FCC TAC IoT Working Group Position Statements

September 23, 2014

Index

Safe Harbor Statement IoT Page 2

IoT Privacy Statement Page 3

IoT EoL Statement Page 6

IoT Coexistence (Etiquette) Statement Page 8

Internet of things (IoT) Safe Harbor Statement:

Many classes of IoT devices operate over a limited range and are expected to have a long life, an 8 year or greater life expectancy. To avoid spectrum support issues over this long period, it is recommended that such devices, and the networks to support them, utilize unlicensed operations where practical.

This recommendation is critical whenever a safe harbor from wireless technology evolution is desired.

IoT Privacy Statement

The ubiquity of information exchange in the Internet of Things is creating privacy challenges for our society. Information on the health, location, buying decisions, finances, and personal habits of individuals will be acquired and used for various purposes. A pervasive collection of information will be acquired, exchanged, maintained and used for various purposes in increasing conjunction with its automatic exchange between organizations or systems that, while providing value to society, increase the difficulties in ensuring that personal information is protected and sensitive information remains private. Today, privacy law is still evolving to encompass the issues raised by an information, data-based society where personal information is acquired, stored, used, and exchanged in every transaction a user has with the Internet. IoT fuels this by adding an enormous amount of information collected not just from the individual, but from sensors and appliances that support, monitor or otherwise interact with the user.

Many organizations are involved in developing policy on consumer privacy. The Federal Trade Commission is the primary agency dealing with issues of consumer privacy and in enforcing privacy policy. The NTIA, through a multi-stakeholder process, has worked towards developing enforceable codes of conduct protecting consumer privacy. Governmental activities continue in this area on federal, state and global levels and various industry forums contribute to this discussion. The FCC engages industry in ensuring that communication service providers effectively implement applicable policies.

There are many issues related to privacy outside the scope of the TAC: e.g. anonymization of data, data access policies, appropriate user consent, length of storage, etc. However, there are some fundamental issues that should be the foundation for future policies to be developed by the stakeholders regarding the data privacy rights of the individual. If not implemented early in the evolution of IoT, this failure may impede attempts to ensure the privacy rights of the individual. For example, the FTC's *Fair Information Practice Principles (FIPPS)* defines guidelines for evaluating and mitigating privacy impacts. The OECD has developed similar guidelines, Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data. Processes utilized by communication service providers to collect, store and distribute consumer information should be capable of supporting these evolving policies.

TAC Recommendations:

Consumer privacy in the Internet of Things is an evolving issue that will engage a broad range of groups in establishing and enforcing consumer privacy rights in a future information based society. The TAC recommendations on this subject are not meant to form the basis for policy or regulation in this area. Rather, these recommendations seek to have the FCC engage with industry in drawing from this evolving body of work to establish the norms necessary to ensure that privacy policy frameworks so established can be supported by the communications services used to collect, store and distribute consumer privacy related data. This should aid in promoting a trusted deployment of IoT, and continue to spur innovation and applications that benefit the society at large. To this end we recommend that the Commission:

1. Working with industry, develop an understanding of current approaches that support the secure acquisition, transport, use and exchange of information across different vertical service/market groups.
2. Work with appropriate agencies and industry that define norms applicable to Internet of Things.
3. Understand public concern about the intersection between IoT and communications networks. E.g. the amount and variety of data available for potential snooping and hacking

IoT End of Life Statement - Best Practice

Technology, whether for application, transmission capacity, or device, has an expected viable lifetime and IoT capable products will be no different. However, End of Life issues associated with IoT can be especially challenging given the intersection of the very low cost and long expected life nature of many IoT devices. Therefore, the Federal Communication Commission - TAC IoT WG recommends the following End of Life guidelines be considered to mitigate the impact of IoT technology obsolescence. While there can be IoT End of Life concerns with devices, continuity of connectivity (spectrum/wireless technology), and Cloud based services, this document focuses especially on the connectivity aspects given the key linkage to spectrum use. This recommendation is not advocating regulatory action but is grounded in the Commission's desire to support the wireless carrier's transition to next generation technology (e.g., where the displacement of legacy technologies and applications are a desired outcome). Of particular note and added benefit is supporting a focus on efficient spectrum use:

- Choice of spectrum used for different deployments will be dependent on many factors, including mobility, coverage, QoS/latency, interference resistance, robustness, cost, power consumption, expected life span, and security needs, etc.
  - For short (3 years or less) - and medium-life (3-8 years)

devices where access is Wide Area and mobile, licensed or unlicensed spectrum are both options for consideration. However, the IoT solution owner should always be aware of the velocity of technology change impacting licensed spectrum networks, especially given ever increasing bandwidth demands.
  - For long lived devices (lifespans 8 years or greater), particularly those used in Personal Area and Local Area Networks where proxy/hub gateway devices are common, unlicensed operation should be considered.

- IoT providers should consider software solution capabilities (e.g., cloud computing) when ease of deployment or modification are critical. Benefits are reduced burden of moves, adds, changes, and deletes, reduced impact of power consumption, improved network resiliency, easier security upgrades, and general solution migration.

- End of Life guidelines should be coordinated with relevant Government Agencies as appropriate with the following considerations in mind:
  - End of Life Announcements be made publicly available sufficiently in advance to allow parties to manage the impact of End of Life actions (e.g., download any relevant documentation, install final patches, etc.)
  - End of Life Announcements should consider - and where possible highlight - critical exposures that the End of Life action might create (e.g., increased security issues)

FCC TAC Coexistence in Unlicensed Bands (Etiquette)

Licensed and unlicensed spectrum is vitally important in meeting the nation’s communications needs and enabling US IoT leadership and innovation. IoT spectrum preference varies today between licensed and unlicensed depending on whether a device or product requires PAN, LAN, or WAN range connectivity; the technology (and spectrum) preference could range from ZigBee, UWB, Bluetooth, WiFi, etc. on the unlicensed end, to 3G, 4G LTE/LTE Advanced, and in the future, 5G at the licensed end. The TAC does not believe that IoT-specific spectrum allocations are necessary at this time. Licensed spectrum provides networks and users with protection from harmful interference by providing the licensee exclusive use of the licensee's spectrum. In unlicensed bands, FCC rules provide that unlicensed users must accept interference (and may not cause harmful interference). At its inception, unlicensed communication devices were a rarity and therefore interference from other devices was unlikely. As market growth evolved, there have been identified instances of a ‘crowding of the commons’. The heavy utilization of the 900 MHz unlicensed band caused a migration of cordless phones manufacturers to other unlicensed bands in search of the higher quality of service required for their application. Early Bluetooth devices caused significant impact on Wi-Fi operations until protocol changes implemented by the controlling standards groups’ minimized interference potential. There are also many examples of unlicensed devices successfully sharing spectrum. Unlicensed devices operating in the 5 GHz bands successfully share the spectrum with military radar based upon government-industry collaboration. While standards bodies have done a commendable job in seeking to act as responsible stewards of the commons, and often market forces require peaceful coexistence with popular consumer technologies, one of the most important attributes of unlicensed spectrum is that it does not require deployment of only standards based technology, but rather, as implemented by the FCC, permits any form of innovation provided that rules governing power levels and emission limits are observed. This has the benefit of placing the least restriction on product/technology innovation.

As IoT evolves, we may enter an environment where the number of wireless interconnected devices will be measured in the many billions of devices and where it is expected that many of these devices may well utilize unlicensed bands. All stakeholders should have a common interest in achieving co-existence, and there are different ways to meet this goal, depending on the technologies involved. The TAC has identified a series of best practices targeted at protecting the commons.

The TAC notes and supports the increased focus on spectrum sharing in even the most challenging scenarios. It is the TAC's view that unlicensed devices can successfully protect legacy and other devices from harmful interference where both legacy and unlicensed stakeholders work together to develop sharing solutions and implement best practices. The TAC recommends the following as best practice policies:

1. Standards-based solutions should continue to aim for co-existence. The major standards groups should develop and coordinate voluntary, industry led open standards solutions to protect standardized technologies from harmful interference.

2. Likewise, non-standard wireless solutions should strive to protect the commons in ways that allow the operation of other technologies within a shared spectrum space. For example, techniques such as carrier sensing or defined transmission time limits allow sharing of common spectrum resources with other technologies. Special modulation schemes such as spread spectrum may also serve to limit impact on other technologies or devices within a shared ecosystem. Whatever the approach, there should be a recognition of a shared commons and an objective of coexistence with other systems.
3. Instances in which the preceding best practices cannot be implemented should ideally be limited in scope and take into consideration the full ecosystem into which such devices might be deployed. For example, it’s possible that the use of proprietary technologies within a controlled environment would pose no risk to the commons.
4. The effective utilization of future technologies both spectrally ultra-efficient and permitting high degrees of spectrum sharing may be dependent upon all users employing similar technology within a spectrum band. While FCC policy in general has been to be nonspecific on technology that may be used within a spectrum band, the FCC should be open to future policy supporting ultra-efficient spectral technologies which may require that allocated bands be restricted to use of specific technologies and or control protocols.
5. The projected growth in demand for wirelessly connected IoT devices may potentially exhaust the currently assigned and available unlicensed and licensed spectrum. As new frequency

bands are allocated for both licensed and unlicensed use there may be significant value in re-examining co-existence techniques for unlicensed spectrum.

6. The IPv6 network protocol offers several advantages over IPv4 in terms of mobility, power usage and spectrum efficiency, and should be used where feasible.