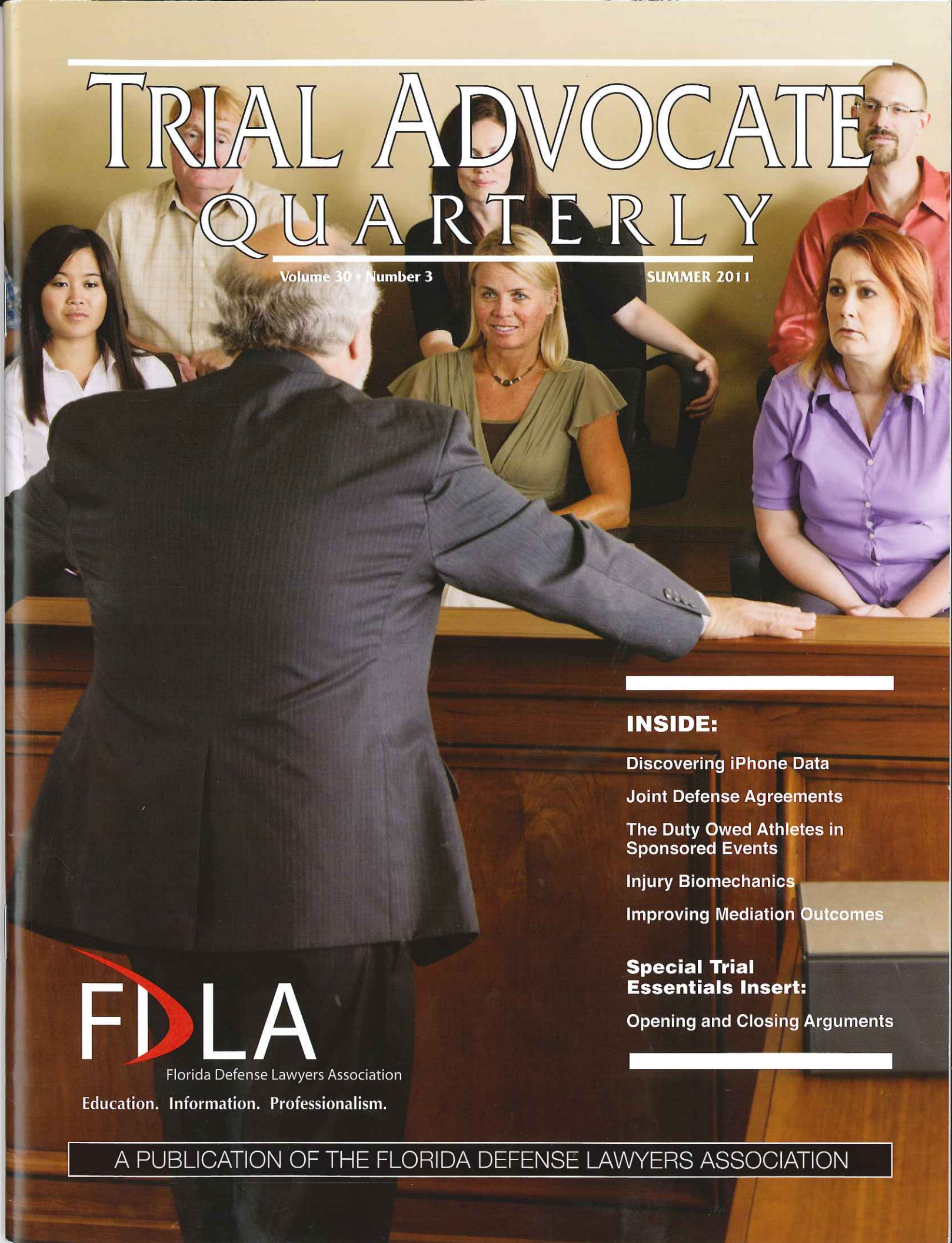

TRIAL ADVOCATE QUARTERLY

Volume 30 • Number 3 SUMMER 2011

INSIDE:

Discovering iPhone Data

Joint Defense Agreements

The Duty Owed Athletes in Sponsored Events

Injury Biomechanics

Improving Mediation Outcomes

Special Trial Essentials Insert:

Opening and Closing Arguments

FDLA

Florida Defense Lawyers Association

Education. Information. Professionalism.

A PUBLICATION OF THE FLORIDA DEFENSE LAWYERS ASSOCIATION

Using iPhone Location Data in Discovery

By Christopher Hopkins

The popularity of "smart phones" and the ever-expanding number of applications available to smart phone users depends, in part, on the collection and storage of user-specific data. This data can be obtained in discovery and used for some of the same reasons that a lawyer might use more traditional surveillance methods.

In late April 2011, the mainstream media was abuzz that the iPhone was tracking and recording users' every move. Politicians, privacy rights groups, and iPhone users responded with various emotions. Lawyers, however, likely had a different response: could this be used in discovery? If a witness or party to a lawsuit has an iPhone, and that person's whereabouts at a specific time and date since June 2010 are relevant to the case, there are practical methods and legal grounds to obtain their iPhone location data.

What is the potential benefit of tracking a party or witness? Likely some of the same reasons a defense lawyer might resort to (more expensive) surveillance. A personal injury plaintiff or workers' compensation claimant may argue that they can never leave the house or have a restricted ability to travel. An employee with a business-issued phone may claim that he was at the worksite at a certain date and time. You may want to prove a witness was at the stated location when an event happened. Or someone has an alibi and needs objective proof to support it — much like the Duke lacrosse player who used his cell phone records to prove he was not at the off-campus party at the time of the alleged assault.[1] Matrimonial lawyers, as well, may want to establish a spouse's whereabouts.

How is it that our smartphones started tracking us?[2] Blame it, at least in part, on the rise of the "app stores." Consumers want an optimized smartphone which interfaces with our surroundings and enhances our activities. To do that, apps need to collect and apply user-specific data which end up residing on our phone and computer. Around the advent of the App Store, Apple organized user data into structured libraries so that third party applications — such as Facebook, Yelp, Google Maps, and others — knew where to find personal and historical data inside each person's iPhone in order to customize the user's experience. By creating these fixed libraries, user data is easily available to app developers — as well as to forensic experts and lawyers. Millions of iPhones have been sold; studies suggest the average user downloads nearly 40 apps.[3] That amounts to a lot of (silently backed-up) customized data about the iPhone user. The residual data from these apps have drawn the attention of forensic computer analysts and, now, lawyers looking for discoverable information.[4]

The first step in discovering that information is to understand geolocation technology and the smartphone file directory. At issue are artifact files of timestamp and geolocation data which exist, unecrypted, on an iPhone and the computer with which it is synced. In short, the iPhone periodically records where you were and the time and date you were there.

The iPhone employs various sources of information to log its location. While a user travels, the iPhone detects location via GPS, cell towers, and Skyhook (a location service using WiFi), and creates a digital trail of bread crumbs. Note that this is not an exact location, but it is a close approximation recorded periodically during the day.

Next, to record the time and date

ABOUT THE AUTHOR...

CHRISTOPHER B. HOPKINS is a shareholder at Akerman Senterfitt. Mr. Hopkins developed two iPhone applications for Florida lawyers (ClawApp.com). He is the Chair of the Palm Beach County Bar Association Technology Committee as well as the host of InternetLawCommentary.com. He can be reached at Christopher.Hopkins@Akerman.com.

when the user was at a specific location, the iPhone accesses AT&T/Verizon's cellular system clock and timestamps the phone's location. That data is stored in a log file called "consolidated.db." When the user synchronizes the iPhone to a computer, the phone is backed up and some data is exchanged, including the consolidated.db file. Thus, the historical location data resides on both the iPhone and the computer hard drive.

The iPhone has two levels of data: System Data and User Data. The System Data is hidden in its own partition, which is not accessed by the standard white iPhone cable. Even app developers are barred from this area. Inside the User Data level, however, there are five accessible libraries, only one of which is encrypted (your passwords). To encourage app development, Apple fixed the structure of the User Data and intentionally made those directories accessible so that apps could personalize their functions. In short, experts, app developers, and savvy enthusiasts were handed a key to five libraries which hold nearly limitless iPhone user data.

The existence of consolidated.db has been known by forensic computer experts since 2010.[5] This became widespread news in Spring 2011, however, when two researchers publicly released an open source Mac application called iPhone Tracker which read the consolidated.db file and plotted the locations on a map.[6] Shortly thereafter, several Windows versions (*e.g.*, iPhoneTrackerWin and iPhoneLocationTracker) appeared on the Internet. In short, as easily as opening a PDF document, a non-expert could easily plot the past location of someone's iPhone.

To prove the simplicity of these steps, if you are an iPhone user, download a program called iPhone Backup Extractor.[7] After a quick search, it will locate the backup folder for your iPhone and provide the details about the device and the folder which retains the iPhone data.[8] See Exhibit A. Under "Available Data," you can extract the "Location data" (Exhibit A, bottom right) to be saved onto the desktop or a thumbdrive.

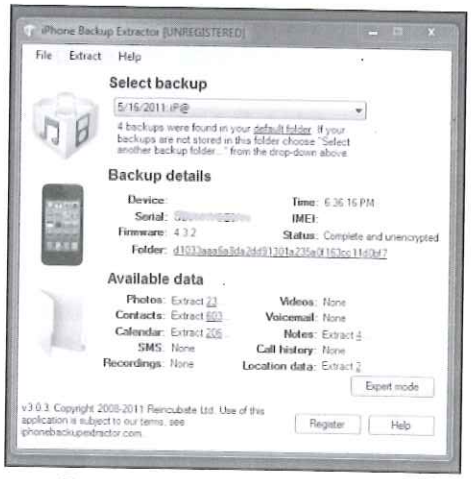

Exhibit A, Forensic Data on an iPhone

This information can then be plotted on Google Maps using iOSTracker.NET or other similar forensic applications. Download and run iPhoneTracker to see a "movie" of the iPhone's chronological travels on a map dating back to mid-2010. On the map, you can zoom to move precise locations. See Exhibit B1-B2, Selected location of author's iPhone on June 24, 2010.

According to Alex Levinson, author of *iOS Forensic Analysis*, the iPhone had been gathering location data even before June 2010. The so-called Core Location data (location and direction) has been collected and stored by the iPhone for some time; however, it was not until the June 2010 release of iOS 4 that the location data was moved to the easily-accessible consolidated.db log file. Prior to iOS 4, the location information was stored in a hidden file called h-cells.plist. Once iOS 4 was released, the data was moved to consolidated.db, which was neither hidden nor encrypted. It was only a matter of time before computer enthusiasts were able to obtain and manipulate the data.

So how does a lawyer obtain this information in discovery? First, be aware that, as of May 6, 2011, anyone who installed iOS 4.3.3 encrypted their location data (which was the key reason behind Apple's update). At least as of this writing, few forensic experts are publicly claiming that they can locate and unecrypt that data on an iPhone running iOS 4.3.3.

Second, if you have access to the iPhone and the computer with which it is synced, you may obtain the location data by running the iPhone Backup Extractor and then saving the file to disc or USB drive. Once on another computer, you can freely run the tracking and inspection software referenced above without risk of corrupting the original data.

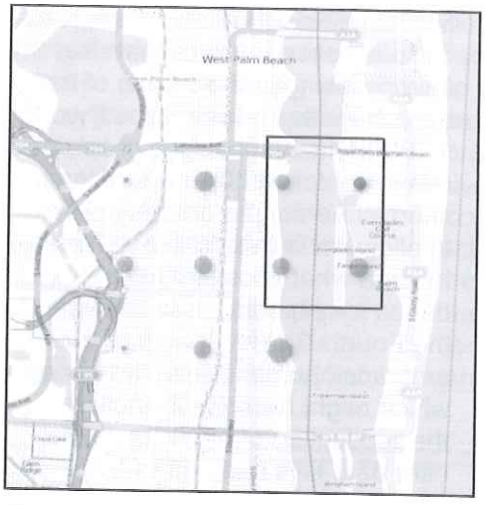

Exhibit B-1, Selected Locations of Author's iPhone on June 24, 2010

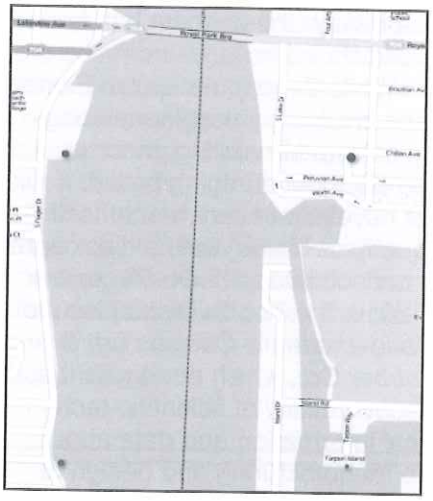

Exhibit B-2, Close-Up of Selected Locations of Author's iPhone on June 24, 2010

If you need to obtain the data via subpoena or discovery request, an image of the iPhone or hard drive should be obtained by an expert who will likely use some of

the applications mentioned in this article as well as forensic software such as Lantern or Oxygen (forensic expert Alex Levinson offers a remarkable case study on how a husband's "lost evening" was uncovered via iPhone forensics[9]). If you are on a limited discovery budget you might convince a court to have the computer's custodian run the Extractor program and produce the data file, but that may create some evidentiary and custody issues.

Thus we have confirmed the technology-side of the equation: the data exists and it can forensically be recovered. The second step is whether it is discoverable. E-discovery has been a hot, if not over-emphasized, issue, and broad discovery orders have been the subject of several appeals. That said, there is no known published case involving subpoenaing iPhone location data — likely due to the "newness" of the revelation — although the concept has been raised.[10]

If corporate trade secrets are not beyond the reach of discovery, likely the contents of a relevant, unencrypted iPhone file are within the scope of discovery.

While there is no known Florida case involving smartphone imaging or data harvesting, there is one case encouraging broad, if not novel, discovery which itself is equally as "fresh" as the disclosure of consolidated.db. On December 1, 2010, the Fourth District issued *Mario Alvarez v. Cooper Tire & Rubber Co.*, which dealt with the discoverability of scientific-technical information and data about the manufacturing and design of automobile tires (including information about prior cases and trade secrets). As the court described the issue, the defendant raised an affirmative defense and the plaintiff sought detailed discovery into the technical data which supported the defense.[11]

After a discussion of the breadth of discovery, the court noted that the "scope of discovery extends to anything not privileged, possibly relevant to the 'subject matter' of the claim or defense as being reasonably calculated to lead to admissible evidence."[12] Recognizing that even trade secrets could be discoverable, the court acknowledged that trial judges may invoke, "suitable safeguards as to disclosure and use of the information or data — both within and outside the litigation. But any need for such protection is not a valid basis to bar discovery outright to keep such information hidden."[13] If corporate trade secrets are not beyond the reach of discovery, likely the contents of a relevant, unencrypted iPhone file are within the scope of discovery.

The panel noted that the Second and Fifth Districts had restricted discovery of "substantially similar" prior incidents, and had decried them as "fishing expedition." The Fourth District disagreed: "it does not seem to us that discovery fishing in the waters of the subject matter is foreclosed by rule 1.280(b)(1). An enlarged scope of relevancy for discovery purposes seems to embrace a strong policy to allow parties to do some *fishing* to learn what possible trial evidence may be out there."[14] In short, the Fourth District appears to have embraced some discovery "fishing" which might reasonably include the production of highly technical user data files relevant to a specific case.

As to the production of iPhone data in discovery, the 2010 *Alvarez* decision seems to squarely support production of "what possible trial evidence may be out there." While there are certainly "suitable safeguards" for the production of imaged hard drives, which may contain privileged data and communications, the narrowed production of consolidated.db should be reasonably fashioned so as to permit disclosure in matters where the user's location is within the subject matter of discovery.

1 "Key Evidence Supports Alibi in Potential Rape Defense for One Indicted Duke Player," ABC News/Good Morning America, April 19, 2006. *See* http://abcn.ws/kXNgUD.

2 While this article focuses on Apple iPhone, this kind of data is also collected by competing smartphone devices. "Apple, Google Collect User Data," Wall Street Journal, April 22, 2011. *See* http://on.wsj.com/lfM9oO.

3 "The State of Mobile Apps" at http://bit.ly/jfEZmO (Nielsen June 2010 study found that the average iPhone user downloads 37 apps).

4 Several books on iOS forensics are available on Amazon.com including "iPhone and iOS Forensics," "iOS Forensic Analysis for iPhone, iPad, and iPod," and "iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets." Readers are cautioned that Apple's frequent update schedule — especially iOS 4.3.3 in May 2011 — makes some of this reading outdated. Non-technical readers are cautioned about the density of these texts.

5 "The iPhone Tracking Fiasco and What You Can Do About It," Engadget (April 21, 2011). *See* http://engt.co/lypZHg.

6 "Your iPhone and iPad are Tracking You, Researchers Say," Washington Post (April 20, 2011). *See* http://wapo.st/k9Y0m6.

7 iPhoneBackupExtractor.com.

8 As iPhone Backup Extractor shows, there is a wealth of information on an iPhone beyond simply tracking prior locations. As a matter of housekeeping, I delete old SMS/text and voicemail messages. For people who are not so digitally tidy, those would be readily recoverable using this simple software.

9 Alex Levinson et al., "Third Party Application Forensics on Apple Mobile Devices," 44th Hawaii International Conference on Systems Science, January 2011. *See* http://bit.ly/iZqjpm.

10 "Why You Should Care About the iPhone Location-Tracking Issue," CNN-Tech/WIRED, April 25, 2011. *See* http://bit.ly/msukm7 and even in the blogs, "Need to Know Where Someone Was? Subpoena Their iOS consolidated.db file," Anonlaw.com, April 20, 2011. *See* http://bit.ly/jbz2We.

11 *Mario A. Alvarez v. Cooper Tire & Rubber Co.*, __ So. 3d __, 2010 WL 4861514, *2 (Fla. 4th DCA Dec. 1, 2010).

12 *Id.* at *3.

13 *Id.*

14 *Id.* at *6-7.