

[« Bankruptcy Filings and Civil Litigation - Judicial Estoppel in Action | Main | Preconstruction Service Liens: A New Chapter in Utah's Mechanics' Lien Law »](#)

Location-Based Electronic Discovery in Criminal and Civil Litigation - Part 2

by David K. Isom

This paper examines the impact of location technology upon civil and criminal legal processes in the United States, in two parts: Part 1 summarized the location-based digital technology that has recently become ubiquitous and readily accessible. This Part 2 explores the important legal and ethical issues that location-based electronic discovery (LBED) raises for civil and criminal judicial proceedings.

Part 2: Location-Based Law, Ethics and Privacy

Why Location Matters in Civil Litigation and Law Enforcement

Good trial lawyers know that the when and where are the foundation of selling or persuading or proving the what. There are, of course, cases in which the where is undisputed, and some where it is unimportant. But when the where is disputed and important, the very ability to prove a person's location at a key moment can exonerate or inculcate.

In one case, for example, my corporate client and I were able to prove that the client had overpaid for several large commercial construction projects because subcontractors had bribed the client's purchasing agent with prostitutes and cash. We discovered this by figuring out the location of each main player at important times, which led to photos, diaries, and confessions.

The essence of many criminal prosecutions is the location of the defendant at the critical moment. Location determines alibi. The where and when often tell the who, what, and why.

Location Privacy


The phrase "location privacy" is emerging because it is under attack. 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.

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 of these sources. That principle is that privacy analysis begins with gauging a person's "reasonable expectation of privacy" under the circumstances at issue.

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. See *United States v. Walker*, 771 F. Supp. 2d 803, 810-11 (W.D. Mich. 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...." *Id.* at 811.

Search

powered by 

About

This page contains a single entry from the blog posted on **November 7, 2011 9:10 AM.**

The previous post in this blog was [Bankruptcy Filings and Civil Litigation – Judicial Estoppel in Action.](#)

The next post in this blog is [Preconstruction Service Liens: A New Chapter in Utah's Mechanics' Lien Law.](#)

Many more can be found on the [main index page](#) or by looking through [the archives.](#)

[Subscribe to this feed](#)

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. In 2010 and 2011, many congressional hearings were held, and some proposed amendments introduced, but no amendments have emerged yet.

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's 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 ECPA, including the SCA, and other federal and state laws. See, e.g., *Shefts v. Petrakis*, 758 F. Supp. 2d 620, 629-30 (C.D. Ill. 2010).

Retention of Location Data

A recent Wall Street Journal article examined which of 101 popular iPhone and Android apps created and stored cellphone location information. See Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, Wall St. J., Dec. 17, 2010, <http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html>. The Journal reported that forty-seven of the 101 apps in the study collected and transmitted geolocation data. See *id.* Some app providers sold the user data they collected from cellphones to third parties, including geolocation information and device ID numbers, without the user's permission or knowledge. See *id.* In both civil and criminal litigation where location is in dispute, the important question is where the relevant electronically stored location information ("ESI") is stored and for how long.

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 minor child, through his father as next friend, sued the mayor of Detroit and others alleging inadequate investigation of the 2004 shooting death of his mother. See Flagg v. City of Detroit, 447 F. Supp. 2d 824, 825 (E.D. Mich. 2006). Some four years after the mother's death, the plaintiff discovered that SkyTel still had text messages about the shooting that he believed might be relevant to the lawsuit. See Flagg, 252 F.R.D. at 347-38. The court ordered city officials to provide PIN numbers, and ordered SkyTel to produce the text messages. See id. at 357.

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*, 244 P.3d 501 (Cal. 2011) (5-2 decision), Diaz was arrested and charged with selling a controlled substance. See id. at 503. Police grabbed Diaz's cellphone shortly after his arrest and used evidence from the cellphone to convict him. See id. at 502-03. Diaz claimed that the seizure and use of cellphone information violated his Fourth Amendment privilege against unreasonable searches and seizures. See id. at 503.

The California Supreme Court ruled 5-2 that prosecutors had a right to access Diaz's cellphone information on the ground that the phone, in Diaz's pocket when he was arrested, was in his immediate control. See id. at 505. Under United States Supreme Court precedent, the California court held that the phone was taken legally because it was taken "incident to a lawful arrest." See id. at 503-05. 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, 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. See id. at 513 (Werdegarr, J., dissenting in which Moreno, J., joined). The dissenting justices emphasized that "[n]ever before has it been possible to carry so much personal or business information in one's pocket or purse." See id. (Werdegarr, J., dissenting in which Moreno, J., joined).

LBED in Civil Litigation

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

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.

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 undiscoversable, 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, tablet, or other device, and any of the parties' 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 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.

Metadata and Production Format

Metadata is obscene. Five years ago, metadata seemed obscene in the nasty sense, i.e., off-colored, dangerous, lewd, or offensive. Now it is clear that metadata is merely obscene in the other sense. The etymology of “obscene” is “ob scaena” 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.

Subpoenas, Document Requests, and the Stored Communications Act

The SCA, which is under 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. See *Devine v. Kapasi*, 729 F. Supp. 2d 1024, 1026-28 (N.D. Ill. 2010) (mem.). Several courts have held that data held by an ESC are exempt from the reach of subpoenas in civil actions. In re *Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 611-612 (E.D. Va. 2008). 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 ECSs and RCSs that could not be subpoenaed directly by the non-customer opposing party under the SCA. See *Flagg v. City of Detroit*, 252 F.R.D. 346, 357-58 (E.D. Mich. 2008).

Ethics of LBED

Most of the ethical 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.

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 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. See *New York State Ethics Op. 749* (2001). 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.” See *Florida State Ethics Op. 06-02* (Sept. 15, 2006). The Florida opinion made it clear, however, that the ethical proscription did not apply to metadata embedded in electronic data produced in formal discovery. See *id.*

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. See *ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 06-442* (2006). 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. See ABA, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/ch The ABA maintains a webpage that collects these opinions. See *id.*

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. See *Philadelphia Bar Assoc., Prof’l Guidance Comm. Op. 2009-02*; *New York City Bar, Comm. on Prof’l Ethics, Formal Op. 2010-2*. 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. See *id.*

In 2010, the New York City Bar reached the opposite conclusion: “[W]e 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.” New York City Bar, Comm. on Prof’l Ethics, Formal Op. 2010-2. The New York City Bar emphasized, however, that only truthful information could be used in sending such a friend request. See *id.* 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. See *id.* & n.4.

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.

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. 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.

Posted by [BlogStaff](#) on November 7, 2011 9:10 AM | [Permalink](#)

The Utah State Bar presents this web site as a service to our members and to the public. Information presented in this site is NOT legal advice. Please review the [Terms of Use](#) for more policy, disclaimer & liability information - ©Utah State Bar email: info@utahbar.org