Enforcement in Dynamic Spectrum Access Systems

Martin BH Weiss William H. Lehr Liu Cui Mohammed Altamimi

Abstract

The spectrum access rights granted by the Federal government to spectrum users come with the expectation of protection from harmful interference. As a consequence of the growth of wireless demand and services of all types, technical progress enabling smart agile radio networks, and on-going spectrum management reform, there is both a need and opportunity to use and share spectrum more intensively and dynamically. A key element of any framework for managing harmful interference is the mechanism for enforcement of those rights. Since the rights to use spectrum and to protection from harmful interference vary by band (licensed/unlicensed, legacy/newly reformed) and type of use/users (primary/secondary, overlay/underlay), it is reasonable to expect that the enforcement mechanisms may need to vary as well.

In this paper, we present a taxonomy for evaluating alternative mechanisms for enforcing interference protection for spectrum usage rights, with special attention to the potential changes that may be expected from wider deployment of Dynamic Spectrum Access (DSA) systems. Our exploration of how the design of the enforcement regime interacts with and influences the incentives of radio operators under different rights regimes and market scenarios is intended to assist in refining thinking about appropriate access rights regimes and how best to incentivize investment and growth in more efficient and valuable uses of the radio frequency spectrum.

1 INTRODUCTION

The future of wireless necessitates that we use our Radio Frequency (RF) resources more efficiently, which in turn, requires us to transition to a future in which spectrum is shared more intensively. The growing demand pressure for expanded access for legacy and new uses and the need for significant spectrum reform to enable such sharing was noted by the FCC's Spectrum Policy Task Force, was reaffirmed by the National Broadband Plan and the

President's call for an additional 500MHz of spectrum for mobile broadband, and most recently in the PCAST report on government spectrum.[1]

Realizing the future where spectrum sharing is the norm requires us to commercialize next generation radio technologies such as Cognitive Radios (CRs) and Software Defined Radios (SDRs)[2] to enable the Dynamic Spectrum Access (DSA)[3] systems needed to support higher utilization of our RF resources. These technologies enable new business models and spectrum sharing regimes that pose a host of opportunities and challenges for spectrum managers and the entire wireless ecosystem. For example, the FCC recognized the challenges posed by SDRs as early as 2000.[4] As commercial and academic interest evolved from SDRs to DSA systems, the questions first raised by the FCC in 2000 -- some of which involved enforcement -- have become more complex.

The enforcement challenges around SDRs were largely confined to ensuring compliance with radio certification requirements, but the enforcement challenges for DSA systems are more complex, including ensuring the rights of license holders under opportunistic sharing

---

[1] See FCC (2002), FCC (2010), White Houe (2010), and PCAST (2012).

[2] Cognitive Radios (CRs) and Software Defined Radios (SDRs) are often referred to together and sometimes the terms may be used interchangeably. In this paper, we will follow that practice since the distinctions are not ones we focus on here, but they do have important implications for standardization and regulatory compliance. CRs distribute decision-making functionality into the radio access network, and ultimately to the handsets – allowing them to make operational decisions, including such functionality as sensing the RF environment for spectrum white spaces, controlling frequency selection, power, or other operating parameters/modes. In contrast, SDRs are an implementation technology, implementing in software what previously would have been implemented in radio hardware. As such, SDRs are a key enabling technology for CRs. For further discussion of how SDRs and CRs are distinct yet related, see http://www.wirelessinnovation.org/Defining_CR_and_DSA or Scoville et al. (2006).

[3] DSA, like SDRs and CRs, is another term that may be interpreted narrowly or broadly. In its narrow definition, DSA refers to the use of CR/SDR and related radio technologies to enable more dynamic (in time, space, and operating modes) management of RF spectrum. Used more broadly, DSA refers to the whole class of technologies, business models, and policies that enable spectrum resources to be shared more intensively across users, uses, and locations (where "locations" refers to the full dimensionality of the RF electrospace – in time, space, waveform, etcetera). In this paper, we will use DSA in both senses. It is the need to share spectrum more broadly that provides the principal economic driver for adopting novel radio technologies like CR/SDR but it is the special regulatory enforcement challenges and opportunities associated with these new radio technologies that are the principal focus of this paper.

[4] FCC *In the Matter of: Inquiry regarding Software Defined Radios* ET Docket 00-47, March 21, 2000.

(i.e., protection from "harmful interference"[5]), “fair” spectrum sharing among secondary users, primary and secondary user conformance with contracts, and detection of “free riders.” Faulhaber (2006) noted the importance of dispute resolution and enforcement, and in particular, with regard to cognitive radios, he wrote:

> The deployment of cognitive radio promises to be a nightmare for enforcement against interference in either a property regime or a commons regime. In most cases, a licensee will have but a few neighbors in frequency or geographic space and will have no difficulty discovering who is the cause of interference and then determining if the interferer is violating her license restrictions. With cognitive radio, the interferer can show up in any frequency band, briefly (but significantly) interfere, and then disappear undetectably. Enforcing restrictions on such fast-moving opportunistic interferers is virtually impossible; widespread abuse is likely to be the result, earning this technology the sobriquet ‘‘hit and run radio’’

Herein, we argue that such a prognosis is overly alarmist and narrow in its construction of what constitutes DSA, how it might be implemented (i.e., the specific sharing regime that is anticipated and the technologies and context used to realize that sharing regime), and what that in turn implies for the DSA enforcement challenge. In Weiss and Lehr (2009) we highlighted the diversity of cooperative and non-cooperative sharing regimes that already exist or may exist with more enlightened business and regulatory policies. In this richer world of DSA, we expect there to be multiple layers of enforcement that will mutually re-enforce each other, helping to protect spectrum users from the sort of "run amok" scenario anticipated by Faulhaber, and if properly approached, heralding a much brighter future for efficiency-enhancing novel radio technologies like CR/SDRs (Chapin & Lehr, 2007b). As we shall explain, different enforcement strategies are better for different types of DSA systems.

This is not the first paper to consider enforcement in connection with DSA systems. Most notably, a series of papers by Sahai and his co-authors consider mechanisms to enforce sharing (Atia, Sahai & Saligrama, 2008; Harrison & Sahai, 2011; Tandra & Sahai, 2007, 2008; or Woyach & Sahai, 2011). As with Faulhaber’s work, Sahai’s papers are focused on opportunistic sharing enabled by cognitive radios that actively sense and respond to their local environments, and the focus of enforcement in those papers is on mechanisms that are embedded in the CR technology.

---

[5] The question of what constitutes "harmful" interference is an important question for spectrum management, and is explicit or implicitly defined by the property rights regime and its associated enforcement regime. In this paper we do not take a position on what should be the appropriate definition, and put it in quotes here to signal our recognition that this is an appropriately ambiguous and contentious term.

The emergent opportunities for spectrum sharing, however, are not limited to opportunistic sharing that depends on CRs. Instead, there is considerable commercial interest in the static spectrum holes of the TV White Spaces (TVWS) and cooperative forms of spectrum sharing, such as Mobile Virtual Network Operator (MVNO) contracts that have been a part of the mobile landscape for a number of years (Weiss, 2011). The enforcement of such regimes will depend, in part on the technology, but also importantly on the business models/practices, market conditions, and regulatory rules and institutional frameworks in which the DSA takes place. The evolution of this ecosystem will require changes in the technology, but also in business models, markets and policy frameworks – and those changes will induce feedback and learning. Experience and trust built in one mode of DSA sharing will contribute to building trust and experience for other modes; progress toward establishing business contracting norms for cooperative sharing (even in static spectrum environments) will contribute to building trust for more dynamic CR-enabled forms of sharing. Lower transaction costs for legal remedies for enforcement will complement and re-enforce CR-enabled enforcement techniques, and visa versa. Thus, we conclude it is important to consider enforcement in a broader sense with respect to DSA-based systems.

The purpose of this paper is to construct such a broader framework for evaluating enforcement under various modes of spectrum sharing. This will involve extending Faulhaber's and Sahai's work through the application of principles from the law and economics literature. We accomplish this by first discussing the general aspects of enforcement. From our analysis, we conclude that

- A single, generic enforcement regime is unlikely to emerge for DSA systems because of the large diversity of rights regimes and operational ecosystems (i.e., business, market, regulatory and technology environments);
- An enforcement regime that is adaptive and responsive to learning as these ecosystems emerge, evolve and mature is important to the ultimate success of DSA systems;

2 GENERAL ASPECTS OF ENFORCEMENT

According to Merriam-Webster, there are five definitions of "enforce" (**Enforce, 2012**). (1) to give force to, (2) to urge with energy, (3) constrain, compel, (4) obsolete, and (5) to carry out effectively. From the point of view of law and economics, enforcement makes regulation (laws, agency rules) and contracts (voluntary *ex ante* commitments governing post-contracting behavior) effective.

Indeed, as Demsetz (1964) points out, enforcement is a key component of any property rights regime. Property rights are a social construct necessitated by our desire to separate ownership and decision-making (as a consequence of economic specialization). Property rights facilitate the coordination of action across parties by specifying what usage and decision-making rights *and* responsibilities different economic actors have with respect to

goods and services exchanged in the economy. Enforcement renders the specification of property rights credible and effective.

Absent some sort of enforcement mechanism, the constraints on a firm's behavior are non-binding and thus are subject to "cheap talk" analysis (Farrell, 1996). The ultimate goal of enforcement is to induce socially optimal behavior, which may deviate from individually-optimal behavior because of externalities, mistakes, or other sources of market failures. Socially optimal behavior includes investments in protection (harm avoidance) technology and in operating behavior that results in socially desirable outcomes (which generally means behavior that is in conformance with the rules[6]). The enforcement mechanism may mandate (or proscribe) certain behaviors (e.g., safety regulations that specify construction materials, standards, or functionality) or impose rewards/sanctions that may induce incentives toward desirable behaviors or penalize undesirable behaviors or outcomes (harms).

Shavell (1993) focuses on three important aspects of any enforcement regime: (1) the timing of enforcement action (whether *ex ante* – before a potentially "harmful" action has occurred; or *ex post* – after a potentially harmful action has occurred, but potentially before or after an actual harm has been realized); (2) the form of enforcement sanctions (whether monetary or otherwise, where latter may include criminal incarceration); and (3) whether private or public enforcement (i.e., what role do private individuals play in detecting bad behaviors or harms, or in implementing sanctions and responses). Compliance with enforcement mechanisms may be voluntary (e.g. self-regulation, self-enforcement) or compulsory (e.g., enforced by the third parties). The third parties might be other market players (e.g., other firms, consumers , or market research firms) or they could be regulatory authorities (i.e., the "police"). Regulatory authorities could be an agency (e.g., FCC, NTIA), an administrative court, or a general court. Further, agency power may be delegated to an industry enforcement bureau or agency (like towing services in Washington, DC, and private security forces). The industry delegate might be an approved industry self-regulation authority, including a formal arbitration society like the AAA.[7] Hybrid approaches exist as well. For example, Braithwaite (1982) proposed "enforced self-regulation," where the goal is to force companies to internalize enforcement costs since government-based external enforcement is expensive and ineffective due to asymmetric information problems and bureaucracy costs. He argues that industry self-regulation can be enforced by government monitoring of the compliance activity by determining if it is independent, appropriately structured (i.e., has the requisite resources to complete its task, appropriate incentives), etc.

Funding of the enforcement infrastructure is yet another important question. Several methods for funding have been applied in different industries. For example, in many contexts, the enforcement action is funded from general government tax receipts (e.g., Homeland Security), while in others, industry-specific taxes or fees (e.g., license fees for

---

[6] We say "generally" because following the rules is not always socially optimal (e.g., the driver who exceeds the speed limit in a medical emergency) nor is rule-deviating behavior necessarily intentional (e.g., mistakes may be common).

[7] See http://www.adr.org/.

hunting and fishing) may be used to fund the enforcement effort. Additionally, funds collected in the form of sanctions may be used to help defray enforcement costs. For example, the Environmental Protection Agency (EPA) uses the fines it collects from violators of environmental regulations to partially fund its activities. The choice of funding source and its level have a direct impact on the effectiveness of the enforcement regime (e.g., more police results in lower crime rates, but costs more as well) and the incentives of participants to comply (e.g., excessive certification or licensing fees may deter potential participants).

An optimal enforcement mechanism is inextricably linked to the property rights regime and economic environment in which it is expected to function. The costs of inducing good behavior (avoiding bad behavior) must be balanced against the social costs and benefits under different scenarios. A critical component of those costs are the costs of the enforcement mechanism itself. For example, an important enforcement cost is associated with the collection of evidence and establishing its provenance at various stages in the process. The process needs to anticipate the challenges of detecting "bad" behaviors (i.e., behaviors that have a high probability of resulting in actual harms) or actual harms[8]; establishing liability[9]; adjudicating whatever sanctions are appropriate[10]; and then imposing those sanctions[11]. Evidence collection can be done by the market participants or by a third party (such as government). The costs of such information processing/decision-making may be significant and these costs need to be weighed with due consideration of the costs/benefits associated with the rights that the enforcement mechanism is intended to enable. Thus, when it is difficult (expensive) to detect harmful behavior or undertake the other steps required by the enforcement mechanism, it may be preferable to rely on

---

[8] The connection between behaviors deemed harmful and the actual incidence of harms is often tentative. For example, shooting a gun in public may not hit anyone; yet, we sanction such behavior and apply escalating penalties based on the nature of the crime and extent of harm that results: illegal discharge of a weapon may earn a citation, killing someone by accident a manslaughter charge, and premeditated murder a much more severe penalty.

[9] The party who engages in the bad behavior may not be the party who is deemed responsible. The company who manufacturers an unsafe product may be liable for the harm caused by a consumer using the product. The assignment of liability impacts incentives – in the product liability case, it may strengthen the incentive of manufacturers to design safe products, while at the same time, lessening the incentive of consumers to use products safely (e.g., read product safety manuals) if the consumers believe they will be absolved from any resulting harm. Apportioning liability is part of the enforcement mechanism and a key feature of the property rights regime.

[10] The regulatory process may involve multiple rounds of appeals and costly bureaucratic process to help mitigate the risk of imposing sanctions unfairly or inappropriately (e.g., Type I or II errors in the enforcement process which may fail to detect bad behavior or may label good behavior bad).

[11] Getting delinquent parents to pay child support payments or collecting parking ticket proceeds involves significant resources in *ex post* enforcement.

stronger *ex ante* rules (if the prospective harms are large) or simply tolerate the adverse effects of the bad behaviors (if the benefits of allowing more operating freedom exceed the prospects for significant social harms).

Furthermore, for *ex post* enforcement to have appropriate *ex ante* deterrence effects, the enforcement remedies must be credible. Rational actors will consider the costs of enforcement in their assessment of how likely it is that the promised remedies will actually be assigned. The need to provide for appeal procedures and other process protections to protect against abuse of the enforcement mechanism to abuse innocent parties adds to the costs of enforcement. If an agent believes the principal's enforcement costs are excessive, it will not believe the enforcement threat is credible.The participation of both the agents whose behavior the enforcement mechanism seeks to influence *and* the agents responsible for operating the enforcement mechanism (e.g., the police) needs to be incentive compatible.

The choice of how to design the enforcement mechanism directly and indirectly impacts the effectiveness of the mechanism and its costs. Moreover, these are likely to evolve over time with the market, technology, and policy.[12]

For example, the EPA used to regulate water and air quality with only a few metrics (like dissolved particles per volume); but then improvements in detection and monitoring technologies coupled with greater understanding of the relative risks from the presence of specific toxins induced a move to more complex rules that specified concentrations for specific compounds (e.g, cyanide PPM, etc.). Adoption of such rules, enabled by better monitoring technologies, induced changes throughout the environmental regulation ecosystem (better control technology, lawyers with more expertise about specific harms and technology-specific regulations and evidence rules, new monitoring infrastructures) that induced further dynamic responses. The sources of information (whether collected from the basic operating infrastructure as a byproduct of normal operations, contributed by market participants as part of mandatory or voluntary testing, or collected by third-party watch dogs) impacts how it may be used in the regulatory (enforcement) process (e.g, to target enforcement investigations, to prove liability, to monitor compliance with rules, etc.).

[12] Enforcement costs may fall as users and enforcers become more familiar with the mechanism. However, this is not always the case since dedicated criminatls may become more sophisticated in avoiding detection or the police in catching criminals – implying an arm's race. The incentives of participants to pursue such an arm's race is also something that may be considered as part of the design of the enforcement mechanism.

2.1 *EX ANTE* VS. *EX POST* ENFORCEMENT

According to Stewart (1981), *ex ante* licensing, clearance, or certification processes provide a prophylactic strategy of ensuring that unsafe technologies or processes that result in undesirable social performance are never applied. These may include a mix of mandates/proscriptions against certain behaviors or incentives (rewards/sanctions) to induce actors to adopt good (avoid bad) behaviors. Examples include limits on radio functionality (e.g., making non-software radios harder to modify *ex post* to operate illegally), unleaded fuel standards, or power limits and spectrum masks on transmitters. Good process rules and audits make it more likely that bad behavior will be detected before significant harm occurs, and when harms occur, may facilitate remediation (minimizing or compensating harms).

As noted earlier, when it is costly to detect harmful behaviors and enforce sanctions, then it may be preferrable to simply proscribe the behavior. For example, those who accept Faulhaber's assessment (cited earlier) of the potential risks from CRs and the lack of effective enforcement remedies might opt for simply precluding the certification of CRs and sanctions against vendors who sell or contribute to the sale of such devices, in the same way as gun control advocates argue against the sale of automatic weapons or armor-piercing bullets. The cost of strong *ex ante* rules is that they need to be enforceable and pose the risk of overly restricting behaviors that may be welfare enhancing (e.g., innovation). For example, a lack of clarity on what constitutes contributing to the sale of proscribed automatic weapons (e.g., who is an authorized seller/buyer?) may make the *ex ante* proscription ineffective; or, too much clarity might raise the costs of selling even legal guns to such an extent as to suppress socially-beneficial economic activity.

Often when the range of behaviors becomes more complex and the interaction between specific actions and potential harms harder to track, it is advisable to allow the actors who best understand those implications greater discretion. This is a key motivation for shifting from rate of return regulation to price cap regulation for public utilities. A shift from specific rules to incentive-based rules is one way in which such discretion may be enabled.[13] However, a shift to incentives, with reliance on sanctions/rewards that may be imposed *ex post*, confronts its own information/implementation challenges.[14]

---

[13] Regulatory forbearance offers an option for permitting greater latitude for discretion without having to formally change the rules.

[14] For example, increased discretion provides greater latitude for firms to evade regulatory controls. Analogously, permitting regulatory agencies significant latitude to engage in forebearance risks legislators losing control of the agency, which may act in ways contrary to the public interest (e.g., in

For example, *ex post* enforcement via penalties/rewards is uncertain because firms' responses to such incentives are often difficult to predict. The *ex post* enforcement remedies may include the revocation of licenses, fines, product recalls, or modifications to operating rights. The point of penalties is they impose a cost on the guilty party that induces *ex ante* behavior ("I do not park illegally because of the threat of parking tickets"). To provide an effective deterrent, the expected incidence of the penalty being imposed, taking into account the implications of imperfect enforcement (not all crimes are punished), has to be sufficiently large to offset the private benefits from undertaking the bad behavior. However, if penalties are too large, the risk of imperfect detection penalizing innocents may deter economically beneficial behavior (e.g,. investment). In the event of harm having occurred, the enforcement mechanism also has to minimize the social costs of the harm and allocate the cost burden. If the enforcement mechanism is able to sufficiently compensate the injured parties (e.g., those causing the harm pay those who suffered either in money or spectrum access preferences), thereby reducing the expected harm from the bad behavior, then the deterrence value of enforcement is less. When the harm is excessive congestion ("pollution") with negative effects that are diffuse (i.e., cause a small harm to a large number of users, resulting in a large aggregate harm), while the benefits of the bad behavior (i.e., excessive consumption of resources) are realized by the individual undertaking the behavior then the transaction costs associated with compensating all of those harmed (and thus rendering the harm "reversible") is likely to be large and *ex ante* deterrence becomes more important. There may also be rewards (the mirror images of these sanctions) for good behaviors. Because some of the costs of *ex post* enforcement are contingent, computing the prospective costs of enforcement is inherently uncertain.[15]

The *ex ante* and *ex post* enforcement effects are inextricably linked. For example, if the *ex ante* rules and processes are sufficiently strong then *ex post* harms may be prevented before they occur. Also, certain types of *ex ante* rules may be easier to monitor and hence lower the cost of enforcement. Even strong *ex ante* rules may require *ex post* enforcement; for example, licensing approval for equipment is usually based on a prototype or pre-production unit, but compliance of production units may require some kind of policing to ensure compliance.

---

failing to prosecute violators of environmental regulations that the public and its legislators have deemed worthy of enforcement).

[15] For example, large sanctions may successfully deter bad behavior, and consequently, never be imposed. As the probability of imposing a sanction decreases, its ability to induce good behavior may also decline. For example, catastrophic failures are difficult to provision for since they are, by design, rare events, and their rarity may depend on behaviors that are hard to enforce (e.g., maintaining adequate redundant capacity).

2.2 CENTRALIZED VS. DECENTRALIZED ENFORCEMENT

In general, the enforcement can be centralized or decentralized, or more generally, a mix of both. The classic form of centralized enforcement relies on a regulator such as the FCC or NTIA, but could be undertaken by a spectrum sharing broker or band manager (i.e., a New York Stock Exchange for spectrum management). Decentralized enforcement mechanisms might include other radios in the environment that might, for example, refuse to forward packets or connect to radios that are behaving badly (e.g, as implemented in a mesh protocol); or might rely on rights holders pursuing tort or trespass claims against alleged infringers.

Both centralized and decentralized enforcement mechanisms may include technical, market, and institutional components. For example, a beaconing signal with information about the availability of spectrum holes or other operating instructions or a database system (for managing access to TV white spaces) may be employed as centralized technical enforcement components; while radio "black boxes" or collaborative sensing (Weiss et al, 2010) might be employed as elements in decentralized enforcement mechanisms. The centralized or decentralized enforcement might rely on reputation effects (are the radios likely to interact over time, and if so, are they identifiable for purposes of assigning reputations to specific radios or operators?).

The data collected or behaviors managed by such technical elements would contribute to the evidentiary basis for any enforcement adjudication process (e.g., statistically significant measurement of proscribed transmission behavior may be used to assign liability in a civil torts claim). The viability of this depends on the radio modes of operation and the property rights regime in force. For example, is the alleged offender a "hit-and-run" situation like that anticipated by Faulhaber's mobile CR or a fixed location radio that may be dynamically selecting operating frequencies? Or, is the standard for bringing a harm claim based on the ability of the plaintiff to demonstrate an economic harm or merely detect the existence of transmission energy in the rights space of the plaintiff? In the former case, the need to prove an economic harm would likely imply a higher enforcement cost than the need to simply prove the existence of transmissions, although focusing on economic harm is closer to the efficiency goal for spectrum management.[16]

[16] As noted earlier, full consideration of what an appropriate definition of harmful interference should be is beyond the scope of this paper. For some further discussion of possible approaches to this, see for example, de Vries (2010) or de Vries & Sieh (2012).

Radio "black boxes" are an especially interesting enforcement mechanism.[17] Like the "black boxes" on airplanes that are used for forensic crash analysis, it would be feasible to include similar elements in radio devices to assist in forensic analysis of radio behaviors. This would provide a credible and potentially light-weight mechanism for auditing radio behaviors. A mix of black boxes and the ability to audit database registration information can be combined to flexibly mix centralized and decentralized control mechanisms. Radios might be required to register their location and operating requirements with a database (or databases), and operating rights might be granted with time-limited-leases that have to be renewed (Chapin & Lehr, 2007b). The PCAST (2012) report advocates using such mechanisms, especially database registration with time-limited authorizations, as important enforcement mechanisms for sharing in government spectrum bands, but as PCAST (2012) notes, experience learned there will benefit all spectrum users in all bands.

The ability to credibly track radio behavior is obviously valuable for provisioning (forecasting capacity needs) as well as real-time operation (identifying spectrum white space), and the benefits of those activities might be sufficient to warrant adoption of a database approach in its own right. However, the ability to support forensic accounting contributes to the enforcement function. It helps reduce enforcement transaction costs, and thereby, improves the credibility of enforcement. Potential offenders may face a higher expectation that they will be detected and prosecuted, and innocents may have less fear of unfair prosecution. As PCAST (2012) and users of airplane "black boxes" recognize, unrestricted access to the audit trail of behavior poses a threat to privacy and confidentiality.[18] To address these challenges as well as to secure the databases and other spectrum management infrastructure sufficiently to ensure its reliability (e.g, protect it against attacks), access to the management infrastructure, including the databases, needs to be authorized.

Another focus for decentralized enforcement involves advances in spectrum sharing policy language research. A “policy language” is a selection of facts specifying spectrum sharing rules and procedures. A "policy reasoner" within the CR uses the information about allowed policies and various environment data (e.g., location, real-time RF sensing data, etc.) to make predictable decisions about its operating behavior, allowing the CR to adapt in real-time. The formalization of these design elements involves a significant amount of industry

[17] The authors would like to especially acknowledge John Chapin for first calling to our attention this idea and for helpful discussions on this and other elements of the enforcement challenge.

[18] The privacy concerns are a special concern in government spectrum sharing because of the many uses of the RF for national defense and security applications.

standardization.[19] The IEEE Standards Coordinating Committee 41 (SCC41) is currently engaged in standards projects in the areas of DSA, CRs, interference management, coordination of wireless systems, advanced spectrum management, and policy languages for next generation radio systems. The 1900.x working groups are part of SCC41 (IEEE, 2008). For example, IEEE 1900.5 Working Group is focusing on policy language and policy architectures for managing CR for DSA applications.

While policy language-based CR approaches hold great promise, they need to be nested within an enforcement ecosystem that ensures compliance with the rules and supplements the detection and enforcement adjudication process with complementary mechanisms. For example, policy-smart CRs are often unhelpful in dealing with rogue transmitters.

The level of involvement of either centralized or decentralized enforcement will vary based on the type of sharing environment (e.g. static, periodic or stochastic), transparency and clarity of spectrum rights, and the range of technical mechanisms that are available. Generally, the best solution will include a mix of centralized and decentralized technical and non-technical mechanisms for enforcing compliance with the sharing regime.

3 ENFORCEMENT IN DSA SYSTEMS

A principal goal of spectrum management is to prevent harmful interference. From an economics perspective, interference is harmful when it impedes the ability of the party holding usage rights to fully exploit the RF electrospace in question (Vany et al., 1969; Matheson, 2006). In practical terms, interference results in system capacity reductions, which can result in system malfunctions which may translate into lost profits. In some systems, such as public safety communications systems, interference can have life-and-death consequences.

Interference is experienced at the receiver when the receiver seeks to decode signals intended for it. Signals from other transmitters may appear as noise, limiting the ability of the receiver to perform its function. A perfect receiver could use any of the dimensions of electrospace (location, frequency, angle, time, code, etc.) to disentangle the signals, but real world limitations require transmissions to be separated in electrospace. Better technologies for transmitters and receivers, and for the radio and other networks in which they are embedded, can support higher utilization of the electrospace as a whole.

Traditionally, interference is classified as in-band interference and out-of-band interference. In-band interference is mainly due to other systems' electronic emissions, and out-of-band

[19] Industry standards are a mechanism for coordinating the decentralized behavior of multiple market actors.

interference is partially due to receiver sensitivity. From an enforcement perspective, what determines whether there is or is not harmful interference is a function of what the property rights regime is. For example, under some interpretations of exclusively-licensed spectrum, the licensee (primary user) has a right to exclude other users/uses from the spectrum. This interpretation is analogous to the law of trespass in real property, which protects the property-owner from unauthorized use of the property by others. Even in real estate, the existence of easements, zoning restrictions, and a diversity of remedies to enforce real estate property rights[20] attest to the limitations on the exclusion right; similarly, provisions for secondary use by Ultrawideband (UWB), Part 15, or TVWS devices in different bands might overlay and potentially conflict with incumbent primary licensed claims.

In contrast, the traditional view of unlicensed use, as it occurs under Part 15 rules and in the ISM bands used by cordless telephones, microwave ovens, and WiFi devices, requires the devices to conform with power and other operating protocol restrictions, and to tolerate interference from other devices. The Part 15 devices have no property right to exclude other conforming devices, but they do have an implicit right to interference protection. The design of the rules is such that operators may form reasonable expectations of interference.

Traditionally interference is managed *ex ante* in wireless systems through a combination of transmitter specifications, receiver specifications and white spaces. Transmitter specifications include "emission masks" which indicate how signal energy may be transmitted in frequency and antenna parameters, including type and height. Together, these transmitter specifications can be used to predict, with high likelihood, the electrospace the signal/service will occupy. Receiver specifications include factors such as bandwidth and sensitivity that, together with transmitter specifications, are useful in predicting the performance of a wireless communications system. White spaces are a generic term for gaps in time, space and frequency between adjacent blocks of electrospace to prevent interference.

Traditional approaches to enforcement largely assume fixed transmitters. Because they are fixed, the cost of *ex post* enforcement is relatively low and the *ex ante* measures are relatively easy to write. When systems become mobile, the locus of the transmitter is uncertain, making *ex ante* measures based on transmitter specifications less successful in avoiding interference (willful or not).

---

[20] For example, a tort claim for damages associated with trespass may be limited to the economic harm realized. The injured party may also seek injunctive relief against the trespasser which might induce police enforcement of the rights. Grants of public rights of way and other zoning restrictions may constrain trespass claims.

Traditionally, the *ex ante* parameters are designed into the hardware of the transmitters and receivers. These then undergo acceptance testing to ensure compliance with the regulations before they are used. After being in operation, the components used in transmitters and receivers may change due to age, heat and other environmental factors, which cause the transmitters and receivers to perform in unexpected (illegal) ways, which may cause interference with adjacent electrospace. Engineers may also deliberately alter these components to commercially benefit the owner of the transmitter, which may also cause interference. These potential outcomes (and others as well, such as rogue transmitters) raise the need for *ex post* enforcement.

When interference occurs, the FCC's Enforcement Bureau is expected to investigate and adjudicate. This often involves bringing the offending transmitter back into compliance, but can require spectrum monitoring to gather data to support an action. In practice, as Sandvig (2011) indicates in his case studies, interference mitigation may be more informal and may involve direct or mediated interaction between the interfered party and the offender.

From the perspective of enforcement, there are two general types of enforcement actions that are needed: enforcement associated with "everyday" use and enforcement associated with rogue radios (either deliberate bad actors or malfunctioning radios). Enforcement of the first kind is more often associated with events such as spurious interference due to rare RF propagation irregularies, equipment de-tuning or production faults, and other largely unintentional interference. This includes reconciling interference disputes when property rights are unclear (e.g., a "legal" transmitter causes interference for a "legal" receiver). In contrast, enforcement of the second kind is associated with attacks, deliberate acts, or severly malfunctioning radios. We focus on the former kind, which is associated with "normal" system operations rather than unpredicable "rogue" events where the goals and modality are unpredictable.

To highlight this, we consider the analogy of traffic laws and enforcement. In managing traffic, society has constructed a collection of *ex ante* rules (e.g., traffic flows on the right or left but not both, speed limits, etc.). Some of these rules require less enforcement (e.g. locus of traffic flow) and others require more (e.g., speed limits) in order to prevent these rules from being merely benign advice (i.e., cheap talk). In the case of the latter, society uses a mix of fixed speed cameras and mobile police; of these, speed cameras are more suitable for routine enforcement whereas the latter are better suited for special circumstances (e.g., traffic congestion, construction, weather emergencies, etc.). This also highlights a tradeoff between enforcement precision and cost, with speed cameras being non-adaptive to circumstances but relatively cheap and police officers being highly adaptive (and precise) but expensive.

Moreover, these different enforcement "technologies" complement and alter the optimal mode of operation of each. Police are *ex ante* and *ex post* – they act to detect bad acts

(before harm happens – by giving citations for cars with illegal brake lights or for driving too fast, even if not unsafely – and they have discretion); their presence provides assurance of enforcement so deters bad behavior just by being there; and they enforce *ex post* when harm has happened – by assessing liability in accidents, penalizing unsafe driving with stronger tickets, and by testifying in court. The police behave differently in a world with cameras; that is, they know where traffic is most likely to require their oversight, know what evidence they need to establish at the scene vs. what is recorded remotely. Traffic laws can also change with technology. For example one can image a "speed pass" that allows different vehicles to travel at different speeds based on some criteria (e.g., *ex ante* driver skill certification), variable charging for use of HOV lanes during congestion periods, or modifications to car operation in response to car/road real-time diagnostics (e.g., detection of low tire pressure and bad road conditions).

3.1 IMPLICATIONS OF CR, SDR, AND DSA FOR ENFORCEMENT

The enforcement challenges and practices noted above are not new and existed before the invention of SDRs, CRs, and the other technologies that enable DSA. The need to secure critical infrastructures like electronic communications capabilities against attacks by hostiles and to ensure appropriate quality of service has always been important. However the move to DSA has important implications for the entire wireless ecosystem, and in particular for the enforcement challenge.

On the one hand, the transition to DSA exacerbates the interference enforcement challenge. First, by enabling more intensive use of the electrospace, DSA increases the likelihood of interference harms occurring. With more radios, users, and uses sharing the electrospace, there are many more opportunities for the signals to interfere. Traditional approaches to limiting this are threatened by the desire to treat white spaces (in geography, time, frequency, or code space) that had previously been part of guard bands as opportunities for additional spectrum use.

Second, DSA enhances the dynamic flexibility of radios, allowing them to be more mobile. SDR and CR technologies raise the potential of "hit-and-run" operation – but whether this is a significant threat (as posited by Faulhaber, 2006) or just something we have to deal with is an interesting question. Mobility certainly raises issues for detection and reputation-based enforcement incentives.

On the other hand, DSA can alleviate many enforcement concerns. By enabling increased utilization of scarce RF, DSA helps reduce the costs of scarcity. This includes facilitating the growth in wireless and the attendant opportunities for smart infrastructure, green technologies, smart healthcare, and all of the other market opportunities that might otherwise be precluded from emerging without expanded access to spectrum resources. The desire to enable such growth and the potential benefits it promises for overall economic

productivity and innovation are key motivators behind the National Broadband Plan (FCC, 2010) and the White House's call for an additional 500MHz of spectrum for mobile broadband (White House, 2010). The potential harms from increased interference for legacy uses and old radio technologies needs to be balanced against the potential gains from allowing the new uses. As the potential for unrealized benefits rises, the balance tilts away from excessive caution in protecting against interference harms.

Moreover, DSA and other new radio technologies contribute to making radio systems more robust to interference. Radios capable of multiple operating modes can switch radio modes to avoid interference, just as today's mobile broadband services offload data traffic from cellular networks (where capacity is scarce) to WiFi (where capacity is relatively plentiful) when feasible. With DSA the technical options for switching are greatly expanded. Abuse of this flexibility could result in "hit and run" operations that would be hard to control and might allow bad actors to more easily circumvent radio rules. For example, SDRs were originally perceived to raise enforcement risks because they could be altered post certification by updating the software, and because of the increased range of operating modes, and therefore posed a more complex/difficult challenge for certification (of safe use). However, hardware radios can also be altered post-manufacture (even if that is potentially a bit more difficult) and suitable technical controls on how software radio updates are managed can help address the challenges of post-certification modifications.

While DSA embeds functionality that poses additional enforcement challenges, it also offers new tools for technical enforcement. Distributed intelligence to the radios means that the radios are increasingly capable of participating in intelligent and dynamic automated enforcement mechanisms. Through protocols, policy-based language frameworks, and other tools, the radio systems ability to technically manage its compliance with sharing protocols has been enhanced. Responses like database registrations (PCAST, 2012), time-limited-leases (Chapin & Lehr, 2007b), and protocol-based identification schemes (Atia, Sahai, & Saligrama, 2008) offer mechanisms for addressing these challenges. Most of the technical literature cited earlier on CR/SDR and DSA enforcement addresses such technical remedies.

However, the enforcement challenge does not depend solely on the technical remedies. Institutional remedies that include the risk of legal prosecution complement and interact with the technical remedies (like the highway cameras noted earlier). Informed automobile drivers know that their mileage would be enhanced if they disabled pollution control devices like catalytic converters, and some drivers do precisely that, however most drivers obey the laws. Whether drivers obey the regulations designed to limit car pollution because of their concern for the environment, fear of legal prosecution, or lack of expertise in effecting the necessary device modifications matters less than the fact that all of these motivations are part of the overall enforcement ecosystem.

With respect to the other general features of enforcement mechanisms, it is at present unclear how the transition to DSA might tip the system. For example, in the choice between *ex ante* versus *ex post* enforcement or centralized versus decentralized enforcement, arguments may be made in both directions. On the one hand, DSA radios are more complex and capable of more local decision-making, which generically inclines one toward allowing increased discretion and potentially toward increased reliance on *ex post* enforcement. It also allows more intelligence and hence control of functionality to be distributed, which would seem to favor decentralized enforcement. On the other hand, the mobility of DSA radios poses significant challenges for detection of potential harms that may render *ex post* enforcement overly expensive and hence ineffective. Or, the ability to communicate with a central operator may render DSA radios more amenable to centralized control (e.g., if control is via a beaconing system). But this is a naïve interpretation. Surely the right response is for modifications to *both ex post* and *ex ante* enforcement. Progress in the design of secure software systems and policy-language CRs can help make certification easier (facilitating control of proscribed behaviors); progress with technologies like collaborative sensing and radio identification schemas may help reduce the detection burden (facilitating operational control and forensic analysis); and new institutional frameworks or property rights regimes can help provide structured (band-specific) enforcement regimes.

In the next sub-section, we consider the diversity of property regimes that already exist and may be expected to continue to exist to enable the many types of spectrum sharing and DSA that are likely to be needed.

3.2 DSA, PROPERTY RIGHTS, AND ENFORCEMENT

Early in the discussion of spectrum management reform, a number of analysts focused on the binary choice between licensed and unlicensed spectrum – identifying the former with "property rights" (which was short for "private property rights," most often analogized to real estate) and the latter with "commons" (where no one had a private property right).[21] While this syllogism proved useful in clarifying thinking, it is overly simplistic and has lead to confusion or silly "yes/no" debates about whether all spectrum should be exclusive licensed or unlicensed. Today, policymakers generally recognize the need for multiple regimes, and the potential for hierarchies of rights. As discussed earlier, exclusively licensed spectrum encompasses a diversity of regimes: PCS licensees have different rights and obligations than do 700MHz licensees or TV broadcast stations. Additionally, users in a commons regime are subject to protocol restrictions and norms that govern use. In the end, we need to recognize that all property rights regimes imply a mix of rights and obligations for users. Following Demsetz (1967):

[21] See, for example, Faulhaber & Farber (2002) or Hazlett (2001).

> "In the world of Robinson Crusoe property rights play no role. Property rights are an instrument of society and derive their significance from the fact that they help a man form those expectations which he can reasonably hold in his dealings with others. These expectations find expression in the laws, customs, and mores of a society. An owner of property rights possesses the consent of fellowmen to allow him to act in particular ways. An owner expects the community to prevent others from interfering with his actions, provided that these actions are not prohibited in the specifications of his rights."

This quote applies equally well to private and commons property, and any other property rights regime one might anticipate – and moreover, that sort of generality is helpful.

Peha (2009), Buddhikot (2007), Weiss and Lehr (2009) among others have shown that "DSA" is not a single technology but a cluster of technologies. Spectrum sharing regimes are allocations of usage rights over the electrospace. Because the usage of an electrospace may result in incidental or deliberate interference, enforcement seeks to ensure compliance with the usage rights regime. It stands to reason, then, that different sharing modes (i.e., rights regimes) suggest different enforcement mechanisms. Weiss and Lehr (2009) proposed a taxonomy of the principle sharing modes for DSA; see Table 1.

Table 1 - Taxonomy of generic DSA approches

	Non-Cooperative	Cooperative
Primary	Unlicensed, WiFi	Secondary markets (spectrum license trading)
Secondary	Easements, Opportunistic use, TV White Spaces, UWB	MVNO, secondary use (negotiated)

The distinction between non-cooperative and cooperative sharing focuses on the presence (or absence) of explicit coordination over usage; while the distinction between primary and secondary delineates a partial hierarchy in interference protection rights. Primary users have a prior claim to interference protection from secondary users, who generally are presumed to be allowed to operate only as long as they do not cause harmful interference to the primary user, where what constitutes harmful interference may be determined exogenously by the sharing regime (non-cooperatively) or endogenously by the parties sharing the spectrum (cooperative). The entries in the table provide illustrative examples (but are hardly exhaustive) of different DSA-enabled sharing instances.

In non-cooperative, primary sharing, each spectrum user has similar usage rights. Most unlicensed approaches fall into this category. While these systems may use a form of spectrum etiquette (Satapathy & Peha, 1997; Raychaudhuri & Xianpeng, 2003) this is less an explicit coordination than it is an algorithm for synchronizing usage as peers among similar kinds of users. The use of a shared etiquette is not a requirement for using unlicensed bands but may be an interoperability requirement for some kinds of systems (e.g., IEEE 802.11-based WLANs)

Non-cooperative secondary sharing involves a hierarchy of rights, with the license holder having dominant rights and the sharer having subordinate rights. The subordinate rights are typically granted by the regulatory agency (as is the case in the FCC's TV White Spaces policies) and require that the sharer operate without causing interference to the licenseholder. There is no explicit coordination between the license holder and the sharer, hence the "non-cooperative" designation.

In contrast, cooperative secondary sharing involves explicit agreements between the license holder and the sharer (also called the primary and secondary users). A classic example of cooperative secondary sharing is the Mobile Virtual Network Operator (MVNO) agreement, in which a primary and secondary user negotiate a spectrum sharing arrangement that is contractually specified. In these agreements, the secondary user typically uses *virtual* capacity rather than physically sharing regions of electrospace; thus, the secondary user takes advantage of the primary user's infrastructure. But it is equally possible for parties to enter into an agreement in which electrospace is shared through explicit coordination, as was studied by Tonmukayakul and Weiss (2008).

Clearly, each of these sharing modes imply different rights schema. Since we are focusing on sharing in DSA, the distinction between ownership and usage rights of the spectrum must be observed. Further, the set of enforcement strategies must be clear about which right should be enforced and how. For the purposes of this research, we will focus on the enforcement of *usage* rights, not ownership rights.[22]

Just as clearly, each of these sharing modes implies a different enforcement regime. The requirements of cooperative regimes depend heavily on the specific concerns and priorities

[22] A key motivation for adopting property rights systems discussed by Demsetz (1964) is to enable markets to better take account of what are sometimes referred to as "externalities" but he prefers to refer to as "side effects." The property rights allow potential users to understand what it is they own and that facilitates the transfer of those property rights, and in so doing, to allow appropriate interpretation by market participants of the price signals from transactions for those rights. The usage of property rights and their ownership/transfer are obviously related, but there are a whole set of other rules/regulations that may govern how the property rights may be transferred and what that may imply for enforcement that are beyond the scope of this paper.

of the sharing parties; for example, a spectrum owner who has a highly sensitive application may be particularly keen on ensuring that very little energy “spillover” occurs outside the shared electrospace, and would find it worthwhile to invest in enforcement mechanisms that ensure this. Other agreements might be focused more on measuring usage and associating remuneration accordingly. At a high-level, enforcement in cooperative sharing regimes looks like a contracting regime where the parties may negotiate arbitrarily complex terms to constrain their behavior. At one extreme, we might view cooperative sharing as equivalent to exclusive control of the spectrum assets. For example, one might view a mobile operators management of spectrum sharing across multiple (potentially discontiguous) spectrum bands via LTE as an extreme form of cooperative spectrum sharing. Negotiated sharing between LTE operators for co-primary or primary/secondary access all have great potential to realize the benefits of DSA and the increased resource use it promises.

The cooperative sharing/contracting perspective allows the parties to custom-design their enforcement mechanisms to a great extent, and in so doing, leverage the substantial institutional structure for legal enforcement of contracts and spectrum licenses. Private negotiated contracts might provide for third-party monitoring, escrow accounts, binding arbitration for dispute resolution, private police, as well as a host of technical remedies that might be more difficult to impose on non-cooperative sharing environments. For example, cooperating parties might be willing to share detailed operating plans and data to allow higher utilization sharing, or comply with specific resource allocation protocols that tightly regulate each party's access. Ideally, such cooperative sharing might aspire to the ideal of the Coasian bargaining solution.

While these are very interesting it is difficult to speculate about what might be optimal from an enforcement perspective without considering the specific case. Thus, in the balance of this paper, we shall pay more attention to the enforcement challenge in non-cooperative situations. However, we emphasize once again that the broader consideration of the enforcement challenge is necessary since what we adopt in the way of infrastructure for enforcement and learn in non-cooperative or cooperative situations will be mutually beneficial. We expect the two types of regimes to complement and interact with each other over times. In some cases, we might expect applications to emerge first in non-cooperative regimes and then seek to move to cooperative regimes once sufficient experience and activity demonstrates that the further customization of the enforcement regime offered by cooperative sharing is warranted. Alternatively, we might expect certain DSA capabilities to be developed first in cooperative regimes where the added flexibility to provide for enforcement and internalize potential harms (externalities) provides additional comfort against bad outcomes.

3.3 ENFORCEMENT IN DIFFERENT DSA ENVIRONMENTS

As should be clear from the above, the key element of any framework for managing harmful interference[23] is the mechanism for enforcement of usage rights, regardless of how those rights were obtained. The rights to use spectrum and to protection from harmful interference vary by band (licensed/unlicensed), type of users (primary/secondary, overlay/underlay) and type of use (fixed/mobile).

The general enforcement framework described above suggests a combination of *ex ante* and *ex post* measures that balance the cost of enforcement with the needed precision. *Ex ante* mechanisms deter undesirable behavior while *ex post* mechanisms remediate the consequences of that behavior.

Table 2- Varieties of DSA enforcement environments

	Non-Subordinate Rights		Subordinate Rights	
	Exclusive use	**Shared Use**	**Exclusive Use**	**Shared Use**
Fixed	Broadcasting, radars, point-to-point wireless systems	Wireless LAN, unlicensed band sharing	Inter-agency spectrum sharing (federal)	Fixed TV White Space devices
Mobile	CMRS, public safety		Federal-commercial spectrum sharing (e.g., 1755-1850 MHz)	General cogntive radio systems

In the table, the term "fixed" refers to the transmitter location. In general, enforcement of fixed usage rights is easier (cheaper) because the position of the transmitter is known. When transmitters might be mobile, usage rights might be based on the "worst case" transmitter location; such an approach to defining the rights minimizes interference at the cost of spectrum efficiency. The notion of subordination of rights reflects whether the use is as a "primary" (non-subordinate) or "secondary" (subordinate). PCAST (2012) suggests even richer hierarchies of rights – where in addition to secondary rights holders, there might be tertiary rights holds holders who could operate only if such operation would not interfere with either primary or secondary users. In that construction, the secondary users of

[23] Note that interference need not be harmful; for example, Weiss and Cui (2012) proposed a framework for trading interference rights and Ofcom's Spectrum Usage Rights (SURs) allow bargaining over interference as well (Cave & Webb, 2012). Note also that IEEE-USA has called for a revised definition of harmful interference (http://www.ieeeusa.org/policy/whitepapers/IEEEUSAWP-HarmfulInterference0712.pdf, retrieved on 10 August 2012).

government spectrum might be afforded a level of predictable spectrum access (for a price) that might be more conduscive to investing in use of such spectrum, while still preserving the option for unlicensed access when that is not inconsistent with the primary and secondary users' needs. In this model, the secondary use looks more like a form of cooperative sharing arrangement (based on a contractual arrangement) and the tertiary use is non-cooperative. The regimes may be mixed in such ways to facilitate sharing.

From the point of view of enforcement, the existence of subordinate rights makes it more difficult to determine legitimate use. In cases of subordinate rights, enforcement must consider the behavior of the licensee as well as the owner of the secondary usage rights, as either party could be subject to an enfocement proceeding. Finally, shared use might involve multiple rights holders with symmetric rights (e.g., co-primary, co-secondary, etc.) in an electrospace. Such users may rely on a mix of explicit coordination (e.g., via a beaconing channel that could assign time or frequency slots to manage access) or via a protocol or spectrum etiquette (e.g., analogous to contention based traffic management like the slow start mechanism in TCP). These technical solutions may be augmented by non-technical incentive based arrangements, such as a dispute resolution framework to resolve disputes over what constitutes "legal" usage when rights are ambiguous. It is not the case that clarifying the rights to make them more extensive and rigid (bright line) is always the preferred solution.[24]

However, unclear rights assignments coupled to cumbersome dispute resolution mechanisms results in an unpredictable and costly enforcement mechanism. An advantage of SDR/CRs is that they have the technical capacity to include much more complicated sets of rules and ensure more predictable performance if the CR reasoning functionality can be sufficiently secured – however, with the increased complexity comes the added challenge of trying to anticipate all possible operating modes. The difficulty of doing that *ex ante* is a common problem of any complex system, and is not unique to DSA or software systems. When it is not possible to anticipate all possible bad-behavior scenarios, then the emphasis needs to shift from *ex ante* to *ex post* remediation: accept that problems will occur and work on technologies that detect and correct behaviors sooner to minimize harms. PCAST (2012) recognizes the importance of building trust in sharing regimes with government users and devotes an entire appendix to discussing the requirements of a dispute resolution

[24] Clear property rights and dispute resolution are both complements and substitutes. Clearer property rights might render dispute resolution easier; but if dispute resolution is very light-weight and easy then it may be better to have loose property rights. The assignment of property rights can influence this choice. Thus, Part 15 rules simply say that Part 15 devices have no claim for interference protection which essentially eliminates the dispute resolution process altogether. Alternatively, a simple parking ticket system may tolerate a high degree of illegal parking which is socially optimal, and in the margin, may approach the performance of peak pricing regimes.

mechanism. According to PCAST (2012), such a mechanism needs to be dependable, timely, and efficient.

3.3.1 COST OF ENFORCEMENT

As noted above, Smith (2002) examines the tradeoff between enforcement cost and precision with respect to instutional arrangements that obtain. In general, enforcement becomes more costly as transmitters become mobile and the structure of usage rights becomes more complex. Although discussing "precision" at some length, Smith does not offer a succinct definition. Instead he discusses the attributes of precision, which include:

- "Precision of property rights seems intuitive but really stands for a cluster of related components, making precision itself a bundle of measurable properties but not measurable itself"
- "Rights are precise or specified to the extent that they protect attributes by preventing a range of unauthorized actions."
- "Precision here is an index that blends the distinguishing of attributes from one another and the distinguishing of levels of attributes from each other."

Thus precision is about the ability to exclude unauthorized or undesireable users and uses to a more or less fine degree. He goes on to illustrate these notions by considering (i) a jointly owned taxi cab and (ii) a fence around property. In the first case, Smith makes the case that the sharing agreement is more precise "when the benefits in loss prevention make it worthwhile" (e.g., gasoline usage or tire wear and tear). Costs that are coslty to measure or attribute (e.g., upholstery wear and tear) are defined less precisely and become a shared cost. In the second case, a fence around a property is a measure that prevents stealing of crops by virtue of blocking entry, but only imprecisely so because it also prevents a variety of behaviors that do not involve theft and might be otherwise benign. Increased precision could be obtained by employing a person to monitor boundary crossings and differentiate between malicious and benign uses, clearly at higher cost.

In radio spectrum, more precise enforcement differentiates legitimate users and uses from illegitimate ones. The complexity (hence cost) of this task depends on some attributes of the system itself. Following Smith, the maximum practical cost of enforcement is closely linked to the value of the resource: as the resource becomes more valuable, the more worthwhile it is to invest in precise enforcement.

If the cost of the needed precision is above the value of the resource, then the cost of bad behavior rationally becomes a common cost (roughly analogous to the cost of wear and tear on upholstery in the shared taxi example given above). In cooperative sharing, this common cost is a matter of negotiation and would presumably be allocated via Coasian bargaining.

In non-cooperative sharing, the problem of common costs is more difficult. Let us begin with the case of non-cooperative secondary sharing. In this case, the secondary users' usage

rights are subordinate to the primary users. Thus, secondary users must cede their usage rights to the license holder according to some algorithm, which may be determined by a third party (e.g., a regulator, standards organization) or through some other process (e.g., bargaining, interference rights). One such algorithm is that the secondary user abandons the channel as soon as the primary user begins transmitting. This case is typified by cognitive radio networks and TV whitespaces.

Let us now consider the enforcement-related factors of this case. *Ex ante*, primary and secondary users would understand the rights hierarchy and usage transfer algorithm; the equipment certification process could ensure that the users' equipment behaved according to those rules in some pre-defined test sequences. *Ex post* monitoring of primary users is generally a part of the secondary users' pre-existing system (since they must execute the channel vacation algorithm). Generally speaking, primary users would have an incentive to monitor secondary users' compliance with the channel vacation algorithm, since failure to do so could cause interference and could build evidence for future interference damage claims.

Ideally, the enforcement regime should be sufficiently precise to at least allow the identification of the user who is not in full compliance, and, better still, the particular radio whose behavior is non-compliant (assuming that a "user" may have more than one radio). The cost of achieving this precision depends on many technical factors, such as the power of the radio being used and the air interface being used: lower power systems may be more difficult to detect than higher power systems, and spread spectrum systems are much more difficult to detect than narrowband systems.[25]

The costs of enforcement may be partially recovered from the sharing parties and partially from third parties. For example, unlicensed devices might be subject to a certification or licensing fee per device, collected at the time of manufacture, which might be easier than trying to recover enforcement-related costs from usage-related fees, which in any case, would be counter to the basic idea of unlicensed (generally, free) access. In contrast, we might suspect that primary users might have an incentive to monitor the behavior of secondary users to ensure compliance on their own, and presumably, they might be required to pay for the superior interference protection implicit in their primary access usage rights. A portion of any proceeds received for the primary access (whether via auction, spectrum usage fees, or royalty charges) should be allocated to recovering the costs of enforcement.

[25] Difficulty of detection and immunity to jamming were among the prinicple reasons why the military invested in the development of spread spectrum technology in the first place.

3.4 DSA ENFORCEMENT AND EVOLUTION

As we discussed above, DSA is not a single regime, but a complex array of regimes, spanning a continuum from command & control to exclusive-use licensed to unlicensed, and a variations of models in between. We also argued that each regime implied different rights and enforcement regime. A final aspect is that *any* DSA regime is best described as nascent in the sense that:

- The technologies used by operators are still being developed. There are early examples of these systems or system components (e.g., white space devices, cognitive radios, spectrum databases) and standards are emerging (e.g., IEEE P1900.x), but virtually no engineer believes that future devices will operate as today's devices do.
- The institutional arrangements between stakeholders are still emerging. Good regulatory approaches for the array of spectrum sharing technologies (even ones that have not yet been thought of) have still to be developed and analyzed.

Even were we to favor a less complex set of regimes (say a few instead of the many we have today), we must recognize that spectrum reform takes a long time with a clockspeed that greatly lags technology and market developments. Indeed, the fact that the current regime is so out-of-step with current technical capabilities (DSA) and market needs (mobile broadband growth) is a principal driver for reform and the motivation to move to DSA models that enable higher-utilization and sharing of scarce spectrum resources. In the present context, what this means is that we perforce must live with a range of management regimes – legacy licenses and usage rights assignments overlap in time and market space with new reforms. The notion that we might transform overnight from the mix of legacy and new approaches we have today to a clean slate of a new and improved management regime is unrealistic. This is not to diminish arguments for more substantive reform, but only to suggest the small likelihood that they will be realized in fact. The reality seems to be that change will be slower and more incremental than reform advocates might like.

Thus, evolutionary change that allows for experimentation and learning may actually be the optimal approach. Moving from legacy spectrum management models to a world that embraces sharing and DSA as the norm requires a paradigm shift – it is *not* an incremental change involving a few adjustments at the edges. Moreover, the requisite changes are *not* solely technical but require the co-evolution of business models, markets, and policy frameworks. Moving this ecosystem of spectrum technologies, uses, and users to the new paradigm will involve complex dynamics, and is more of a search problem than an optimization problem. We will learn as we evolve to vibrant markets for DSA. While we may hypothesize what models of sharing spectrum may be best for which users/uses and what

technologies will be most successful for realizing those market opportunities, we simply do not know at this stage in the evolution to DSA.

The diversity of regimes provides us ample opportunity to experiment. The notion that we need to enable the potential for multiple regimes does not imply that we expect all of those regimes to be successful in the real world. However, enabling the diversity provides the opportunity for market actors to experiment and learn. The learning will be cumulative and we should expect that experiments in DSA in one direction will have beneficial cost and demand impacts in others (see Chapin & Lehr, 2007a).

4 TOWARD THE DESIGN OF AN ENFORCEMENT REGIME FOR DSA

The objective of this paper is to provide a framework for the design and development of enforcement regimes for DSA systems. An enforcement regime for DSA is necessary to ensure that the holders of usage rights have predictable protection of those rights. Without the ability to protect usage rights, usage rights holders will not be able to build systems that will perform in a predictable way, making investments uncertain. As we showed above, these usage rights are dependent on the particular mode of sharing. In this section, we would like to illustrate how the ideas presented in this paper might be used to develop requirements for an enforcement regime for a hypothetical system.

Table 2 above shows eight general types of DSA enforcement situations and Table 3 below considers just the first row of that table in somewhat more detail, identifying some of the enforcement requirements as well as the observations about these requirements. Clearly system requirements become more complex as electrospace sharing and rights subordination come into play. Adding mobility may not change the requirements much, but could well increase the cost of enforcement. Institutional factors come into play as well; for example, usage rights subordination can occur through negotiated agreements (e.g., in the case of pure cooperative sharing) or through regulatory fiat (e.g. an easement for UWB operation below the noise floor). The origin of the subordination matters to the enforcement regime because negotiated subordination may include enforcement and remediation clauses that are contractual and would be subject to contract enforcement mechanisms (e.g., civil tort claim or binding arbitration, as defined by the contract). In regulatory subordination (e.g., TV white spaces), the locus of *ex post* enforcement may shift to *de jure* venues, including regulatory proceedings, as specified by the regulator.

Above we made the case for the importance of flexibility in developing rights as well as enforcement regimes for DSA. Examining Table 3, it is clear that some of these requirements are more flexible than others. For example, a decentralized enforcement regime that is embedded into radios (as is possible in the shared regimes described below), may only be able to implement changes as quickly as radios are replaced. But the move to SDR/CR radios which are more readily updated may enable faster adaptation of these

sharing environments. Regimes based on negotiation and bargaining have more flexibility to adapt to technological and other environmental changes since the rules and protocols are not fixed.

Table 3 - Generic enforcement requirements of some non-mobile DSA regimes

Case	Enforcement requirements	Observations
Fixed, Exclusive, non-sub.	*Ex ante* • Detect interference and identify bad actors • Build evidence for remediation *Ex post* • *De jure* process to shut down pirates • Negotiation with offender to stop interference events	• Finding bad actors (e.g., pirate broadcasters) can be challenging if transmission is intermittent; • Detection and remediation may be *de facto* as well as *de jure.* • Sensing and data collection may be done in a decentralized way (*i.e.,* affected party); • Remediation may begin with bi-lateral negotiations.

Fixed, Shared, non-sub.	*Ex ante*
	• Ensure regulatory compliance of unlicensed devices
	• Detect and identify etiquette defectors
	• Detect other signals
	Ex post
	• Punish etiquette violators through protocol mechanisms
	• Shift to new electrospace to reduce interference
	  ○ Unilateral action
	  ○ Bilateral bargaining
		• External identification of etiquette violators is challenging, especially if protocols are complex.
		• Unlicensed bands allow many legitimate uses and protocols (e.g. WLAN and Zigbee and Bluetooth).
		• What does enforcement mean in these bands beyond compliance with transmitter emission masks and standards?

Fixed, Exclusive, Subordinate	*Ex ante* • Detect and identify bad actors (primary *and* secondary users); • Build evidence for remediation (bi-lateral) *Ex post* • Execute remediation procedures embedded in negotiated subordination agreement • Remuneration and penalties (if applicable)	• Enforcement procedures must consider subordination agreements/policies. • License *and* use holders could be bad actors.
Fixed, Shared, Subordinate	*Ex ante* • Ensure regulatory compliance; • Detect and identify bad actors; • Detect and identify etiquette violators; • Build evidence for remediation; *Ex post* • Punish etiquette violators (protocol) • Seek compliance with subordination agreement • Remuneration and penalties (if applicable)	• Subordination agreements *and* spectrum etiquette violations must be detected • Multiplicity of possible bad actors

5 CONCLUSIONS AND DIRECTIONS FOR FUTURE RESEARCH

To meet the demand from legacy and new wireless services, we will need to share our spectrum much more extensively than we do today. Technologies like SDR and CR are key to enabling the DSA systems that will share spectrum much more intensively. These DSA systems may be deployed in a diverse array of environments, including cooperative and non-cooperative sharing among and between primary and secondary users. A key component of any sharing regime are the property rights that adhere to different classes of users and uses, which differ by context and band.

This paper focuses on the enforcement challenge which is an intrinsic component of any property rights regime, lending force to the rights regime to constrain both *ex ante* behavior and assist in remedying harms. The enforcement regime is comprised of technical and non-technical elements, where the latter include the business processes, market norms, and policy institutions and frameworks that reinforce and interact with the technical enforcement solutions. The emphasis in the literature on DSA enforcement has been on the challenges confronted specifically by SDR/CR-enabled smart radios seeking to share with primary users opportunistically, without causing interference for the primary users. A richer interpretation of the diversity of DSA frameworks recognizes that both primary and secondary users have property rights and obligations with respect to enforcing the interference management regime. It is not limited to secondary devices being required to avoid causing interference for primary users.

The challenge of enforcing usage property rights is not new to spectrum management, but the transition to DSA systems and the commercialization of technologies like SDRs and CRs pose both opportunities and challenges that need to be considered when addressing the enforcement challenge. While the increased mobility (in geospace and waveform) of SDRs/CRs poses the risk of "hit-and-run" radios, these technologies also include options for embedding enforcement controls into the radio systems. These include things like policy reasoners in CRs, black boxes, and time limited leases. Moreover, these decentralized, edge-based solutions may be integrated with centralized and network-scale enforcement mechanisms like a database for registration and usage tracking (which is useful both for operational management and forensic diagnosis of radio behaviors, including dispute resolution), sensing infrastructure (that can identify spectrum holes and help detect bad radios), and beaconing/control channels (that can be used to support public safety preemption of other uses in emergencies). And, these technical solutions are supplemented with business practices like contracting terms and industry standards (that specify system designs and performance standards) and regulatory frameworks and institutions. The third-party institutions include market researchers, arbitration services, and private and public "spectrum" police that may actively monitor and enforce compliance with DSA regimes.

Much of the enforcement apparatus – technical and non-technical – is shared across DSA regimes. Experiences gained in one DSA market will build competency for the extension of DSA functionality in other markets. For example, certain forms of CR flexibility may be deemed too risky to allow in general non-cooperative sharing regimes because of the inability to implement an effective (which also means cost-effective) enforcement mechanism at the current stage of development. These may be more easily deployed and experimented with in cooperative sharing environments; or potentially, in specific non-cooperative sharing regimes until such time as adequate confidence in the enforcement mechanisms has been gained. This argues for a more holistic and adaptive view to the enforcement challenge.

A key challenge to gaining this experience is to enable experimentation, especially operational level experimentation. As an illustrative example, consider the case of spectrum sharing between public safety and commercial users which is desirable for multiple reasons. First, the usage profiles of commercial and public safety users are sufficiently uncorrelated as to suggest that there would be significant white space in a regime that allocated spectrum exclusively to commercial uses or exclusively to public safety uses. Public safety's peak usage needs are likely to be different in location and time than commercial users. Second, future models for public safety communications anticipate the need for much greater interoperability and sharing between commercial and public safety users. Third, meeting the needs for mobile broadband of both commercial and public safety users will require significant investments in non-spectrum (as well as spectrum) resources. These costs could be lower for everyone if they could be effectively shared. While the case for public safety and commercial sharing is compelling, there are significant technical (public safety reliability and availability needs are different from commercial users), business (public safety is typically not-for-profit service), and regulatory (public safety is subject to heavy regulation) challenges to realizing such sharing. The DSA regime that may be right for public safety and the enforcement requirements that imposes are likely to be different than for commercial DSA (where contractual options are different). In keeping with the themes of this paper, progress toward sharing with public safety ought to be an important research priority and a focus for operational testing in the near future.

Another important challenge for research in this area is to engage more multidisciplinary work. Designing a protocol that enables incentive-compatible, decentralized enforcement of efficient spectrum sharing, requires that there also be a way to ensure the protocol is implemented, which means paying attention to the incentive compatibility for businesses of investing in developing such a market and of policymakers in ensuring compliance with the protocol. The optimal enforcement framework involves a mix of centralized and decentralized, *ex ante* and *ex post*, specific and common enforcement components – and these must co-evolve with the technology, markets and policies as a complex ecosystem.

6 ACKNOWLEDGEMENTS

The authors would like to thank Dr. John Chapin for his insightful comments and conversations regarding enforcement in DSA systems, especially as those relate to the potential use of "black boxes". This work was supported in part by the U.S. National Science Foundation under Grants 1149422, 1040020, and by the MIT Communications Futures Program (http://cfp.mit.edu). The opinions and any errors expressed herein are solely the responsibility of the authors.

7 REFERENCES

Atia, G.; A. Sahai and V. Saligrama. 2008. "Spectrum Enforcement and Liability Assignment in Cognitive Radio Systems," *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on.* 1-12.

Braithwaite, John. 1982. "Enforced Self-Regulation: A New Strategy for Corporate Crime Control." *Michigan Law Review*, 80(7), 1466-507.

Buddhikot, M. M. 2007. "Understanding Dynamic Spectrum Access: Models,Taxonomy and Challenges," New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on. 649-63.

Cave, Martin and William Webb. 2012. "The Unfinished History of Usage Rights for Spectrum." *Telecommunications Policy*, 36(4), 293-300.

Chapin, J. and W. Lehr (2007a), "The path to market success for dynamic spectrum access technologies," IEEE Communications Magazine, May 2007 (pdf=http://people.csail.mit.edu/wlehr/Lehr-Papers_files/chapin_lehr_IEEE_communications_submitted.pdf)

Chapin, J. and W. Lehr (2007b), "Time-limited Leases for Innovative Radios," with John Chapin, IEEE Communications Magazine, June 2007.

de Vries, P. and K. Sieh. 2012. "Reception-Oriented Radio Rights: Increasing the Value of Wireless by Explicitly Defining and Delegating Radio Operating Rights." *Telecommunications Policy*, 36(7), 522-30.

de Vries, P. 2010. "How I Learned to Stop Worrying and Love Interference: Using Well-Defined Radio Rights to Boost Concurrent Operation (September 5, 2010). Available at SSRN: HTTP://SSRN.COM/Abstract=1672375.

Demsetz, Harold. 1964. "The Exchange and Enforcement of Property Rights." *Journal of Law and Economics*, 7(ArticleType: research-article / Full publication date: Oct., 1964 / Copyright ¬© 1964 The University of Chicago), 11-26.

Demsetz, Harold. 1967. "Toward a Theory of Property Rights." *The American Economic Review*, 57(2), 347-59.

Enforce. 2012. In Merriam-Webster.com. Retrieved July 18, 2012, from http://www.merriam-webster.com/dictionary/enforce

Farrell, Joseph and Matthew Rabin. 1996. "Cheap Talk." *The Journal of Economic Perspectives*, 10(3), 103-18.

Faulhaber G. R. 2006. "The future of wireless telecommunications: Spectrum as a critical resource," *Information Economics and Policy* , p. 256–271

Faulhaber, G. and D. Farber (2002), "Spectrum Management: Property Rights, Markets, and the Commons," AEI-Brookings Joint Center, Working Paper 02-12 (December 2002).

FCC . 2002. Spectrum Policy Task Force Report, Federal Communications Commission, ET Docket No. 02-135, November 2002 (available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-228542A1.pdf).

FCC. 2010. "Connecting America: The National Broadband Plan," Federal Communications Commission, Washington, DC, March 16.

Harrison, K. and A. Sahai. 2011. "Potential Collapse of Whitespaces and the Prospect for a Universal Power Rule," *New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on.* 316-27.

Hazlett, Thomas (2001) "The Wireless Craze, The Unlimited Bandwidth Myth, The Spectrum Auction Faux Pas, and the Punchline to Ronald Coase's "Big Joke": An Essay on Airwave Allocation Policy" Harvard Journal of Law and Technology (Spring 2001).

IEEE. 2008. "IEEE Standard Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging Wireless Networks, System Functionality, and Spectrum Management." *IEEE Std 1900.1-2008*, c1-48.

Matheson, RJ. 2006. "Principles of Flexible-Use Spectrum Rights." *Journal of Communications and Networks*, 8(2), 144.

PCAST (2012), "Report to the President Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth," Executive Office of the President, President's Council of Advisors on Science and Technology (PCAST), July 2012 (available at:

http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast_spectrum_report_final_july_20_2012.pdf)

Peha, J. 2009. "Sharing Spectrum through Spectrum Policy Reform and Cognitive Radio." *Proceedings of the IEEE*, 97(4), 708-19.

Raychaudhuri, D. and Jing Xiangpeng. 2003. "A Spectrum Etiquette Protocol for Efficient Coordination of Radio Devices in Unlicensed Bands," *Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on.* 172-76 Vol.1.

Sandvig, C. 2011. "Spectrum Miscreants, Vigilantes, and Kangaroo Courts: The Return of the Wireless Wars." *Fed. Comm. LJ*, 63, 481-553.

Satapathy, D. P. and J. M. Peha. 1997. "Performance of Unlicensed Devices with a Spectrum Etiquette" *Global Telecommunications Conference, 1997. GLOBECOM '97., IEEE.* 414-18 vol.1.

Scoville, M.; S. Berger; R.C. Reinhart and J.E. Smith. 2006. "The Software-Defined Radio & Cognitive Radio Inter-Consortia Affiliation," *MILCOM2006 (Military Communications Conference, October 2006, Washington DC).*

Shavell, Steven. 1993. "The Optimal Structure of Law Enforcement." *Journal of Law and Economics*, 36(1), 255-87.

Smith, Henry, E. 2002. "Exclusion Versus Governance: Two Strategies for Delineating Property Rights." *The Journal of Legal Studies*, 31(S2), S453-S87.

Stewart, Richard B. 1981. "Regulation, Innovation, and Administrative Law: A Conceptual Framework." *California Law Review*, 69(5), 1256-377.

Tandra, R. and A. Sahai. 2007. "SNR Walls for Feature Detectors," New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on. 559-70.

Tandra, R. and A. Sahai. 2008. "Overcoming Snr Walls through Macroscale Features," *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on.* 583-90.

Tonmukayakul, Arnon and Weiss, Martin B.H., 2008"A study of secondary spectrum use using agent-based computational economics ," *Netnomics*, vol.9, no. 2, pp. 125-151.

Vany, Arthur S. de; Ross D. Eckert; Charles J. Meyers; Donald J. O'Hara and Richard C. Scott. 1969. "A Property System for Market Allocation of the Electromagnetic Spectrum: A Legal-Economic-Engineering Study." *Stanford Law Review*, 21(6), 1499-561.

Weiss, Martin B.H. 2011, “Spatio-Temporal Spectrum Holes and the Secondary User”, IEEE DySPAN

Weiss, Martin B.H. and Cui, Liu. 2012, "Spectrum Trading with Interference Rights," *7th International Conference on Cognitive Radio Oriented Wireless Networks (CrownCom)*.

Weiss, Martin B.H., Delaere, Simon, and Lehr, William H. 2010. "Sensing as a Service: An exploration into the practical implementation of DSA," *IEEE DySPAN*.

Weiss, Martin B.H. and William H. Lehr, *Market Based Approaches for Dynamic Spectrum Assignment*, Working Paper, 2009. Available from http://d-scholarship.pitt.edu/2824/

White House (2010), "Presidential Memorandum: Unleashing the Wireless Broadband Revolution," The White House, Office of the Press Secretary, June 28, 2010 (available at: http://www.whitehouse.gov/the-press-office/presidential-memorandum-unleashing-wireless-broadband-revolution).

Woyach, K. and A. Sahai. 2011. "Why the Caged Cognitive Radio Sings," New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on. 431-42.