A Review of Canadian Radiocommunications Law Around "Jammers"

Tyson Macaulay†‡

Introduction

This comment argues that the *Radiocommunications Act should be amended to relax the prohibition on specific types of "smart" jamming in the Industry Science* Medicine (ISM) bands. Specifically, the legislation requires increased flexibility and granularity to accommodate new wireless technologies in the ISM bands — particularly wireless LAN (WLAN) technologies like IEEEE 802.11b/IEEE 802.11g (WiFi), and IEEE 802.11a (henceforth collectively know as "ISM radios").

The availability of cheap, mass-produced ISM radios hardware and the proliferation of applications using the ISM spectrum bands of 2.4Ghz and 5Ghz present a variety of security and privacy concerns that cannot be effectively addressed by existing legislation, regulation, and law enforcement agencies. "Jamming" in certain forms represents a necessary, defensive capability for both users and non-users of the ISM-band applications.

To start at the end:

- It is proposed that jamming in the ISM bands — particularly for WLAN devices — should be redefined as a legal but licensable measure for organizations and individuals.
- It is proposed that the caveats put forth in this paper around ISM jamming be simultaneously employed to retain a prohibition against malicious or negligent use of jamming devices. Different "smart" jamming techniques and capabilities should be defined as permissible for usage, while certain forms of aggressive "dumb" broadcast jamming techniques can remain prohibited.

The proliferation of ISM networking devices, and specifically WLAN devices, has made this capability a requirement for corporate security and privacy protection. Additionally, the rationale used to maintain the prohibition around "cell phone silencers" does not apply to ISM networking: the spectrum is shared, not licensed, and there is no reasonable expectation of access to communications through ISM for "emergency communications" as articulated in the cell phone silencer debate.

Background to the Radiocommunications Jamming Debate in Canada

The jamming prohibition as it exists in Canada is represented by the *Radiocommunications Act*,[1] paragraph 9(1)(*b):*

> **9.** (1) No person shall
>
> (b) without lawful excuse, interfere with or obstruct any Radiocommunication;

"Lawful excuse" is clarified in Exemption Order No. 2002-1:[2]

> **2.** (1) Subject to sections 3 and 4, Her Majesty in right of Canada, as represented by the Royal Canadian Mounted Police and the Canadian Forces, is exempt from the application of subsection 4(1) and paragraph 9(1)(*b) of the Act for the period beginning on June 17, 2002 and ending on* June 29, 2002.
>
> (2) An exemption under subsection (1) is limited to that part of Alberta within the quadrilateral defined by points having the following geographic coordinates: 50° 45 N; 113° 34 W; 50° 45 N; 115° 30 W; 51° 6 N; 113° 34 W; 51° 6 N; 115° 30 W.
>
> **Conditions**
>
> **3.** An exemption under section 2 in respect of subsection 4(1) of the Act applies only if the radio apparatus referred to in that subsection is installed, operated or possessed in order to carry out interference with or obstruction of a radiocommunication in accordance with subsection 4(2) for the purpose of security or safety, international relations or national defence.
>
> **4.** (1) An exemption under section 2 in respect of paragraph 9(1)(*b) of the Act applies only if the radiocommunication is interfered with or obstructed for the purpose of* security or safety, international relations or national defence.
>
> (2) Every reasonable effort shall be made to confine or restrict to the extent possible interference with or obstruction of a radiocommunication referred to in subsection (1) to the smallest physical area, the fewest number of frequencies and the minimum duration required to accomplish the objectives of the interference or obstruction.

‡CISSP CISA

The above is a broad and sweeping prohibition of jamming and has been partially reviewed through the recent public consultation around "cell phone silencers". [3] From March 2001 to June 2002, a public consultation was held by Industry Canada around the utility of cellular phone "silencing" equipment. In the consultation paper, "silencing" was considered to employ up to 5 possible techniques:[4]

1. **Jamming Devices** — By way of radio frequency interference, the device prevents pagers and mobile phones from transmitting or receiving calls by transmitting a jamming signal.
2. ***Intelligent Disablers*** — *By way of a signal detection function, the device communicates with the base station of the mobile phone users' wireless service provider indicating that particular mobile phone is in a quiet zone and consequently communication is not established.*
3. ***Intelligent Beacon Disablers*** — *By way of beacon-like operation, the device instructs any compatible mobile phone to disable its ringer, turn down its volume or to switch the phone to a vibrate-signalling mode.*
4. ***Direct Receive and Transmit Jammers*** — *By way of base station-like features, the device interacts with the operation of local mobile phones in its proximity to break or unhook the* communications link, before returning to a passive mode.
5. **Passive Jamming Devices** — By way of electromagnetic interference (EMI) suppression techniques, a defined space/room is constructed in a way that prevents the transmission or reception of radio signals within the shielded space/room (commonly know as a Faraday Cage).

The definitions above use either "disabler" or "jammer" when referring to the different silencing techniques. The distinction in these terms represents the distinction between two broader categories of signal jamming: denial of service (DOS) jamming and deceptive jamming.

DOS jamming essentially has an impact on all wireless devices on a given frequency in a given area, much like a DOS attack on an Internet address will have an impact on all users and applications operating from a given Internet address, or possibly the entire network segment.

Deceptive jamming is also referred to as "smart" amming, whereby specific devices can be disabled, eaving other devices using the same radio spectrum to perate normally. This would be analogous to disabling e computer on the local LAN while leaving all the er computers (and users) unaffected and functioning.

The final decision from Industry Canada in Gazette ice DGTP 005-02 specifically disallowed all radio cers. [5] They are illegal for sale, manufacture, use, or import into Canada for entities other than those exempted specifically in the *Radiocommunications Act.*

The primary reason given for this position is that cellular radio communications in particular are now considered as critical communications tools. The examples of on-call doctors and emergency response staff like firefighters were cited in the decision as justification for the ban. This position represents a rational fear of uncontrolled "jamming" and the chaos it could inflict upon society and essential services; however, it fails to consider the unanticipated impact of blanket regulations *vis-à-vis unregulated portions of the radio spectrum, the ISM bands.*

The telecommunications carrier industry was, at the time, united in its opposition to radio silencers, basing its opposition on the "emergency communications" argument. This was a rational position at the time given that any potential, uncontrolled degradation in service (from private jammers) had a potentially massive impact on the perceived value of the wireless communications services on offer.

The general public tended to be split on the issue. Those members of the public who supported jammers cited nuisance and annoyance factors. The supporters advocated regulation via by-laws, in the same way many nuisance issues such as noise and unleashed dogs are regulated. [6]

An important point to note in the cellphone silencer decision is that, while deceptive/"smart" cellphone jammers are prohibited, they also do not exist. Deceptive jammers, as described in the Industry Canada consultation paper, are not manufactured and could not be supported under the currently available cellular infrastructure. Significant improvements and investments would have to occur in both mobile phone and base-station technology. Such investments are not forthcoming in the near future, and there are no current business cases to support such investment. Therefore, the prohibition itself is pre-emptive in the case of cellular services.

The cellphone silencer consultation process was extensive. It is not the intent of this paper to re-open the issue of cellphone silencers. However, the wording of both the consultation paper and the resulting Order in Council amending the *Radiocommunications Act cast a wide net in terms of prohibiting all "wireless" silencing/jamming devices, rather than only cellphone devices. It was likely the intent of Industry Canada to do precisely this: ban all wireless jammers.*

In the case of ISM (specifically WLAN) technologies, the deceptive technology does exist, and there is a business case and requirement for jamming: security and privacy protection. The Order in Council has inadvertently hobbled businesses, consumers, and government from implementing an increasingly important set of information asset safeguards.

Even before the Order in Council was finalized, technology had already substantially changed both the requirements and business case around certain types of jammers, WLAN jammers specifically. Sales of WLAN equipment operating in the ISM 2.4Ghz and 5Ghz bands have skyrocketed. Similarly, the cost of this equipment has fallen very significantly, to the point where it is available to just about any organization or individual. It is now possible to buy "starter" kits consisting of an Access Point and accompanying interface card for less than $100. Additional WLAN radios for standard laptop computers cost less than $50 and can be purchased at any office supply store. The combination of the affordability of WLAN equipment with the savings,[7] convenience, and mobility of wireless communications presents a major potential security and privacy problem that under current regulations is unaddressable, and a legitimate business opportunity around remediation that is prohibited.

The security and privacy problems relating to WLAN radios have been documented and reported extensively in both academic and professional forums, and in the media at large.[8] For the following reasons, WLAN radios can create major security and privacy (therefore possibly regulatory) problems for organizations and individuals:

- Unauthorized backdoors: WLAN radios are very easy to acquire and connect to fixed-line networks without any technical skills. WLAN radios are cheap and very attractive because they are an obviously useful improvement over fixed-line networking, so well-meaning but naive users establish them inside corporate networks without permission. These WLAN radios create a direct, back-door into the network they are attached to, like a second Internet connection, but without the knowledge of the network administrators or the benefit of a firewall.
- Awareness and containment: Unlike fixed-line networks, which require some sort of professionally installed point of demarcation, unauthorized WLAN connections to the network can appear inside organizations literally over lunch, and disappear as quickly. Network or security staff will have a great deal of difficulty spotting these back doors — consequently, in most cases, they are unaware of the extreme vulnerability that has appeared. Even with sophisticated and diligent monitoring of network traffic, the difference between knowing the unauthorized device has appeared and disabling the device is the difference between hearing a barking dog in the night and then locating and muzzling the dog.

Due to these two issues, WLAN radios can present substantial threats to the security and privacy of data. An easing of the ban on "smart" jammers may allow these issues to be addressed.

A Framework for Smart WLAN Jamming

Data security generally consists of three elements: confidentiality, integrity, and availability. Confidentiality relates to the threat of unauthorized disclosure or publication of information, and broadly, loss of privacy. Integrity refers to threats related to corruption, unauthorized alternation, substitution, or removal of data. Availability relates to threats that can make data unavailable or delayed when it is needed. While confidentiality and integrity issues are dealt with extensively by a variety of cryptographic tools and techniques available for modern WLAN radios, it is the element of availability and WLAN radios that presents major security concerns and is impacted by the prohibition on jamming.

For the purposes of this discussion, organizations can be grouped into two classifications: those sanctioning WLAN radios for internal usage and those prohibiting WLAN radios. In the first case, these organizations may use WLAN radios and networks for mission-critical systems and information, and rely on WLAN radios to connect people to core resources. In the second case, organizations may have established a prohibition for any number of security reasons. For instance, risks associated with deliberate or accidental exposures through (difficult to control) wireless interfaces may be too substantial, so information is restricted to fixed-line networks only. In both cases, the availability of WLAN radios is of prime concern. Smart jamming is one of the few means by which these organizations can warrant the security of their data resources.

In the first instance, organizations utilizing WLAN radios benefit from an option to implement security tools to protect and manage the availability of WLAN resources. However, the nature of WLAN radios and networks is such that they are subject to frequent and often substantial fluctuations in services levels. Additionally, traditional network management techniques can address "abusive" devices that threaten availability. Smart jammers are not justified by the needs of these WLAN-"friendly" organizations.

In the second instance, organizations imposing a prohibition on WLAN radios need to have the ability to enforce this prohibition through localized smart jamming of WLAN radio devices. Such a capability is analogous to being able to disallow Internet access to certain parts of the corporate network, or the network as a whole, practices common in organizations with valuable data, such as financial institutions. Under the current policy position of Industry Canada, organizations attempting to enforce prohibitions on WLAN devices for a variety of overwhelming security and privacy imperatives are hamstrung.

In Canada, the United States, and much of the world where sophisticated spectrum regulation is in

place, anti-jamming policy was developed based upon a snapshot in time of wireless technology. In revisiting the regulations around smart jammers, the following criteria may prove useful:

- Smart jammers are only permissible in ISM bands.[9]
- Smart jamming devices must comply with all ISM device regulations.[10]
- Smart jammers cannot be automated, and jamming must be manually invoked by an operator.
- Smart jammers cannot be deployed in such a manner that they impact the legitimate use of ISM devices by any third party.
- Public notices that smart jammers are deployed must be posted, such that potentially impacted third parties are aware of their existence.
- The deployment of smart jamming technology is subject to regulatory notification/licence and associated registration fees.[11]
- Sanctions are associated with inappropriate, negligent, or malicious employment of smart jammers.

Conclusion

Starting in the summer of 2002, the introduction of active, network-based attack counter-measure tools started a debate around what came to be known as "strike-back",[12] a phenomenon whereby protagonists launched counter-attacks against Internet sites that appeared to be the source of network attacks over the Internet. One side of this debate argued that such counter-attacks will inevitably go astray and are counter to our natural response system, which assumes innocence and deplores vigilantism. The other side in this argument claims that self-defense is an immutable right and that these responses are not punitive, but rather, remedial.[13]

The ideas presented in this paper do not represent a wireless version of "strike-back". The Internet and fixed-line networks are too substantially different from WLAN networks to make the comparison sustainable. The fixed-line Internet allows attacks to be launched from the other side of the world. Attacks originating through WLAN networks must be highly localized because of the power limitations of these devices. It is significantly less likely that smart jamming (if regulated as described above) will disable an unintended device or start a catastrophic, cascading series of counter-measures.

The reservation of the ISM spectrum bands for use by low-power, unregulated radios has proven to be a highly productive industrial catalyst. A wide variety of wireless technologies and applications are flourishing in the ISM bands, and will continue to do so. The fundamental condition of ISM that has made it so successful is the limited amount of regulation. The regulation that does exist for ISM has been tempered specifically to allow for innovation.

The "cellphone silencer" consultation led to jamming of all sorts being conclusively prohibited (except for law enforcement and the military). However, cellphone jamming is fundamentally different from the propositions posed here, for two reasons:

1. The cellular and PCS spectrum is reserved, regulated, and paid for through license fees paid by carriers, and in turn, subscribers. Both carriers and subscribers expect unimpeded access to this spectrum for the tariffs they pay. It is also a matter of accessing critical infrastructure for emergency purposes, which was the fundamental basis of the Industry Canada decision. But no one has paid for ISM spectrum access. No one has a reasonable claim to unlimited access. No one can argue that ISM must be available for emergency communications; therefore, engaging all available protections for this spectrum is out of proportion to the reality of the benefits and risks associated with this substantially different use of spectrum.
2. Unlike cellular and PCS equipment, the cost to obtain an ISM (WLAN) radio transmitter and establish a network for it is trivial. Put another way, no one is likely to connect a "rogue" GSM or CDMA basestation to a LAN.

Notes:

[1] *Radiocommunications Act, R.S.C. 1985, http://strategis.ic.gc.ca/epic/* internet/insmt-gst.nsf/en/sf01140e.html.

[2] http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/en/sf05959e.html; SOR/2002-223.

[3] http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/en/sf05408e.html.

[4] http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/en/sf05401e.html.

[5] http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/en/sf05958e.html.

[6] See the comments received by Industry Canada to the consultation paper: http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/en/sf05415e.html.

[7] 802.11 Planet — http://www.80211-planet.com/tutorials/article.php/953691.

[8] WiFi Planet (formerly 802.11 Planet) http://wi-fiplanet.com/ is a rich source of technical news and discussions around ISM and WLAN security. A search on the term "802.11 security" returns over 1500 articles.

[9] Until such time as they become viable for metropolitan area networks such as cellular services.

[10] For instance, no enhanced broadcasting power.

[11] Similar to the way point-to-point wireless links in 23/28Ghrz must be licensed for a nominal fee.

[12] Crypto-gram, December 2002 — http://www.counterpane.com/crypto-gram-0212.html.

[13] Strikeback Whitepaper — http://www.hammerofgod.com.