2012

Check In on Your Privacy

Frank Gonello
Seton Hall Law

Check In on Your Privacy

Frank Gonello

You Are Here | An Introduction

Global positioning systems, or "GPS" as it is commonly referred to, has become a household term in just the past few years. Nearly everyone is familiar with the uses of GPS, and a great many use the technology in their daily lives. But whether navigating to Grandma's house, fishing a wreck at sea, checking the distance to the pin out on the course, or "checking-in" with Foursquare on a mobile phone, what do we really know about the geo-location data that is being collected, transmitted, and stored? How private is this data, especially when intentionally disclosed on social sites like Facebook, Foursquare, and Google Latitude? And even more importantly, can this data be used as admissible, reliable evidence in a court of law?

Though the latter question has yet to be directly addressed by any court of high precedence, the following analysis seeks to provide some perspective as to where the courts may be headed. Our trip begins with a discussion of the technology itself, to put the reader in a better position to understand what geo-location data is, the principles

behind GPS technologies and the limitations that exist in present-day geo-location hardware and software. Next, we will check out "checking-in," the most recent social networking phenomenon, to understand more fully the nature of the geo-location data that individuals are releasing into the public, sometimes unknowingly. Last, we arrive at the legal points of interest, exploring relevant court opinions, digital evidence standards and guidelines, and the Federal Rules of Evidence. So locate a tall cup o' joe, check-in to your favorite sofa or recliner, and navigate to the next section of this pun-infused paper to get a fix on where you stand in the world of geo-location data privacy.

Point of Origin | Technologies Behind Geo-location Data

To appreciate why social networking services such as Facebook Places, Foursquare and Google Latitude generate so much complexity when considering their data for use as evidence at trial, a fundamental understanding of the hardware, software, and transmission of data is required.

GPS Satellites

The GPS was developed in the early 1970's by the United States Department of Defense for use in aiding the military to navigate unknown, foreign terrains and to drop payloads or supplies on particular targets with accuracy and precision. It exists today as a system of 24 satellites orbiting around the earth, which broadcast signals to GPS receivers down below which contain information such as the satellite's location

Figure 1. Visualization of GPS satellites in orbit.

in the sky and a reading of its current date and time. Satellites also broadcast unique identifier codes so that GPS receivers know exactly which satellite it is receiving location information from.[1]

GPS satellites are in constant orbit around Earth, spaced out in an array that allows for receivers to essentially "see" more than one from any point below, be it from land, sea or air. (*See Fig. 1*)[2]. Satellites maintain their trajectories based on correctional instructions sent by government-maintained ground stations. This corrective data accounts for errors caused by atmospheric delays inaccurate position reports, and clock imperfections.[3]

Though not initially intended for use by civilians, the satellites broadcast two types of signals, designated L1 and L2, with the former being set aside entirely for civilian usage. Satellites transmit these signals through line-of-sight frequencies, meaning that obstructions other than clouds, glass, and some plastics may interfere with the wireless communication. Buildings and dense foliage, for example, could obstruct or reflect GPS signal transmissions; alternatively, these signals might reach a receiver that is located inside a vehicle by penetrating the glass of its dashboard.[4]

GPS Receivers

A GPS receiver is necessary to process these satellite signals. A receiver is an electronic device can determine its geographic position when it has established a "lock"

[1] *Chad Strawn, Tech Journal, "Expanding the Potential for GPS Evidence Acquisition", Small Scale Digital Device Forensics Journal, Vol. 3, No. 1. Page 1 (June, 2009)*
[2] *http://www8.garmin.com/aboutGPS/ [Accessed 5/6/2011]*
[3] *Strawn, at 2*
[4] *http://www8.garmin.com/aboutGPS/ [Accessed 5/6/2011]*

or "fix" on a satellite, and can more precisely define its position when getting multiple satellite locks. A lock occurs when the receiver is able to communicate with a satellite without interruption and can therefore mathematically compute its geographic coordinates using the time, date, and orbital positioning information sent by that satellite. The accuracy of a lock is enhanced when more than three different satellite signals can be received, since the receiver can utilize both locations in calculating its relative position; any potential error in position caused by signal reflection or refraction due to obstructions or atmospheric distortions, is minimized further when multiple locks are made on satellites spaced further apart from one another. (*See Fig. 2*)[5]. Today's receivers can typically obtain global positions accurate up to 5 meters once acquiring a lock on three or more satellites.

Figure 2. Visualization of a GPS receiver with multiple satellite locks

GPS receivers come in a variety of forms. Initially, they were most commonly found built into the control panels of automotive, aeronautical, and nautical vehicles to assist drivers, pilots, and captains in navigation. GPS receivers also exist as standalone, handheld devices, useful for commercial purposes like deliveries and shipment tracking, as well as recreational uses like off-piste skiing and hiking. Today, every mobile phone that

[5] http://commons.wikimedia.org/wiki/File:Good_gdop.png *[Accessed 5/6/2011]*

reaches American markets is required to have some type of geo-location functionality built-in for emergency 911 purposes[6], though with the growth in popularity of smartphones and mobile applications ("apps"), other location-based services are expanding rapidly in number.

Location-Aware Mobile Devices

To give some perspective as to the number of GPS-receiving mobile devices in the market today, 293 million smartphones, nearly all of which contain some GPS or geo-location functionality, were shipped globally during the 2010 calendar year alone.[7] However, these devices are not without their own limitations. A great number of these gadgets are commonly used in urban environments where buildings and other structures can interfere with the accuracy of GPS satellite signals. Furthermore, the fact that these multi-function instruments are not dedicated purely to global positioning tasks increases the possibility of inaccurate readings and increased lock times. These shortcomings are addressed by a cellular technology known as assisted GPS ("aGPS"), a process by which cellular networks act as a middle-man in computing GPS calculations and relays the processed location data to handsets. Since mobile networks already know what cellular tower a mobile device is communicating with, it can estimate the general whereabouts of the user and provide the mobile device with an approximate location for which to base its calculations. This results in substantial improvements on initial

[6] http://www.gpo.gov/fdsys/pkg/CFR-2010-title47-vol1/xml/CFR-2010-title47-vol1-part9.xml *[Accessed 5/6/2011]*

[7] http://www.marketwatch.com/story/strategy-analytics-global-smartphone-shipments-reach-record-94-million-units-in-q4-2010-2011-01-27 *[Accessed 5/6/2011]*

lock times.[8]

[8] *Strawn, at 2*

Not all location-aware mobile devices have standalone GPS receivers as part of their specifications. These devices are able to rely solely upon aGPS data from the cellular provider to make use of geo-location data because of the relative accuracy of aGPS and the general lack of need for absolute location precision (1-15 meter) when using most location-based services. For example, if aGPS data can inform a smartphone that the device is within 100 meters of a particular geographic point, an app that searches for nearby Italian restaurants can return results based on that 100 meter radius. The device does not need a precise lock to perform its location-based task. Conversely, mobile devices that do not have access to aGPS data, either due to cellular network reception or the lack of compatible hardware, but contain standalone GPS receivers may

still obtain a satellite lock and calculate the unit's location. The lock may take longer to establish initially, since the mobile device is processing all of the GPS data on its own. However, once the device has established GPS locks, it can be as accurate as GPS-dedicated systems.

GPS Data on Mobile Devices

Though it may be understood at this point how GPS satellites and receivers

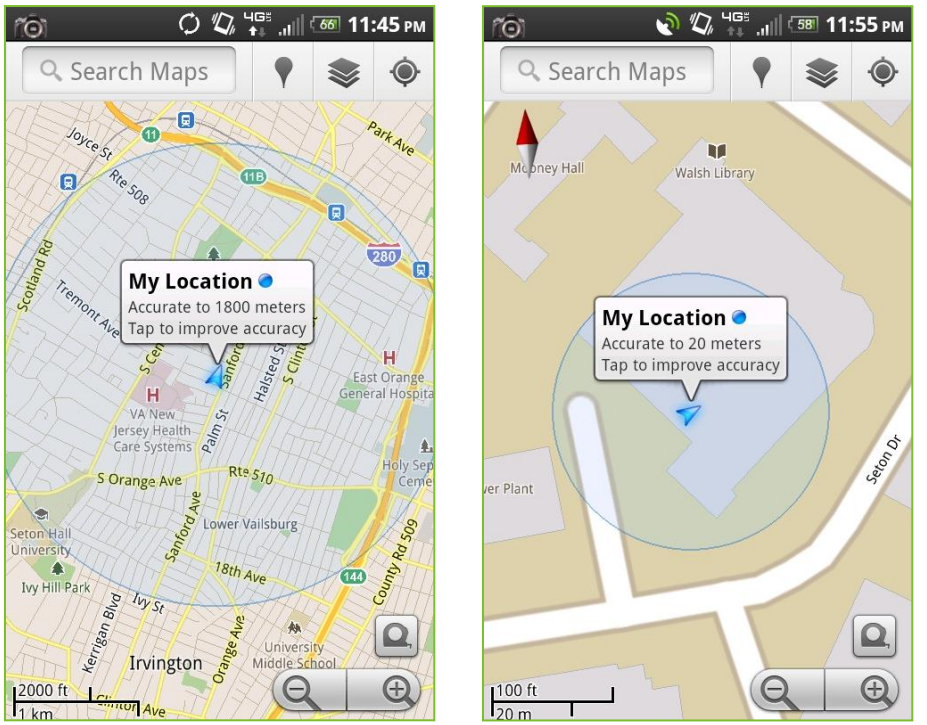

Figure 3. A mobile device relying solely on aGPS data (left) vs. the same device relying upon GPS satellite locks

communicate with one another, one important question still remains that necessarily flows from any discussion on privacy in the digital age: What sort of data is being transmitted, used, and stored in this entire geo-positioning process?

As discussed above, GPS satellites transmit time-stamped information about

their own whereabouts, which GPS receivers are able to process to calculate their own positions. These positions are stored and used locally on the device in the form of trackpoints, track logs, waypoints, and routes. Trackpoints and track logs can be classified as system-level data, whereas waypoints and routes are based on user-input.

A *trackpoint* is the most basic building block of local GPS data, and is nothing more than a location stored by the GPS unit as a record of where the unit was at a particular time. The unit creates trackpoints automatically, and the user cannot modify them. Trackpoints are recorded at either predefined or user-defined intervals for the most fundamental GPS purpose: establishing a location at a given time. Trackpoints, therefore, are the foundation of geo-location data, and provide the most meaningful information to forensic investigators since they can establish that a device was in a certain place at a specific time.[9]

TIME	LATITUDE	LONGITUDE
2011-04-21T12:58:05Z	40.743179	-74.252725
2011-04-21T12:58:06Z	40.743174	-74.252793
2011-04-21T12:58:50Z	40.743376	-74.252827
2011-04-21T13:00:20Z	40.743334	-74.25286
2011-04-21T13:00:25Z	40.743291	-74.252794
2011-04-21T13:00:29Z	40.743288	-74.252726
2011-04-21T13:00:32Z	40.743309	-74.252657
2011-04-21T13:00:34Z	40.743321	-74.252596
2011-04-21T13:00:37Z	40.743334	-74.25252
2011-04-21T13:01:12Z	40.743288	-74.25253
2011-04-21T13:01:37Z	40.74324	-74.252537
2011-04-21T13:01:53Z	40.743229	-74.252474
2011-04-21T13:01:58Z	40.743262	-74.252422
2011-04-21T13:01:59Z	40.743336	-74.252449
2011-04-21T13:02:00Z	40.743383	-74.252492
2011-04-21T13:02:01Z	40.743415	-74.252549

Figure 4. A track log consisting of a series of trackpoints recorded at one second intervals.

When a GPS is turned on and has acquired a satellite lock, it essentially begins to record an "electronic breadcrumb trail" by logging each of these recorded trackpoints in a *track log*. Track logs list of all of the trackpoints that have been created by the unit while locked on GPS

[9] http://www.dfinews.com/article/enhancing-investigations-gps-evidence *[Accessed 5/6/2011]*

satellites. (*See Figure 4, supra; Figure 5, infra)*[10]. This data is useful for retracing steps, or backtracking, because a GPS unit can navigate back to previous trackpoints in reverse order of recording them. The trackpoints then function as waypoints, in a sense.[11]

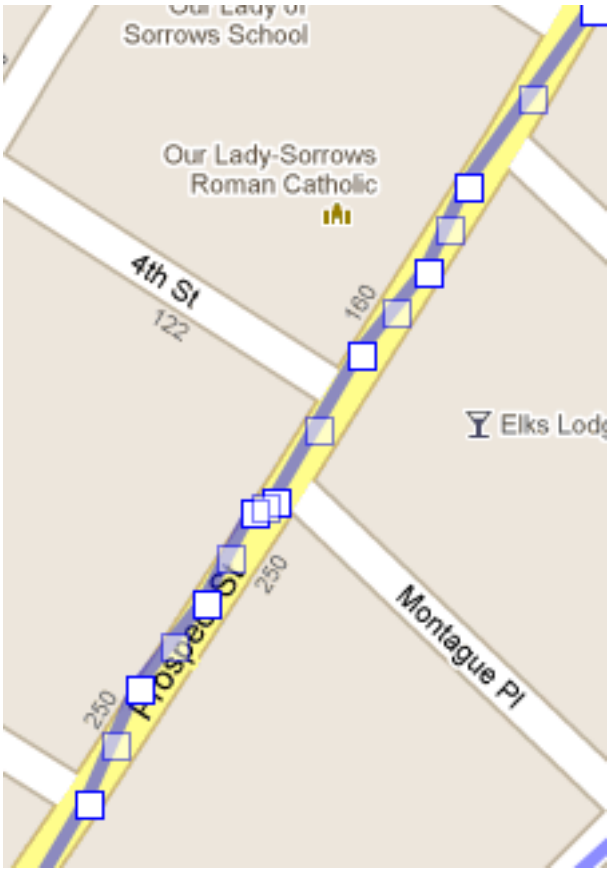

Figure 5. Visualization of a track log. This also reflects what a unit-generated route would looks like for traveling down Prospect Street.

A *waypoint* is a location that the user inputs into a GPS via software methods or is a trackpoint previously recorded which tells the GPS unit a destination to go to in the future. For example, in a navigation application, a waypoint can be a home address that a user enters into the program, which software could then convert into longitude/latitude coordinates and designate the location as a waypoint. Finally, the application would plan a route for getting to this location from the present location of the unit.[12]

Routes, then, are just a sequence of unit-generated waypoints that are calculated to bring the unit to the user's requested location. GPS units typically calculate routes initially, and correct them in real-time. If during travel a unit begins registering

[10] *Data courtesy Google MyTracks for Android*
[11] *http://www.dfinews.com/article/enhancing-investigations-gps-evidence [Accessed 5/6/2011]*
[12] *Id.*

trackpoints that do not align with the generated route, it will adjust from the present trackpoint and generate a new route from there. The result is that the user is not required to backtrack to a trackpoint the unit previously prescribed just to proceed to his or her desired destination.[13]

Because of the variety of mobile applications, this basic GPS data can be stored and used for various purposes. Navigation applications for mobile devices, such as Google Maps and CoPilot, store trackpoints and record track logs whenever the software is opened, store waypoints whenever a location is saved or accessed (when location history is enabled), and generate routes upon user request. Google Maps also integrates with the "cloud," meaning that it can save this same data to its own servers so that users may access it on the internet using their Google accounts at some later time.[14]

Still, the majority of mobile applications only utilize single trackpoints for just-in-time location resolution. GPS-capable mobile phones often have built-in cameras, which can "tag" photos with the location they were snapped just by pinging GPS satellites for a single trackpoint. Commonly, such geo-tagging is enabled in mobile devices by default. Similarly, location-based social "check-in" services, the primary subject of this paper, utilize a mobile phone's GPS to establish a trackpoint, and then present the user with a list of places nearby for the user to publish as his or her present location. This user-selected location is then published to the web as the user's present location,

[13] *Id.*
[14] http://maps.google.com/support/bin/answer.py?answer=173398 *[Accessed 5/6/2011]*

regardless of the trackpoint's precise coordinates.

Recently, mobile phone operating system ("OS") manufacturers themselves have been under the magnifying glass for their use and storage of GPS data without users' knowledge. Google's Android OS requests permission from the user to send anonymous location data back to Google's servers during the device's initial setup, in order to enhance its services for Android users. Google claims this information is not traceable to any users, and no remnants of this data are maintained locally on the device. This is in stark contrast to the controversy ignited by a recent study that shows Apple's current iPhone OS ("iOS") has been logging location data in an unencrypted file on the phone itself.[15] According to the report, this cannot be disabled, and users are not notified of this data collection at any time.[16] Though the scope of this privacy debate extends beyond the focus of this paper, it is important to recognize the types of data that may be collected on a device, both with and without a user's express approval.

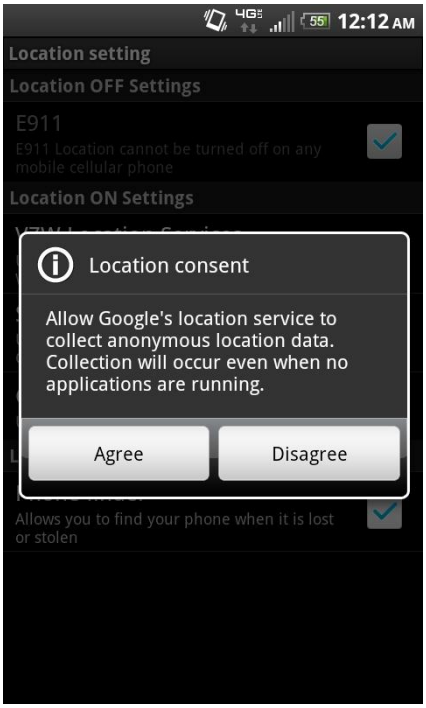

Figure 6. Google's Android OS requesting permission from user to collect anonymous location data.

In general, it is locally stored system-level data such as trackpoints and track logs that prove to be most valuable to investigators. This data is difficult to fabricate since it

[15] http://www.bloomberg.com/news/2011-04-25/apple-accused-in-suit-of-tracking-ipad-iphone-user-location-1-.html *[Accessed 5/6/2011]*
[16] http://petewarden.github.com/iPhoneTracker/#7 *[Accessed 5/6/2011]*

is stored by the unit directly onto the device itself, without the input of a user. Thus, it provides investigators with evidence that a device was at a location at a certain time, without the need for excessive corroborating evidence. User-level data, on the other hand, is useful for proving intent of a user to go to a particular location, since waypoints and routes do not prove a device was ever at those places. Finally, data stored on social sites utilizing user-modified system data for establishing location seem to provide little evidentiary value standing alone, requiring considerable corroborating evidence to prove a basis in fact.

Your Destination | Social Media Check-In Services

Even with the fundamentals of how mobile devices obtain and store their geo-location data explained, a familiarization with today's fleet of location-based social media services and the basic functionality they offer is still necessary in the valuation of one of the service's data in a court of law. The advent of the social media check-in service is the latest Web 2.0 trend, and these services have been growing in popularity dramatically in just the past year.

A "check-in" consists of a user logging in to a particular service via a mobile phone application or through a web site, and publicly declaring through that application or site that they are at a specific business location, venue, or other place. In doing so, the user notifies friends of his or her whereabouts. Similarly, a user can see if other users are checked-in at that location, or look up his or her friends to see where they have checked-in at. Aside from simply sharing location details, users can be

rewarded for their check-in activity, either through business incentives like discounts, or through recognition on the sites themselves. For example, Foursquare often notifies users of "Special Deals" at nearby businesses, as well as offering "badges" just for fun when users meet various check-in criteria.[17]

The following section discusses three of the leading check-in services, namely Foursquare, Facebook Places, and Google Latitude, and explores each service's primary purpose and core functionality. Though each differs somewhat from the next in operation and aesthetics, it soon becomes clear that a common feature they share is actually a common flaw for legal purposes: the absence of precise location authentication, while streamlining the user experience, negatively impacts evidentiary value to a large degree.

Foursquare

Foursquare is one of the premier check-in services, and has grown astronomically over the past two years. Since it's inception in 2009, it has garnered over 6 million users. In 2010, it reported 381,576,305 user check-ins, and 3400% growth over the previous year.[18] Foursquare allows check-ins through its mobile applications, now featured on all of the leading smartphone operating systems, as well as limited functionality through its mobile web page.

Users must run the free Foursquare application on their mobile devices and check in through the application in order to receive badges for their check-ins and get

[17] http://theweek.com/article/index/200751/what-is-foursquare *[Accessed 5/6/2011]*
[18] https://foursquare.com/2010infographic *[Accessed 5/6/2011]*

the most of Foursquare's offerings. This application can be downloaded through any platform-specific "app store." During initial setup, the application will ask the user to register with a Foursquare account, match address book contacts with other registered Foursquare users, and link Facebook and Twitter accounts for easy publication of Foursquare check-ins.[19]

After this initial setup, users simply load the Foursquare application when they wish to check-in, and the application automatically accesses the device's GPS to get an approximate fix on location. Once a general location [20] is established, the application presents users with a list of nearby locations available for check-in. If a user does not see his or her desired check-in location, the user may use the application's search feature that expands the location radius. If the user's desired check-in location does not exist, the user may create a new location that will be saved for other users to check-in at. After the

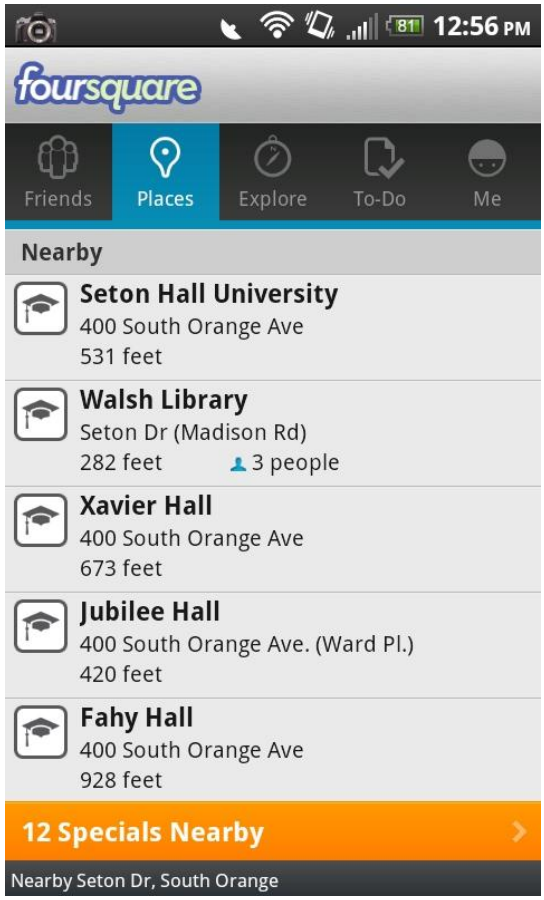

Figure 7. The Foursquare application user interface for Android devices. Users can select a suggested location, search other locations, or create a new place from within the application.

[19] http://www.howcast.com/videos/386406-How-To-Unlock-Your-World-With-Foursquare *[Accessed 5/6/2011]*

[20] *Foursquare, like most check-in sites, does not need an exact location in order to return potential check-in locations. Foursquare can function using non-precise aGPS data alone. This is discussed further in the following section.*

user confirms the check-in, it is shared with the user's Foursquare friends, and through Facebook and Twitter updates, if enabled. Users can post short message "tips" for the locations they've visited, so that future Foursquare explorers might benefit from the information.

Users without smartphones can also check-in to places by utilizing the Foursquare mobile web page or using SMS messaging, though this user experience is starkly different from the application method. Aside from the obvious diminution in the application user interface's aesthetic appeal, the most notable change is the ability to manually provide Foursquare with the user's location, without limitation. Users of both the SMS and mobile web check-in method can essentially check in anywhere in the world, appearing to friends and other Foursquare users as though they are there, with only a few interface-guided steps. The only checks in place for

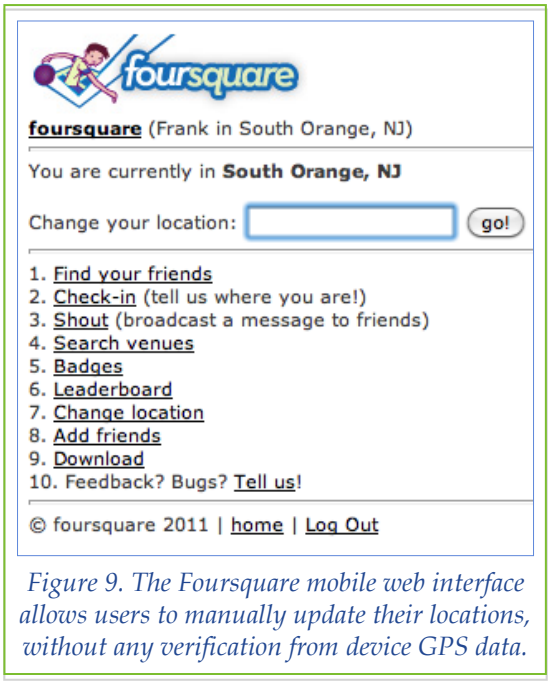

Figure 9. The Foursquare mobile web interface allows users to manually update their locations, without any verification from device GPS data.

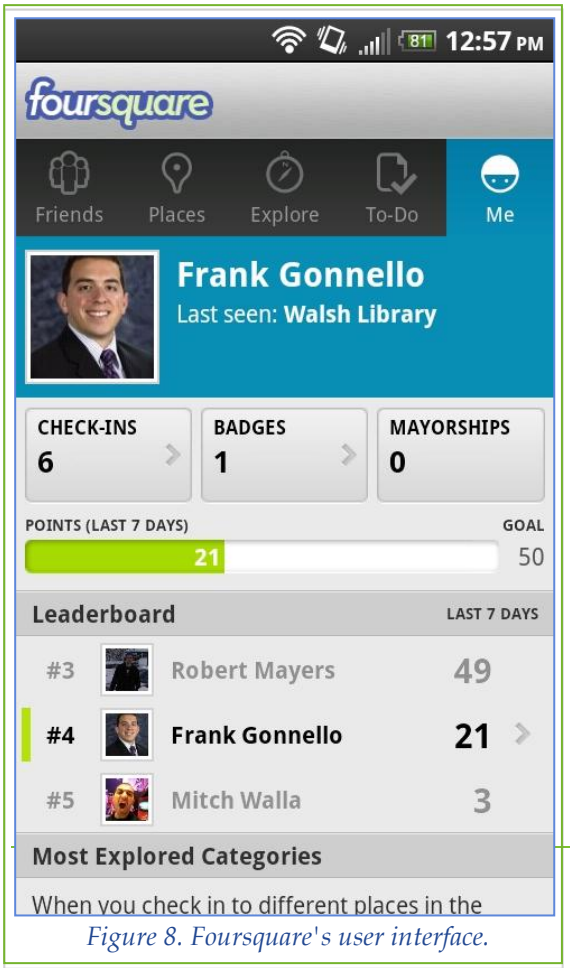

Figure 8. Foursquare's user interface.

such activity is that users are not rewarded with badges or "mayorships," a title bestowed upon users that frequent a location more often than anyone else, for their activity conducted through this method. Except for the lack of rewards, there is no distinction made between these types of check-ins when they are published to the site. A similar limitation exists for users checking-in at extremely frequent intervals, known as "drive-by" or "walk-by" check-ins, as Foursquare vows to withhold points for such physically impossible behavior. [21]

The Foursquare application *(see Figure 9, supra)*, as well as the mobile and desktop web pages, allows users to browse their friends' activities in Foursquare and view other information about the user's location history. When clicking on the "Friends" menu within Foursquare, the user is brought to a list of places where his or her friends have checked into last, and the user is able to view these locations in greater detail. The data-filled "Me" tab provides plenty of data about the individual user as well, like a breakdown of the number of times a user has checked in, badges the user has acquired,

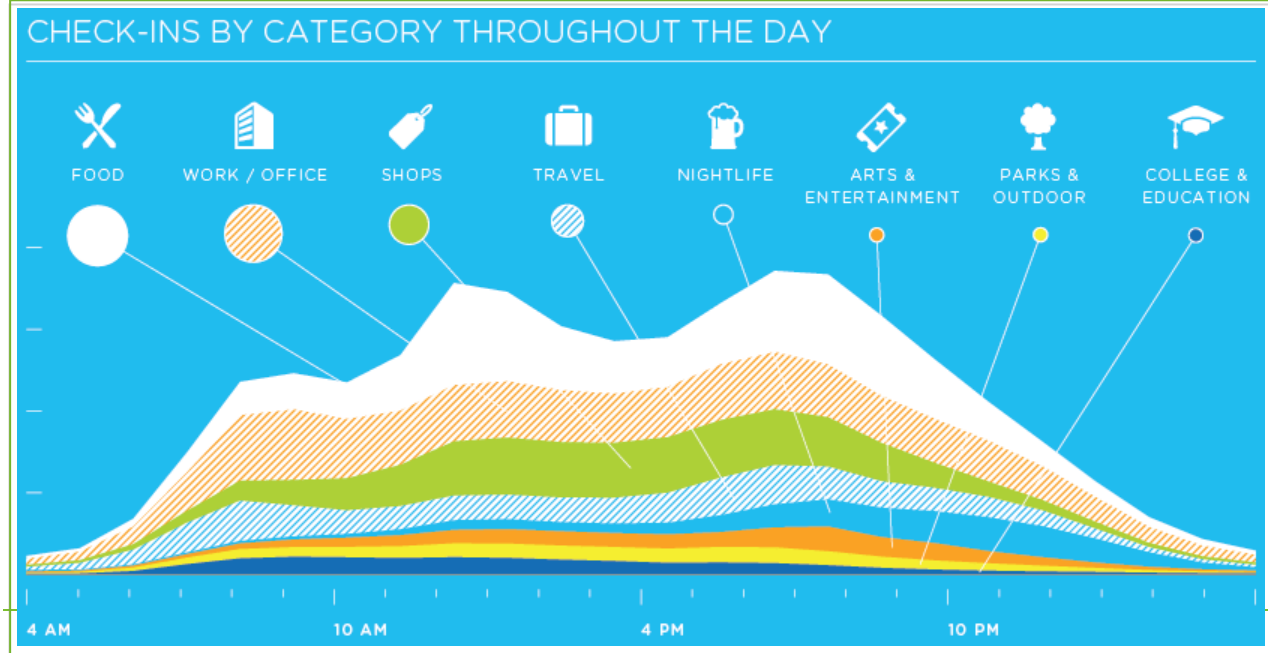

Figure 10. Visualization of proportion of categories that users checked-in to on Foursquare during 2010.

mayorship appointments, points accrued during the past week, a rating system for comparing the user's check-in numbers with his or her friends, and the user's most explored categories, just to name a few.

Foursquare is poised to continue growing in popularity and usage in the years to come, given its push for local businesses to play along in the check-in game. As a testament to its successes, especially in the East Coast, New York City Mayor Michael Bloomberg recently proclaimed Saturday, April 16, 2011, to be "Foursquare Day."[22] Because of the service's ease of use, simplified user interface, and integration with other social media sharing sites, legal practitioners should not expect Foursquare to check-out of courtroom controversy any time soon.

Facebook Places

Shortly after the breakout successes of Foursquare and similar check-in sites, the 500-million-users-strong social networking giant Facebook decided that it, too, would navigate the waters of location-based services. With more than 200 million of these users logging in to Facebook each day, and 55 million status updates created every 24 hours, Facebook appears as primed as any for the next big social networking breakthrough.[23] It's version of the check-in service came to be known as Facebook Places (hereafter, "Places"). As with Foursquare, Places is only available through mobile phone applications or via a mobile web browser, though the user experience is nearly identical in both formats. Places does not offer a SMS check-in equivalent. And

[22] http://mashable.com/2011/04/14/nyc-mayor-foursquare-day/ *[Accessed 5/6/2011]*
[23] http://mashable.com/2010/02/10/facebook-growth-infographic/ *[Accessed 5/6/2011]*

although Facebook's desktop site does not offer Places functionality besides viewing other users' check-ins, one only needs to enter "touch.facebook.com" into a desktop browser's address bar in order to access the mobile site.

Places begins with the user loading the ordinary Facebook application on his or her mobile phone, and navigating to the center button labeled Places. From there, the user is presented with his or her last check-in location (if they have used the feature before), as well as a long list of the user's friends' last check-ins. (*See Fig. 11*). From there, it's just a simple matter of pressing the "Check In" button in the top right of the screen. At this point, the application directs the mobile device to switch on its location services. (See Fig. 12). As with Foursquare, an actual GPS lock is not required in order to see places nearby, and any places not listed can be searched for by proximity, or created by the user on-the-fly. Once the user selects or creates the place they wish to check-in to, they are asked to leave a comment on their activity describing what he or she

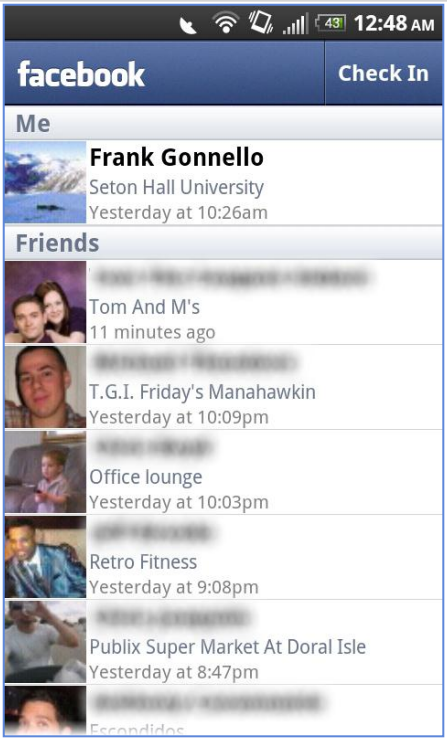

Figure 11. The Places home screen within Android's Facebook application.

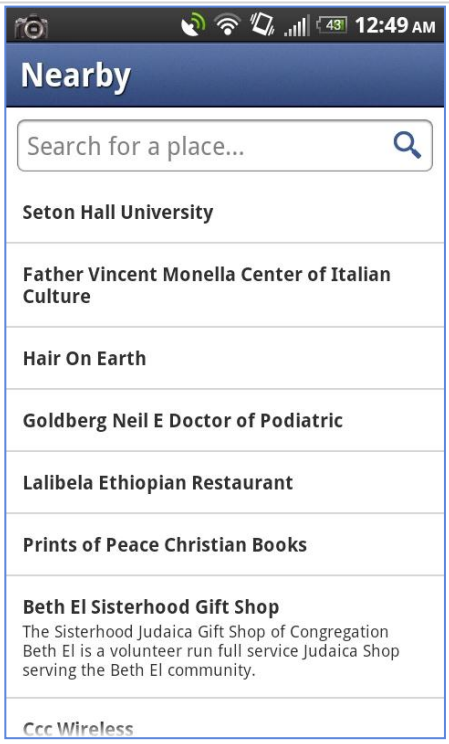

Figure 12. Places displays locations nearby, but allows searching in a wider proximity using device location data.

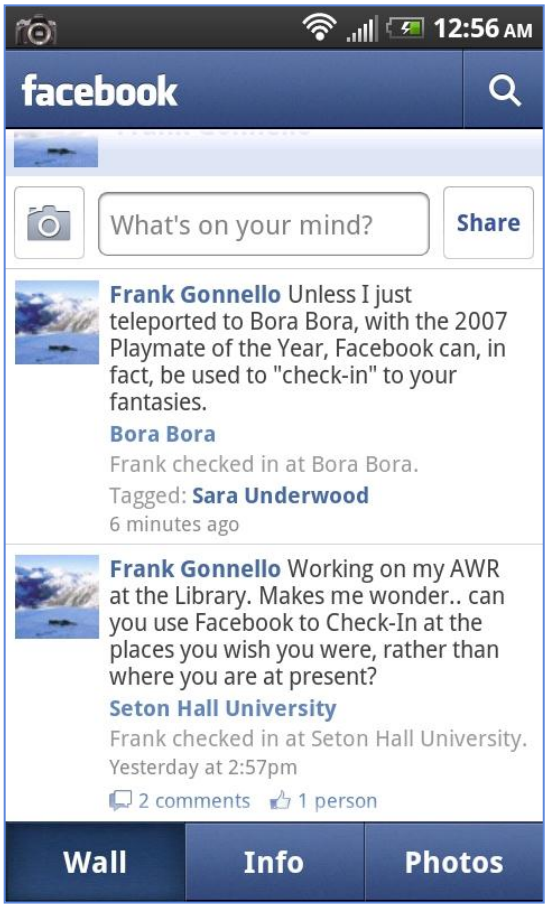

Figure 13. Demonstration of the ability to "tag" a user at a location that neither user is actually at.

is doing, and to "tag" other Facebook contacts that are at that location with you.

This tagging feature is a significant departure from the Foursquare check-in model. Since Foursquare distributes points and badges as a game for checking-in frequently, it has more incentive to limit check-in ability only to the user himself. With Places, a user may tag another user as if they were at a location without requiring that second user to ever confirm the tag. What's more, no verification of location is conducted, so the user may be tagged when they are not, in fact, at the location. Users may opt-out of this "tagability" feature at any time by digging through Facebook's privacy settings and disabling automatic tagging permissions.

When users complete the check-in process, they are able to view their own check-ins on their walls, and their check-ins appear on the news feeds of any friends that have been granted the privacy permissions to view this information. Default Places settings also allow others who check-in to the same locations to see what users are presently there, and connect with those users. Unlike with Foursquare, Places prohibits check-ins that occur too geographically far away in a short period of time. Though it is unclear

what measurements Places employs to keep checks on check-ins, it is hardly precise, and likely functions more as a barrier to spam, or an unwelcome flood of broadcasted check-in updates, than anything else. [24]

As mentioned previously, the mobile web method of checking in gives users a nearly identical experience, as the application user interface is essentially just a replication of the Facebook mobile web page. However, where Foursquare openly allows users to change their locations manually with the sacrifice of badges and points, the mobile web version of Places does not permit this sort of change, utilizing only the location data made available by the device. Still, this is quite easy to override with the use of a web browser plugin such as Geolocater for Firefox, which allows a user to "spoof" or trick a browser into reporting it is located anywhere in the world.[25] Places also launched its "Deals" functionality in November of 2010, where businesses may list special offers available only to those that check-in at their establishment at a certain time[26], though the shortcoming in check-in verification could be a reason why many businesses have yet to explore it. Places does not distinguish between mobile web and application check-ins in any way, users browsing such check-ins have no real way of knowing the validity of the check-in.

Where Foursquare is designed as a game to incentivize people to visit commercial places and retail stores, Places is more designed for social interaction and

[24] *In testing, I was able to check-in at Bora Bora after checking-in at Seton Hall University in South Orange, NJ, after approximately 10 hours, a trip that would have taken approximately 20 hours from start to finish. This was accomplished using only Firefox, the Geolocater plug-in, and touch.facebook.com.*
[25] *https://addons.mozilla.org/en-us/firefox/addon/geolocater/ [Accessed 5/6/2011]*
[26] *http://www.facebook.com/blog.php?post=446183422130 [Accessed 5/6/2011]*

conversation. Because of the inherent nature of the millions of Facebook users worldwide to share their activities with friends, Places does not need its own point system or rewards badges to keep usage up. The integration Places has with the basic functionality of Facebook is enough of a reason to keep checking-in, and because of the sheer number of active Facebook users, it is only a matter of time before Places gets tagged in a courtroom near you.

Google Latitude

The last of the location-based services to be discussed in this paper is also the last one to check-in at the party. Google Latitude (hereafter, "Latitude") is a feature of Google Maps that allows users to see where their Google contacts are on the map and facilitate communications between them. Latitude differed at birth from the previously discussed location-based services, as it began as software that *automatically* logged and broadcasted a user's location to its contacts as long as the service was running on the user's mobile device at the time. Latitude sought to provide the answer the question of "Where is my friend/relative?" with just a glance at its application. It also served as a tool for Google to optimize local search results for users utilizing Google's search engine from the same connected devices, since Google knew the user's location prior to inputting any search terms. Google claimed to have 9 million active users in 2010[27],

[27] http://googlemobile.blogspot.com/2010/12/introducing-google-latitude-app-for.html *[Accessed 5/6/2011]*

though this number seems off if personal experience is to be any guide.[28]

Regardless, Google felt it was missing out on a market of those users who wanted to selectively check-in and publicize their action, rather than continually broadcast their whereabouts. Thus, Google launched Latitude's "Check In" feature in early 2011, bringing its own twist to checking-in while largely borrowing the best features of Foursquare's successful formula. Google Latitude now operates in two ways based on the user's preference: the always-on, always-tracking method which records and publishes a user's location continually at the street, town, or state level, or the (optionally automatic) check-in/automatic check-out method.

As with both of the other check-in sites discussed previously, a user simply needs to open the Latitude application on their mobile device. Sharing a location begins when you accept the terms of service and agree to have the location data published to your Google profile. Users also have the choice at initial setup to allow Google to record your location history indefinitely. After agreeing and completing the setup, the user is sharing his or her location until they manually sign out of the service. At all times in which the user is signed in to Latitude, the mobile device's GPS and location data is being polled for updates on location. The precision of this location is determined by the user's preferences, and may include GPS locks for precision up to a few meters. Users can also log their locations via web browser as well as view their contacts' shared

[28] *Of my 600+ Google Contacts, only 6 have ever requested or confirmed a Latitude sharing request. My results are not atypical, as blogger Adam Jackson points out. (See http://adam-jackson.net/blog/2010/12/14/i-believe-there-are-nine-million-google-latitude-users/ [Accessed 5/6/2011]).*

locations by using the iGoogle[29] home page and Latitude widget. A limitation of this method is that iGoogle does not support check-in functionality at this time.

To begin more targeted sharing of the user's location, the user must send an invitation to share location information to a friend within the user's contact list. When a friend accepts the invitation, his or her location will be revealed to the user on Latitude's map, and core Latitude functionality is obtained. Since February of 2011, however, more advanced features have been introduced, allowing check-in functionality at any Google Places location.

Figure 14. Google Latitude's map visualizes contacts' locations on an interactive map.

Similar to Facebook Places, a simple tap on the Latitude application's "Check-In" icon will bring up a list of suggested places nearby. A user may select from this list, or manually search for a location to check in to anywhere in the world, regardless of the device's reported location data. While the legitimate benefits of allowing users to manually adjust for suggestion errors is clear, this can create a mismatch of the user's published location. However, since locations are broadcast visually, in real-time, only with the contacts a user has connected with in Latitude, there is no public bread crumb trail to

[29] http://Google.com/ig *[Accessed 5/6/2011]*

trace another user's previous locations.[30] Within the user's stored Location History, however, these mismatches would be logged and accounted for.

Other features within Latitude include the optional ability to set a location to be automatically checked-into when the device is nearby, and the automation of checking-out when the device leaves a location. In addition, Google began to offer Latitude Deals in April of 2011, an incentive based program designed, like Foursquare, to reward users for frequent check-ins at their favorite retail establishments.[31] When checking-in to certain outlets, Latitude will provide the user with a discount depending on how many times the user has checked-in to the location.[32] The more times a user checks-in, the higher their "status" is at that locale, and therefore the better the discount that user can receive.

Given the logging of location data in real-time, the detailed storage of location history in a user-accessible format, and the relatively more advanced (albeit, possible) difficulty of spoofing a mobile device's location in real-time, Google Latitude may be the most valuable location-based service in the court room, if its data is obtained legally.

Weak Signal | Legal Issues in Using Check-In Data as Reliable, Admissible Evidence

It is hopefully understood at this point the various location-based check-in

[30] *A Latitude user can opt-in to record his or her own location history for as long as they are signed in to the Latitude service. The implications of this private location history record are discussed in further detail, infra.*

[31] *At the time of publication, only 12 franchises have been listed in Places "offers." See* http://goo.gl/LUnCb *[Accessed 5/6/2011])*

[32] http://mashable.com/2011/04/07/google-latitude-checkin-deals/ *[Accessed 5/6/2011]*

services available to location-aware mobile device users and their means of operation. Quite clearly, individuals are making it publicly available where they are, who they're with, and what they're doing, and for the most part, are doing so voluntarily. Knowing full well what a user can and cannot do with these services should lead any legal practitioner to one all-important question: what can these services provide in the form of evidence for or against my clients? The answer, for the most part: very little.

No doubt, there will exist cases where social media will supply defense teams with an alibi, such as the acquittal of robbery charges for a Brooklyn teenager that posted a status update on Facebook from his home computer at the time of the crime.[33] But these stories of how social media can set you free only tell half of the defense's story. For social media to be admissible in court or have any evidentiary value at trial, the content needs to pass muster under ordinary evidence rules; many times, this means a considerable amount of corroborating evidence to establish reliability. This hurdle stands especially tall in cases of location-based check-in services, given the fact that each of these services provides no way of verifying the authenticity of the alleged locational contentions.

Legal Issues Pertaining to Privately Stored Location Data as Reliable, Admissible Evidence

There is quite a distinction to be made between social check-ins data and the raw data output of GPS units. GPS data extracted from GPS-receiving devices has been used

[33] *http://www.eweek.com/c/a/Data-Storage/Facebook-Case-Sets-Up-Google-Latitude-as-Tempting-Legal-Tool-481851/ [Accessed 5/6/2011]*

as evidence in courts for years. Reliability of raw GPS data, as previously discussed, is considerably high, as the output of these receivers does not depend on user interaction. Controversy arises in these cases not so often in questions of reliability, but rather in the discovery and admissibility of the evidence in light of the Fourth Amendment's "reasonable expectation of privacy."[34] Thus, the challenge in many of the cases that use relevant raw GPS data is overcoming a warrant requirement if no warrant is obtained beforehand. The legal issues pertaining to these traditional circumstances are imputed to the usage of Google Latitude's private location history data as well.

In *United States v. Maynard*[35], the court addressed location tracking of an individual via a GPS device hidden on the suspect's vehicle which reported the location of the vehicle in real-time. In *Maynard*, Washington D.C. nightclub owner and co-defendant Antoine Jones was under investigation for alleged involvement in a cocaine-selling operation.[36] Prosecutors successfully obtained a warrant to attach a GPS tracking device to defendant's car, but under the stipulations of the warrant, this needed to be done within the jurisdiction of Washington D.C., and within 10 days.[37] However, investigators installed the tracker on the 11th day, in Maryland, contending that the warrant they previously obtained was no longer required.[38] Using the tracker, police monitored Jones' globe-trotting for a month, eventually obtaining enough evidence to

[34] *Katz v. United States, 389 U.S. 347, 360-61, 88 S. Ct. 507, 514, 19 L. Ed. 2d 576 (1967).*
[35] *United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) cert. granted by U.S. v. Jones, U.S., June 27, 2011, 131 S. Ct. 671, 178 L. Ed. 2d 500 (U.S. 2010).*
[36] *Id. at 549.*
[37] *United States v. Jones*, 2011 WL 5360051, 16*:15-18* (Oral Argument, heard November 8, 2011)
[38] *Id.*

put him behind bars for a life sentence.[39]

On appeal, the question as to whether a warrant should have been required for the installation of a GPS tracking device on defendant's vehicle was answered in the affirmative.[40] The court reasoned that a month's worth of location tracking provides an intimate picture of the subject's life, one not meaningfully subjected to public exposure since sustained physical surveillance over such a period is effectively impossible.[41] "A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain 'disconnected and anonymous[.]"[42]

The government suggested that Jones' expectation of privacy was unreasonable because his movements were taking place within a vehicle, not the home, and on public roadways.[43] However, the court rejected this theory as dispositive of the expectation of privacy, stating that "a person does not leave his privacy behind when he walks out his front door[.]"[44] The court also rejected the government's attempt to equate GPS-based surveillance to traditional forms of "tailing" and visual surveillance, stating that the means used to uncover private information does matter with regards to the Fourth Amendment.[45]

---

[39] *Maynard, 615 F.3d 544, 549.*
[40] *Id. at 568.*
[41] *Id. at 560-64.*
[42] *Id. citing Nader v. Gen. Motors Corp., 25 N.Y.2d 560, 572 (1970).*
[43] *Id. at 563.*
[44] *Id.*
[45] *Id. at 565-66.*

In concluding that the government's use of a GPS tracking device was distinguishable from traditional visual surveillance methods and that such an investigative arrangement should trigger a warrant requirement, the *Maynard* court placed enormous emphasis on the fact that tracking a person's movement beyond just a specific individual trip, "thereby discovering the totality and pattern of his movements from place to place to place," violated an individual's reasonable expectation of privacy regarding the "intimate picture of his life."[46] The court left open the possibility that prolonged visual surveillance could implicate a need for a warrant, but that due to practical considerations regarding the manpower and resources needed to obtain the same degree of information as a GPS tracking device, visual surveillance is usually terminated before this level of exposure is rarely reached.[47]

Borrowing from the logic of *Maynard*[48], district courts in Texas and New York have both concluded that historical cell-site information ("CSI"), a log of technical pings by a mobile device to it's cellular service provider's towers which reveal a device's location with considerable precision, require a warrant under some circumstances. In New York, Magistrate Judge Orenstein found it appropriate to obtain CSI without a warrant because of the length of time in which surveillance was requested.[49] There, the government sought an order directing AT&T Wireless to disclose CSI for a three-day period and six-day period, weeks apart, for one telephone, as well as a 12-day period

[46] *Id. at 556-58. See also* United States v. Knotts, *460 U.S. 276, 278, 103 S. Ct. 1081, 1088, 75 L. Ed. 2d 55 (1983).*
[47] *Id. at 565.*
[48] At the time of this paper's publication, *Maynard* has been granted certiorari by *U.S. v. Jones*, U.S., June 27, 2011
[49] *See Application for Historical Cell Site Information, 2011 U.S. Dist. LEXIS 15457 (EDNY).*

for a second telephone. Judge Orenstein distinguished the facts from those in *Maynard*, deciding that the information gleaned over shorter periods, separated by weeks or months, would not be as revealing as the sustained month-long monitoring at issue in *Maynard*.[50]

Though noting length of time of surveillance as a factor to consider, Magistrate Judge Smith of the Southern District of Texas placed more emphasis on the nature of CSI surveillance than the time frame for which the government seeks to obtain it.[51] Judge Smith distinguishes the GPS tracking device of defendant's car in *Maynard* from the "far more intrusive" data collection of an individual's cell site records, because such records essentially track a person's movements and activity within the home. Smith also notes that the "temporal distinction between prospective and historical location tracking is not compelling, because the degree of invasiveness is the same."[52]

Notably, Smith cites to Justice Scalia's view from *Kyllo v. United States*, that "[i]n the home . . . *all* details are intimate details, because the entire area is held safe from prying government eyes." (Emphasis in original).[53] In *Kyllo*, the defendant was being investigated for growing marijuana in his home when investigators, without a warrant, used a thermal imaging device on the exterior walls of defendant's home to detect heat generated by common indoor heat lamps.[54] There, the court held that where "the Government uses a device that is not in general public use, to explore details of a

[50] *Id. at 2.*
[51] *See In re U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010).*
[52] *In re U.S. for Historical Cell Site Data, 747 F.Supp.2d at 839.*
[53] *Kyllo v. United States, 533 U.S. 27, 37, 121 S. Ct. 2038, 2041, 150 L. Ed. 2d 94 (2001).*
[54] *Id. at 27.*

private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment "search," and is presumptively unreasonable without a warrant."

There are many parallels to be drawn to these cases with regards to Google Latitude's stored location history. While the information collection is opt-in, it is for the individual user's eyes only. This history is not shared publicly, and the privacy of this information is listed in plain language on the page in which users can enable the feature. It seems obvious that a reasonable expectation of privacy exists with regards to this data, at least with regards to third party disclosure. Furthermore, Latitude's location history is recording by the minute, at precision of both on-board GPS and CSI levels. This data is continual, and gaps only exist when a user manually deactivates the feature or manually removes certain pings. For the same reasons as stated by the Southern District of Texas, the information is far more intrusive, going within the home to trace a user's activity. As stated in *Katz*, a "search" would occur "when the individual manifests a subjective expectation of pricacy in the searched object, and society is willing to recognize that expectation as reasonable." It would seem, therefore, that the Government's seizing of Google Latitude location history for any period, extended or not, would constitute a "search," and a valid warrant would need to be obtained prior to the search. After that, authentication could be established with relative ease.

Legal Issues Pertaining to Voluntarily Conveyed Location Data as Reliable, Admissible Evidence

With social media utilizing GPS data loosely and allowing for users to modify

the output of their published check-ins, discoverability, admissibility, and reliability are all called into question. Discovery and constitutional challenges for acquiring location-based social media data are perhaps weaker arguments to make, given the fact that for most of the services, check-ins are made with the purpose of the action to be publicly announced and published. As the Supreme Court stated in *Katz v. United States*, "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[55] More specifically, "whether an expectation of privacy is reasonable depends in large part upon whether that expectation relates to information that has been 'expose[d] to the public.'"[56]

While there are many hypotheticals that could be concocted, it would seem clear that check-ins in both Facebook Places and Foursquare are knowing public exhibits by a user of their location at a given time, as they notify others browsing the locations of what users are presently there. Google Latitude's check-in functionality is the only service that permits users to check-in privately, only for their own records. Whether a valid expectation of privacy exists as to require a warrant for collecting this data remains to be decided by any court of precedence.

Despite the relative ease in obtaining this evidence due to the absence of reasonable privacy expectations, reliability of this user-created evidence in itself is presumptively null, making its admissibility dependent upon a substantial showing of authenticity. As one Texas court pointed out (and what comedian Daniel Tosh makes

[55] *Katz, 389 U.S. at 351.*
[56] *Id.*

his living based on)[57], "anyone can put anything onto the internet," and information discovered on the internet is "inherently untrustworthy."[58] In *St. Clair v. Johnny's Oyster and Shrimp, Inc.*, plaintiff St. Clair brought claims for personal injuries alleged to have been sustained while employed as a seaman for defendant Johnny's Oyster & Shrimp, Inc.[59] In its motion to dismiss, the defendant claimed that he was not, at the time of injury, the owner of the seacraft involved in the incident, and requested dismissal under Federal Rule of Civil Procedure 12(b)(6).[60] However, the electronic "evidence" plaintiff procured from the internet to rebut defendant's 12(b)(6) claims was ruled to be "totally insufficient to withstand [the motion]."[61] The court took a firm, albeit reasonable, stance against using evidence procured off of the internet:

> "While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. . . . [T]his so-called Web provides no way of verifying the authenticity of the alleged contention that Plaintiff wishes to rely upon. . . Anyone can put anything on the Internet. No web-site is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on *any* web-site from *any* location at *any* time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of

[57] *"Tosh.0". Comedy Central. (Television, 2011). http://tosh.comedycentral.com.*
[58] *St. Clair v. Johnny's Oyster and Shrimp, Inc., F.Supp.2d 773, 774-775 (S.D.Tex.1999).*
[59] *Id. at 774.*
[60] *Id.*
[61] *Id.*

the hearsay exception rules[.]"[62]

While Judges may permit these social media check-ins to be discovered through preliminary hearings on admissibility, it becomes a jury determination as to the credibility and authenticity of such evidence based on supporting testimony and other authentication evidence.[63] Based on the preceding descriptions of these services alone, it is clear that check-in data is not optimal for precise, reliable establishment of a person's location at a given time without substantial corroborating evidence. In both Foursquare and Facebook Places, check-ins can be spoofed from both mobile devices and desktop computers, with little more knowledge than what a simple Google search can yield.[64] As such, several factors should be considered when laying the groundwork for checking-in data from location-based services as reliable, admissible evidence.

First and foremost, the user's location-based service account must be authenticated to the person, verifying ownership by providing information like a valid user name and password. Associated email accounts registered to the site can be used to link a person to account, if relevant email activity took place by the person pertaining to such accounts.[65] Second, proof that a device associated with the user was what registered the check-in or location ping is critical in bridging the gap between the user and his or her device's purported location. This data would ordinarily be obtained from the location-based service provider itself, and corroborated with records of the mobile

[62] *Id. at 774-75.*
[63] *Fed. R. Evid. § 104(a)-(b).*
[64] *http://lmgtfy.com/?q=spoof+check-ins [Accessed 5/6/2011]*
[65] *For instance, a user received a Facebook notification to his work email, to which he replies using the same email account.*

device's internet service provider for confirmation. Serial/ID numbers, IP/MAC addresses, and any internal identifications utilized by the service providers could be compared with billing information to verify. Accuracy of the purported location will also be called to question. This requires corroborating evidence that proves a user can, and did, travel to all of his or her purported and confirmed locations at the time the user or some other witness claims the user has done so (*see fn. 24, supra*). Additionally, proof that the user performed the mobile check-in himself at a particular time could be critical to the defense or prosecution of an individual. However, to establish this would mean to have testimony linking the individual to a particular time and place, compelling evidence in itself. It would be difficult to imagine a scenario where the testimony of a person that links a user's check-in to that user at a particular time and place would be given less weight than just a screen-grab of that user's check-in. Essentially, if a party has all of this corroborating evidence already, the evidentiary value of the check-in effectively provides zero net gain.

Checking Out | Conclusions

With so much corroborating testimony needed to introduce social media check-in data as reliable, admissible evidence, it is hard to see the standalone value of any check-in that user creates. There will be circumstances, as always, where the visualization of a suspect declaring his or her whereabouts will mean more to a jury than simply hearing this fact from another party, but these situations will be few and far between. Furthermore, location data that is logged in real-time by services such as

Google Latitude still requires authenticating corroborative evidence, but tends to give a more reliable, detailed depiction of a user's whereabouts. As a consequence, Latitude's location history data 180 days old or less[66] will likely require a warrant under the court's reasoning in *Maynard*[67].

If one thing is to be predicted based on the growth trends of all of the location-based services discussed in this paper, these services will only continue to expand in their user bases while adapting to the advancement of location technologies. One can only hope that the Federal Rules of Evidence, the Federal Rules of Civil Procedure, and the multitude of investigative procedure guidelines track these issues more precisely, giving privacy more latitude and allowing the courts to see where they should stand on these issues before they even arrive in their circuits.

[66] *The Stored Communications Act, 18 U.S.C. § 2703(d) states that a court order may be issued to release digital communications stored for more than 180 days by a service provider only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. Disclosure of stored communications dating less than 180 days may only be required of a provider pursuant to a warrant.*

[67] *Dependent, of course, on how the Supreme Court rules on Maynard (U.S. v. Jones) on appeal.*

 [68]

[68] *By the conclusion of this paper, I achieved* ***0*** *mayoral positions in Foursquare, my friends no longer believe I am where I purport to be on Facebook, and Google has a several-month saved history of where I live, work, and commute every day. On a brighter note, by completing this report I have effectively checked-in to my final year at Seton Hall Law. For my own satisfaction, I created this Advanced Writing Requirement Foursquare Badge, awarding it to myself as a way to boast about my academic achievement to friends that are following my progress.*