

The viewpoints of Google, Microsoft and other technology groups opposed to the petition appear to be misanthropic and callous in regards to security.

Property is “a priori” when considering security as well as the foundation of law. There is no way to get around this when discussing Wi-Fi. When you go in to a store, you expect the property owner to provide a safe, secure and tranquil place and to use whatever means necessary to keep it that way. However, when it comes to Wi-Fi, some “experts” want to dispense with providing security for the sake of upholding some supposed rule.

Fundamentally, the question must be asked, who is ultimately responsible for the security of the Wi-Fi network? What risks are introduced by limiting the number of actions a network operator can take? What is so sacred about the deauthentication procedure that other means are required? No one has provided practical and logical reason as to why the deauthentication procedure should be banned in managing a Wi-Fi network other than to suggest it is rude and can be construed or used as a malicious attack. The attempts to compare deauthentication to jamming is not workable because deauthentication is very localized, temporary and takes place between two or more legal devices in short range of each other. (I suspect the reason Google and Microsoft have interest in this issue has to do with ulterior motives of wanting to establish city-wide Wi-Fi networks and are merely taking advantage of current FCC rules on Wi-Fi to circumvent licensing requirements and other political encumbrances. While such companies have honorable motives in providing free public Wi-Fi, the hotel industry provides more free Wi-Fi to more people than Google and Microsoft combined. The hotel industry could simply decide not to offer Wi-Fi at all.)

The operator of a stationary Wi-Fi network has an obligatory first responsibility to protect the rightful Wi-Fi users of their network as they are on their own property. This is not about monopolizing a frequency but self-defense. The network operator should not be forced to consult a plethora of regulations to determine what actions are acceptable to protect their network and property. In contrast, the owner of a mobile “hot spot” is accountable to no one but themselves and are only marginally inconvenienced by any action the Wi-Fi network operator takes to secure the system and can move out of the way of the stationary Wi-Fi network. Ultimately, the property owner does have one form of carte blanche authority over the Wi-Fi network. They can unplug it forever which would limit people to wired internet and mobile Wi-Fi hotspots. Or the property owner can shut the power off and evacuate the building and only let back in those who will comply with the will of the property owner.

With the complexities of networking and the current FCC rules which the “experts” disagree on, there is little reason for anyone to set up a public Wi-Fi network because enforcing security or holding anyone accountable has been made too complicated. To keep and read the current rules so onerously will merely discourage ownership of stationary Wi-Fi routers and discourage demand for public Wi-Fi as it would not be secure. The reason the USA is falling behind on this technology is the culture demands something for nothing and the end result is they get nothing. This is why people end up with unsecure but free public Wi-Fi networks which get bogged down by a lack of bandwidth. No one wants to invest in and operate a public Wi-Fi network that cannot be secured.

Many, such as Google and Microsoft, are merely reading FCC rules designed for radio, television and phones which are strictly forms of long distance communication and are trying to apply them to short distance Wi-Fi. However, Wi-Fi is not just mere communication. Wi-Fi helps everyone to avoid the encumbrances of cables and infrastructure which are forms of property. This is why people use Wi-Fi and its short range frequency as part of their home systems to connect numerous devices. It is a utility of the property. However, such connections have drawbacks in group settings. Steve Jobs of Apple Corporation had a very public experience with the problems of mobile Wi-Fi “hot spots” in a presentation in 2010 where he had to request attendees to turn off their “hot spots” so he could load his presentation. This is the hard problematic reality of mobile Wi-Fi “hot spots” and example where the “hot spot” owners yielded the right of way to the stationary Wi-Fi.

Furthermore, as the technology advances, a security hole continues to widen beyond the understanding of all the commentators. For example, the product known as the Square can be connected to an iPhone or iPad and take credit card transactions and signatures. (The iPad makes for a very workable cash register for a business I recently visited.) These devices have the ability to be their own “hot spot” (not to be confused with tethering). This could be used by street vendor or a brick-and-mortar establishment. Such device can be misused or easily stolen. The thief may attempt to connect such device to a local Wi-Fi network or their own “hot spot” to quickly copy and transfer the data they have stolen. A stationary Wi-Fi operator may be able to spot such activity and stop it if properly informed but security requires collaboration. A mobile “hot spot” user would need to communicate with operators of stationary Wi-Fi networks of whose property they are on. Through collaboration, they can both benefit. Criminals will collaborate and with the use of such mobile devices can overwhelm a Wi-Fi network.

As for the FCC Enforcement Bureau, it should err in the favor of security instead of giving the public 600,000 reasons not to have a Wi-Fi network and Wi-Fi connections. Cisco has provided the FCC with the most eloquent and level headed approach in their submission and I would encourage everyone to read it. They understand the problems involving the devices their company sells as well as how the FCC processes rules, regulations and policies. Cisco states, “. . .it is both unwise and premature for the Commission to try to establish formal rules that would distinguish between permitted and banned network management practices. The problem, simply stated, is that those who abuse Wi-Fi for illegitimate ends are clever and constantly devising new methods to take advantage of opportunities for wrongdoing. As a result, industry is constantly playing “catch up”, reacting as new techniques for abuse are developed. As a result, it would be a mistake for the Commission to take a snapshot of the current situation and develop a comprehensive regulatory regime that could preclude industry from addressing new threats as they arise.”

However, the FCC has apparently already established, at least through the Enforcement Bureau, formal rules that would distinguish between permitted and banned network management practices as it has resulted in a fine and a petition for a rule change. The FCC needs to insure stationary Wi-Fi operators have broad discretion in dealing with conflicts on and near their network as well as security concerns.

