Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Carrier Current Systems, including Broadband over Power Line Systems	)	(ET Docket No. 03-104)
	)	
	)	
Amendment of Part 15 regarding new requirements and measurement guidelines for Access Broadband over Power Line Systems	)	ET Docket No. 04-37

REPLY COMMENTS ON NOTICE OF PROPOSED RULE MAKING

Commissioners:

This is a second reply to FEMA's (U.S. Dept. of Homeland Security) letter of January 8, 2004 to Michael K. Powell, Chairman, FCC, which appeared as a comment for this docket, posted 3/23/2004 and again 04/01/2004. FEMA's January 8, 2004 letter was itself a "clarification" of their earlier December 4, 2003 comments, which itself seemed to me to be more direct and explicit than the clarification. But that's okay, I love a good mystery!

FEMA now has expressed a vote of confidence in the FCC's sensitivity to some vague concerns of potential interference from BPL to HF emergency communications, but has more or less left the matter up in the air. The great but fictional Sherlock Holmes once said, "The observer who has thoroughly understood one link in a series of incidents should be able to accurately state all the other ones, both before and after."[1] I recall that FEMA has in the past defended amateur radio frequencies from potential interference——see supplement——, as the amateurs have done a worthy job of conducting emergency communications, so I suppose that if we were to thoroughly understand the amateurs' concerns, those of FEMA would be covered too. The amateurs certainly have not been bashful about stating theirs.

FEMA ended their letter by offering "assistance in any way the Commission might find helpful," and in fact there is some FEMA material which can be extrapolated (à la Sherlock Holmes) in regards to the proposed "interference mitigation techniques [which] would include ... the ability to include or exclude specific operating frequencies or bands" (**FCC 04-29, ¶ 40**). True, FEMA may not have yet experienced "a material interference

[1] Sir Conan Doyle, The Five Orange Pips

problem" (letter), but then BPL test sites are in out-of-the-way places and actual emergencies have been (mercifully) few and far between, so we might not have expected them to. And yet, FEMA has reference——see supplement——linked to their web site of instruction which includes instruction in communications issues, and one of them is the need for adaptive frequency use——see supplement——when applied to fighting fires, the need for a separate tactical frequency. I realize having a fireman switch his radio to a tactical channel when the main channel is too busy to get through is a different frequency adaptation from having a BPL operation move off a frequency they are jamming, but lacking data on the latter, Sherlock Holmes might want to extrapolate from the former.

> Among the most well-documented cases of a communications failure contributing to firefighter fatalities, was the July 1, 1988, fire at Hackensack Ford in Hackensack, New Jersey. ... In 1988, Demers wrote about the Hackensack fire, concluding that a "major contributing factor" resulting in the firefighter deaths was the "lack of effective fireground communications both on the fireground and between fireground commanders and fire headquarters."[2] ...
>
> Demers analyzed the sequence of communications made by the trapped firefighters, which extended over a 15 minute and 50 second period.
>
> Among the points Demers made was that Hackensack's single radio channel was inadequate to perform all the functions expected of it, including dispatching apparatus, fireground operations, recall of off-duty personnel, and emergency medical calls. Demers cited numerous times when the dispatcher "over-rode" the radio transmissions of fireground units, including urgent requests for help by the trapped firefighters[3]. [4]

In my own comments, made from the perspective of an amateur radio operator, I had suggested that BPL companies be required to maintain an interference hotline which a party being interfered with can phone and enter his frequency in kilocycles on the keypad of his phone to have the BPL company close down that frequency plus and minus 10 kc., for an hour. I suggested there be a ten minute time limit after which the whole operation would be required to close down if it could not respond in time, and furthermore that there would be a closed loop "deadman's switch" which would shut down the BPL system if they could not phone their own number with a dummy code and get an acknowledgement in ten minutes. If those firefighters had only fifteen minutes in which to get their communications through before it was too late, then getting the BPL interference

---

[2] D.P. Demers, Five Fire Fighter Fatalities: Hackensack, New Jersey: July 1, 1988. (Lunenberg, MA: Demers Associates ,1988) p. 1

[3] Ibid., p. 15.

[4] http://www.usfa.fema.gov/fire-service/nfa/courses/oncampus/abstracts/tr_96cv.shtm

to move off frequency within ten minutes might save them just as having switched to an unoccupied tactical frequency in ten minutes would have.

Pursuing our investigation, Sherlock Holmes also said, "There is nothing more deceptive than an obvious fact."[5] The obvious——and oh, so deceptive——fact here is that BPL signals are weak. Yes. How weak? Well, nobody knows the actual power level because it looks like they won't be required to measure the injection, and there really isn't much competent literature on the subject, but one of the commenters cared to speculate:

> If the drop-end signal level is 10 milliWatts peak power and the total coupling loss or level shift is 40 dB, the main Access BPL distribution power level must be 100 Watts peak. The majority of amateur radio HF transceivers' transmitter power output is 100 Watts. ...
>
> ... Given the previous speculative scenario with 40 dB power level change, the outgoing Access BPL signal would have to be at a 10 Watt power level to achieve a 1 milliWatt head-end power level. The 10 Watt level would be at the subscriber end and itself under scrutiny for incidental RF radiation. The downlink power level versus uplink power level on the main Access BPL route would then be 100 W to 1 mW or 50 dB. For asynchronous data flow that would be a most difficult task.[6]

Amateur radio operators are permitted less operating power than, say, international broadcasters, but most of our HF sets only put out 100 watts which still is enough for worldwide communication. The other day I surprised myself by working a station on an island in the Indian Ocean from my home in Oregon running just 100 watts to a dipole on 30 meters. There were other stations calling him, and I didn't expect him to come back to me, but he did. I was deceived by my low power and simple antenna which did better than I expected.

Running under ten watts, I managed to obtain a certificate for Worked All States and one for Worked All Continents. I've also had stations on distant continents return my low power call rather than someone else's. Low power is deceptive because it can work wonders at times.

I've worked stations in many countries running 2 watts on ten meters, and running 2 Watts PEP which is about 1 watt average, I've worked as far as Tennessee on a handheld with a whip antenna. I was surprised and the other station was surprised too.

Running 750 mW to a 130 ft. loop on 40 meters I could consistently check into a QRP net covering the neighboring states. Still, it would surprise me sometimes. It seems to me the BPL companies' claim of noninterference based on their low power falls into that same deception.

My own comments from an amateur's perspective recall that an FM translator running 1 Watt or more must identify itself every hour in Morse code. Sine BPL companies will run similar or more or less power than that, at least spread out across town

---

[5] Doyle, The Boscombe Valley Mystery

[6] Comment on 04-37, Leonard H. Anderson, 03/09/2004, pp. 7,8.

by their power line antennas, they should be required to identify at least once an hour on every band they occupy. My suggestion is that they transmit a seven digit number changed daily at midnight, along with their power company's or their own initials (but not SOS), so that a party being interfered with could call their hotline number and enter the received i.d. #, to have that band taken out of use until midnight again.

My third quote from Sherlock Holmes is, "I was already firmly convinced, Watson, that there were not three separate mysteries here, but only one."[7] There are three mysteries presented to us by the BPL companies. The first is how an rf source connected to a sky-hook (antenna) is nothing but a point source. Very mysterious whatever happened to Maxwell's wave equations and all their applications over the decades.

Secondly, even with BPL's limited and unpublicized BPL tests, there have been some interference complaints I've heard of in ham circles, especially to mobile operations, but the BPL companies have claimed none, and furthermore, they want to proceed at full speed to catch up with the other countries trying BPL, when such and such countries have ended up banning BPL because of all the gross interference it caused. But not a word about that. Very mysterious, what happened to all the reported interference.

Thirdly, BPL companies have touted their system as a boon to homeland security, when homeland security requires cooperation and coordination, and the BPL companies have given the cold shoulder to amateurs and others who might need clear frequencies in an emergency. I mean, the BPL companies flatly deny any possibility of interference, they do not invite amateur radio organizations to their test sites or to their demonstrations, they do not link their web sites to the many ones portraying the interference problems BPL has caused and can cause, and they don't mention anything about interference and its supreme remedy to the press when they promote their system. If they are so bent on homeland security, where is the cooperation and coordination that's to be part of it?

I believe these three mysteries all have a common $ource. It's elemonetary, my dear Watson.

Perhaps an analogy might help. Take cell phones, a new technology back in the 1980's. The FCC sees itself as promoting new technologies: cell phones and BPL. Cell phones can and do have a public safety benefit, although from what I've heard them used for in public, it's mostly inane conversation. BPL likewise could be a factor in achieving homeland security objectives according to FEMA. But mostly it would be used for whatever the internet is mostly used for. Okay.

During a *major* disaster, cell phone systems get tied up and overwhelmed or the towers themselves are out of service rendering cell phones useless. Likewise, BPL is very dependent on an up and running infrastructure in order for it to at all work. Big disaster happens, we might not have BPL where it's needed and would have to depend on a backup system anyway.

Okay, let's look at this article from the Associated Press which I clipped out of my newspaper yesterday——see supplement. It seems that the FCC assigned cell phones to the same band as public safety radio, not anticipating the cell phone boom. That has caused some interference problems with cell phones interfering with police calls. The

[7] Doyle, The Musgrave Ritual

press seems to be blaming the FCC for lack of foresight. We sure wouldn't want that to happen again.

One "plan would divide the 800 MHz band, giving one section to public safety agencies and another to cell companies. That idea is backed by various national law enforcement groups, as well as Mitchell's fire chiefs association."[8] That seems to me to be like the favored plan of radio amateurs and other HF spectrum users, to relegate BPL to microwave frequencies, above 500 MHz, and leave the HF band for its incumbents.

"Opponents want to leave the spectrum alone, but require each company that causes interference to eliminate it at its own cost after a public safety agency reports a problem."[9] That sounds more like the foresight of the FCC regarding BPL, except that the BPL companies would take less of the burden than I would like to see. I believe they should also be required to transmit an identification with their injected signal and have an automated telephone system for eliminating interference in real time. I don't know what they would think of this idea, but it might go something like this (to borrow a conversation from a novel):

> "What is important, Ted," Lucille Guillard said smoothly, "is that the bank and the switching station come up with a real-time environment that makes it possible for Sergeant Boldt to track certain withdrawals."
>
> "I understand that, Lucy. But what I'm trying to point out—to *both* of you—is that real-time monitoring just isn't possible across the entire network. No such software exists—not that I know of. It's just not something we're set up to do. What? What, Lucy? Why are you looking that way at me?"
>
> "It is something you *must* do. At the moment, Sergeant Boldt is asking politely. None of us, the police, the bank, wants to initiate legal steps. The idea is that we cooperate."
>
> Ted Perch looked a little hurt. She knew more than he did, and he did not like that. And if he tried to look up her skirt one more time, Boldt was going to say something about it.
>
> He nodded slowly at her, made a sucking sound in his teeth, and directed himself to Boldt. "The way the system works is this, Sergeant. The account in question is with Pac-West. Clear? If a Pac-West ATM is used to access this account, as I'm sure Lucy explained to you, then that request goes directly to their server. Several verifications are made almost instantaneously, the server okays the withdrawal and instructs the ATM to dispense the cash. Wham-bam, thank you, ma'am. But in the case of a Pac-West customer using say a First Interstate ATM, that's where we come in. First, the PIN—the personal identification number—is encrypted by the machine, so as it travels along these phone lines, no one can

[8] www.registerguard.com , *The Register Guard*, Eugene, Oregon, April 6, 2004, p. A6 Copyright 2004, The Associated Press

[9] Ibid.

grab it. Next, the account number and a BIN number——the bank identification number——are routed directly on to the First Interstate server in California, which recognizes that the BIN number is not theirs, and they then route the request back to us. Our computers reroute the new request according to the BIN number——in this case, to Pac-West. Pac-West confirms the account information and approves the withdrawal, routing the approval and an individual authorization code, through us, back to First Interstate, which then instructs the ATM to dispense the cash. In some cases, the request may pass through the national switch first, and then be routed to us, back to the national switch, back to the bank in question. At any rate, this entire process I've just described takes three-point-two seconds. There are four-point-one million credit and debit cards in use in the North-west alone——and eighty million in the U.S. And to give you an idea of volume, of usage, of the number of hits we receive: ATMs in Washington and Oregon alone produce one *billion* dollars a month. That works out to somewhere around twenty million dollars a day Friday, Saturday, and Sunday. That's four hundred thousand hits per day! And you want us not only to pull an individual hit on this system, but to pull it *real-time?* Are you beginning to see my problem?"

His intention had been to mow Boldt down with the facts and figures, and he did just that. Four hundred thousand withdrawals a day. The number fifty million rang in his head.

"Have we met before?" Perch asked, as if Boldt had just walked through the door.

"No."

"You look damn familiar to me. Do you play racquetball?"

"Piano. Jazz piano."

"A club! Am I right?"

"The Big Joke."

"Exactly. I *knew* I'd seen you before." To Lucille Guillard he said, "He's good." To Boldt he said, "You're *very* good. Happy hour. Right?"

Boldt thanked him and pointed out that he had to drop the piano when a case like this came along.

"A case like what? You're not Fraud, are you, Sergeant? Not unless you just transferred. I *know* the guys from Fraud, believe me."

"Homicide," Boldt said.

It was a word that hit most people sideways, and Ted Perch was no exception. He actually jerked his head back as if he'd been struck. "The big leagues," he said.

"Just another division."

"What is this thing? Blackmail? No, extortion——right?"

"Right."

"Bet someone's dead," Perch guessed, "or what would you be doing here?"

"Someone's dead," Boldt confirmed. "Maybe others if we don't hurry."

"If people's lives are at stake, that's different."

"We *need* your help," Lucille Guillard said earnestly. "The problem is that by the time a real-time system identifies a hit, Sergeant Boldt has about ten seconds——or less——to apprehend this person.

Boldt added, "And that's not enough. Not even close."

"Slow down the entire system?" Perch queried. "(A) It's not possible——not that I know of, and (B) I would be hanged. If the system goes down for five minutes, it makes the news these days. People have gotten *used* to ATMs. They expect them to work. Twenty-million a *day*, don't forget."

"Does it have to be the whole system? Couldn't we isolate just these requests?" Boldt asked.

"It doesn't work like that. Sometimes there are two, three, even four ATMs installed right alongside one another. What's this person going to think when his transaction takes forever and the guy next to him receives service as usual? Let me tell you something: People have built-in clocks when it comes to ATMs. They *know* how long a transaction is supposed to take. The average transaction takes twelve seconds. You stretch it to forty and a guy like this, someone jerking the system around, is going to notice. Plain and simple. He's gone."

Boldt was glad that Perch had the gender wrong.

Guillard said, "But if the whole network were to slow down. Or at least every request in the city. What then, Ted? So it makes the papers for a couple days?"

Boldt agreed. "Oddly enough, that kind of publicity might help us. Might convince him it's a regional problem."

"Help you, maybe. It'd get me fired. I can tell you that. But it's all moot anyway. I've never heard of such a thing. You can't just slow down the network by flipping some switch."

"That is what I told the sergeant. But I was hoping you might know more than I do." She hit Perch right where he lived. He *wanted* to know more than she did, and he didn't see the trap she had laid for him.

"We have some software techs. I could ask them."

"Our people are looking into it, too," she said, adding a sense of competition.

"I'll need permission from the nationals," Perch already a step ahead. "There would be some serious explaining to do."

"We're long on people capable of serious explanations. That shouldn't be a problem," Boldt offered.

Perch suggested, "Let me circle the wagons. How soon you need this?"

Lucille Guillard recrossed her legs and Perch didn't even notice.

That was when Boldt knew he had him.[10]

[10] Ridley Pearson, No Witnesses (New York: Dell Publishing, 1996) pp. 172-6.

I included that long passage because I saw in it some similarities to the BPL solutions I had been proposing, that some capability of real-time (Morse) identification be included with a near-instantaneous shutdown of offending frequencies, all done in a spirit of cooperation although it might be complicated, because of the safety issues involved.

Respectfully Submitted,
Earl S. Gosnell III