Spring Privacy Series: Mobile Device Tracking
Comments

Since 2008, the company I founded has been actively developing certain beacon technologies. Our patented systems re-imagine how network names (especially Wi-Fi SSID's and Bluetooth UUID's) can be used as beaconing tools to deliver non-network name data between nearby devices without establishing formal connections between them. Our Wi-Fi beaconing system, for example, allows a user to share actionable code(s) in the name of their mobile hot spot, router, or battery-powered Wi-Fi beacon(s). Wi-Fi SSID's are malleable & were not intended to be unique. By contrast, MAC Addresses were designed to be unique & persistent identifiers (which of course is helpful for augmenting Location-Based services, but their persistence can also become a drawback for user privacy). My company's Bluetooth beaconing system works in a similar manner, but with the UUID's instead of SSID's.

In early 2008, about the time we first began developing our beacon technology, the computer company Apple announced that they would begin using MAC addresses to augment their Location-Based Services [search article, "Jobs, iPhone have Skyhook pointed in right direction by Jefferson Graham, USA TODAY 1/23/2008."]. The company I founded remained largely unaffected by that Apple decision. It was probably an unintentional coincidence, but two weeks after our first patent published in 2010, Apple suddenly removed all Wi-Fi scanning apps from their App Store and announced that they would no longer allow any apps in their App Store to control any aspect of Wi-Fi [search article, "Apple removes Wi-Fi finders from App Store, Jim Dalrymple, CNET, March 4, 2010"]. By removing all competing Wi-Fi apps from their App Store, Apple declared themselves to be the only party that could scan for Wi-Fi on iPhones and iPads (including our network name scans that are limited to known codes). Apple's action created a substantial negative situation for our company because our entire Wi-Fi product line was immediately blocked (and still is) from the Apple App Store. Within weeks of the Apple announcement in 2010, we lost our only corporate sponsor…. they reneged on their commitment to fund our next stage of development ($500k) citing the need for our system to work on Apple Devices. Instead of quitting or crying foul, we continued to innovate, albeit with greatly reduced access to capital (plus we were operating in the turbulent economic environment of the Great Recession).

Considering recent iBeacon announcements, Apple now considers themselves to be major players in the beacon space [search article, "Inside iOS7: iBeacons enhance apps' location awareness via Bluetooth LE, by Daniel Eran Dilger, AppleInsider, June 19, 2013"]. In addition to our Wi-Fi beacons mentioned above, my company would also like to deploy our patented, privacy-enhanced Bluetooth LE beacons that are un-mappable by third parties (including by operating systems). However, Apple's current rules for BLE apps force those apps to turn 'on' Apple's Location-Based Services even though we do not use Location [see "iOS 7: Understanding Location Services" at the Apple.com website in the Support category].

I strongly believe that Proximity and Location are actually two separate categories that accidentally get considered as one single category (both are used to achieve context, but Proximity does so apart from Location). I even noticed that panelists and speakers at the FTC event repeatedly referred to Bluetooth Low Energy beacons as being part of Location-Based Services. However, many such beacons are highly mobile. Apple has even stated that every iPhone since 4 is itself a mobile iBeacon [see "Core Bluetooth Programming Guide" at the Apple.com website in the iOS Developer Library]. A Venn diagram (last page) shows Proximity-Based Services and Location-Based Services overlapping where the beacons are tied to a map (MAC address mapping is in the overlap, for example). Current Apple App store rules force users of all BLE scanning apps to share their Location, even though Proximity-Based apps like ours don't need or desire to gather this information.

Proximity-Based Services put users in control by allowing them to send and receive context cues directly between mobile devices (without the need to share Location with, or receive any context from, third party intermediaries such as operating systems). Apps can achieve this context locally on the device (or at least apart from Location). Apps can even be privately turned on or off (automatically) based on these Proximity-Based cues received from beacons (as described in paragraph 300 of our Patent Application 20110244798). Interestingly, Apple recently announced that iBeacons can turn apps 'on' [search article:

"Apple iBeacons: With great power comes great potential to annoy" by Adrian Kingsley-Hughes, Hardware 2.0, March 17, 2014]. By determining which apps get turned on / off under different scenarios, Apple can control context. Winners and losers will get decided when those types of decisions are made. For example, imagine the scenario where an operating system turns 'on' a product search app instead of a bricks and mortar retailer's app when a user approaches a BLE beacon in the store. Whether this functionality is right or wrong is not my point…. just that it's A LOT of power to turn apps on and off. Current BLE beacons are mappable by third parties, meaning that operating systems have almost total control (as opposed to the owners of the beacons themselves, who are left with very little control). Our Wi-Fi and Bluetooth beacons achieve their patented, unmappable privacy characteristics by applying the very features described as necessary by your panelist, Seth Schoen, Senior Staff Technologist at the Electronic Frontier Foundation) [see "Spring Privacy Series: Mobile Device Tracking" video archive from time 1:18:00 to 1:19:00).

Closing remarks:

A) There is a difference between Proximity-Based Services and Location-Based Services, and people accidentally tend to think of them as the same…. the fundamental goal of each is to achieve context. Proximity-Based context generally evolves more rapidly than Location-Based context because scenarios can change rapidly within an unchanging location.

B) My company would prefer to win in the marketplace (with our products) rather than the courts (with our patents).

C) We have heard that Congress is considering limiting patent infringement lawsuits to companies that have product(s)… and yet some of our products are not allowed on both app stores…which makes it difficult for us to raise the necessary capital to build & deploy the product(s).

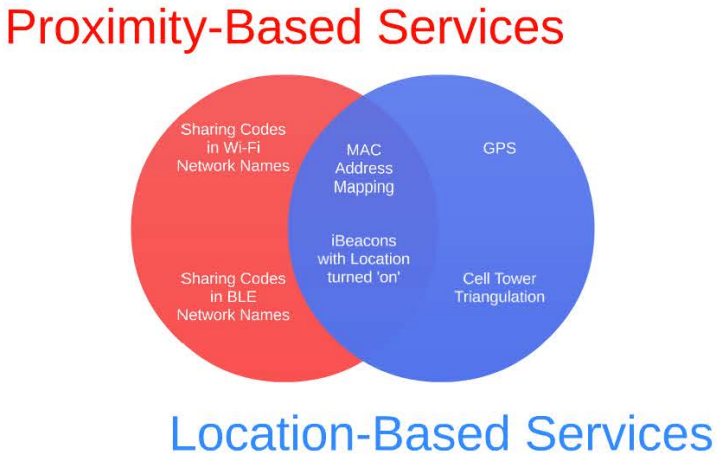
D) Companies like mine operate in an environment of increased business risk when one or two companies are allowed to control the 'on' and 'off' switch to our success.

E) The folks at Google have been much more open with their Android Operating System. We might not have been able to develop our privacy solution without Android.

F) Our experience during the past six years reveals that our ability to raise capital and serve customers was diminished by at least 95% as a result of our not being able to place our apps in both app stores.

G) I hope the FTC takes a leading role on the implications of nano technologies, especially as it relates to wearable / implantable beacons.

H) I am available to further explain anything in this submission as needed. I can also provide more specific suggestions upon request. Please see next page for Venn Diagram.


Proximity-Based Services
Sharing Codes in Wi-Fi Network Names
MAC Address Mapping
GPS
iBeacons with Location turned 'on'
Sharing Codes in BLE Network Names
Cell Tower Triangulation
Location-Based Services