Chapter seven was all about wireless connections, and the security concerns surrounding them. The chapter began by explaining the difference between different generations of cellular wireless networks. This was actually quite interesting for me, as beforehand I didn't know much about the differences between the generations, only that things got faster as the number went up. I was a little disappointed that the book didn't go over 5G networks much, as I was interested to learn a bit more about them; to me, I feel like whenever my phone connects to a 5G network, it's actually a slower and weaker connection than 4G LTE. Sadly, at the book's time of writing, 5G was more of a concept than a technology we could adequately compare to older generations. The first section of the chapter continues on to discuss the various types of wireless networks, such as Wi-Fi LANs, Bluetooth PANs, and the like, which I was already fairly familiar with.

The second section reviews WEP, WFA, other Wi-Fi restrictions, and other security vulnerbilities for different technologies, such as Bluetooth. I personally felt that some of the restrictions they were recommending for a home Wi-Fi – disabling SSID and MAC address filtering – were extreme for a mere home network, and would prove inconvenient whenever connecting a new device or having company over. I also wish they explained the difference between WEP and WFA in greater detail. The main difference is that WFA doesn't broadcast the encryption key before sending data, which, of course, is more secure, but the book never explains how the recipient obtains the key to unencrypt the encrypted packets once they're received. I really would have liked to see that explained a bit more.