement actions are adjudicated from FCC headquarters in Washington, D.C.), and whether the offending party was a licensee.

The document analysis provided a foundation as to what enforcement gaps currently exist. Moreover, the cases provided a snapshot of how the FCC respond to occurrences of interferences and violations within today's diverse spectrum environment. By conducting a document analysis from the FCC's Enforcement Bureau's data, I noticed there is an enforcement disparity in which "would be offenders" are not necessarily dissuaded from interfering with radio spectrum. As seen in figure 4, there is a surge of frequency specific violations that occurred in 2017 when compared to other years. This observation suggests that future research in this area may be beneficial to policymakers as there appears to be a trend of increasing spectrum interference violations. Due to this result being a singular instance, I cannot in good conscience conclude that this occurrence is or will be persistent. However, in terms of the research goals of this paper, it does provide merit that a more innovative approach to spectrum regulation could prove fruitful, especially if this singular instance becomes a trend as more technologies continue to emerge within the spectrum environment.

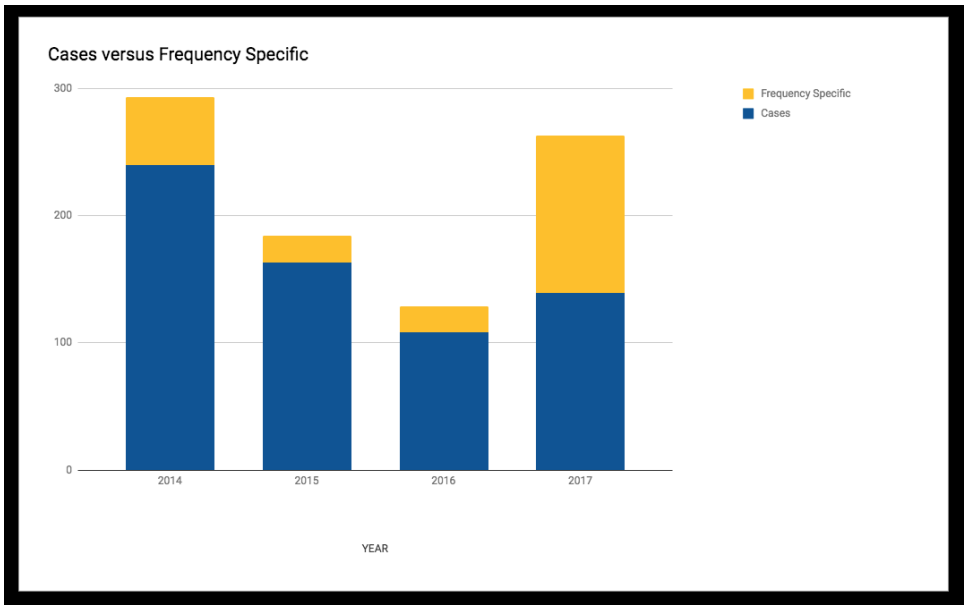

Figure 4: Enforcement Bureau Intervention 2017-2014

Assessment for a New Approach to Enforcement

The principle dimensions of law as described by Shavell were adopted to analyze how current radio spectrum enforcement measure against an optimal enforcement paradigm. In Shavell's work he includes tort law and criminal law, however, for the scope of the FCC, these components have been converted in the regulatory guidance more aligned with the FCC's authority such as the United States Code (USC) and CFR.

Enforcement Doctrine	
United States Code (USC)	
47 U.S.	
Code § 151	Purposes of chapter; Federal Communications Commission created
Code § 154	Federal Communications Commission
Code § 302a	Devices that interfere with radio reception
Code § 303	Powers and duties of Commission
Code § 308	Requirements for license
Code § 312	Administrative sanctions
Code § 325	False, fraudulent, or unauthorized transmissions
Code § 320	Stations liable to interfere with distress signals; designation and regulation
Code § 323	Interference between Government and commercial stations
Code § 332	Mobile services
Code § 333	Willful or malicious interference
Code § 398	Federal interference or control
Code § 401	Enforcement provisions

Code § 407	Order for payment of money; petition for enforcement; procedure; order of Commission as prima facie evidence; costs; attorneys' fees
Code § 502	Violation of rules, regulations, etc.
Code § 504	Forfeitures
Code § 510	Forfeiture of communications devices
Code § 1403	Enforcement
Code of Federal Regulations (CFR)	
CFR Part 8	Protecting and promoting the open internet
CFR Part 15	Radio frequency devices

This list is not exhaustive in nature as there are many statues that fall under the FCC's purview, however, regulations that explicitly negate the FCC's enforcement power have been added into the table in order to provide a roadmap to establishing a hierarchy of enforcement actions that can be incorporated into an automated enforcement structure. When assessed in conjunction with Shavell's dimensions of enforcement table, it becomes increasingly clear that there are areas where the FCC can compose their enforcement approach into one that operates in a more events based manner.

Assessing the current legal enforcement power of the FCC in conjunction with the dimensions of enforcement table by Shavell, an optimal enforcement scheme for the FCC would need to take each act of interference and/or violation into account and rate them according to level. This level could be realized or perceived harm due to explicit or implicit actions leading to interference of spectrum and/or frequency of violations by an entity depending on the FCCs agenda. Furthermore, by recognizing that enforcement should be enforced in a more consistent manner (e.g. unlicensed operators who consistently disregard warnings should be penalized in a similar manner, yet differently from an individual who purposely deploy a signal jammer that is causing interference with public safety frequency bands). Furthermore, the enforcement adjudication measures should complement interference/violation actions such as a warning for deliberately interfering with the New York Police Departments frequency may not deter the wrongdoer as the regulatory invention may be perceived as trivial when the crime could yield life threatening results. This is to mean that there should be consistent enforcement measures that should fit the violation.

In order to better determine what kind of enforcement approach may need to be adopted in order to automate enforcement for radio spectrum, other automated enforcement frameworks have been investigated in order to better understand how innovative enforcement approaches are being utilized in today's society.

Modeling System Requirements

Idealistically, the use of a model system requirements as a method to develop the conceptual framework would encompass all of the components of the agile method. However, for this

framework, I kept the scope of the conceptual framework narrow and focused on 5 out of the 10 suggested steps for leveraging agile methods as prescribed by the Government Accountability Office (GAO). The agile components I focused on included an agile adoption strategy, conveying requirements, suggested adoption at the organization level (FCC), identifying impediments, and as opposed to utilizing user stores provide decision tables, contextual diagram, and level 0 data flow diagram (DFD). By accomplishing these tasks of the GAO agile method, this ensures that the conceptual framework would be aligned with FCC and other governmental agency requirements.

In order to assess some of the requirements needed to develop a large scale automated enforcement framework, I referred to some existing automated enforcement schemes that are currently being used within the United States.

Current automated enforcement systems currently in use include, but are not limited to traffic enforcement (speed and red light cameras), copyright, and vessel monitoring systems, each of which will be discussed in further detail below. As discussed previously, each of these automated enforcement mechanisms have their own affordances and drawbacks unique to their specific area of regulation. "While governance solutions may not involve the creation of enforceable rights, it can often mitigate some of the more serious negative aspects of commons" (Cui et al 2014). The cases discussed below encompass best efforts to mitigate undesired behaviors with some having more harmful circumstances than others.

Automated Traffic Enforcement of Road Violations

These systems may be used at the Federal, state, and/ or municipal levels. Despite a national initiative to automate traffic violations and adjudication, less than half of the states in the contiguous United States are using automated enforcement. Current automated enforcement measures are focused on speed and red-light violations. "Automated traffic applications typically encompass the detection and segmentation of moving vehicles as a crucial process" (Marikhu et al 2013). This automated enforcement mechanism for traffic and road violations bore out a need to decrease fatalities and risky driving behaviors. "Automated enforcement programs can be an effective countermeasure for reducing crashes at high risk locations" (NHTSA 2010). The typical framework for automated traffic enforcement is comprised of speed cameras and red light cameras. However, it is not an enforcement structure that has been adopted nation-wide. Overall, this type of automated enforcement leverages the existing scheme for adjudicating traffic violations by taking a photo of the offender's license plate.

Automated Enforcement of Copyright

Unlike automated traffic enforcement, automated copyright enforcement is initiated by the owner of the copyrighted material and/or intellectual good. "Today's major digital communities include: P2P file sharing systems, chat applications and social networking sites" (Hughes et al 2008). With this high volume of sharing also came an increased amount of copyright infringement. In order to mitigate these copyright violations, the digital rights management in conjunction with the digital millennium copyright act and other stakeholders have been implementing measures to safeguard copyrighted materials online. The "DRM represents just the first wave of a class of technologies that aspire to not only implement copyright-protecting usage controls on computing devices, but increasingly to take on the enforcement of a broader set of organizational and public policies" (Erickson & Mulligan 2004). There are additional services where the owner of the material can

pay to have their content professionally monitored and tracked. In each of these cases, most times, initiatives for automated enforcement of copyright (through DMCA.com) working closely with internet service providers and other stakeholders to ensure that content is not illegally used or disseminated. Unfortunately, the drawback to this approach is that it does not account for exceptions to copyright such as fair use. Due to this literal application of enforcement of copyright online, an atmosphere that is very reminiscent of "chilled speech" has begun to permeate within online environments where users are extremely cautious of using or posting any materials that should/are copyrighted materials, even if they do fall under the scope of the fair use doctrine.

Vessel Monitoring System

Another automated enforcement system is the Vessel Monitoring System (VMS). This system focuses on fisheries as well as nautical search and recovery missions. In order to accomplish this, VMS utilizes "satellite communications and GPS technology, this system provides near-real time two-way communication between fishing vessels and enforcement monitoring centers monitoring fishing vessel activity throughout the United States EEZ, Pacific Ocean and Atlantic Ocean" (NMFS 2005). The benefits of this approach are that incumbents and enforcers appear to be working in tandem in order to meet their respective objectives. As of the conclusion of my research, no negative effects to this automated enforcement method have been identified.

Assessing Automation as an Enforcement Scheme

Although automated enforcement schemes between traffic, copyright, and vessels are decidedly different, they are all similar in detecting and reporting enforceable actions. Evermore, users (possible violators) are aware that there is an enforcement mechanism in place that is essentially "always watching". "If there is no chance of being caught, then there is very little incentive to invest serious engineering effort in complying with the regulations" (Atia et al 2008). This digression of "being caught" is not as much in the forefront to would be spectrum violators as it is the users of each of these three systems. Although there are less than desirable outcomes to the automated traffic enforcement and online copyright enforcement, these approaches appear to have met the desired expectations of the enforcement entities within these areas.

Innovative Spectrum Regulation & Enforcement Approach

In order to resolve the problems identified in the background section, the solutions proposed also manifested in a triad structure. In order to develop the conceptual framework, it was imperative to also create a more optimal enforcement framework where attributes from existing schemes were adopted as a foundation as to what other attributes would be necessary in order to create and deploy an automated enforcement system with national scalability. Additionally, a decision table was designed to foster more *in eventus* regulatory enforcement for radio spectrum. Lastly, the conceptual framework was then formed.

Defining Requirements

As discussed in the method and determining factors sections, it is imperative to have a more concise cause and effect structure regarding radio spectrum enforcement. As it stands, based on the data analysis conducted the FCC's enforcement approach appears to be any cause can lead to any number of enforcement actions, when in reality – especially in the context of having an enforcement model that can be transferred to an automated system – there needs to be the approach of "this specific act" renders this level of adjudication from the FCC. Additionally, as concise as the enforcement actions need to be, they also need to decidedly deter unwanted behaviors from both legal (licensed) incumbents as well as the general unlicensed individual who is able to enjoy spectrum amenities such as Wi-Fi.

Requirement Prioritizations

In terms of initial implementation, prioritization of enforcement should more than likely be given to interference and violations that could cause actual harm. By doing so, this aligns with some of the agile methodologies discussed earlier in the paper. Modulation of system development and implementation would allow for observation of what works best for the FCC and which attributes need to be fine-tuned further. Furthermore, it would act as a use to determine if an automated enforcement system of that level of scalability is actually feasible and if it would aid in other FCC initiatives.

Framework Development

With the statutory authority of the FCC in mind, figure 5 as shown below encompasses a high-level overview of unlicensed and licensed users and possible actions. Figure 5 is the overall decision table which exhibits four types of circumstances that each type of entity can experience. Although this may not be all encompassing of the types of actors and conditions/actions that can prompt FCC intervention, this is a preliminary glance on how a decision mechanism for a policy based automated enforcement structure can be determined.

Conditions/Actions	Rules							
	Individual				Business			
Licensed	X	X			X	X		
Unlicensed			X	X			X	X
Intentional (E.g. unlicensed radio, exceeded power limits, jammer/blocker, etc.)	X		X		X		X	
Unintentional (e.g. hardware failure)		X		X		X		X

Figure 5: Decision Table

Figure 6 (shown below), is the first condition and action where the users are licensed and intentionally causing interference. The interference they are causing could be harmful or not. Under these circumstances, the FCC has a number of options for adjudication. However, as indicated from the enforcement bureau database for 2017 cases, most times a warning or notice of apparent liability is used as an enforcement mechanism.

Conditions/Actions	Rules							
		Individual				Business		
Licensed	X	X			X	X		
Unlicensed			X	X			X	X
Intentional (e.g. unlicensed radio, exceeded power limits, jammer/blocker, etc.)	X		X		X		X	
Unintentional (e.g. hardware failure)		X		X		X		X

Figure 6: Licensed and Intentional Violation

The next circumstance as shown in figure 7 illustrates users who are licensed, yet cause unintentional interference and/or an unintentional violation. Under these considerations, the FCC's enforcement bureau may impose a warning, notice of violation, or other enforcement action.

Conditions/Actions	Rules							
		Individual				Business		
Licensed	X	X			X	X		
Unlicensed			X	X			X	X
Intentional (e.g. unlicensed radio, exceeded power limits, jammer/blocker, etc.)	X		X		X		X	
Unintentional (e.g. hardware failure)		X		X		X		X

Figure 7: Licensed and Unintentional Violation

Additionally, figure 8 the users are unlicensed and intentionally causing interference. In this event the enforcement bureau may provide the violator with a warning, notice of apparent liability, forfeiture order, or another enforcement action such as an imposed penalty.

Conditions/Actions	Rules							
		Individual				Business		
Licensed	X	X			X	X		
Unlicensed			X	X			X	X
Intentional (e.g. unlicensed radio, exceeded power limits, jammer/blocker, etc.)	X		X		X		X	
Unintentional (e.g. hardware failure)		X		X		X		X

Figure 8: Unlicensed and Intentional Interference

Conditions/Actions	Rules							
	Individual				Business			
Licensed	X	X			X	X		
Unlicensed			X	X			X	X
Intentional (e.g. unlicensed radio, exceeded power limits, jammer/blocker, etc.)	X		X		X		X	
Unintentional (e.g. hardware failure)		X		X		X		X

Figure 9: Unlicensed and Unintentional Violation

Lastly, in figure 9, users are unlicensed and unintentionally causing interference or unknowingly violating FCC regulations. Most commonly in these circumstances the user is provided with a warning, however, that enforcement action is not guaranteed.

Figures 5-9 there are more of an overview of how level/hierarchal based enforcement schemes could provide much needed clarity, which could in turn be translated into an automated system. Following the hierarchy exhibited, figures 10 and 11 depict the contextual diagram and level zero data flow diagram provide additional context as to how this system would be developed. The figures take the current enforcement process – which was described at the beginning of this paper – and make those actions compatible for system adaptation.

Furthermore, if the FCC were to incorporate the level-based enforcement approach, the determination that dictates which interference and violation cases could be adopted into the system process. For example, the component 2.0 in figure 11 that generates the reports prior to FCC adjudication could be updated to encompass the attribution of enforcement response to the interference or violation.

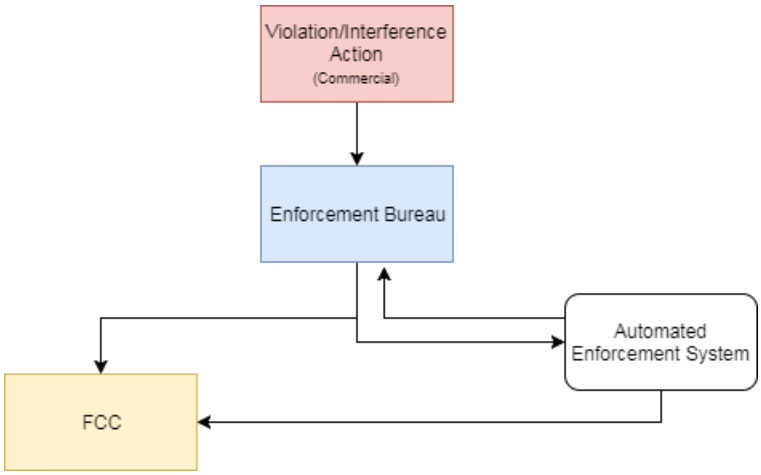

Figure 10: Contextual Diagram Regulatory Authority Automated Enforcement

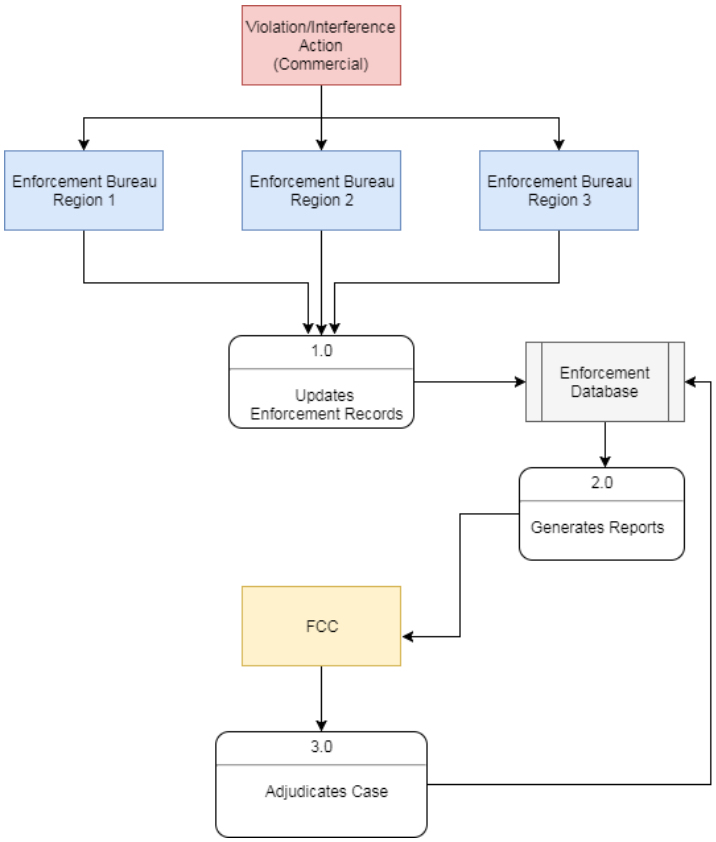

Figure 11: Data Flow Diagram level 0

Analysis & Evaluation

On December 12, 2017 the Government Accountability Office (GAO) published a report entitled *"The FCC Should Improve Monitoring of Industry Efforts to Strengthen Wireless Network Resiliency".* In this report, the main focus appears to be natural disasters, manmade events (such as digging), accidental outages, and "other. Despite the focus of resiliency being concentrated on wireless outages as an effect of natural disasters, the conceptual framework suggested in this paper may aid in provided wireless resiliency in conjunction with efforts to regulate spectrum in an *in eventus* manner.

The GAO outlines that there were significant outages to wireless and the FCC's response "reported outages was due to increases in both the number of wireless customers and wireless infrastructure over this period" (GAO 2017). Furthermore, GAO continued to report that the resolution methods suggested by the FCC were not made widely disseminated to incumbents. In figure 12 provided below a more overall view of the volume as well as the cause of outages can be seen.

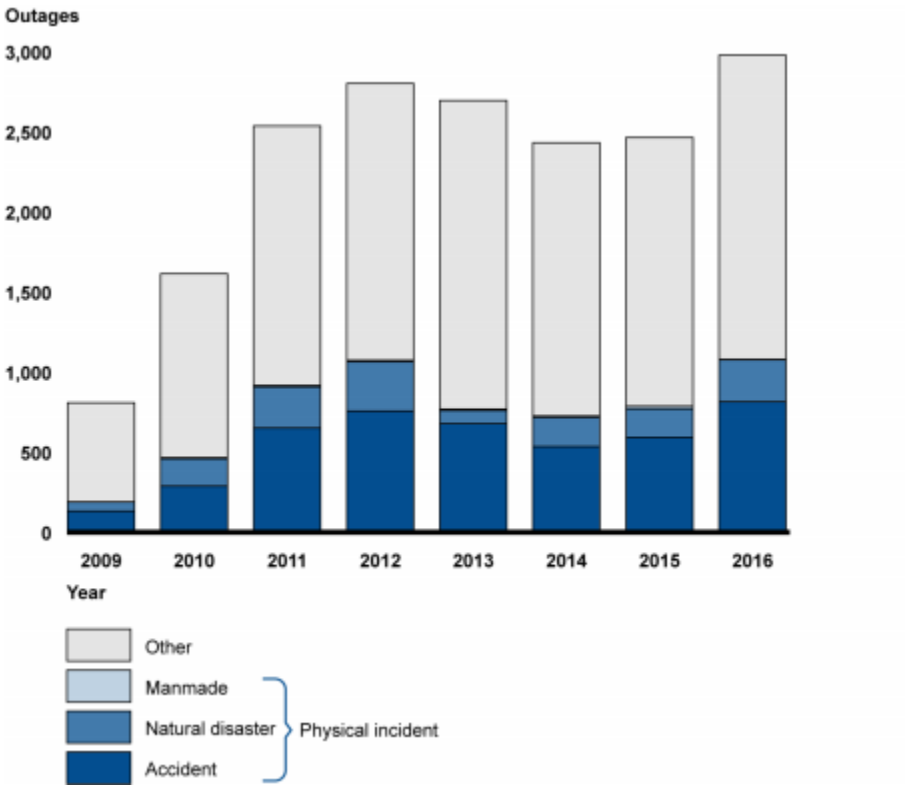

Figure 12: Number of Reported Wireless Outages and Wireless Outages with a Physical Incident as the Root Cause, 2009–2016

Interestingly enough, there are no calculations accounted for the year of 2017 despite this report being made available in December.

The affordance of the FCC adopting an automated enforcement framework as conceptualized in my research is that the system may yield far greater returns than just exerting better efforts to police intensively shared spectrum environments.

In order to evaluate the conceptual framework against the current needs of the Federal Communications Commission, I have created an analysis matrix where I have utilized required and proposed considerations based on the Deputy Assistant Secretary of Defense for Systems Engineering. Although the parameters prescribed by this office are arguably more stringent than what is required for the FCC, it has provided a baseline of what this system would need to encompass in order to be adopted by a federal agency.

Design Considerations	Conceptual Framework	Future Work
Accessibility	N/A	X
Affordability	N/A	X
Anti-Counterfeiting	N/A	X
Commercial – Off – the- Shelf	N/A	X
Interoperability/Dependencies	N/A	X
Modular Design	X	X
Operational Energy	N/A	X
Reliability & Maintainability Engineering	N/A	X
Spectrum Management	X	X
Standardization	X	X
Supportability	N/A	X
Survivability & Susceptibility	N/A	X
Gather Detailed Information	X	X
Define Requirements	X	X
Prioritize Requirements	X	X
Develop user-interface dialogs	X	X

Many of the considerations provided within this table are not immediately relevant to the conceptual framework prescribed within this work. This is twofold. Firstly, the conceptual framework for automated radio spectrum enforcement was developed as a "first step" measure to for the FCC to approach enforcement. Secondly, neither the FCC nor the GAO provide an analysis matrix that pertain to the FCC's systems and applications.

Discussion

As American society becomes more entangled with technology, regulation, enforcement, and arbitration regarding infractions and violations within virtual and real-world spaces has turned towards leveraging technology in order to adjudicate enforcement actions. The automated enforcement schemes implemented from an *ex post* manner will need to be linked to an *ex ante* and *in eventus* framework in order to fully be sustainable. Moreover, a more formalized and visible approach to radio spectrum enforcement may ensure that licensed and unlicensed spectrum users alike would inherently become more aware of the expectations and boundaries of what actions are and are not permissible.

The framework provided in this paper is only an initial "first steps" measure towards automating enforcement from a regulatory authority perspective. Additional research will include attributes, circumstances, and a system design in more of a fine-grained manner. Furthermore, extension to the decision table to include attributes such as harmful, reckless, or perspective harm may be included in future iterations based on the distinction of what constitutes as a harmful, possibly/ prospectively harmful, and reckless actions which could cause irreparable danger to operations that utilize radio frequency for public safety, FAA, and other measures that could in effect be life endangering. Furthermore, as suggested previously, by adopting an automated enforcement system, other FCC initiatives such as wireless resiliency may be able to be incorporated which would provide both the FCC and other stakeholders with a more responsive approach to outages and other network issues.

Developing an automated enforcement scheme, further consideration of how this system could be implemented following a more agile approach to system design would be more advantageous than following the seemingly waterfall design current telecommunications policy and regulations abide by. Moreover, creation of a dialog diagram or clickable wireframe architecture of how regulatory authorities would access and utilize this system (whether in tandem with other automated enforcement mechanisms more specifically tailored towards detection and/or *ex post* enforcement mechanisms), would need to be constructed in order to actualize this conceptual framework further.

Lastly, security and privacy measures will need to be adopted into this framework. However, it is unclear as to what privacy and security needs the FCC has regarding cases of violation and/or interference as their information is transparent and available publicly.

Limitations of this research include, utilizing the FCC enforcement bureau database to develop requirements due to lack of data regarding the processed of how the enforcement bureau operates, lack of availability of materials that investigate the actual mechanisms and technical parameters for automated enforcement for traffic violations, online copyright enforcement, and vessel monitoring systems (many of the literary works discuss these operations in a high-level manner), and transparency of how federal users enforce radio spectrum as it would have provided a more well-rounded conceptual framework and may have aided in developing requirements for an automated enforcement system further.

This paper has discussed the prevalence of interference within spectrum environments, current adjudication for spectrum violations, and an innovative approach for spectrum policy.

References

Altamaimi, M., Weiss, M. B. H., & McHenry, M. (2013). Enforcement and spectrum sharing: Case studies of federal-commercial sharing.

Atia, G., Sahai, A., & Saligrama, V. (2008). Spectrum enforcement and liability assignment in cognitive radio systems. Paper presented at the 1-12. doi:10.1109/DYSPAN.2008.53

Bari, M. F., Chowdhury, S. R., Ahmed, R., & Boutaba, R. (2013, November). PolicyCop: An autonomic QoS policy enforcement framework for software defined networks. In *Future Networks and Services (SDN4FNS), 2013 IEEE SDN For* (pp. 1-7). IEEE.

Brown, S. W., & Swartz, T. A. (1989). A gap analysis of professional service quality. *The Journal of Marketing*, 92-98.

Coopman, T. M. (1999). FCC enforcement difficulties with unlicensed micro radio. *Journal of Broadcasting & Electronic Media, 43*(4), 582-602. doi:10.1080/08838159909364511

Cui, L., Gomez, M., & Weiss, M. B. H. (2014). Dimensions of cooperative spectrum sharing: Rights and enforcement.

Cunningham, C., Hummer, J., & Moon, J. P. (2008). Analysis of automated speed enforcement cameras in Charlotte, North Carolina. *Transportation Research Record: Journal of the Transportation Research Board*, (2078), 127-134.

Decina, L. E., Thomas, L., Srinivasan, R., & Staplin, L. (2007). *Automated enforcement: A compendium of worldwide evaluations of results* (No. HS-810 763).

Enguehard, R. A., Devillers, R., & Hoeber, O. (2013). Comparing interactive and automated mapping systems for supporting fisheries enforcement activities—a case study on vessel monitoring systems (VMS). *Journal of coastal conservation, 17*(1), 105-119.

Erickson, J. S., & Mulligan, D. K. (2004). The technical and legal dangers of code-based fair use enforcement. *Proceedings of the IEEE, 92*(6), 985-996.

Government Accounting Office. (2017). The FCC Should Improve Monitoring of Industry Efforts to Strengthen Wireless Network Resiliency. Washington, DC: Government Printing Office.

Hazlett, T. W., Porter, D., & Smith, V. (2011). Radio spectrum and the disruptive clarity of ronald coase. *The Journal of Law & Economics, 54*(S4), S125-S165. doi:10.1086/662992

Huang, H. H. (2010). A control-theoretic approach to automated local policy enforcement in computational grids.

Hughes, D., Rayson, P., Walkerdine, J., Lee, K., Greenwood, P., Rashid, A., & Brennan, M. (2008). Supporting law enforcement in digital communities through natural language analysis. *Computational Forensics*, 122-134.

Joh, E. E. (2007). Discretionless policing: technology and the fourth amendment. *California Law Review*, 199-234.

Johnson, N. (1969). Towers of babel: The chaos in radio spectrum utilization and allocation. *Law and Contemporary Problems, 34*(3), 505-534.

Kim, G., Behr, K., & Spafford, G. (2014). The phoenix project: A novel about IT, DevOps, and helping your business win. Blue Ridge Summit;Portland;: IT Revolution Press.

Markovic, I., Jain, S., El-Gayyar, M., Cremers, A. B., & Stojanovic, N. (2009, May). Modeling and enforcement of business policies on process models with maestro. In European Semantic Web Conference (pp. 873-877). Springer, Berlin, Heidelberg.

McCollum, C. J., Messing, J. R., & Notargiacomo, L. (1990, May). Beyond the pale of MAC and DAC-defining new forms of access control. In *Research in Security and Privacy, 1990. Proceedings. 1990 IEEE Computer Society Symposium on* (pp. 190-200). IEEE.

Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A. R., & Tarkoma, S. (2017, June). IoT Sentinel: Automated device-type identification for security enforcement in IoT. In *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on* (pp. 2177-2184). IEEE.

Nicolette, D. (2015). Software development metrics (1st ed.). Shelter Island: Manning.
Park, J., Reed, J. H., Beex, A. A., Clancy, T. C., Kumar, V., & Bahrak, B. (2014). Security and enforcement in spectrum sharing. *Proceedings of the IEEE, 102*(3), 270-281. doi:10.1109/JPROC.2014.2301972 .

Office of the Deputy Assistant Secretary of Defense of Defense for Systems Engineering. (2017). Design Consideration Standards. Defense Acquisition Guidebook. Washington, DC: Under Secretary of Defense for Acquisition, Technology, & Logisitcs.

Park, J., Reed, J. H., Beex, A. A., Clancy, T. C., Kumar, V., \& Bahrak, B. (2014). Security and enforcement in spectrum sharing. Proceedings of the IEEE, 102(3), 270-281. doi:10.1109/JPROC.2014.2301972

Schmidt, C. (2016). Agile software development teams: The impact of agile development on team performance. Cham, Switzerland: Springer.

Shavell, S. (1993). The optimal structure of law enforcement. *The Journal of Law & Economics, 36*(1), 255-287. doi:10.1086/467275

Tenhula, Peter A., Enforcement of Spectrum Usage Rights: Fair and Expedient Resolution of 'Interference' Disputes (March 31, 2012). 2012 TRPC. Available at SSRN: https://ssrn.com/abstract=2032312 or http://dx.doi.org/10.2139/ssrn.2032312

U.S. Congress. House Committee on Transportation and Infrastructure. (2010). Utilization and impacts of automated traffic enforcement. Congressional hearing, 2010-06-30.

U.S. Congress. House Committee on Transportation and Infrastructure. (2010). Utilization and impacts of automated traffic enforcement. Congressional hearing, 2010-06-30.
United States. Congress. Senate. Committee on Homeland Security and Governmental Affairs. Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, & United States. Government Accountability Office. (2012). Software development: Effective practices and federal challenges in applying agile methods: Report to the subcommittee on federal financial management, government information, federal services, and international security, committee on homeland security and governmental affairs, united states senate. Washington, D.C.: U.S. Govt. Accountability Office.

Vaccani, P. (1989, May). Combining automated monitoring with a national licensing database for radio spectrum enforcement. In *Electromagnetic Compatibility, 1989. IEEE 1989 National Symposium on* (pp. 228-233). IEEE.

Wasson, G., & Humphrey, M. (2003, November). Policy and enforcement in virtual organizations. In *Proceedings of the 4th International Workshop on Grid Computing* (p. 125). IEEE Computer Society.

Weiss, M. B. H. (1991). *The standards development process: A view from political theory*. School of Library and Information Science, University of Pittsburgh.