Getting to Where:

Location Based Electronic Discovery in Criminal and Civil Litigation

© David K. Isom[1]

2010 was the year that geolocation technologies such as mobile social networks and check-ins exploded into general use and awareness in the United States. In the final quarter of 2010, more mobile phones (100 million) were sold worldwide than PCs (92 million) for the first time. IDC Survey. This paper summarizes how mass location based technology will impact criminal and civil litigation, and how people and companies can understand and manage the legal risk associated with location technologies.

Three major developments in geo-technology and the way people use that technology portend a new world of location based electronic discovery ("LBED") in civil and criminal litigation.

The first technological development is that computers have become so small, powerful, cheap, robust and connected – in short, so mobile – that most Americans now carry one in their purse or pocket.

The second development is the growing use of a constellation of location technologies that, especially when combined, create and store location metadata (off-screen data that makes the on-screen data work) that is becoming ever more accurate, accessible and, for the truly "wired" (non-wired?), nearly continuous.

---

[1] David Isom is an attorney who does corporate litigation and electronic discovery consulting at Isom Law Firm headquartered in Salt Lake City, Utah.

The third development arises from the first two: location based services and applications ("apps") are changing the American business and social landscape as much as any development since the advent of automobiles and highways.

For example, navigation is migrating from stand-alone personal navigation devices such as Garmin and Tom Tom to mobile phone-based Google Maps and a new welter of smartphone navigation apps.

Because of its ability to identify and persuade prime, segregated potential customers, location based marketing is grabbing a sharply increasing percentage of companies' advertising budgets.

Apple, Facebook, Google and Twitter are leading the way, but a host of ingenious apps providers such as Groupon and Foursquare are adding to the location craze. Social networks on mobile devices have added dazzling (or scary, or intimidating, or all of these, depending upon your perspective) real-time location features.

A growing percentage of cellphone cameras and even camera cameras embed GPS location data in photos and videos that end up on Flickr and YouTube and elsewhere on the Internet. And relentlessly, silently, gather a person's time-stamped locations with such precision that sometimes his speed and direction can be calculated. And record the location data on drives up to 64 gigabytes that keep the data for months or longer, even after deletion.

Every indication is that we have seen only the beginning of these important services and technologies. Still, surveys indicate that most people fail to appreciate how much and how persistent and how revealing the location information is that they

generate, and how important – whether helpful or harmful -- that information is likely to be in litigation. Or they are simply willing to sacrifice some privacy for the siren benefits of mobile connectedness.

To be sure, information technology developments over the last 30 years have persistently created new ways – from credit cards to Wi-Fi hotspots to telephones to highway toll stations to security cameras to radio frequency identification (RFID) -- to track a person's location, and "location privacy" has become a common phrase exactly because it is disappearing.

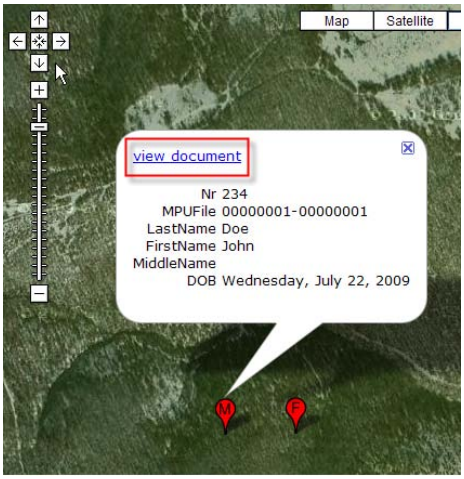
But the location technology that constellated in 2010 will make location, location, location more important in civil litigation and criminal prosecutions than ever before. *Subjective* location *data* – i.e., what people *say* about their location, such as when a person sends a text message that she is at a certain Starbucks -- will continue to be important. But the importance of *objective* location *metadata* – what a *device* says about its own location – is growing with each new technology that frees a device to roam tethered only by electrons and leaving only digital footprints.

The appendix to this paper has exercises that you can do to get a feel for some of the location data that you may be creating or that may be accessible in litigation.

I. Why Location Matters in Civil Litigation and Law Enforcement

Trial lawyers, like playwrights and novelists and marketers, know that the when and where are the foundation of selling or persuading or proving the what. There are, of course, cases where the where is undisputed, and some where the where is unimportant. But where the where is disputed and important, the very ability to prove a person's location at a key moment can exonerate or inculpate. Zylab, for example,

enhanced the war crimes case against Slobodan Milosevic by mining geolocation data and presenting the data on Google maps.



In a case where my corporate client was sued by a building contractor for alleged underpayment for the construction of bottling plants around the country, we were able to prove that the client had in fact overpaid because subcontractors had inflated bids and invoices because of commercial bribes consisting of dinners and prostitutes. We discovered this by figuring out the location of each main player at important times, which led to photos and diaries and confessions. And to the recovery of the overpayments.

The essence of many criminal prosecutions is the location of the defendant at the critical moment. Location determines alibi.

Where were he and she at the moment of the alleged sexual harassment? Who attended the meeting at which the product in a patent case was discussed? Did Smith attend the meeting that is alleged to have started the price fixing conspiracy? Has an injury required a person to remain homebound? The where and when often tell the who and what and why.

II. Overview of the New Location Technology Landscape

What are still mostly called smartphones or mobile phones or cellphones are mobile computers. These devices are telephones, to be sure, but an increasing percentage of cellphones are "smart" devices for surfing, friending, following, texting, photographing, recording, posting, videotaping, tracking, locating, listening, watching, joining, playing, paying and meeting. These smartphones have drives that create, receive, send and store gigabytes of information – up to 64 gigabytes and climbing. Smartphone speed and storage capacity will continue to increase and prices will continue to drop for the foreseeable future.

A 2010 Pew Research survey concluded that 85% of adult Americans had cellphones, and 96% of Americans ages 14 to 29 had cellphones. 2010 Pew Research Survey. Cellphone users now send more emails and text messages by SMS (Short Message Service) or smartphone apps than voice calls. More Text. Indeed, the number of social network messages using Twitter and Facebook may soon outpace emails.

The location information that cellphones create, reveal and store, both in real time and in hindsight, has become robust, intimate and ever more accurate. This location technology has outpaced the awareness of all but a small fraction of those who use the phones. July 30 2010 WSJ.

The increase in cellphone location information is the result of the combination and increasing granularity of several technologies. A basic understanding of these technologies is helpful for understanding what location information is created and the

sources from which such information may be obtained by request or subpoena for litigation.

III. Cellphone Location Technology

Developments in the technology of cellphone location tracking have been spurred in part by federal regulations requiring the creation and retention of location information for 911 emergency services. Cellphone providers were required by FCC regulations known as E911 to make a certain percentage of phones "location capable" by the end of 2005 (Nuvio v. FCC, 473 F.3d 302 (D.C. Cir. 2006)), and new location specifications must be met by September 11, 2012. Wikipedia E911. Taken together, these regulations require cellphone companies to assure that 95% of their phones provide location information to local government Public Safety Answering Points (PSAPs) with longitude and latitude data accurate to 300 meters within six minutes of a request by a PSAP. Id. The FCC is currently considering further refinements of these E911 location requirements. FCC E911 2011. The FCC, in a project dubbed Next Generation 911 or NG911, is also studying how to expand 911 capabilities to allow emergency communication of geotagged photos, video, text messages and other technologies beyond the current capability of 911systems. NG911.

The following are the four principal technologies that create, communicate and store cellphone location data.

A. Cell Tower Data

Cellphones are called cellphones because they receive signals from transmitters whose range encompasses a specific geographic area known as a cell. For a cellphone to be able to receive a call, the cellphone must be identified as being located within the

cell whose signal covers the area in which the phone is located. This requires signals to be sent continuously between the cellphone tower and all served cellphones within the cell area. This occurs whenever a cellphone's power is on and within the cell, even if a call is not in progress. Burr: ECPA Principles for Reform p.13.

The strength of this type of metadata for locating a cellphone is that the data are voluminous, real time and virtually continuous. The limitations of the metadata for locating the cellphone include the fact that the metadata are voluminous and therefore unwieldy, and that the metadata generally show only that the phone is within the cell area. In some cases, cell tower data may be able to show the speed and direction of travel from cell to cell and that a person (or at least a phone) was in an overlap area between two cells. In re Application for Order to ECS to Disclose.

The diameter of the cell area depends essentially upon the density of the population of cellphone users within the cell. ECPA Reform Hearing pp. 12 - 15. Cell diameters can be as large as several miles, or as small as a microcell covering only one room in a building, ECPA Reform Hearing pp. 12 - 15, and now there are "personal" cell "towers" the size of a Rubik's cube. Rubik's Cube Towers. "The number of cellular base stations in the U.S. has tripled over the last decade, and the rate of growth is accelerating. By one industry estimate, there are now over 251,000 reported cell sites operating in the United States." *In re Application for Historical Cell Site Data,* 2010 U.S. Dist. LEXIS 115529 (S.D. Tex. 2010) ("*2010 Cell Site Data Case*"). This number will continue to rise sharply as the volume of wireless data continues to rise and the size of cell diameters and of cell transmitting devices shrink.

B. GPS and Cellphones

The Global Positioning System (GPS) is a system of U.S. satellites that broadcast signals to terrestrial receivers to allow the determination of geolocation by triangulating signals from three or more satellites. GPS is comprised of at least 24 satellites constantly orbiting the earth in six low earth orbits. GPS devices started being included in some cellphones in the early 2000s, and the use of GPS in cellphones since then has grown dramatically. GPS is now included in most cellphones sold in the U.S -- approximately 80% of cellphones sold at the end of 2011 will have GPS. iSuppli Report.

Though no precise definition of "smartphone" has emerged, GPS is now one of the hallmarks of phone smartness. The use of navigation software in cellphones is projected to overtake personal navigation devices (PNDs) such as Garmin and Tom Tom by 2014, and many of the PND providers now offer navigation apps for smartphones. iSuppli Report.

The strengths of GPS for determining location are accuracy and frequency.

Accuracy: The accuracy of GPS-based geolocation data depends upon several factors, including the GPS technology, obstructions such as mountains and buildings, and the strength of the satellite signal. Many sources report accuracy of cellphone GPS data to be within the range of a few feet – close enough to measure the distance to the green in golfing, close enough to guide friends to meet in the mall. Magistrate Judge Stephen Smith recently found that "current GPS technology can achieve spatial resolution typically within ten meters." *2010 Cell Site Data Case, supra.* As discussed

below, even greater accuracy is possible with the combination of various cellphone location technologies.

Frequency: In early GPS-enabled cellphones, GPS consumed a large amount of energy, and was activated only when 911 was dialed. Which meant that GPS information was created and stored only on the rare occasion of dialing 911. Today the operating system of Apple's iPhone 4 (iOS 4), for example, allows multitasking – and allows GPS to run in the background while other features of the iPhone are in use. GPS is activated only when apps or other functions are in use that require GPS, but that can be at least several times a day. (On an iPhone, a purple  in the upper right-hand corner indicates when GPS is active.)

For example, Verizon began installing GPS in all of its phones in 2004, but at that time the GPS function was only activated for 911 calls. Verizon Data. Now, Verizon's iPhone 4 and other cellphones have GPS-enabled apps, including navigation, marketing and social services that can create near-constant location metadata. As Verizon says: "With VZ Navigator your phone becomes a fully loaded next generation GPS. Updated every 60 seconds from 1.8 billion traffic probes in the U.S., VZ Navigator Smart Traffic gives you spoken alerts and options to reroute around traffic jams." VZ Navigator Ad.

C. UTDOA

Another developing cellphone location technology involves triangulating the time that it takes radio signals to reach certain known terrestrial locations, such as Uplink Time Difference of Arrival (UTDOA). ECPA Reform Hearing pp. 126-28. Whereas GPS triangulates the time it takes for radio waves to travel from cellphones to three or more satellites, UTDOA measures and triangulates time of radio signals from cellphones to

receivers called Location Measurement Units (LMUs) co-located at cellphone base stations or towers. Because of the shorter distances between the cellphone and the known location measuring devices, and the ability to adjust the power output of handsets several times per second, UTDOA can provide accurate location data for cellphones and other devices in places (in particular indoors) where GPS may not be accurate or reliable.

D. WiFi

WiFi technology increases the ubiquity, accuracy and reliability of cellphone location data. Use of cellphones and other devices such as laptops and tablets (e.g., iPad) using WiFi creates and stores geolocation data from Wireless Access Points (WAP) and IP Address data, discussed in more detail below. WiFi broadcasts signals within a small area (such a private area is sometimes called an “access point” and the area is often called a “hotspot” if public, but the terms are often interchangeable) and connects those signals to the Internet. Some WiFi signals are encrypted, and some are password protected, but many are neither encrypted nor password protected.

Determining the number of WiFi hotspots is difficult, partly because of the varieties of definitions of these terms. But there are a lot of WiFi hotspots, and understanding WiFi is important for doing LBED.

If “hotspot” is defined as the range of a stationary wireless network -- such as in a coffee shop or business or hospital or home -- and of mobile hotspots -- such as in cellphones, dongles, pockets, buses and now cars like the dust cloud around Pig Pen -- the number of hotspots is huge. Fon, for example, claims over 3.5 million hotspots

worldwide, but is just one of many mobile WiFi providers. Fon. Stationary public hotspots number at least in the hundreds of thousands in the U.S.

WiFi is now a major source of geolocation technology. Skyhook, for example, has collected data about 3.5 million stationery WiFi hotspots and cellphone towers around the world, and triangulates data from WiFi with cell tower and GPS to increase the accuracy and reliability of geolocation services. Skyhook. Apple and Google and many other companies provide WiFi-based geolocation technology. Each WiFi hotspot creates location metadata that is potentially discoverable for litigation.

IV. Cellphone Location Based Apps and Features

At the end of 2010, the iPhone had over 300,000 apps (third party software that delivers services and games), and smartphones using the Android operating system (including Motorola, Droid and AT&T) had some 200,000. Of these, some 6,000 iPhone apps and 900 Android apps were location-based. Location-Aware Apps.

A recent Wall Street Journal article examined which of 101 popular iPhone and Android apps created and stored cellphone location information. WSJ re Smartphone Apps. The Journal reported that 47 of the 101 apps in the study apps collected and transmitted geolocation data. Some app providers sold the user data they collected from cellphones to third parties, including geolocation information and device ID numbers. Google, whose Android operating system hosts more apps than anyone except Apple, said in response to Wall Street Journal questions about the study, that app makers, not Google, "bear the responsibility for how they handle user information." Id. Many apps companies transmitted user location information to third parties without the user's permission or knowledge.

The following is a brief summary of some of the categories and uses of cellphone apps.

a. Social Networks

Social networks have become mobile. By the end of 2010, Facebook was available on 200 million phones, more than triple the number from a year before. Facebook More Mobile. In 2010, Facebook was granted an important geolocation patent whose purpose was summarized: "Search results, including sponsored links and algorithmic search results, are generated in response to a query, and are marked based on frequency of clicks on the search results by members of social network who are within a predetermined degree of separation from the member who submitted the query. The markers are visual tags and comprise either a text string or an image." Facebook Geolocation Patent. Twitter launched its first geolocation API in late 2009 (Twitter Launches Geolocation) and has continued to expand its location services. Foursquare approached 400 million geo-check-ins in 2010, a year of 3400% growth for Foursquare. Foursquare 2010.

Not all social network location data is objective or even reliable. Some are subjective – i.e., based upon what a person says about location. A person might say that her Twitter location is in "Justin Bieber's heart." But more and more social network exchanges include objective, device-generated location metadata that may be discoverable, more or less reliable, and mostly discoverable in litigation.

b. Location Based Marketing and Services

By tracking a phone's location, and marrying geolocation and movement data with other data or guesses about gender, income, ethnicity, age, sexual preference and

political views, marketers can multiply the effectiveness and return on investment of advertising. Groupon's recent Super Bowl ads were offensive to some, but the ads were a reminder that location based marketing is clearly here and growing. Economics are driving a torrid increase in location based commercial activity.

The line between social, marketing and other types of app networks is becoming increasingly blurred. Loopt and Gowalla and Foursquare and Google Latitude are as much social as commercial; Flickr and YouTube are as much social as media.

c. Mobile Payments

Many credit cards have near field communication technology (NFC) that allows the cards to be read at a short distance. NFC is moving to cellphones. Starbucks announced in January 2011 that its stores nationwide now accept payment by scanning a bar code from a customer's smartphone, and the projected expansion of NFC to cellphones suggests that cellphones will gobble a fair piece of the near-cash equivalents market. The iPad 2 and iPhone 5, expected to be released by Apple in 2011, are rumored to have NFC technology, for example. Google's Android Gingerbread 2.3 currently includes NFC technology, and Google appears to be planning expanded NFC applications. Mobile cellphone payments will expand available geolocation data.

d. Location Based Photography

Say you want to sell your motorcycle. If you take a picture of your motorcycle in front of your garage and post the photo online without scrubbing the location metadata in the photo, you take the risk that someone will read the location data embedded in the metadata, come to your place, and steal the motorcycle.

Cellphone cameras with GPS typically embed photographs with longitude and latitude data that can readily be converted to address or other location information using any of a number of Internet tools. E.g., Latitude Conversion. This location metadata is known as Exchangeable Image File Format ("Exif") metadata.

Exif metadata can be stripped from photographs, but if not stripped will typically carry the Exif metadata when stored, emailed or posted online, including at such sites as Twitter, Flickr and YouTube. Friedland & Sommer, Cybercasing (2010). See also icanstalku.com. Facebook currently does not preserve location metadata on photos posted on Facebook. Digital photos taken without Exif location metadata can be "geotagged" by adding this location data with tools readily available on the Internet. Of course, if a cellphone's GPS is disabled, this information is not captured when the photo is taken.

Geotagging photos and using geolocation data from other people's photos are popular for lots of reasons, including building itineraries from others' geotagged photos (Itineraries), creating 3D and other exciting collages (3D Dbrovnik), and cataloguing photos. The price of this convenience includes divulging information that a person may not appreciate and might not want to share.

e. Games, Entertainment and Other Apps

With hundreds of thousands of apps now available, and thousands of geo-apps, and more on the way, apps-engendered location metadata will continue to increase in volume and importance.

V. Stationary Computers: Tablets, Laptops, Desktops, Servers and Cloud Providers

Tablets and laptops are becoming more and more like cellphones in the geolocation information that they store. Many new generation tablets and laptops have GPS, and virtually all create and store WiFi data. Thus, tablets and laptops can generate some of the same location information that cellphones create.

In addition, tablets and laptops create and store most of the same geolocation information that stationary computers create and store.

Stationary computers, though stationary, can be a source of important location information.

For example, such computers create, transmit, receive and store subjective location information – e.g., a person's statement in emails or text messages or other ESI that she was in Topeka or that she will be attending the meeting in Jeffersonville, Ohio. And a stationary computer contains important location information about the computer's user – namely that he is at the location of the computer engaged in certain communications or processing at the time date-stamped in the computer's metadata.

Stationery computers, of course, can receive and store geodata from others' mobile devices. To the extent that stationary computers are connected to, or synced with, or receive objective location data from mobile devices, those data are likely to be recoverable from the stationary computer in addition to the mobile device from which the data came.

The connection of a stationary computer to the Internet also provides complex evidence of location the accuracy and reliability of which can vary with such factors as: (1) the browser employed; (2) whether the computer is connected by WiFi or wire; (3)

the Internet Service Provider (ISP); the use of a geolocation API (Application Programming Interface) such as Google Gears (Geolocation API); and the external Internet Protocol address, or IP address, of the computer's connection to the Internet.

IP Address: To connect to the Internet, a device must have an external Internet Protocol address, or IP address. The connecting device may be a router with the external IP address that assigns an internal IP address to the computer, or the computer may connect directly to the Internet with its own external IP address. Until February 3, 2011, the external IP addresses allocated by the Internet Assigned Numbers Authority (IANA) were a string of digits divided into four groups, with each group divided from the other groups by a period, and each group containing a number from 0 to 255, such as 154.32.1.209. That allowed a bit over 4 billion unique IP addresses, which just wasn't enough. On February 3, the IANA allocated its last four-group external IP addresses (IPv4), and began issuing six-group numbers. IP Address Exhaustion.

IP addresses are allocated by Internet service providers (ISPs) and other local Internet registries. An IP address for a particular computer or router may be static – i.e., always assigned to that device – or dynamic – i.e., the address changes at each sign-in or daily or some other period. The IP address of the device sending a message over the Internet, such as email, is included in the header of the message. An Internet search of the owner and location of that IP address can provide some clue as to location of the ISP and sometimes even of the user's computer, but the detail of such information varies widely among ISPs and devices. Subpoenas or requests served upon ISPs for data connected to an IP address (see the discussion of the Stored

Communications Act below), however, can reveal more detailed and accurate location information.

The location of stationary computers connected to the Internet using WiFi technology can be determined in the same way that the location of mobile computers and phones can be located with the WiFi metadata discussed above.

VI. Other LB Technologies

The ubiquity and variety of other technologies that are generating and will generate LBED are dazzling. RFID tags that give access to buildings will allow merchants in and around the building to make location based marketing pitches to a person in the building. See Schindler v. Otis, 593 F.3d 1275 (Fed. Cir. 2010). LBED-creating technologies will aid the tracking of animals including cattle (Farm--to-Consumer Legal Defense Fund v. Vilsack, 636 F. Supp. 2d 116 (D.D.C. 2009)), fish and other wildlife. Wikipedia Telemetry. From the analysis of disease, to aid in fighting wildfires, to the tracking of trucks, ships, trains, pets, children, patients, convicts, cars and farm machinery, geolocation technologies promise to become ever more amazing, important, beneficial and intrusive.

VII. Privacy

Few Americans realize the pervasiveness, persistence and possible impact of the location data that they are generating. Even the U.S. Air Force recently had to remind its deployed members to disable geolocation features of social networks to avoid revealing location. For those who are learning these facts, reactions range from horror to a resigned acceptance of the tolerable loss of privacy apparently necessary to enjoy the beguiling benefits of location based services. There is no doubt that public debate

about these issues is just getting started. There is also little doubt that technology can be designed to meet the demands of the market that emerge from this tussle.

In the meantime, the law relating to the use and privacy of location data will continue to develop. This section summarizes important legal developments in location privacy.

Though privacy law in the United States arises from three principal sources – the U.S. and state constitutions; federal and state statutes; and federal and state case law – one principle is common to privacy law from all these sources. That principle is that privacy analysis begins with gauging a person's "reasonable expectation of privacy" under the circumstances at issue. That is, the question is usually not whether a party to a lawsuit actually, subjectively, had an expectation that the data at issue would remain private, but whether a person can be deemed to have an objective ("reasonable") expectation of privacy under the circumstances.

A federal court in Michigan recently suggested, ironically, that the very fact that so many Americans carry GPS-enabled cellphones is evidence that they cannot reasonably expect privacy as to their location when they carry such a device. *U.S. v. Walker, 2011 U.S. Dist. LEXIS 13760* (W.D. Mich. February 11, 2011). In deciding that a defendant charged with illegal drugs had no reasonable expectation against officers secretly attaching a GPS tracking device to her car, the court justified attaching the GPS device in part by saying that the attachment was no more intrusive than "duct-taping an iPhone to Defendant's bumper…."

The section on criminal law below summarizes the principal location privacy issues that arise from the U.S. constitution. This section summarizes important LBED statutory and case law issues.

Location Privacy Statutes

The Electronic Communications Privacy Act ("ECPA"), including the Stored Communications Act ("SCA"), is the principal U.S. statute governing privacy of electronic location data. These acts are widely regarded as inadequate to clarify or control access to location data by law enforcement or civil discovery. For example, though the ECPA has been held to apply to cellphone data, the act was adopted in 1986, well before cellphones were publicly available.

The House Judiciary Constitution Subcommittee held three hearings on the ECPA in 2010, including one hearing specifically on location based technologies and services. ECPA Reform Hearing (2010). The Senate Judiciary Committee held ECPA hearings in September 2010. A coalition comprised of diverse members including Google, ACLU, Microsoft, Americans for Tax Reform, Facebook and the Electronic Frontier Foundation presented a Digital Due Process proposal arguing that technology has outpaced the ECPA and proposing principles of location privacy. Digital Due Process. No legislation from these hearings has yet been introduced.

Location Privacy in Civil Litigation

Though there are rare exceptions, privacy is not a bar to discovery in civil actions. The normal protection in civil litigation for private data is to allow discovery of relevant private information subject to a protective order that confines the use and

communication of the private information to the parties and their counsel. Thus, LBED will rarely be barred on privacy grounds.

Employee Privacy

Location data on cellphones will intensify the privacy battles emerging between employees and employers over the extent to which an employee may or may not have privacy or privilege rights in data and metadata on employer cellphones. With proper disclosures, carefully drawn policies, and clear consent, employers can access employee cellphone location metadata on cellphones owned by employers and provided to employees. Unauthorized access to such data, on the other hand, may create civil or criminal liability under the Electronic Communications Privacy Act, including the Stored Communications Act, and other federal and state laws. E.g., Shefts v. Petrakis (2010).

VIII. Retention of Location Data

Real-time collection of streaming location data occurs to some extent in criminal investigations (i.e., surveillance ordered pursuant to a warrant) and is authorized under certain circumstances by the USAPatriot Act, but almost never in civil cases. For civil litigation, and most criminal cases, LBED must rely upon historic geolocation records – data recovered or produced from the devices that create and store the data or devices that receive and store the data. Which means that, to be used in litigation, the owner and/or custodian of the relevant electronically stored location information (ESI) must be determined, and the ESI then acquired by informal self-help, formal request or subpoena.

The law distinguishes three drivers for keeping ESI that might provide clues as to where to find relevant ESI for litigation: (1) retention of ESI not compelled by law, but by inertia, inadvertence or voluntary processes; (2) retention compelled by statute or regulation irrespective of any specific actual or foreseeable retention litigation or other dispute; and (3) preservation of information relevant to a specific actual or foreseeable litigation or other dispute.

The more that lawyers and parties to litigation understand about the technology of potentially relevant location ESI, the better and more targeted their efforts to get this information can be. These issues are usually unique to each case, but a few generalizations are useful.

First, some location metadata is required by law to be kept for a specified period. Such legal requirements for retention can provide a starting place for knowing where to search for relevant information.

Second, most American businesses retain more information than most people in the organization can imagine, or than their written document retention and destruction policies may allow. It is more difficult to destroy all copies of an electronic document in an organization than to assure that the document is retained. Thus, public statements about what information a company destroys are often mistaken.

Third, many companies that create, store, analyze and/or sell location data have made it clear that they retain such information for some period, sometimes for months or years.

Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008) illustrates some of these issues. There, a son sued the Mayor of Detroit and others alleging inadequate

investigation of the 2004 shooting death of his mother. Some four years after the son's death, the plaintiff discovered that SkyTel still had text messages about the shooting that he believed might be relevant to the lawsuit. The court ordered city officials to provide PIN numbers, and ordered SkyTel to produce the text messages.

Four years from now, such recovered text messages that are being created now are likely to be rich in location metadata. What data are actually being retained that might be relevant to a particular case, and by whom and where, ultimately can be known only by specific discovery in the particular case.

IX. Forensics

Cellphones are essentially small, portable computers with limited user interfaces. Because most location data is created, transmitted and stored using familiar operating systems, basic forensics principles typically apply to forensic examination of location data. The following is a brief sample of forensics principles pertinent to an understanding of LBED from, for example, the iPhone 4. See Zdziarski, iPhone Forensics Manual (2008); Hoog, iPhone Forensics (2010).

Deleting data from a cellphone does not remove the actual data, but only the reference or the piece of code necessary to access the data. This deleted data may be overwritten and therefore destroyed by other, later data, but can remain available for weeks or more, depending upon the storage capacity of the cellphone hard drive and the amount of new data on the phone. Users are probably less aware that data remains (hidden) on their mobile devices than they are aware of laptop and desktop data because of the limited user interface to access and delete the data.

Much of the data created by a smartphone that reveals time and place remains available for forensic examination, including time-stamped GPS data, Wi-Fi connection data and keyboard caches that show emails, text messages, passwords and search terms. For example, iPhone 4's retain geolocation data – latitude and longitude – of photographs taken, map queries and pinging any app with a location feature. Call histories, contact lists, emails, text messages and voicemail messages may be recoverable. Taken together, this data can create a crystalline picture of where the cellphone was and when, and inferentially the location and activities of the owner of the phone.

X. LBED in Criminal Law Enforcement

A recent controversial California Supreme Court case illustrates fundamental LBED issues that will be important in law enforcement and criminal prosecutions. In People v. Diaz (Cal. 2011), Diaz was arrested and charged with conspiracy to sell illegal drugs. Police grabbed Diaz' cellphone shortly after his arrest and used evidence from the cellphone to convict him. Diaz claimed that seizure and use of cellphone information violated his Fourth Amendment privilege against unreasonable searches and seizures.

The California Supreme Court ruled 5-2 that prosecutors had a right to access Diaz' cellphone information on the ground that the phone, in Diaz' pocket when arrested, was in his immediate control. Under U.S. Supreme Court precedent, the California court held that the phone was taken legally because it was taken "incident to a lawful arrest." The dissenting justices, who would have suppressed the information from the phone, argued that a cellphone is unique from other objects that might be

taken from a pocket or purse or car incident to arrest because of the enormous store of personal and private information that can be revealed by such a mini-computer. The dissenting justices emphasized that “never before has it been possible to carry so much personal or business information in one's pocket or purse.”

To date, most, but not all, reported cases side with the California Supreme Court’s majority position in *Diaz* and allow prosecutors to use data from any cellphone taken from a defendant at or close to the time of arrest.

With a warrant issued upon a showing of probable cause, prosecutors can obtain an accused criminal’s cellphone and use what is revealed by a full forensic examination of the data on the cellphone.

XI. LBED in Civil Litigation

The following electronic discovery issues will be particularly important with respect to LBED in civil lawsuits.

a. Importance, Proportionality and Cost Management

A basic issue will be whether location is important and disputed. This should be pinned down early – by attorney conferences or requests for admission or otherwise. If location is clearly unimportant, or uncontested, the following processes can be ignored. Until the irrelevance of location can be confirmed, however, the following issues will be important.

b. Preservation

Though location metadata may well be recoverable on active computers and devices for months or longer after the metadata is deleted, the possibility that devices may be lost or destroyed, or that the deleted data may be overwritten and become

undiscoverable, suggests that efforts to preserve the data should be an urgent priority early in any lawsuit.

The first focus of preservation should be the devices of parties that created the relevant location based data – the smartphone or tablet or other device, and any of a party's other computers or devices that may have received the important location data by any sort of transmission, including syncing. This can be done either by making and securing a mirror image (i.e., a bit by bit forensic image) of the device, and then continuing to use the device, or by replacing the device, removing its battery and antenna, and storing the device until the data is needed.

The next focus should be obtaining and preserving the location data from others who may have created or received relevant location metadata, including possibly friends, colleagues, cloud storage facilities, servers, Internet service providers, social networks and apps providers. Of course, knowing who may have this data and how to get or assure preservation of relevant data requires understanding the technology and the networks that may harbor the data.

Prompt letters notifying parties and third parties of the scope of potentially relevant ESI, and requesting preservation of the ESI, are important.

c. Metadata and Production Format

Metadata is obscene. Five years ago, metadata seemed obscene in the nasty sense – off-colored, dangerous, lewd, offensive. Now it is clear that metadata is merely obscene in the other sense. The etymology of "obscene" is "ob scoena" or "off stage." That is, metadata is that part of the data that makes up an electronic document that is "off stage," or off the screen, when electronically stored information is created,

transmitted, stored and recovered. For those who understand metadata, metadata can be more useful than harmful.

Much location data is metadata. Lawyers and parties dealing with location data will need to focus on the rules and law relating to metadata.

The federal rules of civil procedure and similar state rules provide that the party requesting ESI of another party pursuant to Rule 34 or of a nonparty pursuant to Rule 45 may specify the format of production. Failure to specify format may forfeit the right to require that metadata be included in ESI produced in litigation. If metadata is requested, usually either by requesting that ESI be produced in native format, or in an image such as pdf with a load file of associated metadata, the ESI must generally be produced in the requested format.

In the last five years, attitudes in the legal systems of the U.S. about metadata have evolved from ignorance to wariness to familiarity and an appreciation of the usefulness of metadata. For example, metadata is essential to the ability to search, amass, analyze and manipulate information. Metadata can reduce the cost of using ESI in litigation by orders of magnitude. "By now, it is well accepted, if not indisputable, that metadata is generally considered to be an integral part of an electronic record." National Day Laborer Organizing Network v. U.S. Immigration (Feb. 2011) (Judge Shira Scheindlin).

Courts have recently held that metadata must be produced with ESI when requested, and that the failure to preserve and produce metadata may constitute a prohibited and illegal downgrading of ESI for litigation. E.g., National Day Laborer, supra.

Courts have also held that metadata is included in the definitions of records that must be kept and made available pursuant to federal Freedom of Information Act requests and similar state statutes. E.g., National Day Laborer, supra.

Lawyers dealing with LBED will need to understand the metadata associated with location based technologies – how and when it is created; how it can be lost or stripped; and what legitimate tools can be used to evaluate publicly available geo-information from the Internet, social network sites and apps. With the aid of forensics experts in some cases, lawyers dealing with LBED need to understand how metadata can be spoofed or faked, and how metadata can be used to authenticate location based ESI.

d. Subpoenas, Document Requests and the Stored Communications Act

The Stored Communications Act (SCA), which is Title II of the ECPA, complicates the acquisition of location data from an "electronic communication service" (ECS) and from a "remote computing service" (RCS). A company might be an ECS under the SCA even without providing communication services to the public. Devine v. Kapasi (2010). Several courts have held that data held by an ESC are exempt from the reach of subpoenas in civil actions. E.g., In re Subpoena Duces Tecum. But customers can obtain their own data from an ECS and RCS. Some courts have ordered customers who are parties to civil lawsuits to request data from ECS's and RCS's that could not be subpoenaed directly by the non-customer opposing party under the SCA. *Flagg v. City of Detroit,* 252 F.R.D. 346 (E.D. Mich. 2008).

The reach of the SCA exemption from civil subpoenas is far from clear, especially in light of the number and types of companies that may now have access to a person's geolocation metadata, and in light of the fact that ECS's and RCS's were

defined years before the current smartphone and apps technologies. For example, it is unclear how far SCA protection of data may reach with respect to location data gathered by a cellphone, transmitted by Twitter or Facebook publicly or to a list of friends or followers, and then sold to location based services.

Requests and subpoenas for LBED must be narrowly drawn to satisfy strictures of proportionality (balancing need against cost and burden) (Tamburo v. Dworkin) and inaccessibility under Rules 26(b)(2)(B) and 45 (d)(2)(D). See Isom on Inaccessibility, Federal Courts Law Review Articles.

XII. Ethics of LBED

Most of the ethics questions about LBED lie at the intersection of the duties of competence and diligent representation, on the one hand, and the interest in privacy and privilege on the other hand.

Since much potentially available location data is in metadata, the recent debate about the ethics of viewing metadata is a preview of issues that will arise concerning the ethics of LBED. Note that the debate has focused on reviewing metadata in electronically stored information (ESI) *received from an opposing lawyer or party*, and not on metadata in publicly available sources.

In 2001, the New York State Bar issued an opinion that it was unethical in New York for a lawyer to "surreptitiously examine and trace e-mail and other electronic documents" received from an opponent. 2001 New York Ethics Opinion. In 2006, the Florida Bar opined that it was unethical for a lawyer to review the metadata "that the lawyer knows or should know is not intended for the receiving lawyer." (The Florida opinion made it clear, however, that the ethical proscription did not apply to metadata

embedded in electronic data produced in formal discovery.) 2006 Florida Bar Ethics Opinion.

In 2006, the American Bar Association expressly rejected these approaches and opined that there was no ethical prohibition on a lawyer's review of metadata in ESI received from an opponent or opposing lawyer, at least so long as obtaining the data did not involve fraudulent, criminal deceitful or otherwise improper conduct. ABA Formal Opinion 06-442. Though the ABA opinion does not trump the contrary rules or opinions of any state, many states, such as Colorado and Maryland, have issued opinions consonant with the ABA approach. The ABA maintains a webpage that collects these opinions. ABA Formal Opinion 06-442.

Bar associations have started to examine ethical issues relating to obtaining information from an opposing party's social network site such as Facebook, and concluded that such information can be obtained ethically so long as no fraud, deceit or other illegal activity is involved in obtaining the information. In 2009, the Philadelphia bar opined that it is unethical for a lawyer or his agent to request that an opponent agree to be a Facebook friend of the lawyer's agent (to get access to the person's nonpublic Facebook pages) without revealing in the friend request the agency and the purpose for the friend request. Philadelphia Bar Opinion 2009-02.

In 2010, the New York City Bar reached the opposite conclusion: "We conclude that an attorney or her agent may use her real name and profile to send a 'friend request' to obtain information from an unrepresented person's social networking website without also disclosing the reasons for making the request." NYC Bar Opinion 2010-02. The New York City Bar emphasized, however, that only truthful information could be

used in sending such a friend request. The bar also emphasized that, if the opponent was represented by counsel, neither the lawyer nor agent could, consistent with Rule 4.2 of the Model Rules of Professional Conduct, send a friend request or communicate in any other way with the opponent except through the opponent's attorney.

The pivotal issues surrounding the ethics of LBED will revolve around whether the effort needed to access location data is so heroic as to be illegal or to offend notions of privacy. At present, the following seem to be the applicable basic principles.

There is no ethical proscription against mining location metadata from publicly available sources. A person who posts a photograph on the Internet, for example, should be presumed to know that the geolocation Exif metadata associated with that posting is publicly available, even if the person does not in fact know of the metadata embedded in the photo, and even if it takes specialized knowledge or software to access that metadata. Indeed, as the importance and availability of location data becomes better known, lawyers will have an increasingly clear and urgent duty of competence to use LBED. On the other hand, it is unethical to engage in conduct that is either criminal or tortious to access the metadata. Breaking a password to get to the metadata, for example, would be unethical even if technically easy.

XIII. Location Based Evidence

Location based evidence will be vulnerable to several challenges. The fact that a person's cellphone was at a certain place at a certain time does not by itself prove that the cellphone's owner was there, for example. There are readily available scripts that can make almost anyone the "mayor" of a Foursquare location. Location data can easily be spoofed for many apps, and most apps have no way to verify the reported

location data. Proving or disproving spoofing requires sophistication. Data about the percentage of reliability of any given location based app or data are scarce, and evidence of lack of consistency and reliability may prevent admission of some location data.

On the other hand, while some challenges to the admissibility of location based data will, and should, succeed, the flood of location data that will be admitted into evidence will overwhelm the drops of rejected evidence. Especially because location metadata can be triangulated and corroborated from multiple sources in most instances, successful challenges to the admissibility of location based evidence will be rare.

Moreover, because most cases settle during discovery and before admissibility can be challenged or determined, it is location based *discovery*, not location based *evidence*, that will be crucial in most cases where location is relevant and disputed.

The criminal cases discussed above show that some LBED can successfully be suppressed on constitutional grounds, but the early social network and apps cases are routinely admitting such evidence, usually without serious challenge.

Appendix

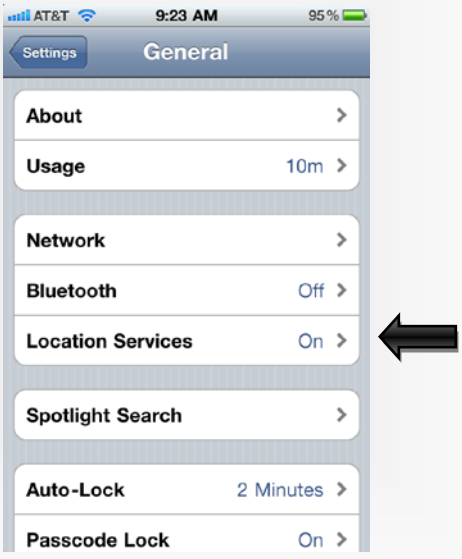
Five Location Exercises

1. Turn On/Off iPhone 4 GPS

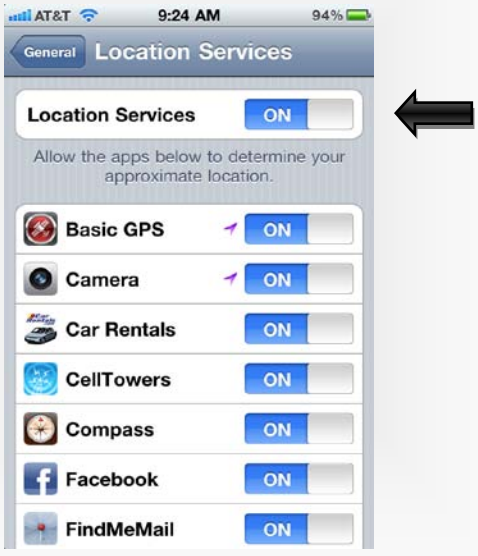
a. Open Settings

b. General

c. Location Services



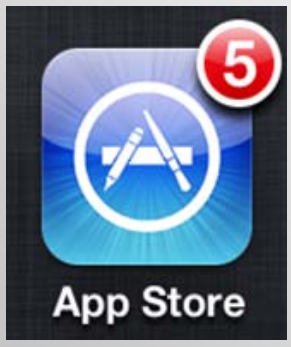
d. Location Services On/Off



(This page also shows which apps use geolocation, and therefore create and store geolocation data on your iPhone. Notice also that the ➤ means that the app has used GPS within the last 24 hours.)

2. Test Accuracy of a GPS app (this illustrates the “Basic GPS” app on an iPhone 4 -- this experiment will cost 99¢)

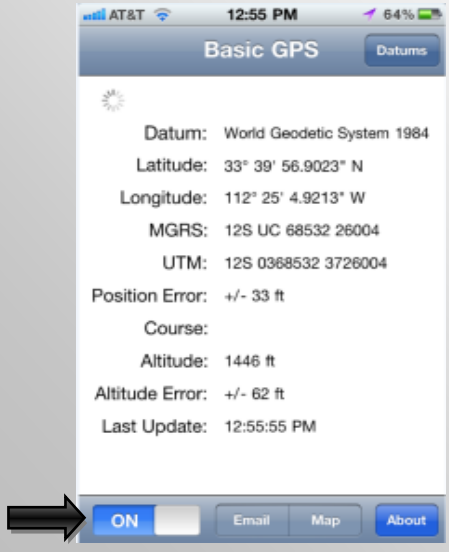
a. Open App Store



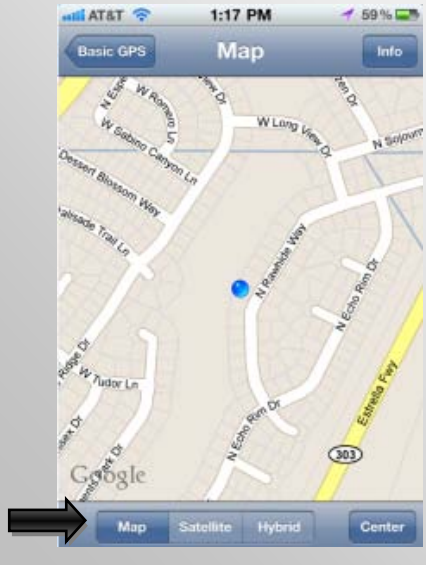
b. Enter, purchase and download “Basic GPS”

c. After installation, open the “Basic GPS” app

d. Slide “On”



e. Click “Map”



f. Go back to “On” and click “Satellite”

g. Check close-up for accuracy

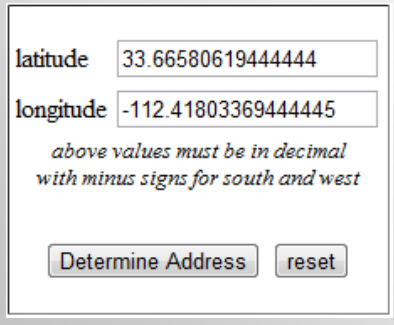
3. Convert Latitude and Longitude into decimal form

a. Plug latitude (33° 39’ 56.9023” N) and longitude (112° 25’ 4.9213” W) (example from above, but use your own latitude and longitude) into conversion to such as Steve Morse's tool.

b. Convert to decimal format.

4. Convert decimal from of Latitude and Longitude into address

a. Use a conversion tool such as Steve Morse's tool.



5. Extract location metadata from GPS-enabled photograph from camera, smartphone, Flickr, YouTube, or other Internet source that includes metadata.

a. Download digital copy of a photo onto laptop or desktop computer.

b. Use a tool to extract Exif location metadata, such as the Picture Information Extractor which can be downloaded at PIE

c. Notice the location information along with significant other metadata.