Marauder's Map

Samuel Anklesaria, Jason Brooks, Alejandro Carrillo

Yale University • CPSC 183

samuel.anklesaria@yale.edu • jason.brooks@yale.edu • alejandro.carrillo@yale.edu

I. Introduction

The United States is unique in its constitutional protection of privacy. Thanks to the Fourth Amendment, the State can not bug us, search our houses, or track our cars without a warrant "particularly describing the place to be searched, and the persons or things to be seized." This precedent was set in *Katz v. United States*. Specifically, in his concurring opinion, Harlan read the Fourth Amendment to protect anyone with a subjective expectation of privacy that society was prepared to recognize as 'reasonable.' But times have changed since Katz. While the case occurred in an era of public telephone booths and tape recorders, we live in a world of computers and networked devices. It's becoming increasingly difficult to pin down what expectations of privacy can be considered reasonable. Here, we look to one form of private information in particular: the MAC address. Pretty much everyone uses WiFi. Yalies connect to YaleSecure the moment they open up their laptops. Their phones switch from access point to access point as their phones helpfully check for new mail. But WiFi isn't directed; packets are broadcast to everyone. Only the link layer identifier, the MAC address, can tell packets meant for one device from packets meant for another. Devices don't have to ignore packets not meant for them; they can in effect see all the other devices using WiFi around them. To show the impact of MAC address sniffing, we distributed two Raspberry Pis equipped with WiFi adapters to monitor to the traffic around them. Every MAC address they saw is timestamped and uploaded to a central database. In our website at yalesniffer.herokuapp.com, students can view all the locations their MAC addresses has been detected over time. The website also contains a form for users to rank how much they thought the process was a violation of privacy. By examining these views, we hope to establish the two prongs of Harlan's test: did Yale students have subjective expectations of MAC address privacy, and, if not, did Yale students at least think such an expectation was reasonable? In practice, however, we didn't capture enough MAC addresses for it to make sense to give out links to the whole student body; most people wouldn't have been captured more than once or twice, if at all. That said, we gather substantial information for a small subset of the student body. Of the roughly 7000 MAC addresses we captured across two days, about 20% were caught by both our Branford dining hall and CEID sniffers. We had successfully traced students' movement. So was this an invasion of privacy? For individuals, the question doesn't matter mutch. Beyond Rosen's 'not cool bro' theory, little prevents civilians from snooping on each other. But what about the government? Could the goverment have done this without a warrant? Examining the situation with an eye to precedent does not reveal any clear rule on either side. On one hand, it seems like MAC address privacy is an unreasonable expectation. It doesn't take any special technology to detect a MAC address; anyone can buy a WiFi adapter at their nearest WalMart. People don't make any effort to hide their MAC addresses. They're not encrypted or hidden from public view; on the contrary, our devices broadcast them to anyone and everyone around us. In addition, MAC addresses only need to be unique at the link layer. Many people could potentially have the same MAC address if they configured it that way. Further more, the MAC address is just a number. Knowing that d8:06:00:34:d6:ff was at a

certain place at a certain time tells you nothing intrinsic about the individual operating the device. On the other hand, it seems pretty reasonable to think that tracking someone around the Yale campus is an invasion of their privacy. Most people don't spoof their MAC addresses, making them unique in practice. Broadcasting their address to everyone around isn't something people do conciously; for the most part, people aren't even aware it's happening. And although it's easy enough to get a WiFi adapter, the average person wouldn't use one to record every MAC address in range. Also, it's not uncommon for organizations to be able to match the fairly anonymous identification of a MAC address to its owner. Yale makes us register all our devices so it can restrict traffic to its students. As a result, they know exactly which MAC addresses belong to each person. Even without knowing who a MAC address identifies, sniffers can easily invade someone's privacy. Say we had one near someone's home. We could estimate how many people were in the house at any given time, and where else these people had gone. We could guess if someone worked from home, even how many friends they had. Is there truly no reasonable expectation of privacy in any of this? Overall, as the technology becomes increasingly ubiquitous, maintaing privacy becomes more and more challenging. Companies are already using WiFi tracking similar to that which we demonstrated in this project in order to acquire retail analytics about consumer behavior[1]. Our courts have already had to decide the legality of everything from heat sensors to GPS tracking devices. With MAC addresses, the Walmart test no longer seems to be enough; our privacy standards may need adjustment yet again.

[1] http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/19/how-stores-use-your-phones-wifi-to-track-your-shopping-habits/