Chris Kalmar
208 1st avenue
Hiawatha ia 52233
Area code 319 phone number 775 5132
Chris451(at)hotmail(dot)com

Office of enginerring and technology

The following section from FCC47CFRpart15.pdf should be reconsidered and struck from the requirements for manufacturers of scanning receivers.

Introduction:
I am a scanner user and amateur radio licensee, and an almost constant user of scanning receiver technology. I maintain a large stock of old and new scanners, many of which predate these rules, and some that are post rulemaking. In my work I am currently an RF engineer. I've studied many of the FCC Rules over the years in the categories of Licensing, antenna towers, Amateur radio, Receivers, and Broadcast, and hold a 2nd class radiotelephone and amateur extra license. I have worked at in RF design for 32 and am currently employed doing the same at a small company.

Complaint:
1) Blocking cellular frequency bands from scanning receivers or general purpose receivers serves no useful purpose, since most cellular systems have migrated to a secure digital format.

2) New receivers meeting the part 15 are expensive to repair and can be un-repairable by even expert users due to potting on the boards and lack of design info and schematics which are useful to repair the radios at low cost. Uniden charges 1/5 the cost of the radio and throws out the bad board board and will not sell parts or board or even case parts (but maybe that's just their policy) Basically this makes our hobby more expensive. All the manufacturers are difficult to get manuals from for continued maintainance of the radios. You have to send it in or reverse engineer it which is a waste of our time.

3) Digital radio formats in use today require IF outputs and decoder adapters to be decoded, such as the "P25" apco-25 which has QAM formats, so an IF output or I/Q output is required to use a receiver for that purpose. A wide IF output is required to tune a TV signal in analog or digital format. A complete spectrum is needed to tune the typical 54-890 cable spectrum.

4) Access to all frequencies is required for use with frequency converters and closed radio systems on coax and for testing antennas. The receivers which are provided with a TV demodulator would need to tune all channels on an analog cable system including those between 806-890.

5) Access to cellular frequencies is required for antenna configuration and testing (especially to locate which system and tower provides a signal to a rural location.

6) The part 15 rules will have a poor security effect for perhaps 50 to 100 years. The effort to block access to cellular frequency bands was a political move by congress and cell companies and did not guarantee any signal security to analog cellular signals (due to legacy equipment) and was

not needed (the political hack job on Gingrich by his opposition where they played his analog cell calls) as the communications privacy act made that illegal already. It is a violation of the constitutioni to attempt to recover all legacy receivers now in the hands of the public.

8) Blocking the cell frequency and meeting all the requirements in the amendments to this rule (spurious reception) resulted in some prize winning band blocking (icom R3 had nearly all of the useful parts of the 800-900 removed by software blocking) making this radio useless for the whole band., and even with the specs I still got CDMA noise on spurious because they are so strong. Yes that means the FCC did not evaluate the radio well enough to catch this. Clue: it used a 1ghz and 2ghz down converter and there was leak through on the downconverter at 1880 so you still hear CDMA there……so even the "worst victim" of this rule still got the cellular band via spurious or leak through. Whatever engineer they had checking it failed to discover this. Even after all the hearings with Bob Grove about image reception they still missed this.
There was one welcome benefit, the new designs have a lot less spurious response than early designs along with very low L.O. leakage.

9) This rule is inconsistent. There are no analog cellular signals on the air in the US. A phase out has occurred of all analog handsets and base stations. There are no more analog control channel. You can't get an analog provider in the USA unless its something like a phone patch on 460mhz. However, PCS (1800 band) has always been digital from the start. There does not appear to be any compromise of these signals because from the start they were designed with encryption on the signaling side with public private encryption key exchange and encryption of the voice traffic (see the IS-95 cdma specs) So many of the radios I have do cover PCS bands, since they are called PCS not Cellular and were always digital).
And, the formats found on pcs are CDMA, GSM, and TDMA. GSM and tdma is frequency hopping which would require a cellphone chipset (you can get those in a handset for 15 dollars now)
.
That CDMA format is the same thing found on 800 cellular now. There is CDMA on A and B systems, and TDMA on the Nextel band(I consider this to be an expansion of the 800 cell bands made just for Nextel lobbyists so they could get into that chunk of spectrum without the interleaved mess they had before "rebanding". So if there is no "harm" in receiving the 1800 band, then the same formats on the 800 band should cause no harm.

10) It is preposterous to assume the cellular security is improved by blocking these bands. The cell companies were forced to change their technology due to widespread phone cloning perhaps due to high pricing. They simply could not get some customers until they went to a digital format. The ruling might have an effect here over a period of 30 – 50 years as the legacy equipment becomes unusable but don't count on it, I still see collection of radios from 60 to 100 years ago.

11) There is no benefit to blocking cellular bands from scanners, the protection of the cell signal lies in its encryption.
To do so requires data capture of both ends of a cellular call at the same time a call is set up, and the ability to break an encryption algorithms. Security all depends on the math. How many bits of encryption do you use. How are the keys managed? How big are the keys? How hard is it to

12) A wide bandwidth IF output is required on a receiver used by amateur radio for wide band data or analog/digital television on the amature bands, and the large receivers,

11) To decode the CDMA and other waveforms, it would be fairly easy to tap in on the guts of a cellphone chipset but even full control of that chipset would not work due to the key exchange encryption, so its pretty well protected at all angles.
.
12) Lack of access ports on and design info on radio chipsets hurts the state of the art in amateur radio where there is interest in software defined radios, and wide band digital formats. CDMA should rely on it's encryption for security.

13) These cell calls all go over digital microwave and land lines, without encryption. If you want real security it has to have encryption end to end, which most cellular does not. CDMA just has it on the air side. GSM and TDMA at the very least would require full control of the appropriate chipsets, which are only available as developer kits for cellular manufacturers, and are very expensive.

14) The U.S. govt uses encryption on many of the radio systems they use, such as P25 or DVP or FIPS or satcom or airborne. You can detect them but not decode them, and they don't seem to be any more or less effective at what they do. That seems to be good enough.

15) True signal security is only available with end to end encryption This can be done with a laptop, a cellular modem, and software such as speakfreely.

16) Access to all frequencies is critical for health and welfare. Example: Because I was able to receive numerous frequencies with my legacy radio equipment, I was able to batten down the hatches at my home in advance of a severe windstorm occurring in July of this year. One radio that suffers from this rulemaking due to spurious is the Icom R3. The radio had an analog TV receiver capability as well as a

17) These rules have a negative impact on the manufacturers of scanners radios and receivers. The old radios can be maintained and have a lower lifetime cost then new ones with potting or lack of documention.

18) There is no harm to anyone in removing all these rules. Cellular companies have a "secure enough" system that prevents "the public" from decoding voice traffic. From what I've read about the various standards, they all have encryption in use for access, they all have digital formats that would require the appropriate chipsets to decode, and I have heard of zero cases in which a CDMA, TDMA, GSM Tetra or Encrypted P25 or DES DVP FIPS communication has been decoded and demodulated by the use of a scanning receiver.

19) This set of rules and many others are obsolete or only serve to tax or redistribute tax (as in license fees) . FCC Rules should expire or be re-justified and are not keeping up with technology shifts, although they do seem to keep up with lobbyists. .

20) Frequency restrictions on receivers signal a decrease in the freedoms of the american people. These restrictions do not exist anywhere else except some contries that use taxes on radios that receive broadcasts, such as France. They seem to find digital cell is adequate security.

21) Communications I've had with the FCC led me to the electronic filing system. I expect to see this appear on the FCC agenda, and I will contact all my federal representatives if this does not get done.

22) Criminal activity has been detected and turned in to law enforcement on analog cellular systems. This has ceased (on the over the air side) since the digitization and encryption of most digital cellular signals.

23) Cellular privacy was not a concern to many analog users. They all seem to realize someone could listen to them, but took the risk with what they were saying. A common attitude was "they will get awefully bored listening to me" Many complained about the poor voice quality of digital.

As far as I can see from history the request to remove cell band from scanners came from politicians and cellular providers, as a stopgap before they really began working on signal security. There was a real battle to stop cloned phones which drove them to the need to change the whole system. They had a desire to reduce the widespread nature of cell cloning from over the air transmissions, by limiting access to the all frequency receivers, but knew they could never eliminate all of it until they redesign the whole system. Thanks to the math wizards at qualcomm and a few other companies, not only could the cell companies secure their services but the signaling as well, and not only that cram more calls into each tower than ever before. So now that they have a "secure enough" signal then justify why there is harm in receiving these digital carriers? Cloning has been rendered too difficult, and demodulation to a voice signal is totally impossible without a truckload of equipment and computers. Its not going to happen and is totally impractical and without motivation.

24) Tracking down interference is not done by the FCC it is done by amateur radio operators, radio shops and some radio experts. The only thing the FCC has to do with it appears to be making phone calls and writing letters based on complaints. As such it is a benefit to have general coverage radios that cover all frequencies.

25) New technology is on its way and we don't need obsolete rules limiting what it can do or what we do with it. It is expected that with new synthesizer chipsets I've been working with, along with SiGi technology, some very wide band radios will become products in the next few years. For example a chipset that can synthesize from 25-4000 mhz exists. I can think of nothing more disgusting then to have that kind of radio with complete coverage other than "analog cell" cut out of it because there used to be analog cellular.

26) The FCC is not serving the citizens by claiming "cellular blocking" secures the cell signals and appear to be against the use of encryption on telephone circuits. It is serving only lobbyists, and pays no attention to its obsolete rules. The attitude of the FCC according to a letter I got from Genekowski is you don't need that, just go buy test equipment to do that.
Meanwhile I could be using a small hand held device and instead he is saying I have to lug around a 15000 dollar spectrum analyzer that runs on AC when I could be using a slick new battery powered pocket sized digitally controlled super radio to do the same thing.

27) Frequency converters are needed by amateur radio to access some of the bands like 220, 902, 1240-1300, due to a lack of manufacturing there. Kits are the only answer I see, and are easier than collecting the parts and working from scratch. Time effort and money are used up.

28) Radios that cover the cell bands are not used to intercept a call. They simply are not useful for that. They are only useful for signal and interference detection, measurement of power versus frequency, mitigation of interference, and tuning to closed RF systems or RF conveter outputs. They are also useful for detecting intentional and unintentional cell phone jammers. Many of these sources are a drifting signal that goes in and out of the bands.

29) Complete signal security is easy with an all digital cellular system, with the use of encryption. Even simple digitization of the signals is not enough, its going to take encryption, so the cellular companies have a vested interest in getting their users to pay for service, so they will have to use encryption. That is what prevents cellphones from being monitored, not blocking out our receivers.

30) Communication act of 1934 provided a law dealing with divulging communications, and to this day that law would apply to anyone tapping in on phone circuits. This law is only broken if the information is divulged.

31) I have checked with US rep office and they say FCC is responsible and they did not look into this complaint they refer me to FCC. I have checked with Charles Grassley's office and he says contact them if I have any trouble with Getting FCC response on this.
I have checked with the FCC and they say use the comment system to address the issue.

32) Should it be replaced? Yes – require encryption for any "private" communication

33) What should be private? Not most public safety. These communications are very helpful for public safety even if you are just a listener. And we the public paid for it and should be able to use it for our own good.

If it is replaced with anything it should say Cellular providers should use adequate encryption to prevent interception of the cellular voice content. That should apply to texting, if that is something you want to protect. That would also apply to paging or any other format that protection is needed for. Encryption is easy and cheap to implement. With a computer, cell modem and software it is possible to communicate with complete security end to end. That is not provided by telephone switches. The part of a cellular call that transits a phone network is not protected. If this is needed justified or required then encryption should be required.
If its good enough for the US Government than its good enough for the consumer.

I have never owned and rarely used analog cell phones except on the land line end. If I did use one it was with the assumption someone was listening, but that they probably don't know who it is. That is still true of analog cordless phones, and even digital as I have found similar brands wil l pick op other (same brand and model) handsets and base stations. So they aren't doing anything but digitizing, with no security. Not true at all of cellular systems. We just get dropped calls.

Here is a quote from cfr47 and the section of part 15. that I would like to be removed.

Section 15.121 Scanning receivers and frequency converters used with scanning receivers.
(a) Except as provided in paragraph (c) of this section, scanning receivers and frequency converters designed or marketed for use with scanning receivers, shall:
(1) Be incapable of operating (tuning), or readily being altered by the user to operate,

within the frequency bands allocated to the Cellular Radiotelephone Service in Part 22 of this chapter
(cellular telephone bands). Scanning receivers capable of "readily being altered by the user" include,
but are not limited to, those for which the ability to receive transmissions in the cellular telephone
bands can be added by clipping the leads of, or installing, a simple component such as a diode,
resistor or jumper wire; replacing a plug-in semiconductor chip; or programming a semiconductor chip
using special access codes or an external device, such as a personal computer. Scanning receivers, and
frequency converters designed for use with scanning receivers, also shall be incapable of converting
digital cellular communication transmissions to analog voice audio.
(2) Be designed so that the tuning, control and filtering circuitry is inaccessible. The
design must be such that any attempts to modify the equipment to receive transmissions from the
Cellular Radiotelephone Service likely will render the receiver inoperable.
54
(b) Except as provided in paragraph (c) of this section, scanning receivers shall reject any
signals from the Cellular Radiotelephone Service frequency bands that are 38 dB or higher based upon
a 12 dB SINAD measurement, which is considered the threshold where a signal can be clearly
discerned from any interference that may be present.
(c) Scanning receivers and frequency converters designed or marketed for use with scanning
receivers, are not subject to the requirements of paragraphs (a) and (b) of this section provided that
they are manufactured exclusively for, and marketed exclusively to, entities described in 18 U.S.C.
Section 2512(2), or are marketed exclusively as test equipment pursuant to § 15.3(dd).
(d) Modification of a scanning receiver to receive transmissions from Cellular Radiotelephone
Service frequency bands will be considered to constitute manufacture of such equipment. This
includes any individual, individuals, entity or organization that modifies one or more scanners. Any
modification to a scanning receiver to receive transmissions from the Cellular Radiotelephone Service
frequency bands voids the certification of the scanning receiver, regardless of the date of manufacture
of the original unit. In addition, the provisions of § 15.23 shall not be interpreted as permitting
modification of a scanning receiver to receiver Cellular Radiotelephone Service transmissions.
(e) Scanning receivers and frequency converters designed for use with scanning receivers shall
not be assembled from kits or marketed in kit form unless they comply with the requirements in
paragraph (a) through (c) of this section.
(f) Scanning receivers shall have a label permanently affixed to the product, and this label
shall be readily visible to the purchaser at the time of purchase. The label shall read as follows:
WARNING: MODIFICATION OF THIS DEVICE TO RECEIVE CELLULAR
RADIOTELEPHONE SERVICE SIGNALS IS PROHIBITED UNDER FCC
RULES AND FEDERAL LAW.
"Permanently affixed" means that the label is etched, engraved, stamped, silkscreened, indelibly printed
or otherwise permanently marked on a permanently attached part of the equipment or on a nameplate
of metal plastic or other material fastened to the equipment by welding, riveting, or permanent

adhesive. The label shall be designed to last the expected lifetime of the equipment in the environment in which the equipment may be operated and must not be readily detachable. The label
shall not be a stick-on, paper label.
Subpart C - Intentional Radiators