Abstract

The role of expanding spectrum as a contributor to economic growth was highlighted in the National Broadband Plan and in the President’s Council of Advisors on Science and Technology report entitled “Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth.” Recommendations in the PCAST report include sharing underutilized Federal spectrum and identifying 1,000 MHz of Federal spectrum to create “the first shared-use spectrum superhighways.” To realize this vision, fundamentally new spectrum access technologies will be developed; therefore, it is important to understand security and privacy implications for these possible new designs. Security and privacy become especially critical concerns in light of the increasing prospects of spectrum sharing between federal government systems and non-government systems. The likelihood of such a spectrum-sharing scenario was heightened by the Federal Communications Commission’s notice of proposed rulemaking (NPRM) for the 3.5 GHz band. The NPRM outlines a geo-location database-driven spectrum sharing scenario where Incumbent Users—namely, federal government, including military, users and fixed satellite service licensees—share spectrum with Secondary Users operating small-cell technologies on an unlicensed basis. Although privacy issues are critical in such a spectrum-sharing scenario, there is little research on those problems.

This paper identifies privacy issues and related laws related to geo-location database driven spectrum sharing. It considers the different issues that will arise depending on the basic design choices for the spectrum sharing system; for example, either a government or private entity might maintain a spectrum-sharing database. It analyzes spectrum sharing from the viewpoint of geo location and the evolving expectation of privacy in location information. The paper identifies questions to be addressed in future spectrum sharing design, and suggests areas for increased legal attention.

I. Introduction

The National Broadband Plan and the President’s Council of Advisors on Science and Technology report entitled “Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth.” [PCA12] promote sharing underutilized Federal spectrum and identifying 1,000 MHz of Federal spectrum to create “the first shared-use spectrum superhighways.” To realize this vision, fundamentally new spectrum access technologies will be developed, including new public-private interfaces for multi use spectrum. The likelihood of such a spectrum-sharing scenario was heightened by the Federal Communications Commission’s notice of proposed rulemaking (NPRM) for the 3.5 GHz band [FCC12]. The NPRM outlines a geo-location database-driven spectrum sharing scenario where Incumbent Users—namely, federal government, including military, users and fixed satellite service licensees—share spectrum with Secondary Users operating small-cell technologies on an unlicensed basis. Privacy needs of the Incumbent Users are widely acknowledged, as police, emergency, and defense must be able to exert priority over shared spectrum use and concurrently mask their location in order to maintain security.

In comparison, privacy considerations for secondary users have received little attention. This paper discusses the legal and policy perspectives of protecting privacy in a spectrum-sharing
framework. It aims to identify issues related to fundamental database choices for such a system, and to identify research questions for further study. Law related to geo-location data and privacy, the evolving expectation of privacy in location information, and private and public access to individual location information need to be considered. Relevant laws and regulations include the Telecommunications Act, Electronic Communications Privacy Act, and the application of the first and Fourth Amendment. Acceptance of a spectrum sharing system by the public will likely depend on a careful design that addresses issues of privacy, civil rights, and communications. This research is a work in progress; identification of the issues is the first step towards an integrative approach to designing a spectrum sharing database that will meet public expectations and legal standards.

A. Database Spectrum Sharing Premises

Technical aspects of implementing geolocation database spectrum sharing are not yet fully developed. In fact, it is the proposition of the authors that legal and policy considerations should inform the adoption of such implementation. It is important to note, however, the basic technical premises upon which the following legal discussion builds.

For our discussion, we assume an architecture with at least two tiers of users, each with different levels of rights and protections.¹ The first tier, Incumbent Users (IUs), includes stationary and mobile federal government users, including military users, and fixed and mobile licensees. These IUs must have priority over and be protected from interference from all other users. The second tier, Secondary Users (SUs), includes all other users that have registered with a Spectrum Access System (SAS) (we also call this entity the database manager). According to the FCC’s NPRM, The SAS refers to a cloud-based spectrum management infrastructure that determines the availability of spectrum, allocates spectrum resources, and manages access amongst users while considering incumbent protection, coexistence, access priority, and quality of service. The SAS server acts as an interface between the users (both IUs and SUs) and the SAS infrastructure, and it receives queries from the SUs and returns corresponding query replies to them. The SAS server is composed of a geolocation database, spectrum allocation engine, and incumbent protection and coexistence manager. A query to the SAS contains an explicit registration identifier, location information, antenna attribute information, and potentially additional transmission parameters. A query response contains a list of one or more available channels, maximum allowed transmission power, maximum antenna height, time interval of the channel’s availability, and possibly other transmission parameters. The specifics of the SAS have not been determined or standardized at this point, hence no one knows exactly what they will look like until one is developed and deployed. This description gives us a potential framework upon which we can discuss privacy issues.

The IU’s operational privacy is essential in this spectrum sharing scenario. When incumbent systems are commercial systems, such as the case in TV spectrum, this is not a critical issue. However, when the IUs are federal government, including military users, then the information leaked by the database query replies can pose a serious threat to the IUs’ operational privacy. This problem cannot be addressed by tightly controlling access to the SAS, since all SUs need access to it to enable spectrum sharing. There are various methods to address the operational privacy of the IU, many of which are well developed. While acknowledging the critical importance of IU operational privacy, our discussion focuses on issues involving the privacy of

¹ A more robust and more likely configuration will include three tiers, as noted by the PCAST report and the FCC NPRM. For purposes of this initial discussion we assume that there are only two tiers.

² The analysis is limited for this preliminary research although other laws may be implicated; for example, the Communications
the SU.

The SU interest in the privacy of a geolocation database is linked to overall concerns for privacy and the particular concerns for privacy in mobile communications, discussed in the following section. Indeed, a trace of database accesses can be used to disclose the location or the spectrum access behavior of SUs, which is especially problematic with access points that are used exclusively by single individuals [Tro11]. Technical means to protect unauthorized access to SU location information could be based on the integration of a PIR protocol into a spectrum database access protocol. However, providing both IU operational privacy and SU location privacy is difficult because the two are inherently incompatible in terms of how the database computes the query replies. The trustworthiness of the database manager, and the legal duty imposed for protecting the communications of the SU, are worth considering with regards to risks to SU privacy and public perceptions of that risk, especially in an environment in which the extent of government surveillance is a matter of public concern.

B. Secondary User Privacy

Individuals have an expectation of privacy, even in an era of increased information sharing and the mobile revolution. A 2012 Pew Internet Research found that 57% of those surveyed had either uninstalled or decided not to install a mobile application due to the amount of personal information collected [Boy12]. Concern about individual privacy and information collection is not abating; a 2013 Pew Research project found that 86% of users surveyed had taken action to hide their identity to avoid information collection online [Rai13]. In the same survey, 54% agreed that it was very important that they be able to control information about their location when they use the Internet [Rai13]. Although the concern varied based on age, 45% of users between 19 and 29 still believed that controlling location information was very important, the lowest percentage of users expressing concern. Lastly, 68% of people in the 2013 survey believed that present laws were insufficient to protect their digital privacy [Rai13].

In February, 2014, the FTC held a seminar on the topic of Mobile Device Tracking, subsequently releasing a public request for comments about types of mobile location tracking and impacts on consumers and their privacy [FTC14]. The seminar presentations showed that on one side consumers do not understand the how, or extent of, mobile tracking and information sharing; and on the other side, commercial entities require the consumer to turn off the location function of their mobile device to prevent tracking or information collection about their location. As the 2013 Federal Trade Commission (FTC) report, Mobile Privacy Disclosures, recognizes, “When people use their mobile devices, they are sharing information about their daily lives with a multitude of players” and therefore the privacy implications are magnified. The FTC reported that 57% of users had either uninstalled a mobile app or declined to install one in order to avoid sharing personal information [FTC13]. This evidence is relevant to the geolocation database because the spectrum allocation database requires that the SU keep the location information always “on.” Because the user must always have a location indicator in use in order to take advantage of the spectrum allocation, privacy concerns are implicated more broadly due to the affect on other applications. Although these ecosystem impacts are not discussed further in the following analysis, they create important future questions.

Privacy concerns, while different in nature, are implicated by both commercial and government intrusion into private life. Since the database manager is as yet unidentified, an analysis should consider concerns from both viewpoints.

II. Statutory Legal Perspectives
SU privacy may be implicate if a database manager shares location information with either commercial or government entities. The primary statutes to be considered for database management privacy are the Telecommunications Act of 1996 and the Electronic Communications Privacy Act. If a government agency manages the spectrum database, the Privacy Act should be considered.²

A. The Telecommunications Act

The Telecommunications Act, US Code 47 USCA, distinguishes between telecommunications carriers and information services providers. Telecommunications is defined as “the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.” In contrast, an information services provider does something more than simply transmit the user information. For example, an Internet service provider would in most cases be characterized an information services provider [Yoo13]. By allocating spectrum for use by the SU, it could be argued that the database manager is an information services provider, similarly to the FCC and court decisions that a broadband provider can be categorized as such because of its domain name system matching function. [Yoo, 13] On the other hand, it could be reasonable to define spectrum matching as simply a routing of the transmission.

If it is categorized as a telecommunications carrier, the spectrum database manager would be subject to §222, Privacy of customer information, which prohibits telecommunications carriers from sharing “customer’s proprietary network information” except under certain circumstances, such as rendering services or with the explicit consent of the customer. Proprietary information includes “information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications services subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship.” (emphasis added)

When customer location information is used for the performance of network communications or to authenticate user identity, no notice to the customer is required. [Edm05; NIT13; USC08]. Otherwise, “without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to-(1) call location information concerning the user of a commercial mobile service . . . or the user of an IP-enabled voice service.” (emphasis added) An exception to customer prior authorization for disclosure is made for emergency or safety uses. Emergency reasons for disclosure encompass widely recognized services in an emergency situation such as fire, medical, law enforcement, public safety, and for dispatchers associated with the same. (222(d)(4)(a)). Importantly, the reason for releasing location information in an emergency situation is limited in scope, “in order to respond to the user’s call for emergency services.”³

Thus, under the Telecommunications Act, a DM will be allowed to share information for the emergency requirements of the SU. There is no exception for the emergency needs of the IU.³ One could imagine a scenario in which the IU faced an attack or diminishment of services and required emergency access to location information of the SU. Explicit consent would be needed.

---

² The analysis is limited for this preliminary research although other laws may be implicated; for example, the Communications Assistance for Law Enforcement Act. We also assume for the sake of this discussion that the information being shared is from a mobile communications device.

³ Access to information by the IU for national security purposes is another important topic, not covered in this discussion.
The nature of explicit consent in a mobile environment, where screens are small and notices can be difficult to read, is an important area for a spectrum sharing database to consider. For means of comparison, the National Telecommunications and Information Agency (NTIA) and the Department of Commerce have worked towards an industry solution for mobile apps by bringing together a stakeholder group to write a draft Code of Conduct for mobile applications. [NTI13] The Code of Conduct promotes the use of a short form notice of what information is collected and how it is shared, made available to consumers in a manner that is designed for ease of use on a small screen (and posting of a long form notice on a website). The short form notice should include how past and current location information is collected. However, the Code of Conduct was not written with the spectrum sharing design in mind. Research is needed to compare any spectrum sharing “application” with those anticipated in the NTIA stakeholder draft Code of Conduct to determine if notice to consumers is the best policy, and if so, whether a short form notice would be effective.

Because longitudinal, centralized, location information and its specificity can be particularly revealing and allow inferences to be drawn about a person, the policy for protecting that information should be very carefully drawn.

B. The Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA)⁴ is the second major statute applying to a spectrum sharing database. The ECPA primarily protects the content of communication based on whether it is; 1) held by an electronic services provider or a remote computing service, and 2) sought during transmission or requested from storage. [Ves13]. Whether the communications are shared with the government or a non-government entity will also be relevant. The history of the ECPA, adopted when storage was expensive and not widely available, explains the awkward, and often criticized, dichotomy of protections based on these categories [Ker14]. The application of the ECPA to modern technologies is a difficult and thorny matter, and the following discussion does not purport to cover the full range or depth of legal issues.

The spectrum database will likely manage both stored and realtime (or proscriptive) communications and SU data. The location of the SU will need to be monitored/known in realtime so as to manage and allocate communications to available spectrum. SU location information will likely be retained, and stored, for a particular period of time for technical and management reasons. Whether and under what circumstances a government or nongovernmental entity may access the SU communications and SU data can affect the acceptance of a spectrum allocation design. Not only will the SU have concerns about maintaining the privacy of their communications, but the database manager will have concerns about liability for unauthorized disclosure of such information as well as the maintenance of customer relationships.

1) Government Access

Interception of electronic communications is prohibited (18 Sec. 2511), unless a specified government official obtains a court order. The court order is granted based on an application that states with particularity the crime that is being investigated or about to be committed, a description of the communications to be intercepted and its location, and the length of the interception. (18 Sec. 2518).

---

⁴ECPA is used to encompass laws otherwise known as the Wiretap Act and the Stored Communications Act.
If communications are in storage, then “a person or entity providing an electronic communications service shall not knowingly divulge to any person or entity the contents” (18-2702(a)(1)) of that stored communications. A remote computing service may likewise not divulge contents of communication “carried or maintained on that service.” (2).

However, the government may access the content of stored communications under processes that depend on the length of the storage and whether the information sought is either content or a record of the SU. A provider is required to disclose content stored for 180 days or less to the government only when served with a warrant. When content is stored for over 180 days, then while the government may utilize a warrant to obtain user content, it may also apply under a lower standard to obtain a court order (18 USC Sec. 2403(d)). This standard requires the government to show “specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . are relevant and material to an ongoing criminal investigation.” It is important to note that several recent court decisions have held this standard, and the relevant provision of the ECPA, to be unconstitutional. Instead, the user’s reasonable expectation of privacy in his or her email would require the government to meet a probable cause standard under the Fourth Amendment (the Fourth Amendment is discussed further in following sections). This area of the law remains in conflict, as conversely the constitutionality was upheld in a different Circuit Court [In re Application, 2013]. Until the Supreme Court rules upon the matter the split in authority will prevent clarity for a future database manager. In the meantime, the American Bar Association has recently proposed standards for access to cell phone location information [Freiwald, 2014].

In summary, the definition of communication in storage versus communication in transit becomes important, as the category of communication will affect the method by which law enforcement may gain access to the information, and the DB will need to follow these standards for granting access. A warrant with probable cause is needed for obtaining access to communication during transmission, while a court order would, assuming its constitutionality, be obtained under a lower standard of proof for communication stored for over 180 days.

How would this be applied to the spectrum allocation database? One might consider that at different points in time the database manager would be performing either transmission or storage. In order to provide security measures for the IU, SU queries would need to be stored for analysis. Dynamic allocation of spectrum by the database as a result of queries by the SU would arguably be transmission information. A request for access to current location information is similar to accessing a conversation in real-time. This interpretation is legally unclear, however. Storage is defined as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof and any storage of such communication by an electronic communication service for purposes of backup protection of such communications” (18 U.S.C. Sec. 2510 (17)). Some courts have interpreted information that is shared with a third party as stored communications, because it must be stored first before it is shared [Pel12]. Courts that have considered the question of the nature of cell phone location information are split [Ker14]. Additionally, courts have viewed historical and prospective cell phone location differently and the Circuit Courts have reached differing conclusions about whether geolocation information would fall within transit or storage definitions [Orr14].

The analysis so far has addressed access to content of the communications, defined in the ECPA as “any information concerning the substance, purport, or meaning of that communication.” [18 USC 2511 3a]. Aside from the more traditionally envisioned content of a message, one could argue that precise location information used for spectrum sharing should be considered content because it communicates an exact location of the user over a long period of time. Use of the
unlicensed spectrum band discussed here would produce location information that could place a person within a small geographical radius; not only within an identified building, but within a specific room within a building. One one hand, spectrum sharing involves similar risks to privacy infringement as most WiFi networks. The more important issue is that unlike WiFi networks, in spectrum sharing, spectrum usage (and related location info) is centrally managed and controlled by the SAS. In contrast, in WiFi networks, spectrum usage is managed in a distributed manner, usually by an individual or group. This specific and centralized location information, collected over time, could infer information about a person, creating meaning; therefore a reasonable argument could be made that it is, by its nature, equivalent to content. However, some courts have held that location information is a record, not content [Zyn14].

The ECPA contains exceptions for disclosure, two of which deserve further analysis in the application of a spectrum sharing database. First, disclosure of content may be made to a government entity if there is an emergency in which the provider believes in good faith that there is “danger of death or serious physical injury to any person” [2702(b)(8)]. Furthermore, a provider is required to disclose records (not content) related to customer information, including name, address, times and durations of telephone calls, individual numbers, and payment information [2703(c)(2)]. Access to further record information requires a warrant or court order. While communications content should continue to be protected vigorously, sharing of record information, narrowly defined, may need more fine grained examination for spectrum sharing to be implemented successfully. For example, cybersecurity measures may depend on access to data that can predict attacks from anomalies in customer use. A network administrator managing a network can use customer data to try to identify “rogue” transmitters -- i.e., transmitters that fail to obey the spectrum access rules. Rogue transmitters are a big concern in federal-commercial spectrum sharing because these radios may cause serious interference to IUs. The data needed for these security measures can include longitudinal customer record data.

2) Non-Government Access

The ECPA prohibits non government access to content without user consent, but does not apply similarly to non government access to noncontent, or user record information. User location information may therefore arguably be shared with commercial entities if it is not considered to be content, but record information.

This revisits the discussion about the appropriate treatment of information that may not be traditionally considered content, but that nonetheless expresses information in a way that essentially mirrors the communicative nature of content. Information about website searches, for example, could potentially be considered content for purposes of the ECPA. However, this argument was unpersuasive in the recent 2014 case of In re Zynga Privacy Litigation, in which subscribers argued that Facebook and Zynga violated the ECPA by sharing referer header information of website searches with third parties, without consent [Zyn14]. In deciding the case, the Ninth Circuit ruled that the disclosure of personally identifiable information (in the referrer header information) does not, in itself, violate the ECPA because record information is distinct from content [Zyn14]. Record information is not protected. However, the Zynga court left the door open for a future situation under which the nature of transactional information might be considered content.

It could be argued that the part of the ECPA known as the pen register provision might apply to government action to install a surveillance device, under the premise that the spectrum database collects signaling information. But see [Ker14]. This is an important issue, but will be left for examination in future research.
C. The Privacy Act

If the database is operated by an arm of the federal government, then the Privacy Act would apply to information that it maintains. Although there are a number of exceptions, including for law enforcement reasons, the Privacy Act limits the use of records with personal identifiers to the intended purpose of the record creation, and prohibits the sharing of that information. For example, because of the threat of mussel infestation the National Park Service (NPS) registers information about boaters on Lake Mead and engages in boater education to spur users to clean their boats before leaving for other waters. Several western states have laws that require inspections at borders; the law enforcement exception allows the NPS to share information about boats that leave without being inspected. However, the NPS does not share information with states that do not have legal restrictions, and it does not share information about boats that have been inspected. Neither does it engage in electronic tracking of the boats. By analogy, records created by a spectrum sharing database may similarly be protected under the Privacy Act and restrictions on their use would be imposed to protect individual privacy, absent applicable exceptions.

III. Constitutional Issues

A. The Fourth Amendment

The 11th Circuit Court recently decided, in June of 2014, whether cell phone location data is protected by the Fourth Amendment, and therefore must be the subject of a warrant under the US Constitution. It found that “cell site location information is within the subscriber’s reasonable expectation of privacy,” and that failure to obtain a warrant for that information resulted in a constitutional violation [US v. Davis, at 10]. The court compared a cell phone to an automobile and analyzed the expectation of privacy in each, finding that a cell phone is much more likely to communicate private information because the owner carries it continuously, in contrast to the more limited intrusion caused by tracking the location of a car. It noted that “even one point of cell site location data can be within a reasonable expectation of privacy,” therefore analyzing the extent of the cell phone data collection was unnecessary [Davis, at 8]. Other courts have rejected the argument that there is an expectation of privacy in cell phone location data, however, and conflicting views of the evolution of a reasonable expectation of privacy persist.

The Davis court rejected the government’s argument that by sharing location information with the telephone company that the consumer had given up any reasonable expectation of privacy because of the third party, business records principle. It agreed with the Third Circuit that cell phone users do not normally understand that companies maintain historical cell phone location records. It should be noted that this approach has been squarely rejected in other cases, where the third party doctrine has been applied to cell phone provider records [See, e.g., US v. Rigmaiden, 2013]. The possible application of the Fourth Amendment to cell site location data and an expectation of privacy in records held by third parties is a “vexing question” that courts have sometimes sidestepped [US v. Jones, 2012, at 205].

The discussion about the nature of privacy, technology, and locational information is an important one that has not yet been fully considered by the Supreme Court of the United States. Two recent Supreme Court cases brought the Supreme Court closer to these issues, however.

Justice Sotomayor’s concurring opinion in U.S. vs. Jones (2012) discusses the Fourth Amendment and whether the government needed a warrant to place a GPS tracking device on a car for 28 days [Uni12], an analysis that resonates with the issue of obtaining proscriptive...
locational information in a spectrum sharing database. Sotomayor observed that tracking a car is essentially the same as tracking a person, and therefore it interferes with a person’s expectation of privacy. This observation applies even more acutely to a cell phone and its user. Following the location of a cell phone as compared to tracking a car is more invasive and finer grained. It can identify personal location with far more precision than the automobile, which is confined to streets. Another concurring opinion, written by Justice Alito and joined by three other justices, focused on the expectation of privacy from another viewpoint. In contrast to Justice Sotomayor’s suggestion that our electronic age could require a new definition of the privacy of information shared with third parties, the Alito concurrence focused on the ill-defined conception of privacy that exists as a result of new technologies. He stated that the legal protection of privacy rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. In addition, he noted that the ubiquity of location sharing tools may blunt or decrease the public’s expectation of privacy. Alito suggested that changing technology and unclear expectations are more amenable to legislative solutions than court imposed ones [Uni12]. The anticipated spectrum sharing paradigm will use technologies that require identification of the device’s location; the intrusive nature of this technology is similar to that pointed out by Justice Sotomajor. Yet as Justice Alito infers, it may take considerable time before consumers understand the potential impact that location sharing could have on their privacy, and by that time they may feel numbed to the intrusion.

In the 2014 case of Riley v. California, the Supreme Court addressed a warrantless search of the contents of a cell phone by police after an arrest. While not directly applicable to location based communication, the decision is nonetheless instructive with regards to the way in which the Supreme Court may generally characterize cell phones and expectations of privacy. Justice Roberts described smart phones as “such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy” [Riley, at 2484]. Equally descriptive, Justice Robert characterized the government’s argument that a search of a cell phone is the functional equivalent to a search of physical items found on an arrestee’s person as “like saying a ride on horseback is materially indistinguishable from a flight to the moon” [Riley, at 2489]. Furthermore, cell phone data is “qualitatively different” from a physical record because it can “reveal where a person has been” based on [h]istorical location information” [Riley, at 2490]. The extent of location information held in the history of a smartphone mirrors the type of information that would be held by a spectrum database manager. Additionally, while courts are now divided about the nature of cell site location information, the decision in this recent Supreme Court case indicates its probable view of this information as highly sensitive, worthy of Fourth Amendment protection.

**B. First Amendment**

If a spectrum database manager is a governmental entity, then First Amendment, freedom of speech rights, must be considered. First Amendment law protects speech in public areas, but also allows for management of public property and resources [Arm14; Zic07]. The place and nature of the speech as well as the extent of the burden on the speech is relevant, and different levels of scrutiny will apply depending on a number of these factors. How a spectrum sharing database manager allocates between traffic, the procedures and reasons for granting or denying access, and any alternative means of routing that communications traffic, may all be elements to be analyzed within the framework of guaranteeing free speech and avoiding discriminatory decision making.

One particular question is whether spectrum allocation implicates public forum analysis. San
Francisco’s 2011 decision to turn off Internet and mobile access on its public transportation system due to protests [Gen14; Wie12], public library Internet access cases, and public school Internet access cases may all be considered in comparing management of spectrum allocation. While similar in some respects, government managed spectrum allocation has unique qualities that would require careful considerations of the particular ways in which it could impact speech. If the public forum doctrine would not apply in ways that protect the public’s non discriminatory access to spectrum, then legislation or administrative action to protect these rights could be necessary.

IV. Geolocational Legislation

Recently, federal legislation has been proposed to protect the location information of citizens. These include the Location Privacy Protection Act, Geolocational Privacy and Surveillance Act, Mobile Privacy Act, and others [Van13]. The most recent proposed law, The Location Privacy Protection Act of 2014, was discussed in subcommittee hearings on June 4, 2014. The legislation would require a non governmental entity to obtain the consent of a user before collecting or sharing location information collected from an electronic device. In contrast, the Geolocation Privacy and Surveillance Act would also apply to government action and would require a warrant for access to location information. These bills are still in committee.

V. Conclusion

This discussion sought to examine, in a preliminary way, the legal questions that could arise in the implementation of a spectrum sharing database. Applying laws to a new technology incurs unique issues; spectrum sharing is particularly difficult from a legal perspective because underlying legal principles related to location sharing and privacy are still evolving. The standard for government access, the definition of content in a locational ecosystem, the third party doctrine for records, and the balance of speech rights with management and security are all important issues for future spectrum sharing discussions. The anticipated centralized source for SU location information, and the necessity for the SU to always have a location indicator “on,” heightens the potential impact on user privacy interests. As a database spectrum sharing system is designed, these issues and the surrounding debates should be carefully considered so that expectations of privacy and security are accounted for in the implementation.

REFERENCES


[Dem12] J.X. Dempsey, “Keynote Address: The Path to ECPA Reform and the Implications of


Cases:

Riley v. California,


In re Zynga Privacy Litigation, 750 F.3d 1098 (9th Cir. 2014).
