THE MEMO OF WIRELESS NETWORKING

I'm guessing a fair number of vendors and device makers in the last few years haven't "gotten the memo" either. As a public service. I hereby present The Memo, for all of those companies doing business in the mobility space who missed it.

The Memo

We're in the year 2014. Now that we're moving to the age of 802.11ac, it should be noted that we're into the fifth generation of wireless access technology as we collectively know it. WLANs are set up for client device access, and thousands upon thousands of users rely on those WLANs. If basic access doesn't work, all of the fancy features you've bolted on to the wireless network are *worthless.*

1. This being said, the days of tolerating poorly written and tested code are over. We should all be better at this by now. Whether it's drivers on Lenovo Ideabooks, the keychain code in Mac OSX, wireless controller code, or whatever– when it's shitty, people suffer. Real people. Thousands and thousands of people, and the admins that support them. Developers need to partner with those of us who have our toes in reality and understand that "little mistakes" and "misjudgments" create havoc for those who are stuck with them.

So, let's be done with catastrophic code failures, and actually start testing our code for real, okay? Like *before* it goes out the door as opposed to relying on end users to find our bugs for us (usually in very unpleasant ways).

2. **When a bug *is* found, we have the opportunity to be perceived as caring, responsible technical professionals– or complete buffoons.** For large, secure, high performance expensive WLAN environments used by thousands of customers, these "recommended workarounds" do not make the author look like a caring, responsible technical professional:

- Disable WMM
- Don't use enterprise security
- Don't use 5 GHz
- Don't do things that you know you have to do in a real network environment

Make this sort of recommendation to paying customers in 2014 where wireless networking is a critical service to most users, and you are casting yourself as an out-of-touch, insensitive individual who probably isn't in the right career field. Worse, your employer sends strong signals of cluelessness. The message counts.

3. **There is no line between consumer and enterprise devices anymore, at least not in the minds of end users.** If you're going to sell wireless printers and projectors, make sure they work on typical enterprise secure wireless networks.

Ad hoc technologies should be killed. Any video mirroring device, TV-style streamer, wearable technology, or resident of the Internet of Things WILL find it's way into the Enterprise, and you know it. So make them flexible enough to actually work on secure wireless networks that exceed a single Class C in size. There are only so many variants of secure wireless. Google it- and figure out how to make your products work on business Wi-Fi networks. Then go back to #1 above and make sure you test.

4. **Networks are sophisticated enough, don't add to the administrative burden with ill-thought out management services, complex and/or frequently changing licensing paradigms,** or other detractors that keep WLAN administrators away from the business of administering WLANs, Because… this is 2014 and thousands and thousands of client devices use the network and our focus should be on them and not the constant baby-sitting of ill-designed servers that violate bullet point #1 above.

5. **Above all, it's about devices being able to reliably connect on standards-based networks.** Without good drivers, good code, and good protocols that were written and tested for 2014's large critical wireless networks, the rest is bullshit. All the slick features and applications are moot if people can't connect and stay connected. Wireless connectivity on enterprise-grade networks should be the one thing that all parties prioritize, and treat as Purpose #1.

Source: https://wirednot.wordpress.com/2014/02/25/the-memo/