WHOOPS!

I know where you go each day. I know what time you go to work, what time you leave, where you meet clients, when you check Facebook over lunch, and when you sent that email to a client while heading to the gym. I know that you carry a "work phone" in addition to your iPhone, and I know the model of your laptop. I even know that you went to your old high-school buddy's apartment last month when you were supposed to be at the dentist.

You assume that I'm the NSA, but I'm not: I'm your humble coffee shop.

Focus Shift

With the last decade's focus on criminal enterprises attacking massive data warehouses, both programmers and lawyers have focused, rightfully, on threats to data stores. Billions of dollars have been spent on ever-more-shiny "security solutions," each promising to end the newest threats. Thousands of attorney hours have been spent drafting privacy policies and binding arbitration agreements that ensure that users can't hold a company liable if their secrets go missing. Programmers have spent the best years of their lives trying to defend virtual castles in the cloud.

Throughout all that, though, we forgot about the users. Increasingly, they're the ones under attack, and we have completely forgotten to defend

HOW YOUR "CONVENIENCE" BROADCASTS YOUR SECRETS

BY BRENDAN O'CONNOR

them. Every attorney, every client, and increasingly every *person* is a user of at least one such device—a computer with more processing power than the Space Shuttle, whether it's called a phone, tablet, laptop, television, or, as popularized by Google, pair of glasses. Attacks on users' devices threaten confidentiality, privilege, and the rest of the ideas that attorneys should consider inviolable. Unfortunately, we—the attorneys, the programmers, and all those who "do" tech—have let it get this bad. For convenience.

First Problem: Data Broadcast

Consider your typical day. You wake up, and before leaving the house, put a smartphone in your pocket, briefcase, or purse. You drive downtown and park before grabbing coffee at the corner shop; then you walk into work.

How did I know that? Every few seconds, your smartphone (or any other WiFi-enabled device that's on; your tablet, for instance) sends out a message. It's a simple message, called a probe request. The message is the digital equivalent of the following:

> Hi! My name is Brendan O'Connor's iPhone. I'm looking for WiFi to connect to. I've connected to Brendan's Home WiFi, Local Coffeeshop, BigLawWiFi, Fred's Pad WiFi, CompetitorWiFi, ClientWiFi, LocalRestaurantWiFi, SecretClientWiFi, BookstoreWiFi, GirlfriendWiFi, LocalCourtWiFi, and BigGymChainWiFi. Are any of those around?

It does this for a few apparently rational reasons. When you get home, it's nice to have your phone automatically connect to the WiFi there so it can run software updates, check email, or generally be ready for your next command. Another reason is battery life: a device uses so much less power on WiFi than on cellular data services that it saves hours, or even days, of battery life to search for WiFi and use it where possible. It's also part of the WiFi specification (IEEE 802.11, for the curious).

The concern is how much data is sent in each request. This data includes the name of *every previously connected network* (sometimes called your "Preferred Network List," and which is difficult or impossible to edit on most mobile devices), the phone's identifier (which, for many people, includes their real name), and a hardware-unique identifier (called a MAC address, with no relation to any Apple product). This is sent when you "Scan for WiFi" (in addition to looking for another type of message, called a beacon). By the way, this all happens even if the device is already connected to WiFi, and even if the WiFi is encrypted; these probes are always sent in plain text.

Anyone can monitor these probe requests. It requires neither specialized hardware nor software (despite the Ninth Circuit's ruling in *Joffe v. Google*, No. 11-17483, 9th Cir. 2013). This isn't a bug. Just as your ears have to monitor a room to listen for someone calling your name, your WiFi adapter has to listen to the radio to hear when it's receiving new data. WiFi, in other words, is not a "wire" to "tap"; it's a crowded room with hundreds of devices screaming their heads off at all times. If you use Mac OS X, monitoring software is built-in; Option-click the WiFi "fan" icon, then click Open Wireless Diagnostics, then go to the Window menu, click Utilities, and finally Frame Capture. That will log not just your WiFi, but that of every person around you (up to about a hundred meters, depending on walls), to your desktop. For everyone else, free, easy-to-use software accomplishes the same thing (such as Kismet, Wireshark, or AiroDump).

Back to your hypothetical day. You sent all this data to your coffee shop, as well as anyone else within 100 meters or so, when you swung by for coffee. The neat thing is that because your phone

is continually broadcasting, I can track your location throughout a city, just by listening for your phone (and its MAC address); if I throw a few sensors around a city, I can store and map your movement. I don't need a lot of hardware to do so; indeed, with the parts for each sensor costing just over $50 in small quantities, I can track the largest part of a city's downtown area for about $500. Even better, from an efficiency perspective, these collectors don't need to be targeted to one person; the collectors can instead track *every* device that wanders by, and I can see later which ones do something interesting. The collectors can even do advanced-level analysis, such as noting that two devices are only seen together; this might indicate that one person carries two phones, or a phone and a tablet. This is the type of detailed, broad-spectrum data collection that people often think is confined to nation-state level intelligence agencies—but it's available on your own laptop, for free.

Second Problem: Data Leak

We've been talking about how much data you leak simply by walking around; let's talk about the data you leak when you sit down to drink that coffee.

Application developers have been bitten by the "big data" bug in the last few years; more precisely, business owners have been convinced that they should collect every possible piece of data, *in the hope* that it later becomes valuable. There is, some are saying, a gold mine out there, and all you have to do is exploit the data of your customers.

The problem isn't that they're collecting this data. (Well, actually, that is a problem; it exposes the collector to liability when their data storage is breached, and we should be discouraging them from collecting it.) The problem is that they're doing it *badly*.

Allow me to illustrate. I looked at the network traffic from a variety of apps on my iPad: a file-sharing app, a dating app, a messaging app, a shopping app, and a news-reading app. All network traffic sent by a device includes the device's unique identifier—the Mac address discussed above. Hence, from each of these, I was able to associate the valuable, private information sent in clear text over the radio with the device that sent it, all without ever touching the device itself.

First, the dating app. It uses transport layer security (TLS)—the same type of technology that protects your credit card when you purchase something online—to protect my username and password. Once inside the app, however, data is sent unencrypted. Some of the data isn't relevant; after all, most information in a dating app is meant to be seen by the public. (It is also possible that, depending on the type of dating site, the mere fact of the person's profile may be of interest to a potential attacker.) If I'm just looking to scoop up all the information on you, however, your photo—and dating websites tend to have fairly clear photos of faces—is very valuable. Each particular dating app tends to have the profile photo at a predictable point in the web page, meaning that it's easy to separate the photo of a phone's owner from the photo of the person with whom they're corresponding. My sniffing devices can thus associate a device—previously unknown—with a face.

Many applications record and send information about the hardware and software on which they're running back to their creator. The messaging and shopping applications I studied do that, as well as (in some circumstances) transmitting my precise location. For example, they might transmit "this is an iPhone 4S, running iOS 7.0.3, sitting at the coffee shop at 3rd and Main." This isn't encrypted—so even though your messages, and what you purchase, are secured against eavesdroppers, this data (the so-called metadata) is sent to anyone who might be listening. To be clear, there is no technical reason to justify this design decision. So now I know how valuable the phone in your pocket is, and precisely where it is—again, because the applications you used told me.

The news-reading application was the most concerning. When I examined it, it was transmitting my full name and email address in clear text, despite my having set the "always encrypt everything" setting.

A brief listen to your traffic—from any location within 100 meters in any direction—therefore gives me your name, email address, model number of your phone, software version, exact location, and even a photo, so I know exactly who you are. All I have to do to access this wealth of data is "sniff" your wireless traffic; any computer can do this, and Mac OS X has the software built in. The same software that collects probe requests can collect everything else, so the same $50 collection devices mentioned previously work just as well here. And sure, one could use encrypted WiFi—but only one use of unencrypted WiFi is all it takes, because once I learn which device is owned by which user, I can save that information for later use.

The effect is this: for about $500 as an initial investment, I can learn everything about you and your routine. I don't need to identify your phone first; I don't need to have a team of experts following your every move. I can simply throw a bunch of small boxes around a city—especially around points of interest—and wait for the data to roll in. For bonus points, I can even create a moving map, with photos of people moving around the city in near-real-time. (I actually did so, and tested it in a highly restricted environment to prevent accidentally collecting

---

Brendan O'Connor, a security researcher and third-year law student at the University of Wisconsin Law School, is set to graduate in May 2014 with a double concentration in criminal law and international law. His security research, via his company, Malice Afterthought, Inc., focuses primarily on enabling access to security and privacy through development of disposable computing and sensing tools. He has taught information warfare to the military, played the violin, transmitted on amateur radio (K3QB), and tried to convince his cats not to eat him when he dies. He welcomes inquiries at brendan@maliceafterthought.com.

the data of others; our hypothetical attacker need not be so selective. For more information, see the link at the end of this article.)

Perhaps the most disturbing part is this: none of this is new. Computer security experts have known all this for years.

So What?

Your coffee shop might be relatively trustworthy. What about every other place you've ever been? When you bring your phone to opposing counsel's office for a deposition, are you sure that their system doesn't log your list of previous networks—including, perhaps, the WiFi network names of your other clients, possible witnesses, or even government agencies? Even if opposing counsel doesn't do such a thing, are you sure that no one has put such a collection box—the size of a deck of cards—anywhere near their office? If you practice criminal or family law, think about tracking every cell phone that goes to a jail, mental health agency, public defender's firm, abortion clinic, gun shop, or crime scene—is it possible that someone might find that data useful? Remember that an attacker doesn't have to know whose phone it is to record its location; later, an identity accidentally broadcast at a coffee shop can be cross-referenced with its historical locations. One broadcast might be all it takes.

In addition, researchers have found that the more past WiFi networks people have in common in their probe requests, the more likely they are to know each other in "real life." (This was without looking at the actual data transmitted.) Those who look for someone's association with "known bad influences" might use this information in unintended ways. ("Signals from the Crowd: Uncovering Social Relationships through Smartphone Probes," Barbera, Epasto, Mei, Perta, and Stefa, in Proceedings of the 2013 Internet Measurement Conference.)

Confidentiality might thus accidentally go out the window, through an attorney's phone's side effect. Worse, privilege might go as well: a client's continuous broadcast of sensitive information might be held to be an inadvertent waiver.

So Now What?

There is no simple solution to this problem. Modern attorneys cannot give up their electronics, because they enable an attorney to be more efficient with client time, and to solve larger problems more quickly. The standard list of solutions—using secured WiFi, using a virtual private network (VPN) to protect data in public, and so forth—doesn't solve the data leakage, not least due to the "one mistake" problem noted earlier. (There are also other technical barriers to solutions that are outside the scope of this article.)

There are some mitigations: turn off your WiFi completely when it's not being used, don't connect—ever—to open WiFi, and clear out the lists of old "preferred" networks (on iOS, "Reset Network Settings"). These don't solve the underlying problem, but they do make it somewhat harder to do serious damage to confidentiality via your phone. The phones of colleagues and clients, of course, remain unprotected.

Ultimately, the solution is a cultural one. The burden falls on those who would like to continue to preserve secrecy to do the hard work of protecting it, and that means disabling WiFi, educating clients, continuously checking for problems—and both deleting unnecessary data wherever it lives and refraining from collecting it in the first place. It's a lot of hard work, and every flaw can be exploited ruthlessly and automatically. However, we have to do the hard work of quieting not just our voices, but also those of the devices that control our world. Continuous vigilance is the only way we will be able to protect the idea that the legal profession is one that knows how to keep a secret. ◆

Note

More information on the underlying research, entitled "CreepyDOL" and presented at the Black Hat USA and DEF CON conferences, can be found at the author's blog: http://blog.ussjoin.com/2013/08/creepydol.html.