MONTHLY LUNCHTIME SEMINAR SERIES

55TH Session:

THE HUNT FOR ESI: EVIDENCE HIDING IN PLAIN SIGHT

Judge Lynn M. Egan
Mr. Trent Walton, CCE, ACE

August 10, 2017

JUDGE LYNN M. EGAN

Judge Lynn M. Egan became a Cook County Circuit Court judge in 1995 and has served in the Law Division for over 21 years. She has presided over high volume motion calls, an Individual Commercial Calendar, an Individual General Calendar and bench and jury trials. She is currently the only Cook County judge assigned to a General Individual Calendar in the Law Division, which includes every type of case filed in the Division, specifically including personal injury actions such as medical & dental malpractice, product liability, infliction of emotional distress, defamation/slander, premises liability, construction & motor vehicle accidents, as well as commercial disputes such as breach of contract, fraud, conspiracy, breach of fiduciary duty, wrongful termination, employment discrimination and legal & accounting malpractice. She manages these cases from time of filing until final disposition, including all motion practice, case management, settlement conferences and trials. Additionally, Judge Egan is committed to assisting parties with the voluntary resolution of cases. As a result, hundreds of cases pending on other judges' calls in the Law & Chancery Divisions & the Municipal Districts are transferred to Judge Egan each year for settlement conferences and she has helped facilitate settlements totaling over 275 million dollars.

Judge Egan has also served as a member of several Illinois Supreme Court Committees, including the Executive Committee, Discovery Procedures Committee, Civil Justice Committee and Education Committee. She has also been a faculty member at dozens of judicial seminars throughout the state, including the annual New Judges' Seminar, regional conferences and the mandatory Education Conference. She has authored numerous articles on subjects such as discovery, requests to admit, restrictive covenants, Day-In-The-Life films, directed verdicts, jury selection & instructions, Dead Man's Act, Supreme Court Rule 213, expert witnesses, reconstruction testimony, court-ordered medical exams, attorney-client/work product privileges, sanctions, special interrogatories, examination of experts and damages. She also serves as a mentor for new judges and currently serves on the Illinois Courts Commission, a seven-member panel responsible for rendering final decisions on matters of judicial discipline.

Judge Egan has served on Bar Association committees and Boards of Directors and has been a frequent speaker at Bar Association seminars. She has taught law school classes and judged trial & appellate advocacy competitions. In 2012, she became a registered CLE provider through the Illinois MCLE Board and provides free CLE seminars for attorneys and judges every month. Since her monthly seminar series began in August 2012, Judge Egan has awarded over 13,000 hours of free CLE credit to Illinois attorneys.

Prior to joining the bench, Judge Egan was an equity partner at Hinshaw & Culbertson, where she focused her practice on medical negligence cases. In addition to trial work, she argued before the Illinois Supreme Court on a matter of first impression in the country in *Cisarik v. Palos Community Hospital*. Similarly, during her earlier career in the Cook County State's Attorney's Office, she worked in the criminal and juvenile divisions and argued before the Illinois Appellate and Supreme Courts on matters of first impression in Illinois.

TRENT WALTON, CCE, ACE

trentwalton@gmail.com, 720-878-3913

eDiscovery Expert and Forensic Computer Examiner

Summary

Trent is currently the National Director of Litigation Technology for U.S. Legal Support. With more than 15 years of experience in litigation support, Trent has been involved at an expert level in nearly all aspects of litigation discovery: computer forensics, eDiscovery, project management, programming and more. He has created two well-known legal software products that are currently being used by customers in the Am Law 100, Fortune 500 and U.S. government.

In his role at U.S. Legal Support, Trent advises law firms and corporations regarding projects ranging from comprehensive, case assessment, large-scale data preservation and internal investigations to customized technological solutions. He has a wealth of experience in executing projects involving data collection, processing, analyzing massive amounts of data, and assisting firms with electronic discovery legal strategy.

Areas of Strength

Computer Forensics
Data Preservation
Incident Response
Data Collection

Electronic Discovery
Information Governance
Early Case Assessment
Litigation Support

Software Development
Cyber Security
Network Defense

Representative Case Types

- Assisting parties in complicated eDiscovery matters related to evidence preservation, collection, early case assessment, processing, document review, production and trial presentation.
- Performing computer forensics analyses on computers, phones, tablets and cloud-based data.

Professional Experience

Trent is the National Director of Legal Technology at U.S. Legal Support. Prior to joining U.S. Legal Support, Trent served as President of both Electronic Legal, LLC, a computer forensics and electronic discovery case management firm, and Cumulus Data, Inc., a cloud-based provider of revolutionary remote forensics collection technology. He is a leading expert in complicated discovery matters - such as cloud computing, computer forensics, electronic data discovery, internal investigations and hosted document review - and has provided consulting services for U.S. and international law firms, corporations and service bureaus.

In his role at U.S. Legal Support, Trent advises corporations and law firms regarding projects ranging from comprehensive, large-scale data preservation and internal investigations to customized technological solutions. He has a wealth of experience in executing projects involving data collection, processing and analyzing massive amounts of data, and managing large attorney review teams.

Trent is a member of the Sedona Conference Working Group on Electronic Document Retention and Production (WG1) and has assisted in developing the Sedona Cloud Computing recommendations. He is a Certified Computer Forensic Examiner (CCE)® #684 from the International Society of Forensic Computer Examiners. He is also a Certified AccessData Examiner (ACE)®, with an additional specialized certification in Windows Forensics by AccessData. In addition, Trent has received certifications in database administration, training, FYI server administration and electronic data discovery administration from Lexis-Nexis, and consulted as the company's nationwide Concordance programming language trainer.

With a knowledge of 13 programming languages, Trent also has developed and written legal software including computer forensics analysis software, SAS cloud remote forensic data collection software and document review software. He created E.L. Native Review™ for Concordance, which is still used by law firms internationally and was awarded a rating of 4.8 out of 5 by TechnoLawyer. In October 2010, Wave Software (Orlando, FL) purchased Electronic Legal Software's related intellectual property. Cumulus Data, Inc., with its flagship product eCloudCollect™, was acquired August 2014 by ZApproved (Seattle, WA).

Prior to founding his first company (Electronic Legal, LLC) in 2006, Trent initiated the litigation support division of the Information Resource Department within Hogan & Hartson, LLP (now known as Hogan & Lovells, LLP) for the company's Denver, Boulder and Colorado Springs offices. He also implemented the litigation support department for Whitaker, Chalk, Swindle and Sawyer in Fort Worth, TX.

In 2004, Trent founded and served as President of the Colorado chapter of the Association of Litigation Support Managers which became the largest chapter in the United States. He has been recognized by states across the country to give accredited continuing legal education seminars on electronic discovery and forensics.

Trent has bachelor's degrees in Computer Information Sciences and Entrepreneurial Management from Texas Christian University.

Technologies

FORENSICS, LITIGATION SUPPORT & SECURITY:
Summation, Concordance, Relativity, InControl, CaseLogistix, Early Data Assessment, Law Pre-Discovery, Trial Director AccessData Forensic Toolkit, AccessData Password Recovery Toolkit, NetAnalysis, Paraben Device Seizure, Paraben (Forensic Replicator, P2 eXplorer, E-mail Examiner, Network E-mail Examiner, Text Searcher, Chat Examiner, Registry Analyzer), X-Ways Forensics, WinHex, Pinpoint Labs (OCCH, SafeCopy, MetaDiscover), RAID Reconstructor, Oxygen Forensic Suite, Nucleus Exchange & oST Recovery, Active@ Password Changer, GetData Mount Image Pro, Elcom Password Recovery, e-Cloud Collect, X1 Social Discovery, DataLifter, FileExtractor Pro, VMWare, Virtual Box

OPERATING SYSTEMS: Windows 2008, 7, 8, 10, 2003, Vista, XP, MacOS, Linux

FILE SYSTEMS: FAT(FAT12, FAT16, FAT3), NTFS

NETWORK SOFTWARE: IIS, Exchange, DNS, DFS, WINS, DHCP, SMT, FTP, cc:Mail, IPSwitch iMail, F-Response, Amazon Web Services (Various Cloud Infrastructures)

SMART DEVICES: Apple iPhone, iPad & Andriod Variants

DATABASES: Microsoft SQL Server, Sybase, SQLite, Microsoft Access

Expert Testimony

ASARCO LLC Chapter 11 Jointly Administered (In the United States Bankruptcy Court for Southern District of Texas, Corpus Christi Division, Case No. 05-21207)

Mr. Walton provided an affidavit regarding developing an alternative and more reasonable electronic data preservation and processing required of ASARCO. The affidavit resulted in the court granting Mr. Walton's approach bringing the estimated eDiscovery costs form an estimated $566,452.12 to $73,270.00.

MARK SIISMETS, vs. MP2 ENERGY LLC (American Arbitration Association, Case No. 01-16-0000-6712)

Mr. Walton provided an affidavit regarding claimant's burdensome request for document scope and application of search terms. The affidavit provided a detailed explanation of proper eDiscovery workflow along with a detailed assessment of data being requested. The affidavit resulted in the Respondent of being required to review 8,199 documents as opposed to an approximate 799,000.

DANIEL PERTILE, et al vs. GENERAL MOTORS, LLC et al. (In the United States District Court for the District of Colorado, Case No.1:15-cv-00518-NYW)

Mr. Walton provided an affidavit suggesting an appropriate ESI protocol for protecting native files subject to a protective order produced to other parties. Mr. Walton's suggested protocol was established allowing his client to receive native file productions.

FARMERS INSURANCE EXCHANGE, et al vs. KENNETH WEBSTER (In the Superior Court of the State of California County of San Diego, Case No. 37-2014-00019065-CU-BC-CTL)

Mr. Walton provided an affidavit in support of an application for an order to compel an additional deposition based on volume of documents received in a recent production and estimated time for review to appropriately prepare for deposition. Judge granted the application based on Mr. Walton's expert opinion.

KELLY EGAN v. TOWN OF FIRESTON, et al (In the United States District Court for the District of Colorado, Case No. 1:2008-cv-00121)

WILLIAMS vs. CHAMBERS (In the United States District Court for the District of Colorado)

Certifications and Licenses

- Certified Computer Forensic Examiner (CCE) #684
  - Issued by the International Society of Forensic Computer Examiners, it demonstrates an in-depth knowledge of file system architecture, collection techniques, analysis and submitting of expert reports.
- AccessData Certified Examiner (ACE), Windows Forensics Specialization
  - The ACE credential demonstrates your proficiency with the AccessData Forensic Toolkit technology.
  - The ACE Windows Specialization credential demonstrates your proficiency with analysis of the Windows operating system.

Other Certifications, Training, and Self-Study

- Certified Electronic Discovery Specialist
- Certified PreDiscovery Electronic Data Discovery User
- Certified Electronic Discovery Specialist
- Certified Concordance Database Administrator
- Certified Concordance Trainer
- Certified Concordance FYI Server Administrator
- Nation-Wide Concordance Programming Language Trainer

Professional Affiliations

- Sedona Conference Working Group on Electronic Document Retention and Production (WG1) – Member
  - Brainstorming Group on Information Governance
- International Society of Forensic Computer Examiners, Member
- President, Colorado Association of Litigation Support Managers (2004 - 2006)
- Board Member, Entrepreneurs Organization, Colorado Chapter (2010 – 2011)

Presentations, Publications, and Instructional Experience

- Approved by more than 15 State Bars to be a presenter of Mandatory Continuing Legal Education (MCLE) courses
- Presenter of over 200 approved MCLE events
- Publisher of computer forensic whitepapers and articles of interest

SECTION A

- ***The Hunt for ESI: Evidence Hiding in Plain Sight*, by Judge Lynn M. Egan, August 2017.**

"The Hunt for ESI: Evidence Hiding in Plain Sight"

by
Judge Lynn M. Egan
August 10, 2017

I. Hard to Find If You Don't Know What It Is

- **Supreme Court Rule 201(b)(4) – Electronically Stored Information.** *"ESI" shall include any writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations in any medium from which electronically stored information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form."*

NOTE: This rule defines "documents" quite broadly. Specifically, subparagraph (b)(1) was expanded to include "all retrievable information in computer storage." As noted in the rule's Committee Comments, "this amendment recognizes the increasing reliability on computer technology and thus obligates a party to produce" relevant materials. *Ill.S.Ct. R. 201, Committee Comments (West 2014).* Just as importantly, it requires a producing party to search its computer storage when responding to a production request. *Ill.S.Ct. R. 214, Committee Comments (West 2014).*

II. The ESI Universe is Vast & Data Can Be Found in Many Galaxies

- Examples of ESI include word processed documents, databases, spreadsheets, presentations, digital photographs, video/audio recordings, voicemail, e-mail messages & attachments, calendar entries, text & instant messages, blog & social media postings.
- ESI can be stored on computer hard drives (home & office desktops/laptops), network servers, thumb (USB) drives, CDs, DVDs, cell phones, smart appliances (phones/tablets), home security systems, fitness trackers, gaming consoles, children's digital learning toys, the Cloud, Amazon Alexa & social media websites.

III. Illinois Rules of Professional Conduct Are Implicated.

The provisions about competency demand your understanding of ESI, how to access it on behalf of your clients, how to advise them & how to protect the confidentiality of their records. As a result, it is essential that lawyers know the sources of ESI and how to preserve it.

- **Preamble**: (7) *"A lawyer should strive to attain the highest level of skill, to improve the law & the legal profession & to exemplify the legal profession's ideals of public service."*

- **Rule 1.1 – Competence**. Comment 8: *"A lawyer should keep abreast of changes in the law & its practice, including the benefits & risks associated with relevant technology..."*
- **Rule 1.6 – Confidentiality of Information**. (e): *"A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."* Comment 18: Reasonableness is judged by: sensitivity of the information, likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards & the extent to which safeguards adversely affect the lawyer's ability to represent clients (e.g., software that is excessively difficult to use.). Obviously, this can be implicated if the lawyer's firm uses Cloud computing, rather than storing ESI in-house. *See also, In re Peshek, M.R. 23794, 2009 PR 00089 (Ill. May 18, 2010)(lawyer suspended for violating Rule 1.6 by writing a blog that contained information that made it possible to identify clients.).*
- **Rule 1.15 – Safekeeping Property.** Must be maintained for seven years after termination of representation. Includes records *"maintained by electronic, photographic, or other media provided that printed copies can be produced, and the records are easily accessible to the lawyer."*
- **Rule 3.4 – Fairness to Opposing Party & Counsel.** *"A lawyer shall not: (a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act."*

IV. What Evidence Is Out There?

While most practitioners understand that email systems and word processing documents contain potentially usable trial evidence, the electronic devices we use every day actually contain significant information that most attorneys never request. For instance, database-tracking software can yield important information. Electronic medical records create audit trails that reveal when and where a medical record was accessed and what actions were taken at the time of access. Similarly, text messages, smart phones and health apps all generate potentially useful information, including geo-location history and call logs. Needless to say, failure to understand this capability can result in devastating consequences for a client, especially if it appears the data was altered after the occurrence in question.

Although it is well known that voice-mail messages and social media platforms are additional sources of potential evidence, attorneys infrequently request them during the discovery phase of litigation. This is a dangerous oversight as it certainly represents a missed opportunity given the fact that many photos posted on such sites are time stamped. More ominously, such an oversight may even represent a violation of Rule 1.1. Thus, lawyers are well advised to start thinking about these sources of evidence at the time suit is filed, and sometimes even before suit is filed. Thus, a search of social media platforms such as Facebook, Twitter, Instagram, LinkedIn, Snapchat and

YouTube is an easy, yet effective, way to fulfill your obligations to your client while at the same time compile useful evidence.

V. Discoverability – Know How To Ask

Due to the massive storage capability of most electronic devices, the days of asking for "any & all" relevant documents are over. Therefore, it is essential that lawyers understand the permissible scope of ESI discovery and the appropriate way to request it, especially because there is currently only a single reported Illinois decision concerning the discoverability of ESI, *Carlson v. Jerousek, 2016 IL App (2d) 151248.* Importantly, in order to understand and fully appreciate the holding in *Carlson*, attorneys must understand the 2014 amendments to the discovery rules as they relate to ESI.

- **Supreme Court Rule 201(c)(3). Proportionality.** The 2014 addition of a proportionality rule is included under the category of "prevention of abuse" and is often the dispositive consideration with ESI requests. The court must determine whether the likely burden or expense of the proposed ESI discovery outweighs the likely benefit, taking into account the amount in controversy, resources of the parties, importance of the issues to the litigation & in resolving the issues *Ill.S.Ct. R. 201(c)(3)(West 2014).*

NOTE: The Committee Comments to this portion of the rule include the following list of ESI categories that are typically considered nondiscoverable:

- Deleted, "slack," "fragmented" or unallocated data on hard drives;
- Random access memory ("RAM") or other ephemeral data;
- On-line access data;
- Data in metadata fields that are frequently updated automatically;
- Backup data that is substantially duplicative of data accessible elsewhere;
- Legacy data;
- Information capable of retrieval absent substantial extra programming or transforming it into another form before search & retrieval;
- Other forms of ESI whose preservation/production requires extraordinary affirmative measures. *Ill.S.Ct. R. 201(c)(3), Committee Comments (West 2014).*

Significantly, the *Carlson* court declared these categories "presumptively nondiscoverable." *Id. at ¶ 49.* As a result, any party requesting such information bears the burden "to justify the making of an exception." *Id.* In an effort to provide guidance in this regard, the appellate court cited with approval the following factors previously used by the Colorado Supreme Court: 1) a compelling need for the information; 2) the information is not available from other sources; and 3) the requesting party is using the least intrusive means to obtain the information. *Id.*[1]

[1] *Although the Appellate Court cited these factors with approval, it declined to formally adopt the analysis used in Colorado, noting "We think that this argument is better directed to our supreme court." Id.*

- **Supreme Court Rule 214. Discovery of Documents, Objects & Tangible Things – Inspection of Real Estate.** Supreme Court Rule 214 was also amended to specifically require a party's production of electronically stored information ("ESI") as defined by Supreme Court Rule 201(b)(4). Additionally, the rule was further revised so as to require the producing party to organize responsive documents "in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms." *Ill.S.Ct. R. 214(b)(West 2014).*

CAUTION: Failure to organize requested documents consistent with the directive of Rule 214(b), or mixing nonresponsive documents with the requested documents, 'constitutes a discovery abuse subject to sanctions under Rule 219." *Ill.S.Ct. R. 213, Committee Comments (West 2014).*

- **Relevance Trumps Privacy.** Because parties are now requesting social media content, more privacy objections are being raised. However, relevance is the touchstone concept, not privacy. Although the discovery rules "are not blind to...privacy interests" (*Carlson v. Jerousek, 2016 IL App (2d) 151248, ¶ 31),* not all "invasions" of privacy are forbidden. Instead, the Illinois constitution only forbids *unreasonable* invasions of privacy. *Id. at 35.* As a result, a user's designation of private content on an Internet site does not shield it from discovery or make a request for access unreasonable, because there is no justifiable expectation of privacy in such a setting. In this context, "reasonableness is a function of relevance." *Kunkel v. Walton, 179 Ill.2d 519, 538 (1997). Accord, Carlson, supra at ¶ 37.* Therefore, parties requesting an opponent's social media information need to make a threshold showing of relevance, which means a showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence. *Id.* While this is a liberal standard, fishing expeditions are not allowed. Instead, practitioners need to craft specific, and technologically sound, requests for information that are consistent with Illinois' amended rules of discovery. Even though ESI makes vast amounts of data readily available, the rules "do not permit the requesting party to [aimlessly] rummage through...files for helpful information." *Id. at ¶ 29.*

- **Guidance From the Appellate Court.** The absence of case law regarding Illinois' proportionality rule changed in December 2016, when the Second District decided *Carlson v. Jerousek, 2016 IL App (2d) 151248.* The case involved a plaintiff injured in a motor vehicle accident who claimed personal injuries, including cognitive disabilities and loss of a normal life. As a result, defendants propounded discovery requests for the following information:
  - Name, web address & user name for all blogs, online forums & social networking websites to which plaintiff belonged since the accident;
  - Internet/email, telephone & cell phone providers;
  - Internet/email passwords & all login information;
  - All ESI relating to the issues in the lawsuit;

- Identification of any destroyed or deleted documents responsive to the requests.

Because plaintiff worked as a senior computer analyst for Baxter Healthcare, defendants also requested the opportunity to inspect any computers or electronic devices he used, specifically including his work computer, in order to assess his claims of cognitive impairment. Additionally, due to suspicion that plaintiff may have researched symptoms of brain injury on the Internet, defendants requested the opportunity to review his history of Internet searches since the accident, "time stamps" for work-related tasks and metadata. Defendants even requested information about the extent of plaintiff's computer gaming and game scores

The trial court eventually ordered plaintiff to submit numerous computers, including a work computer owned by his employer, for forensic imaging, which "would make a mirror copy ...of the entire contents of all of the hard drives" of plaintiff's computers. Defendants proposed to then have their expert search all hard drives, catalogue the results and prepare an executive summary of the findings.

Not surprisingly, the Appellate Court reversed, finding that the trial court abused its discretion because it failed to conduct the balancing test required by the proportionality rule. Carlson, *supra at ¶ 69.* Specifically, the Appellate Court noted that Illinois rules contain "no provision allowing the requesting party to conduct its own search of the responding party's files – regardless of whether those files are physical or electronic." *Id. at 53.* As a result, the order for forensic imaging of plaintiff's computers was without legal support. Nonetheless, the Court noted that "it is possible that such an inversion of traditional discovery protocol might be appropriate in rare circumstances," such as cases where the computer itself is directly involved in the litigation or where there has been a significant history of "demonstrated noncompliance." *Id. at ¶ 55-56.*

As for the scope of the discovery requests, the Appellate Court also criticized the defendants' lack of specificity.

VI. Admissibility – Make Sure You Can Use What You Find

As a threshold matter, lawyers must remain cognizant of the difference between computer-generated and computer-stored evidence because they have different foundational requirements in order to be admissible. "Records directly generated by a computer are admissible as representing the tangible result of the computer's internal operations. In contrast, printouts of computer-stored records constitute statements placed into the computer by out-of-court declarants and cannot be tested by cross-examination and, therefore, are inadmissible absent an exception to the hearsay rule." Anderson v. Alberto-Culver USA, Inc., *337 Ill.App.3d 643, 667 (1st Dist., 2003).*

Examples of **computer-generated evidence** include cell phone records, GPS receiver records, data recorder readings (black boxes), flight recorder data, and billing data generated instantaneously by a computer. *Aliano v. Sears, Roebuck & Co., 2015 IL App (1st) 143367, ¶ 31.* Because such records are not dependent on the observations or reporting of a human declarant, the evidentiary foundation only requires proof that the recording device was accurate and operating properly when the evidence was created. *Bachman v. General Motors Corp., 332 Ill.App.3d 760, 789 (4th Dist., 2002).*

Admission of **computer-stored evidence** can occur pursuant to the business records exception to the hearsay rule if the following foundational information is elicited: 1) the electronic computing equipment is recognized as standard; 2) the input is entered in the regular course of business reasonably close in time to the happening of the event recorded; and 3) the foundational testimony establishes that the source of the information, method and time of preparation indicate its trustworthiness and justifies its admission. *Aliano, supra.* However, if the computer-stored evidence was produced by human input obtained from original documents, the originals must be made available to the opposing party and the proponent of the documents must be able to provide testimony about the facts contained within them from a competent witness who has seen the originals. *Id.* NOTE: If the originals have been destroyed by the party offering the computer-stored version, the latter will be deemed inadmissible unless the proponent can show that the destruction was accidental or done in good faith and without intent to prevent their use at trial. *Id.*

Lawyers must also be conversant with the relevant Illinois Rules of Evidence, which provide as follows:

- **Ill. R. Evid. 901. Requirement of Authentication or Identification**

  b) *General Provision.* The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

- **Ill. R. Evid. 803. Hearsay Exceptions; Availability of Declarant Immaterial**

  (6) *Records of Regularly Conducted Activity.* A memorandum, report, record, or data compilation, in any form, or acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness, but not including criminal cases medical records. The term 'business' as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

- **Silent Witness Rule**

  In the context of ESI, this rule is applicable where automatic devices such as cameras or surveillance systems are involved. *See, People v. Taylor, 2011 IL 110067, ¶ 32.* Pursuant to this rule, "a witness need not testify to the accuracy of the image depicted in the photographic or videotape evidence if the accuracy of the process that produced the evidence is established with an adequate foundation." *Id.*

  The Illinois Supreme Court approved the following "nonexclusive" factors when determining whether an adequate foundation has been established for evidence captured by automatic cameras or surveillance systems that produce videotapes, CDs or DVDs:

  1. The device's capability for recording & general reliability;
  2. Competency of the operator;
  3. Proper operation of the device;
  4. Showing the manner in which the recording was preserved (chain of custody);
  5. Identification of the persons, locale, or objects depicted; and
  6. An explanation of any copying or duplication process. *Id.*

  Notably, the Illinois Supreme Court declared in *Taylor, supra,* that requiring proof that no alterations, deletions or changes have been made when an original DVR recording is copied to videotape is "overly restrictive" and that "a strict chain of custody is not necessary" if other factors demonstrate the recording's authenticity. *Id. at 41-43.* Such gaps merely go to the weight of the evidence, not admissibility. *Id. at 41.*

VII. Illinois Legislative Developments

On June 27, 2017, the Illinois legislature passed the Geolocation Privacy Protection Act (HB 3449). It now awaits Governor Rauner's signature. The original intent of the Act was to protect data privacy by limiting the collection and disclosure of location data from mobile devices by private entities. In final form, the Act requires notification to consumers that their geolocation data is being collected and used. Only a state's attorney or the attorney general may sue violators pursuant to the existing Consumer Fraud and Deceptive Business Practices Act. Under the Act, geolocation information is defined as information generated by or derived from the operation of a mobile device (smart phone, tablet, or laptop) that is sufficient to determine or infer the precise location of the device. Significantly, it does not include the actual contents of any communication. Several exceptions apply.

The Illinois legislature also considered SB 1502, the Right to Know Act, which provides that the operator of a commercial website or online service that collects personally identifiable information about customers who use or visit its site through the Internet must notify them of its information sharing practices and provide the means by which

(email address or toll-free number) to enable customers to request the specific information shared. The Act also provides a private cause of action to customers whose rights are violated under the Act. On May 4, 2017, the Act received its third reading in the Senate and was sent to the House. Although it received its second reading in the House, it was re-referred to the Rules Committee on July 6, 2017.

SECTION B

- *ESI Client Questionnaire*, by Mr. Trent Walton.
- *Sample Preservation Letter to Client*, by Mr. Trent Walton.
- *Sample Stipulation & Order for Social Media Collection and Production*, by Mr. Trent Walton.
- *Sample Expert Affidavit*, by Mr. Trent Walton.
- *"A Whole New World Without The Need For A Genie: Utilizing Social Media Information in Litigation,"* by Mr. Gregory Perez (reprinted with permission).

ELECTRONICALLY STORED INFORMATION ("ESI")
CLIENT QUESTIONNAIRE

	Questions	Client's Answers
A.	**Email System(s)**	
	What e-mail application does client employees currently use (Outlook, Groupwise, Eudora, Netscape, etc.)?	
	Are emails hosted by a provider or a server maintained by client? • If hosted by provider please provide name? • If maintained by client, which email server program is used? (e.g. Microsoft Exchange 2012)	
	Where are the servers located? (Onsite or Offsite)	
	Does the e-mail system have an automatic deletion function? • If so, please provide additional information how it is setup.	
	Where are archived e-mails stored? (e.g. Personal Folders for users are stored on their computer within a PST)	
	Does the client have a documented email backup policy? • If so, how long has it been in place?	
B.	**Word Processing Documents / Spreadsheets / Presentations / Etc. ("E-docs")**	
	What software applications do employees relevant to this lawsuit use? (e.g., Microsoft Office, AutoCad?)	
	Where do employees store e-does? (e.g., network servers, personal drive, shared drive, hard drive, portable media?)	
	Where is/are the named server(s) have relevant data stored? • List server name and type of data that is stored.	
	How is it that E-does are backed up? • How often is this/these server(s) backed up? • Where is the backup medium stored?	

	• Can the backup medium be restored solely for certain custodians? • How long are backups kept? • Is this practice documented in a policy?	
C.	**Database Systems**	
	Does client have document management or project tracking software in place? • If so, what are the names of each software? ◦ When was each one put into place?	
	What software does the client use to manage finances? • If so, what is the name of the software? ◦ When was it put into place?	
D.	**Legacy Systems**	
	Has the client used other applications or back-up systems in the past (i.e. legacy systems)?	
	If there was another back-up system in use and there is still information relevant to those documents, the same questions above need to be answered for the legacy system(s).	
E.	**Text Messages**	
	Does the client use text messaging? • If yes, what device and software application does the client use?	
	Are instant messages electronically stored? • If yes, where? • For how long?	
	Are there backups of instant messages? • If yes, are these full backups or partial backups?	
F.	**Voice-Mail Messages**	
	What voice-mail system does the client use?	
	Can an employee save voice-mail messages in this system? • If yes, where are those saved voice-mail messages stored?	
	Does the voice-mail system create files for each	

	voice-mail message? (e.g., .wav files)	
G.	**Other Sources of Information / Remote Information**	
	Do employees access the client's e-does or e-mails from home computers or other non-company computers? • If yes, is such a practice documented in a policy?	
	Do employees store information in portable devices, like CDs, DVDs or USB (flash) drives?	
H.	**Forensic Analysis**	
	Is there a concern that some relevant ESI may have been intentionally deleted?	

SAMPLE PRESERVATION LETTER TO CLIENT WITH ESI QUESTIONNAIRE

[DATE] , 201_

[CLIENT. ADDRESS]

Re: *Attorney Client Communication Privileged and Confidential*
[CAPTION OF LAWSUIT OR INVESTIGATION]

Dear [NAME OF CLIENT]:

In light of the [potential. pending] litigation in the [described matter]. we are sending you this letter to remind you that you must preserve all information that could reasonably be perceived as relevant to the dispute. You must preserve the relevant information regardless of whether it is a paper document or stored in electronic format.

You are only required to keep information relevant to this dispute and created between [Relevant Time Period]. We should discuss the categories of documents relevant to this dispute and the employees who are likely to have such documents.

In our experience. clients most often encounter difficulties in preserving electronic information. such as emails. text messages. word processing documents. spreadsheets. databases. electronic calendars. telephone logs. voice- mails. back-up tapes. and other back-up media. In most cases. electronic information will form the bulk of the information you have relevant to a dispute. Not surprisingly then. electronic information will also cause the greatest problems for you during the exchange of discovery.

An important step we recommend you take to help avoid these problems is to contact the individuals responsible for your internal information technology. You should coordinate with them to immediately suspend deletion, overwriting and any other possible destruction of electronic information, in particular any sort of back-up systems. You should also consult with them to determine where relevant information is stored. how much information might exist and how to preserve it. For example. you should immediately determine the back-up systems you used during the relevant time period to this dispute and the feasibility of restoring the information contained in those systems.

We advise you circulate the attached litigation hold to all your employees likely to have relevant information. We also suggest you schedule regular circulations of the litigation hold and develop a system for ensuring that its recipients are complying with it.

Attached to this letter is a list of questions that will need to be filled out for our records.

The consequences for failing to abide by electronic preservation policies are severe. Hopefully. by taking these steps. we can reduce the risks presented by failing to preserve documents relevant to this matter.

Please contact me so we can discuss these issues.

Sincerely,
[ATTORNEY]

USLEGAL SUPPORT

SAMPLE STIPULATION AND ORDER FOR COLLECTION AND PRODUCTION SOCIAL MEDIA

Plaintiff ---------- ("PLAINTIFF") and Defendant (the "DEFENDANT") hereby stipulate and agree that the following terms will govern the discovery of electronically stored information in connection with the DEFENDANT's ____ set of Requests for Production of Documents served in the above-captioned action.

I. DEFINITIONS

A. "Electronically stored information" or "ESI," as used herein, means and refers to electronically stored information, including potentially relevant information stored electronically, magnetically, optically or in other computer-readable format.

B. "Native file" means and refers to the original format of a type of ESI in which such information was embodied at the time it was created by its corresponding software application.

C. "Metadata" means and refers to:

1. information embedded in a native file that is not ordinarily viewable or printable from the application that generated, edited, or modified such native file; and

2. information generated automatically by the operation of a computer or other information technology system when a native file is created, modified, transmitted, deleted or otherwise manipulated by a user of such system.

D. "Documents" includes all data stored in a Social Media account electronic form.

II. MEET AND CONFER EFFORTS

SAMPLE STIPULATION AND ORDER FOR COLLECTION AND PRODUCTION SOCIAL MEDIA

<Till in Here>

III. SEARCH PROCESS

A. Scope of ESI.

PLAINTIFF will provide the DEFENDANT's Vendor with access to PLAINTIFF Social Media account by supplying the username and password for each account. All Social Media data available through the API will be collected by a forensic expert using a qualified forensic software tool.

B. Key Custodians.

The parties agree that the following is an initial list of key custodians for whom Social Media accounts will be targeted to identify ESI containing potentially responsive Documents:

1. <Custodian Name>;

The parties will meet and confer as to subsequent lists of additional custodians, if any

C. Collection Process and Scope.

The parties and Vendor will cooperate in arranging a time for Vendor to access PLAINTIFF Social media accounts, which will be scheduled to occur within 10 days of the execution of this Stipulation. At the time agreed upon by the parties, the Vendor will collect all available data from the accounts, ("Recovered Documents"). Defendants will bear the cost of this forensic collection. Upon completion of the forensic collection process of PLAINTIFF Social Media accounts the Vendor will format the ESI to a format

that can be more easily reviewed and tracked by all parties.

D. **Privilege and Confidentiality Review and Time Period.**

1. **Procedure**: Following the completion of formatting of PLAINTIFF collected ESI, the Vendor will assign unique document identification numbers ("DocIDs") to each Recovered Document (*e.g.*, each message string, wall post, photo, etc.) and native file. The Vendor also will extract Metadata and full text for each Document and prepare a load file containing DocIDs, Metadata, full text, and native files in a platform of PLAINTIFF choice to review the Recovered Documents for privilege and/or confidentiality. The load file will be hosted on a document management platform maintained by the Vendor to which PLAINTIFF will have immediate and exclusive access for 20 days. PLAINTIFF will be responsible for paying any fees and/or costs to the Vendor relating to PLAINTIFF review of the Recovered Documents for privilege and/or confidentiality.

Subject only to any extensions agreed upon by the parties, PLAINTIFF will have 20 days from the date the Vendor first gives PLAINTIFF access to the Recovered Documents to provide the Vendor a list of DocIDs of the Documents that PLAINTIFF contend are subject to the attorney-client privilege ("Withheld Document(s)"). PLAINTIFF will also have 20 days from the date they are first given access to the Recovered Documents to provide the DEFENDANT a detailed log identifying the Withheld Documents, whether completely withheld or redacted for privilege. The log will include DocIDs, including DocIDs for any and all attachments, if any, the legal basis

for withholding the Withheld Document, as well as agreed upon Metadata fields for each Withheld Document, for example: DateCreated, CreatedBy, etc. Any challenges to the production and/or the privilege log will be subject to meet and confer requirements between the parties' consistent with the STATE Code of Civil Procedure.

At the expiration of PLAINTIFF 20-day review period, or any extension agreed to by the parties, the Vendor will prepare a load file of the Recovered Documents, excluding the Withheld Documents or relevant portions thereof, for the DEFENDANT containing DocIDs, Metadata, full text, and native files of the Recovered Documents in a platform of the DEFENDANT's choice as well as the Metadata only of the Documents withheld for privilege. If PLAINTIFF do not provide the Vendor with a list identifying the Withheld Documents by the 20th day after receiving access to the Recovered Documents or without an agreement to extend the review deadline, then the Vendor may immediately provide the DEFENDANT access to the Recovered Documents without redaction and/or modification and without further notice.

While PLAINTIFF are performing their privilege review, the Vendor will be directed not to discuss any of the Recovered Documents with the DEFENDANT or its attorneys. In addition, the Vendor will not disclose the nature of the Withheld Documents identified by PLAINTIFF to the DEFENDANT, its attorneys, or anyone else, and will not be made to testify as to the content or nature of any Withheld Documents unless agreed upon the by parties or ordered to do so by the Court.

2. **Confidentiality Agreement**: The parties recognize that the

SAMPLE STIPULATION AND ORDER FOR COLLECTION AND PRODUCTION SOCIAL MEDIA

Recovered Documents may include business records and other material claimed by PLAINTIFF to contain trade secret, confidential, or proprietary information that should not be disclosed, except in a highly restricted manner. The parties further recognize that PLAINTIFF are engaged in proprietary activities which could be jeopardized if non-public financial data, information technology data, business strategies, product or operational information, or other highly sensitive confidential information or documents were disclosed publicly.

(a) Definition: The parties agree that, for the purposes of the review of the Recovered Documents, "Confidential" means any information which belongs to PLAINTIFF, who believe in good faith that the disclosure of such information would create a substantial risk of serious financial or other injury as a result of the disclosure of proprietary information that cannot be avoided by less restrictive means.

(b) Designation: PLAINTIFF must identify only those Documents that are Confidential as described above in section II.D.2.a ("Confidential Document") and provide the Vendor with a list of these Confidential Documents by DocIDs. The Vendor will then affix the legend "Confidential" on each page of any Confidential Document containing such designated Confidential material. The inadvertent failure of PLAINTIFF to identify a Document as "Confidential" shall be without prejudice to any claim that such Document is "Confidential" and PLAINTIFF shall not be held to have waived any rights by such inadvertent production.

In the event that the DEFENDANT objects to a "Confidential" designation, it

shall advise counsel for the PLAINTIFF, in writing, of such objections, the specific Document identified by DocIDs, and the reasons for such objections. Counsel for PLAINTIFF shall have 15 days from receipt of the DEFENDANT's objections to either (a) agree in writing to de-designate the Confidential Document(s) or (b) file a motion with the Court seeking to uphold any or all designations of the Confidential Documents. Pending a resolution of this motion by the Court, all existing designations on the Confidential Documents shall remain in place. PLAINTIFF shall have the burden on any motion of establishing the applicability of their "Confidential" designation. In the event that the designation objections are not timely addressed by PLAINTIFF, then such Confidential Documents shall be de-designated.

In addition, if PLAINTIFF use Confidential Documents in a non-Confidential manner, then the "Confidential" designation no longer applies.

(c) Treatment of Confidential Documents: Access to and/or disclosure of Confidential Documents shall be permitted only to the following persons:

(i) Attorneys of record in the Action and their affiliated attorneys, paralegals, and clerical and secretarial staff employed by such attorneys who are actively involved in the Action;

(ii) In-house counsel to the Parties and the paralegal, and clerical and secretarial staff employed by such counsel;

(iii) Those officers, directors, partners, members, employees and agents of the Parties that counsel for such Parties deems necessary to aid

counsel in the prosecution and defense of this Action; provided, however, that prior to the disclosure of Confidential Documents to any such officer, director, partner, member, employee or agent, counsel for the Party making the disclosure shall deliver a copy of this Stipulation and Order to such person and shall explain that such person is bound to follow the terms of such Order;

(iv) Court reporters in this Action (whether at depositions, hearings, or any other proceeding);

(v) Any deposition, trial or hearing witness in the Action who previously has had access to the Confidential Documents, or who is currently or was previously an officer, director, partner, member, employee or agent of an entity that has had access to the Confidential Documents;

(vi) Any deposition or non-trial hearing witness in the Action who previously did not have access to the Confidential Documents; provided, however, that each such witness given access to Confidential Documents shall be advised that such Documents are being disclosed pursuant to, and are subject to, the terms of this Stipulation and Order and that they may not be disclosed other than pursuant to its terms;

(vii) Mock jury participants, provided, however, that prior to being given access to Confidential Documents each mock jury participant shall be advised that such Documents are being disclosed pursuant to, and are subject to, the terms of this Stipulation and Order and that they may not be disclosed other than pursuant to its terms; and

(viii) Outside experts or expert consultants consulted by the Parties or their counsel in connection with the Action, whether or not retained to testify at any oral hearing; provided, however, that prior to the disclosure of Confidential Documents to any such expert or expert consultant, counsel for the Party making the disclosure shall deliver a copy of this Stipulation and Order to such person, shall explain its terms to such person, and shall secure any such expert or expert consultant's agreement to be bound by the terms of this Stipulation and Order.

Confidential Documents shall be used by the persons receiving them only for the purposes of preparing for, conducting, participating in the conduct of, and/or prosecuting and/or defending the Action, and not for any business or other purpose whatsoever.

If the DEFENDANT receives a subpoena or other process ("Subpoena") from any other person or entity demanding production of Confidential Documents, the DEFENDANT shall promptly give notice of the same by electronic mail transmission, followed by either express mail or overnight delivery to counsel for PLAINTIFF, and shall furnish counsel with a copy of the Subpoena. PLAINTIFF may then, in their sole discretion and at their own cost, move to quash or limit the Subpoena, otherwise oppose production of the Confidential Documents, and/or seek to obtain confidential treatment of such Confidential Documents from the subpoenaing person or entity in any manner available under law. The DEFENDANT may not produce any Confidential Documents pursuant to the Subpoena prior to the date specified for production on the Subpoena.

Where any Confidential Documents are included in any motion or other

proceeding, including discovery motions or proceedings, the Parties shall follow STATE Rules of Court, rules [xxxxx].

The Parties agree that the Confidentiality provision of this Stipulation and Order shall continue to be binding after the conclusion of this Action and all subsequent proceedings arising from this Action. To the extent permitted by law, the Court shall retain jurisdiction to enforce, modify, or reconsider the Confidentiality provision of this Stipulation, even after the Action is terminated.

Inadvertently Produced Materials. In recognition of the timeframe of PLAINTIFF review and potential scope of production, it is possible that some privileged documents may be produced inadvertently. The parties agree that inadvertent production of privileged information or Documents shall not be deemed a waiver in whole or in part of PLAINTIFF claim of privilege. PLAINTIFF shall be entitled to "claw back" any such privileged Documents or information inadvertently produced as part of the Recovered Documents. If the DEFENDANT reasonably believes it received potentially privileged documents, it will provide PLAINTIFF prompt notice of the inadvertent production and destroy all copies of the privileged information or documents, including the electronic copy.

AMERICAN ARBITRATION ASSOCIATION

CASE NO. ---------

[CLAIMANT],

Claimant,

v.

[RESPONDENT]

Respondent.

AFFIDAVIT OF TRENT WALTON

STATE OF COLORADO

CITY AND COUNTY OF DENVER

TRENT WALTON, being duly sworn, deposes and states as follows:

1. I am over the age of 18, competent to provide this affidavit in all respects and the statements contained herein are based upon my personal knowledge. The contents of this affidavit are true and accurate to the best of my knowledge.

2. I am the National Director of Legal Technology at U.S. Legal Support, a litigation support company that provides litigation services to major insurance companies, corporations and law firms nationwide. I am knowledgeable in complicated discovery matters, such as cloud computing, computer forensics, electronic data discovery, internal investigations and hosted document review.

3. In my role as National Director of Legal Technology, I advise corporations and law firms regarding projects ranging from complicated large-scale data preservation and internal

investigations, to customized technological solutions. I have experience in executing projects involving data collection, processing and analysis of massive amounts of data.

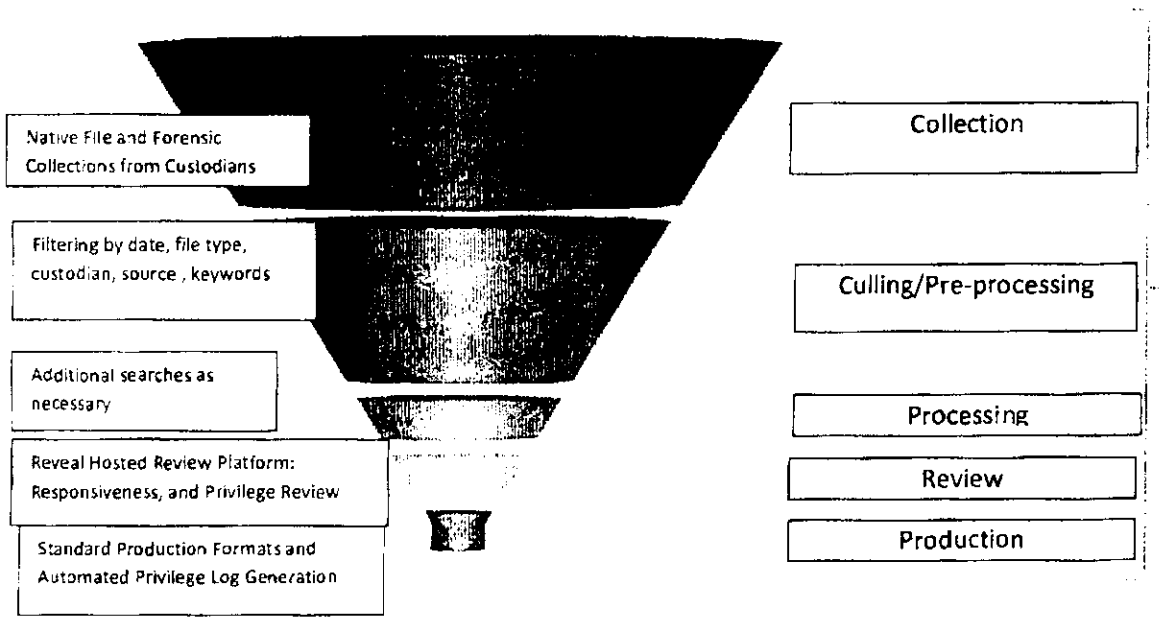
4. I am currently assisting Respondent [RESPONDENT] ("[RSPDT]") in the above-captioned arbitration proceeding with the management of electronically stored information relating to discovery in the above-referenced matter.

A. **Overview of Electronic Data Discovery**

5. "Electronically stored information" or "ESI," means electronically stored data, including potentially relevant information stored electronically, magnetically, optically or in other computer-readable format. One common form of ESI is email.

6. Electronic Data Discovery or "EDD" is the processing and management of evidentiary documents stored in electronic form into a usable sub-set for document review and production. One way to conceptualize EDD is as a process that funnels information from the widest or broadest universe to one or more smaller, more narrow subsets of the same data. The EDD process typically, and in this case in particular, starts with a voluminous set of manually unmanageable data, which, through use of various EDD tools, allows the data to be reduced down to a manageable set of more precise, responsive and non-privileged documents to produce in the case. The following illustration generally depicts the process.

"Funneling": Stages of EDD



7. **Collection**: In order to identify ESI for production and use, the data must first be collected from the custodian. ESI is typically collected from the custodian in Native file format. "Native file" means the original format of a type of ESI in which such information was embodied at the time it was created by its corresponding software application. Stated another way, a Native file format refers to the default file format that an application uses to create or save files. In order to view a Native file, the user must have the software application that the file has been formatted to.

8. **Culling/Pre-Processing**: Pre-processing is also referred to as culling and is the next step after collection of ESI. During pre-processing, one can filter and search the data by keywords, domains, custodians, dates and other criteria. This is a very efficient way to vastly reduce the amount of data that is processed and ultimately reviewed, in order to reduce costs of review.

9. **Processing:** Next, processing takes the data from a somewhat raw stage through the de-duplicating, Optical Character Recognition ("OCR") staging for native or Tagged Image File Format.("tiff") reviews and other processes to get the data ready for review. Through processing, the universe of data is further narrowed to only that remaining data that requires attorney review prior to production. For example, during processing, the files from the custodians can go through electronic ***deduplication***. Where, as in [RSPDT]'s case, there are multiple mailboxes, each having its own user and each being an email "custodian,", many custodians will have one or more copies of their own emails in question, which through this process, only need be reviewed once. Removal of duplicate files is one of the biggest time and cost savers of the processing stage.

10. **Review.** Next, the processed data is loaded into an electronic document review platform. U.S. Legal Support recommends an online electronic document review platform from Reveal Software. Reveal supports sophisticated searches, family and threaded documents, tagging, foldering, redactions of privileged material, document assignments and a wealth of other tools to organize and speed the review process. "Tagging" is a feature offered in Reveal, and most other EDD review software, that allows a user to add a code or "tag" to a document after reviewing it in order to dictate further treatment of the document. Common tags are: "responsive", "non-responsive" and "privileged". Through the use of tagging, privilege logs can be generated automatically from Reveal, which automates a time consuming and burdensome process, especially in cases where there are a large volume of privileged documents. Tagging and foldering further facilitates the efficient, and mostly automated, creation of document indexes, timelines, and other tools litigators commonly use to prepare their case, as compared to the traditional manual techniques.

11 **Production.** When the review is complete, production files are created through a near automated process based on the tags placed by the reviewing attorney or her staff, for production to opposing counsel, in the format requested by opposing counsel. Many large firms these days license their own in-house EDD reviewing software, such as Concordance or Summation, or use a 3rd party provider to host their data in an online review system, for example Relativity or Reveal InControl. Load files for that software can be extracted from Reveal in order to give the opposing counsel similar functionality to Reveal when reviewing the documents for their purposes. For firms without in-house document review software, a Reveal user license can be purchased on a month-to-month basis, which allows for the potential of cost-sharing of the online review platform by opposing parties. For those attorneys not comfortable with using document reviewing platforms, we can produce files from Reveal in PDF file format with Bates labeling on each page to serve as a document identifier. "PDF" is a file format that captures all the elements of a printed document as an electronic image that you can view, navigate, print or forward. It is distinct from a Native file, and in order to produce a document in PDF file format, an electronic conversion of the file must be performed by using a separate software application.

B. [RSPDT]'s ESI and EDD Issues

12. **Collection of [RSPDT] Email Data.** Here, I understand that in order to facilitate the discovery response process, [RSPDT]'s third party email host was instructed, with the help of [RSPDT]'s internal IT department, to extract email files from certain [RSPDT] email custodians, and on July 1, 2016, [RSPDT] forwarded to U.S. Legal Support ESI that totaled approximately 181 gigabytes ("GB") of ESI. In addition, another approximately 15 GB of

additional files from laptops that [CLAIMANT] used during his employment, as well as email files from [LAWFIRM1] have been provided to U.S. Legal Support.

13. I have reviewed portions of the data provided by [RSPDT] which includes Native file email documents in the form of .pst files, and their attachments (if any), also in Native format as applicable.

14. The approximately 196 GB consists of documents includes from the following email account users or "Custodians" at [RSPDT] and [LAWFIRM1]:

1) [CLAIMANT]

2) [CUSTODIAN01]

3) [CUSTODIAN02]

4) ...

15. As a first step in the culling, date filters were applied to all custodian files of January 1, 2013 through the present, based on [CLAIMANT]' hire date with [RSPDT], as requested by its counsel. After this date filter was applied, roughly 20GB and 173,000 documents remained in [CLAIMANT]' email files alone.

16. For the remaining custodians, this left 150 GB and 626,000 separate ***documents*** (not pages).

17 Based on average industry estimated review times, the rate of review for electronic review, such as through Reveal, is approximately 75 logical documents per hour.

18. This is contrasted to the average estimated "paper" or PDF rate of review is approximately 30 logical documents per hour.

19 From my experience the average logical document contains 2.5 pages.

20. Thus, without further culling beyond the current date filtering beyond approximate date of hire, such as application of search terms, review of the ESI provided by [RSPDT] would take approximately 10,653 hours *assuming* that the electronic review platform was used, or approximately 26,633 hours if reviewed in paper or PDF format. Based on my experience, this amount of data would amount to approximately 2 million pages.

21 In addition, U.S. Legal Support was requested to run the following searches of certain [RSPDT] custodians email accounts in our culling software with the following results:

Search 1:
Date Range:**12/27/15 - 12/28/15**
Custodians: **[CUSTODIAN01], [CUSTODIAN02], [CUSTODIAN03]**
Results: **565 documents (not pages); 519 documents after deduplication performed**

Search 2:
Date Range:**1/1/13 - 12/28/15**
Custodians: **[CUSTODIAN01], [CUSTODIAN02], [CUSTODIAN03]**
Search terms: **"Term01" or "Term02"**
Results: **26,277 documents (not pages); 7,680 documents after deduplication performed**

C. **Costs of EDD**

22. The following is a breakdown of the costs associated with this project. Based on my knowledge, experience and training, they are comparable with standard industry charges for the type of service provided.

Project Setup Fee: Waived

- Setup includes, but is not limited to, all administrative functions performed at project commencement, media intake, chain of custody reporting and all other standard reports, configuration of software/ hardware and environment setup.

Data Culling and Processing:

- Emails which were collected are then ingested into LexisNexis Early Data Analyzer (EDA) application. EDA has the ability to de-duplicate, keyword search, date filter, email domain filter and filetype filter.

- $XXGB = **$4,900**

Online Document Review Platform: (InControl by Reveal)

- Hosted Database setup fee: Waived

- Native File Processing: Export keyword responsive and date filtered (culled) data for use in Reveal
  - $XXX/GB = **TBD**

- Monthly Online Data Hosting Fee
  - $XX per GB / month = **TBD**

- User Fees
  - $XX per user / month

Production Rates:

- Native to TIFF Conversion for Production (Requires Native File Processing)
  - $XXX per GB=**TBD**

- Image Branding/Electronic Bates Stamping
  - $XXX per page = **TBD**

Consulting/Tech Time

- Technical Formatting and Project Management
  - $XXX per hour =**TBD**

- Consulting and Expert Witness Fees
  - $XXX per hour=**TBD**

Thus, without further culling, in order to load the approximately 170 GB of ESI into Reveal for review, production and generation of privilege logs and indexes and similar items, the initial cost alone would be $42,500, not including monthly hosting fees, and not including any attorney or staff review time.

D. Conclusion

23. Given the voluminous ESI at issue as describe above, and based my education, experience and training in electronic discovery, use of the EDD process for [RSPDT]s review and production of its ESI, has numerous benefits as compared to manual review of the ESI. In summary such benefits include:

a. cost savings of more efficient review, automated privilege logs and indexes;

b. review by the attorneys and their staff, rather than the party;

c. potential for input and cost savings by opposing party;

d. accuracy of review;

e. avoidance of unintentional alteration of original documents;

f. preventing duplication of work on same or near-same documents;

g. assessment of review costs before start of initial review.

24. In contrast, to the EDD procedures, a "manual" search and review of [RSPDT]'s ESI for even the two example searches above, would involve having each of the users attempting to search their own voluminous mailbox folders for responsive emails and then forwarding duplicative results to [RSPDT]s attorney for review by the attorneys or their staff, for responsiveness, privilege, and then manual conversion from Native format to PDF, and

Bates labeling prior to production to opposing counsel, followed by a manual creation of a privilege log and manual creation of document indexes.

FURTHER AFFIANT SAYETH NOT

Trent Walton

SWORN TO BEFORE ME this __ day of ____ __, ____.

Notary Public

A WHOLE NEW WORLD WITHOUT THE NEED FOR A GENIE: UTILIZING SOCIAL MEDIA INFORMATION IN LITIGATION

BY: GREGORY PEREZ
BROCK PERSON GUERRA REYNA
SAN ANTONIO, TEXAS[1]

I. INTRODUCTION

In the tale of Aladdin, Aladdin needed the help of the infamous Genie and three wishes in order to capture Princess Jasmine's heart. Unfortunately, as attorneys, we are not given three wishes before every trial that allow us to capture the hearts of the jury. But what if we were able to take the jury on a 'magic carpet ride' of evidence and show them a 'Whole New World' of social media information to win their hearts and minds to our cause. All it takes is a little social media investigation to find a wealth of information which could influence the case from start to finish.

As methods of communication and information evolve over time, attorneys would be wise to evolve their litigation practices with them. Therefore, this article will explain where to locate social media information, discuss how to obtain and use this evidence in pre-litigation through discovery, and finally, address how to utilize this evidence at trial.

II. The 'Whole New World:' Social Media Platforms

In the world of litigation, a parties' social media profile can be priceless to a trial attorney. However, unlike the treasure in Aladdin's tale, this wealth of knowledge is not locked away in some inaccessible cave. In fact, this information may be easier to access than some attorneys realize.

So you may be asking yourself: where can I find this potential wealth of information? The answer: it may only be a click away, posted publically for the entire world to see, or privately for "followers" and "friends" to enjoy. Whatever the social media method, Courts are generally allowing parties to utilize social media information all the way through trial.[2]

From 2010 to 2015, the total number of social media users worldwide more than doubled, from 970 million to 2.14 billion people.[3] As of January 2017, there were 2.8 billion active social media users worldwide, and it's estimated that number will rise to 2.95 billion in 2020.[4] Facebook alone has 1.9 billion unique monthly users and 75% of users spend 20 minutes or more on Facebook every day.[5] Millennials and Generation X users, which encompass individuals ages 18-49, spend an estimated seven hours per week on social media.[6] However, Facebook is not the only social media platform an attorney can access. Twitter, Instagram, YouTube, Pinterest, LinkedIn, and Snapchat are just a few of the

---

[1] Gregory Perez is an Associate at Brock Person Guerra Reyna, P.C. in San Antonio, Texas. His practice is mainly focused in First and Third Party Insurance litigation

[2] *See e.g.* Beth C. Boggs & Misty L. Edwards, *Does What Happens on Facebook Stay on Facebook? Discovery, Admissibility, Ethics, and Social* Media, 98 Ill. B.J. 366, 367 (2010).

[3] *Number of Social Media Users Worldwide from 2010 to 2010*, STATISTA: THE STATISTICS PORTAL (2017), https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

[4] *Id.*

[5] Andrew Hutchinson, *Top Social Network Demographics 2017 [Infographic]*, SOCIAL MEDIA TODAY (March 21, 2017), http://www.socialmediatoday.com/social-networks/top-social-network-demographics-2017-infographic.

[6] *Id.*

hundreds of platforms that people use to share the ins and outs of their daily lives. With the rise of Millennials and Generation X, social media information is only going to become more and more prevalent.

While an attorney has the ability to perform a search on each individual platform, sites such as Spokeo.com and Pipl.com, which are social network aggregator sites, accumulate data concerning individuals from a variety of online and offline sources. Any attorney who possesses an individual's e-mail address can immediately identify any and all social media profiles opened by that e-mail address. This is important to remember, as all social media platforms require an e-mail address to set up an account.

III. Social Media Information in Pre-Litigation

With the growing number of individuals on social media, a practice I have adopted while working up a case is performing a social media search on all litigants as soon as the case hits my desk. This practice should be implemented by all trial lawyers, as the information posted on social media platforms at the beginning of a case can be imperative to building a defense. It is not uncommon for information to become more difficult to find as a case trucks on, and as opposing counsel is made aware of what is on their client's pages.

As a "young attorney," and one that also utilizes social media platforms for personal use, I am able to run these searches in little to no time. However, I also appreciate this can seem foreign to attorneys not as familiar with these platforms. Therefore, it is important to note that running theses searches is something *anyone can do*. As a matter of practice, a senior partner in my firm has delegated this task to his paralegal, but this is something that can be done by any member or your support staff, or summer law clerks. Find someone well-versed in social media to monitor it – in anticipation of litigation, lawyers should, at a minimum, conduct social media research on the potential parties, opposing counsel, and potential witnesses.

An investigating lawyer should seek out as much relevant, public social media content as possible, in part because it can form the basis for disclosure of non-public information. Conversely, counsel should try to protect their own client's social media content from an adversary by maximizing the client's privacy settings. Most social media platforms contain privacy settings which enable or limit who can see the information.

Some of you may be thinking, "Is viewing a litigant's social media profile ethical?" The answer is **YES**, as long as an attorney does not engage in deception. Many state and city bar associations have issued ethical guidelines and opinions on the appropriate ways to access social media content. Most of these rules stem from the basic prohibition on directly or indirectly contacting a represented party, absent consent from that party's lawyer.[7]

Generally, a lawyer investigating a case:

1) May access the public portions of a party's or witness's social media account, regardless of whether or not the party or witness is represented.

2) May not access private or non-public portions of a represented

[7] *See* MODEL RULES OF PROF'L CONDUCT R. 4.2.

party's or witness's social media account if the lawyer is required to "friend" or "follow" the account or account user.

3) May "friend" or "follow" an unrepresented party or a witness on social media if the lawyer does not engage in deceptive behavior.

Social media content has typically been deemed public if the information is "available to anyone viewing a social media network without the need for permission from the person whose account is being viewed," including "content available to all members of a social media network and content that is accessible without authorization to non-members."[8]

Ultimately, the investigation of social media content in pre-litigation can be highly effective to help develop a case, frame potential causes of action, or resolve a dispute before reaching full-blown discovery. By way of example, a couple of months ago, I received a pre-litigation matter from a client in which a claimant was making a claim for personal injuries as the result of a fall. These injuries included hip pain and the inability to put weight on the claimant's legs. Following the receipt of this file, I quickly performed a social media search on Instagram and Facebook, using only the claimant's name. Surprisingly, the claimant's Instagram profile was public, and I was able to immediately locate valuable information: a time-stamped photograph, three weeks after the accident, in which the claimant was wake-boarding while carrying a friend on her back. Talented? Yes. Beneficial to her claim? No. Upon bringing this information to the Plaintiff's Attorney, this claim was quickly resolved before the claim proceeded to litigation.

Yet, the vast majority of matters attorneys handle have already proceeded to litigation, and utilizing social media information during the discovery process can both resolve a case before trial and set one up for success at trial.

IV. Social Media Information in Discovery

Once litigation has commenced, attorneys should ensure that all discovery efforts cover social media content. Some important points to remember are:

1) Draft appropriate document requests and interrogatories to reach relevant social media content through party discovery.

2) Follow-up on social media content in depositions of litigants.

3) Determine whether to utilize social media evidence in settlement negotiations or save for trial.

A) Crafting Written Discovery

Often, the discovery of social media information can be more successful through party discovery. As a rule of practice, attorneys should craft document requests to

[8] *See* Mark A. Berman, Ignatius A. Grande, & Ronald J. Hedges, *Social Media Ethics Guidelines of the Commercial and Federal Litigation Section*, NEW YORK STATE BAR ASS'N, May 11, 2017, at A-42, *available at* http://www.nysba.org/socialmediaguidelines17/; see also Committee on Professional Ethics, Opinion No 843, New York State Bar Association, Sept. 10, 2010, *available at* http://www.nysba.org/CustomTemplates/Content.aspx?id=5162.

reach social media information as they would any other documents. Attorneys should pay heed to the fact that, as with all discovery requests, case law makes it clear that social media discovery directed to a party must be narrowly tailored to the issues relevant in the case. Texas decisions, although limited on the subject, favor this approach. In *In re Indeco Sales, Inc.*, No. 09-14-00405-CV, 2014 WL 5490943 (Tex. App.—Beaumont 2014, no pet) (mem. op.), the Beaumont Court of Appeals held that a district court did not abuse its discretion by granting an injured plaintiff's motion for protection as to a discovery request seeking information, data, posts, and conversations from plaintiff's Facebook page, because the request sought every photograph posted since the accident, regardless of when the photograph was taken, and another request seeking all posts or messages she sent or received, regardless of topic.[9] Conversely, in *In re Christus Health Se Tex.*, 399 S.W.3d 343 (Tex. App.—Beaumont 2013, no pet. h.), the Court concluded that a request without a time limit for posts [from Facebook] is overly broad on its face.[10]

Below are some sample interrogatories and requests for production that attorneys can use in cases where they may be relevant:

Interrogatories

1) State the name, web address, and user name for all blogs, online forums, social media sites and applications (including, but not limited, to, Facebook, Snapchat, Twitter, LinkedIn, Instagram, Pinterest, YouTube, or any similar sites or applications) that Plaintiff has registered with, belonged to, or had membership to, from _____ to the present.

2) State the name, web address, and user name for all blogs, online forums, social media sites and applications (including, but not limited, to, Facebook, Snapchat, Twitter, LinkedIn, Instagram, Pinterest, YouTube, or any similar sites or applications) that Plaintiff has used to communicate from the date of the Accident to the present.

Request for Production

1) Please produce all photographs posted, uploaded, or otherwise added to any social networking sites, applications, or blogs (including, but not limited, to, Facebook, Snapchat, Twitter, LinkedIn, Instagram, Pinterest, YouTube, or any similar sites or applications) posted since the date of the Accident alleged in the Complaint.

2) Please produce all communications posted, uploaded, or otherwise added to any social networking sites, applications, or blogs (including, but not limited, to, Facebook, Snapchat, Twitter, LinkedIn, Instagram, Pinterest, YouTube, or any similar sites or applications) posted since the date of the Accident concerning any allegations or events referenced in Plaintiff's Complaint.

3) Please provide copies of all instant messaging logs or transcripts associated with any accounts identified in response to

[9] *In re Indeco Sales, Inc.*, No. 09-14-00405-CV, 2014 WL 5490943 (Tex. App.—Beaumont 2014, no pet) (mem. op.).
[10] *In re Christus Health Se Tex.*, 399 S.W.3d 343 (Tex. App.—Beaumont 2013, no pet. h.).

Interrogatory No. __ concerning any allegations or events in Plaintiff's Complaint.

4) Please produce all postings by Plaintiff on any social media site or application (including, but not limited, to, Facebook, Snapchat, Twitter, LinkedIn, Instagram, Pinterest, YouTube, or any similar sites or applications) that refer or relate to the accident in question.

5) Please provide an electronic copy of your complete Facebook history, including any and all profile information, postings, pictures, and data available pursuant to Facebook's "Download Your Own Information" feature.

6) For each Facebook account maintained by you, please produce your account data for the period of __ __ through present. You may download and print your Facebook data by logging onto your Facebook account, selecting "Account Settings" under the "Account" tab on your homepage, clicking on the "learn more" link beside the "Download Your Information" tab, and following the directions on the "Download Your Information" page.

7) Please produce all postings by Plaintiff on any social media site or application (including, but not limited, to, Facebook, Snapchat, Twitter, LinkedIn, Instagram, Pinterest, Youtube, or any similar sites or applications) that refer or relate to emotional distress or physical injuries that Plaintiff alleges he/she suffered as a result of the accident and any treatment that he/she received subsequent to the accident.

Although it is common sense among practicing attorneys, remember to always request that a sworn verification be produced along with Plaintiff's written discovery responses. The sworn responses to interrogatories, such as those listed above, may be particularly important if the opposing party does not produce social media information and a motion to compel is required to reach that information.

After written discovery has been completed, attorneys should practice following up on social media in a parties' deposition.

B) Following up on Social Media in Depositions

If attempts to gain social media information in written discovery have failed, depositions are another time to press the opposing party, under oath, for social media information.

Questions I have incorporated into my practice include.

Q: Do you have any social media accounts where you post personal information about yourself?

Q: Which social media platforms do you use?

Q: Have you had other social media accounts that you no longer use?

Q: What name(s) do you use for yourself for your social media account(s)?

Q: What e-mail addresses do you use to access your social media accounts?

Q: Since the DOL, have you posted any information related to the accident on any of your social media accounts?

Q: Since the DOL, have you posted any information related to your alleged injuries or damages on your social media accounts?

Q: If we wanted to see the information you post on your social media account(s), what would be the best way to see it?

If previous social media searches have proved fruitful, depositions are the time to try to impeach the opposing party's testimony by questioning them on any adverse information you have found. By way of example, I had a case where a Plaintiff was claiming injuries to his neck and back. Social Media Information had provided Facebook posts by the Plaintiff, time-stamped post-accident, including:

"Thank God I am healed"

"Woke up 2day feeling great"

"I don't need painkillers anymore"

"I haven't felt this good in a long time."

"I am happy to say I am completely healed...I can literally run now, no pain at all."

In his deposition, I asked Plaintiff if he had ever experienced any relief from pain. Plaintiff's response: "No, I have never had any relief since the accident." I questioned Plaintiff further about his activities post-accident. Plaintiff stated he was unable to go to the gym, and was limited in his activities. Little did he know that I was in possession of his Facebook postings, post-accident, stating: *"Day 5 at the gym...ran 4 miles today...played full court basketball...sparred two 3 minute rounds..."*

With Plaintiff's contradictory testimony, I could set my case up for success at the next cross-roads of litigation: settlement or trial.

C) <u>The Choice: Utilizing social media evidence in settlement negotiations, or saving for trial.</u>

As trial attorneys, we do not want to show all the cards in our hand until the time is right. Thus, we often face the decision of deciding whether to reveal our potential impeachment evidence at mediation in an attempt to facilitate settlement, or save that evidence for the time of trial.

In my experience, such decision has been made on the likeliness the case will go to trial, and the amount of social media evidence I have acquired. If I believe a case is likely to settle at mediation, I typically bring the social media evidence to mediation to present in my negotiations as a way to lead Plaintiff into settlement and shave the settlement amount in my client's favor. However, if I believe a case is unlikely to settle, I will typically retain the social media information I have until the trial;[11] not revealing the information until the last possible second, and hopefully using it to impeach Plaintiff's testimony, attack their credibility, or give the jury a reason to limit Plaintiff's damages at trial.

V. Social Media Information at Trial

You have managed to make it to trial, a litigation attorney's dream, but now

[11] However cognizant of the fact that if Plaintiff's attorney is clever enough to propound RFPs asking for this information, I must give it up.

you face common issues concerning the use of your treasure trove of social media information at trial. These issues include:

1) Demonstrating the relevance of social media content for use at trial.

2) Assessing how to authenticate social media content for use at trial.

A) Relevance of Social Media

Obviously, as with any other evidence, social media information has to be relevant to issues in the case. Texas Rule of Evidence 401 defines "relevant evidence" as "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."[12] Further, "[i]n deciding whether evidence is relevant, a trial court should ask whether a reasonable person, with some experience in the real world, would believe the evidence is helpful in determining the truth or falsity of any fact that is of consequence to the lawsuit."[13] Therefore, in determining relevancy, courts look to the purpose for offering the evidence—the material fact to be proved – and whether there is a direct or logical connection between the offered evidence and the proposition to be proved.[14] If there is any reasonable logical nexus, the evidence will survive the relevancy test.[15]

Social media evidence may be relevant to nearly every type of legal dispute primarily because, if you recall the earlier statistics, there are so many people using social media platforms around the world. Thus, it is more than likely litigants are "posting" statements, photographs, 'tweets', etc. that "have the tendency to make the existence of any fact more or less probable."[16]

Further, some Courts have ruled that if a party fails to produce relevant evidence in discovery, there are severe consequences. In *Lester v. Alliance Concrete Co.*, 285 Va. 295 (2013), a Virginia state court reduced a jury award by over four million dollars and ordered the plaintiff and his counsel to pay the defendants over $700,000 in fees and expenses because of deliberate deletion of Facebook photos responsive to discovery requests.[17]

While the burden of demonstrating relevance is low, just because evidence is relevant does not mean that it is admissible.[18]

B) Authenticating Social Media Information

Authenticating social media content for use at trial can be challenging, particularly for static screenshots that do not contain time-stamps, or for a source that is constantly being revised. Courts examining the proper methods to authenticate social media evidence have reached different conclusions on the standard a party must satisfy.

As we all know, Federal Rule of Evidence 901 establishes the requirements for authentication or identification as a condition precedent to the admissibility of

---

[12] TEX. R. EVID. 401; FED. R. EVID. 401.

[13] *Hernandez v. State*, 327 S.W.3d 200, 206 (Tex.App.—San Antonio 2010, pet. ref'd) (citations omitted).

[14] *See e.g., Layton v. State*, 280 S.W.3d 235, 240 (Tex. Crim. App. 2009).

[15] *See Reed v. State*, 59 S.W.3d 278, 281 (Tex. App.—Fort Worth 2001, pet. ref'd).

[16] TEX. R. EVID. 401; FED. R. EVID. 401.

[17] *Lester v. Alliance Concrete Co.*, 285 Va. 295 (2013).

[18] TEX. R. EVID. 403.

non-testimonial evidence.[19] Under Rule 901, before an item may be admitted, the proponent must offer "evidence sufficient to support a finding that the matter in question is what its proponent claims."[20] Federal Rule of Evidence 901(b) gives examples of how authentication can be accomplished.[21]

Some state courts have found that a party may use any form of evidence to authenticate social media content if the party demonstrates to the trial judge that a jury could reasonably find that the proffered evidence is authentic.[22]

Generally, the proponent of the internet printout must provide testimony by live witness or affidavit that the printout is what it purports to be.[23] In *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007), the court discusses how Federal Rule of Evidence 901 works with Federal Rule of Evidence 104 and the necessity for the court to decide authentication as a preliminary question.[24] The Court in *Lorraine* determined that "An original digital photograph may be authenticated the same way as a film photo, by a witness with personal knowledge of the scene depicted who can testify that the photo fairly and accurately depicts it."[25]

Several courts have also followed varying approaches to authentication challenges. For example, a circuit court of appeals held that photographs on a defendant's Facebook page were not properly authenticated because a "photograph's appearance on a personal webpage does not by itself establish that the owner of the page possessed or controlled the items pictured."[26] On the other hand, a United States District Court found that statements made by a plaintiff on her Facebook page were authenticated by her deposition testimony and admissible as a party admission under Federal Rules of Evidence 901(a) and (b)(1).[27]

Further, courts have relied on different rules to authenticate and admit evidence taken from social media. In one example, a United States District Court admitted Facebook posts under the residual hearsay exception in Federal Rule of Evidence 807 based on credible evidence that the posts were authentic.[28] In another case, a circuit court held that screenshots of Facebook pages and YouTube videos retrieved from a Google server were self-authenticating business records under Federal Rule of Evidence 902(11) where they were accompanied by certifications from Facebook and YouTube records custodians.[29]

Since it appears that courts have not yet reached a consensus on the authentication of social media content, attorneys should carefully consider authentication issues during discovery to

---

[19] *See* FED. R. EVID. 901.

[20] TEX. R. EVID. 901(a); FED. R. EVID. 901(a).

[21] *See* FED. R. EVID. 901(b).

[22] *See Tienda v. State*, 358 S.W.3d 633, 638, 642 (Tex. Crim. App. 2012); *see also Parker v. State*, 85 A.3d 682, 687 (Del. 2014).

[23] *See In re Carrsow-Franklin*, 456 B.R. 753, 756-57 (Bankr. D.S.C. 2011) (noting that blogs are not self-authenticating and rejecting blog evidence due to failure to present authentication testimony).

[24] In *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007), *see also* FED. R. EVID. 901; FED. R. EVID. 104.

[25] *Id.*

[26] *United States v. Winters*, 530 F. App'x 390, 395-96 (5th Cir. 2013).

[27] *Targonski v. City of Oak Ridge*, No. 11-269, 2012 WL 2930813, at *10 (E.D. Tenn. July 18, 2012); *see* FED. R. EVID. 901(a); FED. R. EVID. 901(b)(1).

[28] *Ministers & Missionaries Benefit Bd. v. Estate of Clark Fleshe*r, No. 11-9495, 2014 WL 1116846, at *6 (S.D.N.Y. Mar. 18, 2014); *see* FED. R. EVID. 807.

[29] *United States v. Hassan*, 742 F.3d 104, 132-34 (4th Cir. 2014); *see* FED. R. EVID. 902(11).

prepare for trial. For example, ensure that all photographs taken from social media platforms are in color and time stamped, with the date of posting by the litigant attached to the photograph, or use the assistance of a vendor or collection software, which will help minimize authentication challenges. This will provide the basis for a better argument as to why the social media images should be admitted. Authentication may also be something that an attorney can choose to address in depositions, should you have the evidence available and decide to utilize it during that time, so as to avoid a denial or mishap at trial.

VI. CONCLUSION

70% of U.S. adults use some form of social media. 72% of U.S. women and 62% of U.S. men use at least one social media platform. 76% of Facebook accounts are used daily, 52% of Instagram accounts are used daily, and 42% of Twitter accounts are accessed daily.[30] These statistics do not even include all of the hundreds of other social media platforms in the world today. With this sea of information flooding daily onto the world-wide web, you can bet that litigants/potential litigants are posting, tweeting, and uploading information that may be relevant to current and future litigation.

As lawyers we are tasked with competent and diligent representation of our clients. Therefore, as technology changes, lawyers must adapt and utilize new sources of information if they are to continue to represent their clients competently. These new sources of information include social media platforms.

Changing age-old legal practices can be hard, and for many well-practiced attorneys this 'Whole New World' of social media can be intimidating, but as explained in this paper, accessing it can be easily done with a mouse, not a Genie; and utilizing social media information throughout the litigation process can potentially open the doors to case results not previously apparent

[30] *Social Media Fact* Sheet, PEW RESEARCH CENTER (Jan. 12, 2017), *available at* http://www.pewinternet.org/fact-sheet/social-media/ (last visited June 21, 2016).

THE HUNT FOR ESI: EVIDENCE HIDING IN PLAIN SIGHT

Presented By:

Judge Lynn M. Egan

Trent Walton, CCE, ACE

Judge Lynn M. Egan

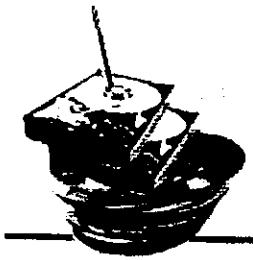
- Cook County Circuit Court Judge, 19 Years
- Member of Illinois Supreme Court Committees
  - Civil Justice Committee
  - Education Committee
  - (Former Member): Executive Committee, oversees all Illinois Supreme Court committees
  - (Former Member): Discovery Procedures Committee, now Civil Justice Committee
- Authored articles on
  - discovery, requests to admit, restrictive covenants, Day-In-The-Life films, directed verdicts, jury selection & instructions, Dead Man's Act, Supreme Court Rule 213, expert witnesses, reconstruction testimony, court-ordered medical exams, attorney-client/work product privileges, sanctions and damages.
- Bar Association committees and Boards of Directors
- Registered CLE provider through the Illinois MCLE Board
  - Awarded over 10,000 hours of CLE credit to Illinois attorneys
- Prior to joining bench
  - Argued before the Illinois Supreme Court: Cisarik v. Palos Community Hospital

USLEGAL SUPPORT

The Power of Commitment™

Trent Walton CCE, ACE

- Sedona Conference – Member
  - Working Group on Electronic Document Retention and Production (WG1)
  - Brainstorming Group on Information Governance
- Computer Forensics & eDiscovery
  - Certified Computer Examiner (CCE)® #684
  - Certified AccessData Examiner (ACE)®
  - Certified in Windows Forensics by AccessData
  - Certified Electronic Discovery Specialist
  - Certified in eDiscovery Software Products ranging from ECA through Review
  - Served as Expert in issues ranging from Computer Forensics to Complex eDiscovery Matters
- Software Development
  - Created E.L. Native Review™ for Concordance, Rated 4.6 out of 5 by TechnoLawyer Publication
    - Acquired by Wave Software in 2010
  - Created eCloudCollect™, now DataCollectPro™
    - Acquired by ZApproved 2014



WHY SHOULD YOU CARE ABOUT FINDING ESI?

Because the Rules of Professional Conduct demand it.

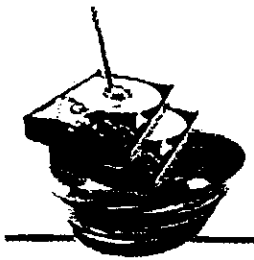
Rule 1.1 – Competence. Comment 8: "A lawyer should keep abreast of changes in the law & its practice, including the benefits & risks associated with relevant technology..."

See also, Rule 1.6 (Confidentiality of Information), Rule 1.15 (Safekeeping Property) & Rule 3.4 (Fairness to Opposing Party & Counsel).

KNOWING HOW TO FIND ESI REQUIRES KNOWING WHAT IT IS

"'ESI shall include any writings, drawings, graphs, charts, photographs, sound recordings, images, & other data or data compilations in any medium from which electronically stored information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form."

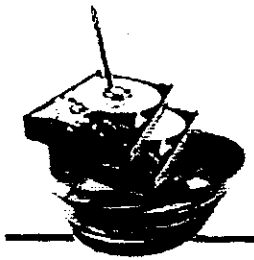
Ill.S.Ct. R. 201(b)(4)(West 2014)



WHAT DOES IT INCLUDE?

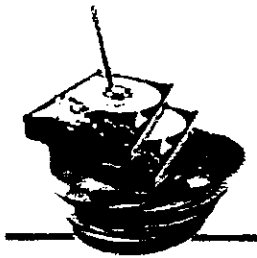
Amended Rule 201 defines "documents" very broadly & now specifically includes "**all retrievable information in computer storage**." *Ill.S.Ct. R. 201(b)(1)(West).*

NOTE: The amended rule requires a producing party to search its computer storage when responding to a production request. *Ill.S.Ct. R. 214, Committee Comments (West 2014).*



EXAMPLES

Word processed documents
Databases
Spreadsheets
Presentations
Digital photographs, video/audio recordings
Voicemail
Email messages & attachments
Calendar entries
Text/instant messages
Blog & social media posts



WHERE CAN IT BE STORED?

Computer hard drives (home & office desktops/laptops)
Network servers
Thumb (USB) drives
CDs, DVDs
Cell phone & smart devices (phones/tablets)
Home security systems
Gaming consoles
The Cloud
Social media websites
Electronic medical records (audit trails)
Fitness trackers

HUNTING FOR ESI EXAMPLES

Basic eDiscovery Terminology

Mobile Data

Photo Meta-Data (EXIF)

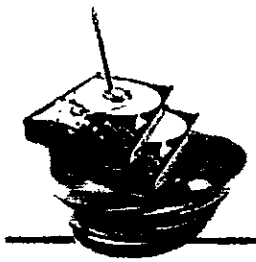
Social Media

Electronic Medical Records (EMR)

On-Board Diagnostics (OBD)

Remotely Piloted Vehicle (RPV)

Algorithmic Techniques

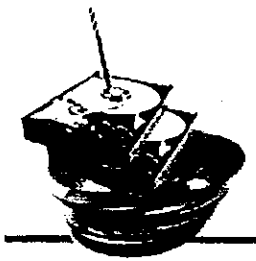


BASIC EDISCOVERY TERMINOLOGY

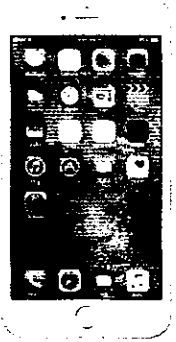
ESI: Electronically Stored Information

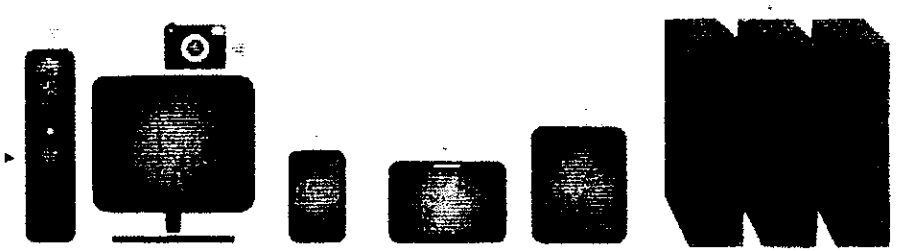
Metadata: data that provides information about other data

Native Format: format used by the application that created the document



WHAT IS "THE CLOUD"





zipcloud box justcloud

OneDrive IDrive

Dropbox Google Drive MediaFire

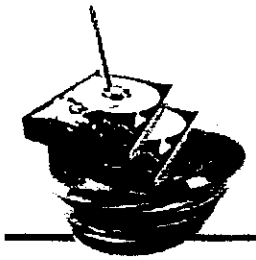
iCloud

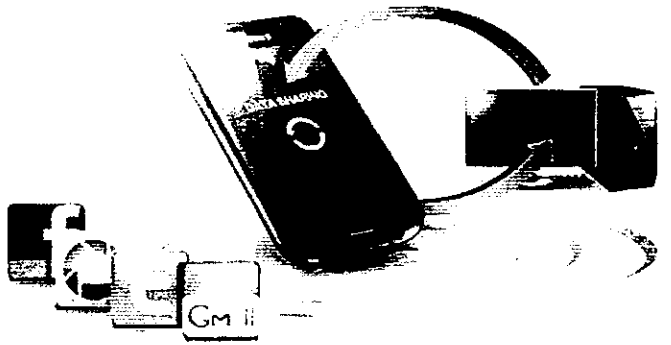
YAHOO! MAIL

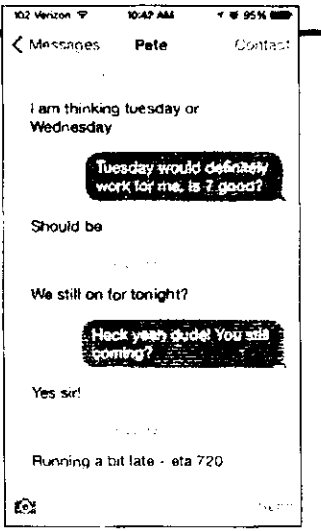
Outlook

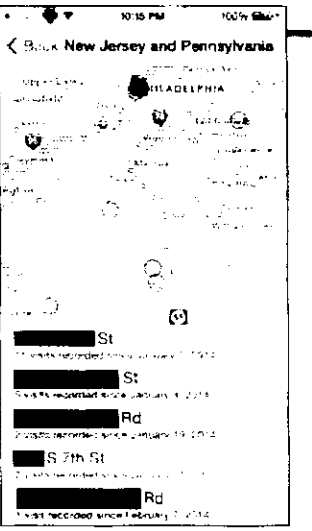
Gmail

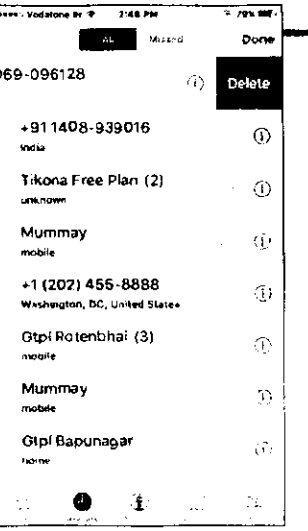
Microsoft Outlook Aol Mail.



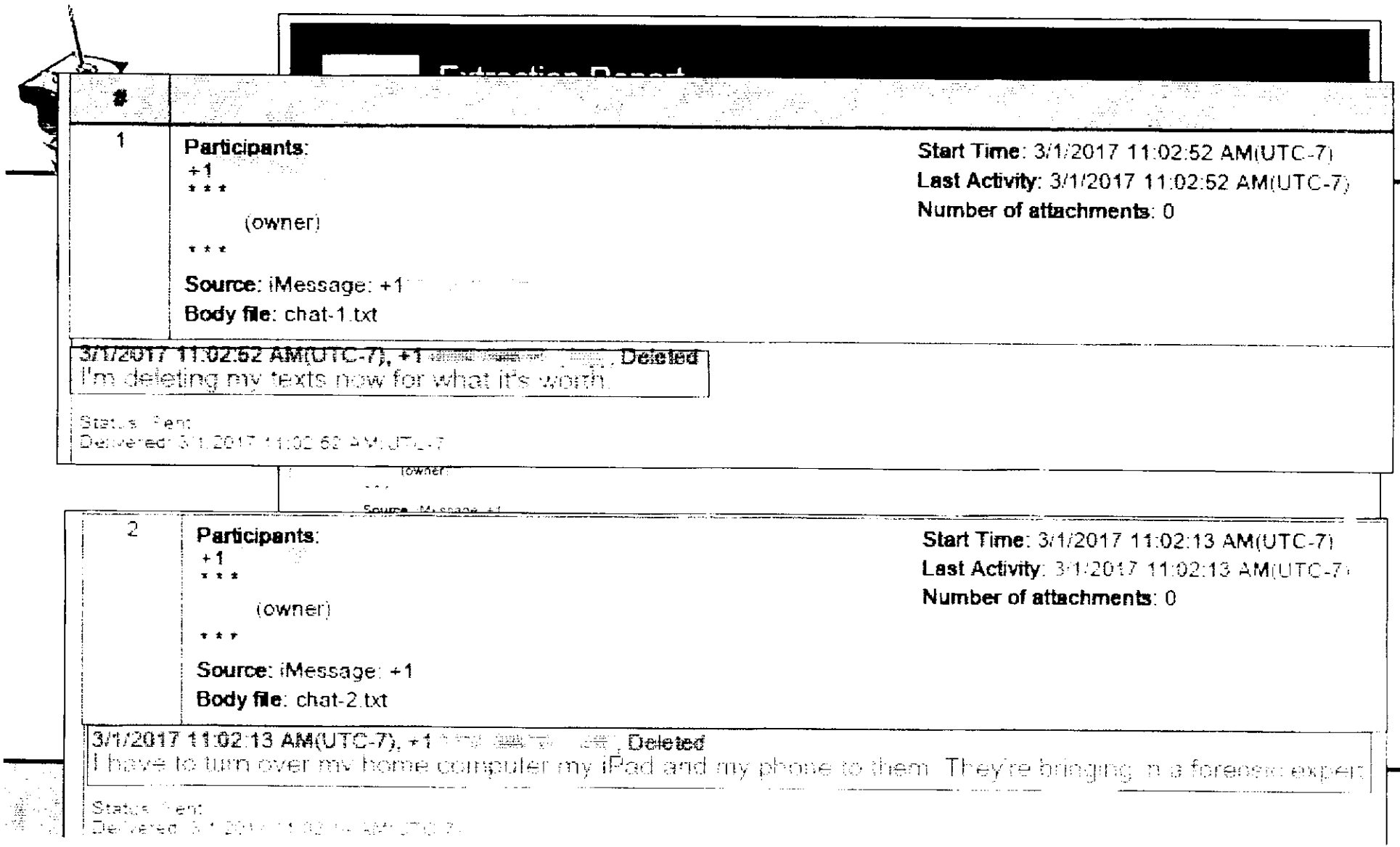








USING MOBILE DATA IN DISCOVERY



#	
1	**Participants:** +1 * * * (owner) * * * **Source:** iMessage: +1 **Body file:** chat-1.txt **Start Time:** 3/1/2017 11:02:52 AM(UTC-7) **Last Activity:** 3/1/2017 11:02:52 AM(UTC-7) **Number of attachments:** 0

3/1/2017 11:02:52 AM(UTC-7), +1 , Deleted
I'm deleting my texts now for what it's worth

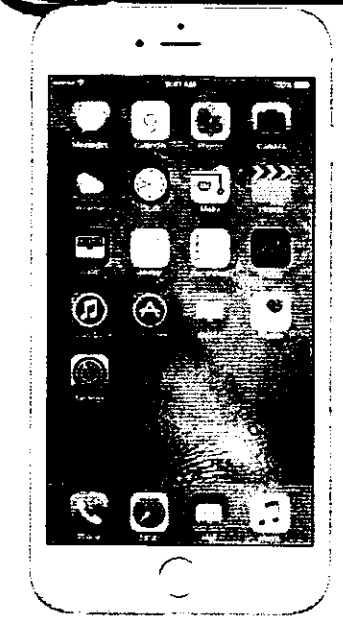
Status: Sent
Delivered: 3/1/2017 11:02:52 AM(UTC-7)

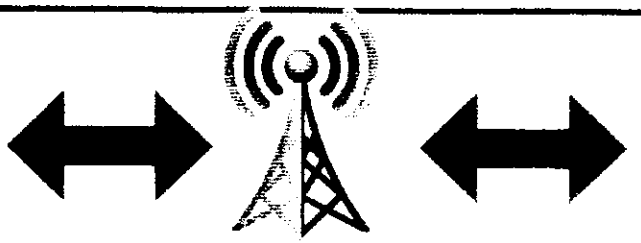
#	
2	**Participants:** +1 * * * (owner) * * * **Source:** iMessage: +1 **Body file:** chat-2.txt **Start Time:** 3/1/2017 11:02:13 AM(UTC-7) **Last Activity:** 3/1/2017 11:02:13 AM(UTC-7) **Number of attachments:** 0

3/1/2017 11:02:13 AM(UTC-7), +1 , Deleted
I have to turn over my home computer my iPad and my phone to them They're bringing in a forensic expert

Status: Sent

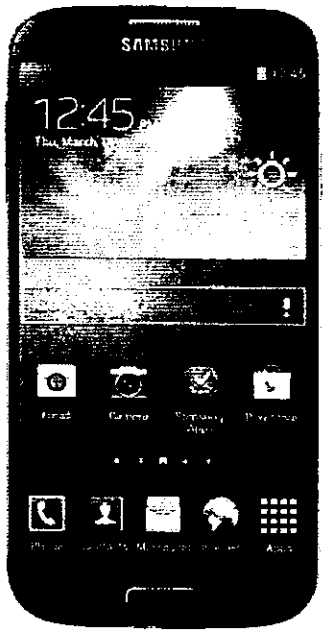
MESSAGES THROUGH CARRIER

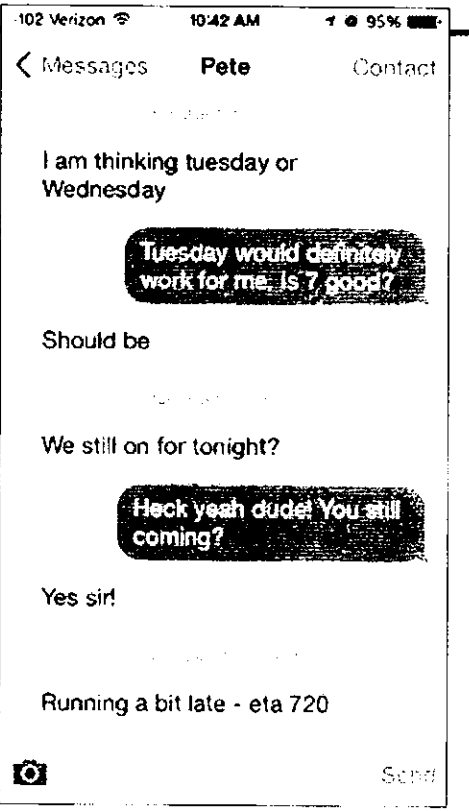




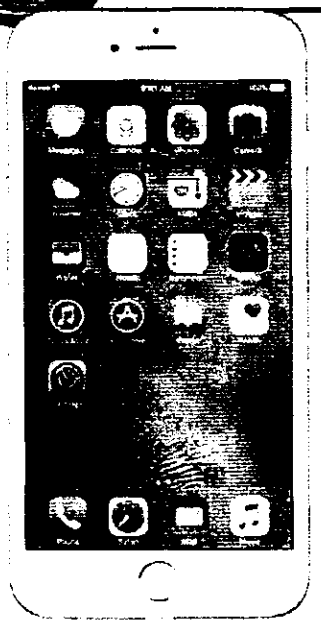
verizonwireless

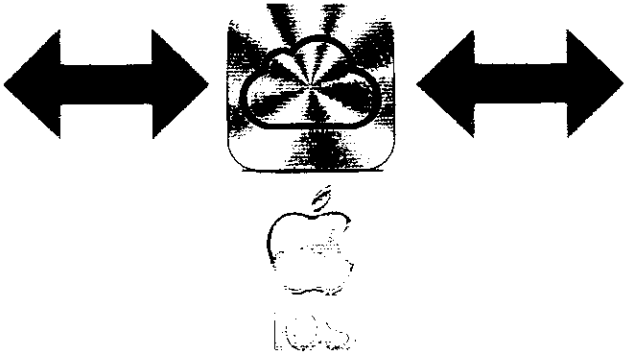
- Call Log
- Text Messages
  - **SMS Messages Only**
  - Last 30-90 Days
  - No Body
  - No Photos
  - No Videos
  - No Audio

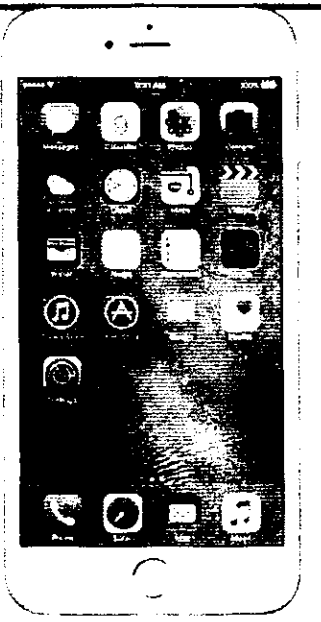




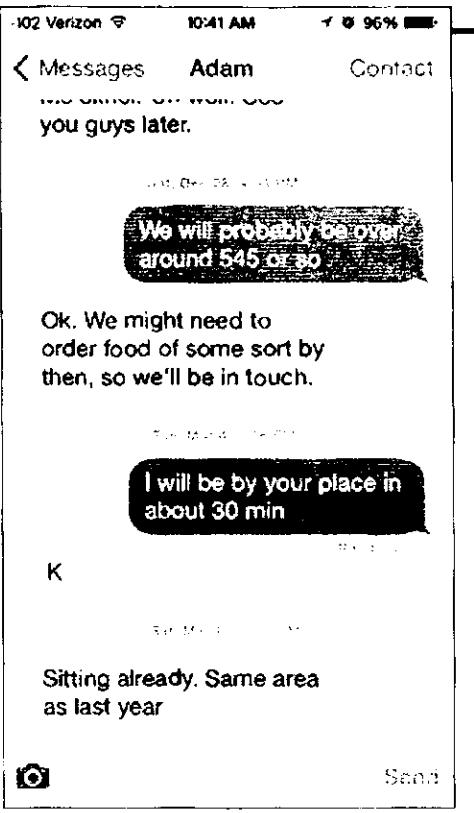
MESSAGES THROUGH APPLE

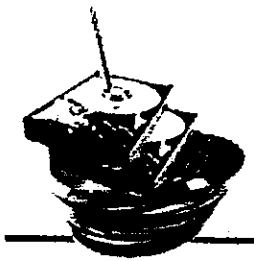






- Text Messages (iMessage & SMS)
- Call Logs, Contacts
- Voicemails
- Video, Images, Audio
- Application Data
- Geo-Location Information
- Health/Fitness Data





LOCATIONS OF DATA (APPLE IOS EXAMPLE)

- Cell Phone Carrier
  - Text: Last 30-90 days
  - Calls: Last 2 Years
- Mobile Device
  - All data
  - Possible deletion
- Computers (iTunes)
  - Back-ups at different times
  - Data prior to deletion
- iCloud
  - Nightly back-ups

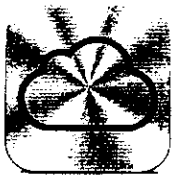


Table Search

Advanced

Chat

Go to

ID:

Source: iMessage: +15108617552

Start Time: 11/16/2013 10:30:22 PM(UTC+0)

Last Activity: 11/16/2013 10:30:22 PM(UTC+0)

Number of attachments: 0

Participants

+15108617552

Conversation

Go to

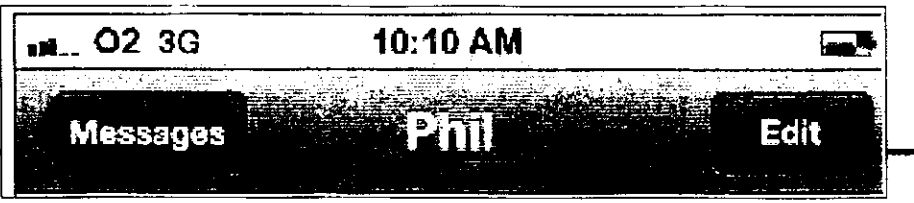
Select/Deselect...

Enter text to filter ...

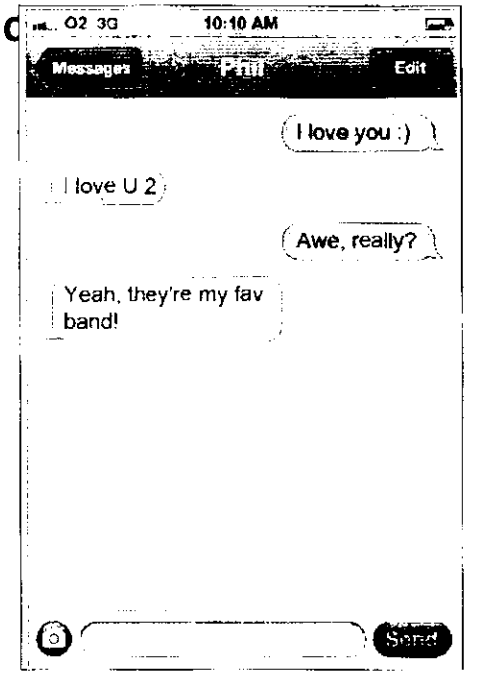
+... 11/16/2013 10:30:22 PM(UTC+0)

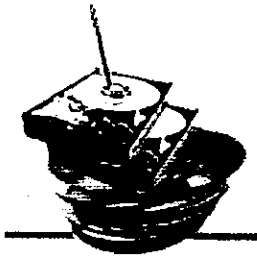
Sorry my phone was dead. How are you feeling? Better I hope

Delivered: 11/16/2013 10:30:23 PM(UTC+0)



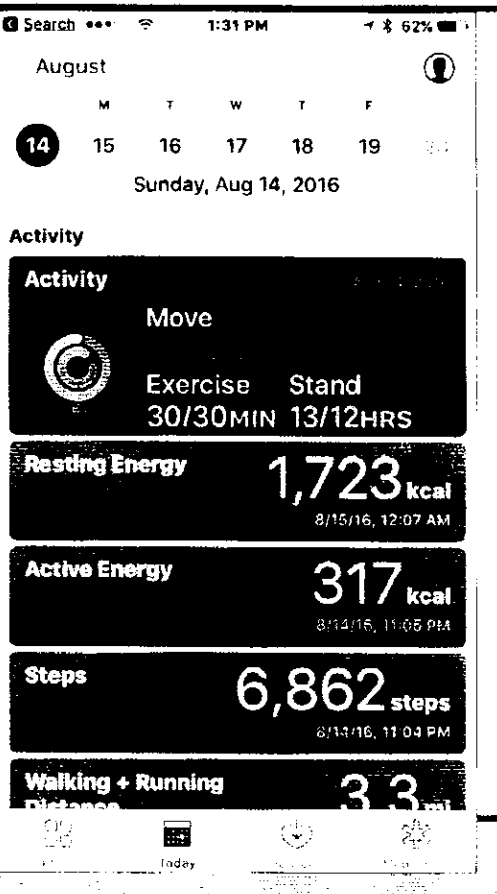
Self-Collec





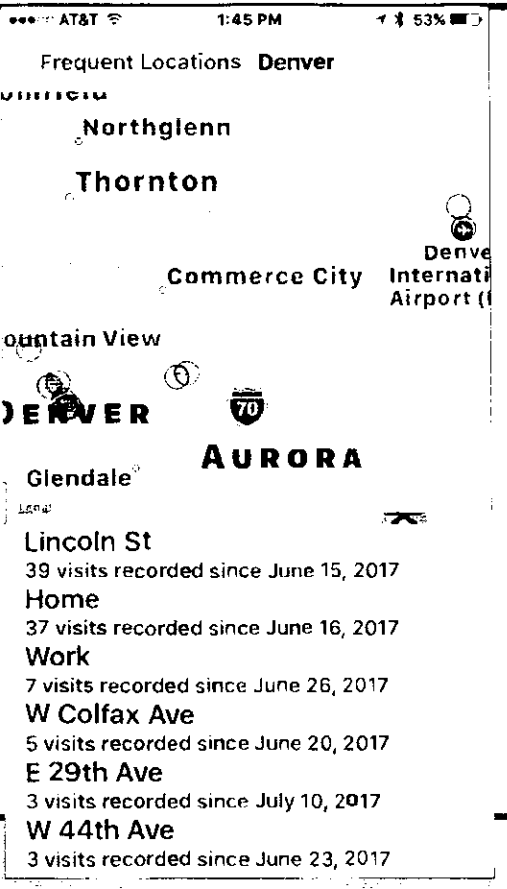
APPLICATION DATA: HEALTH KIT

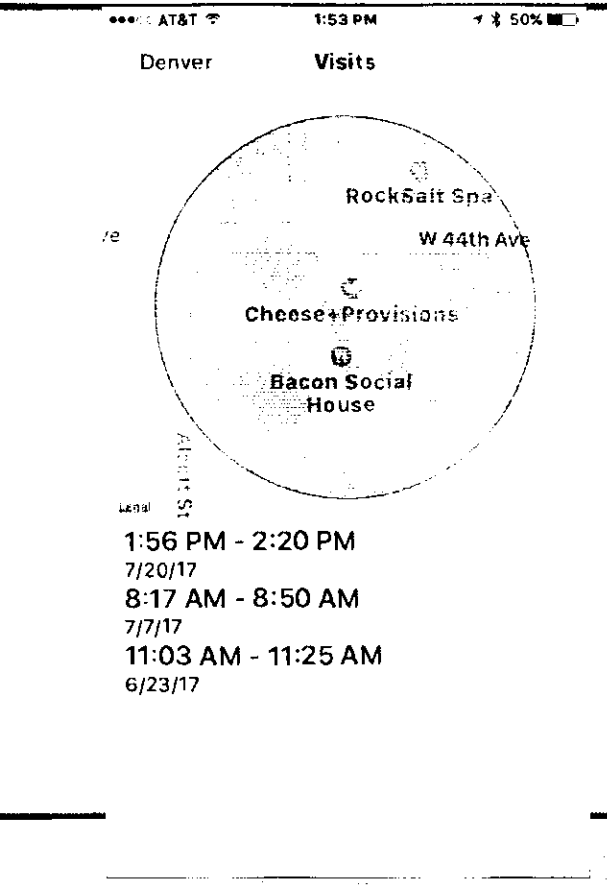
- Recorded by iPhone or watch
- Steps
- Walking/running distance
- Flights climbed
- Exercise minutes
- Heart rate
- Standing hours

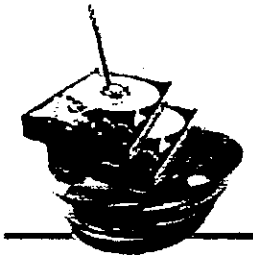


IOS LOCATION SERVICES

- On by default
- Accessed by Apps
- Improves GPS accuracy
- Crowd-sourced Wi-Fi
- Emergency calls
- Saves battery life

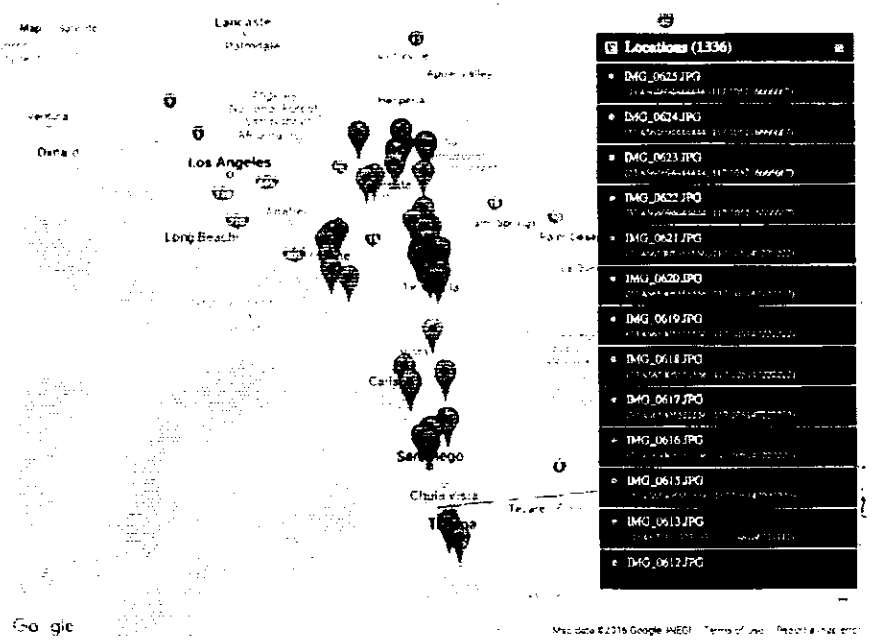


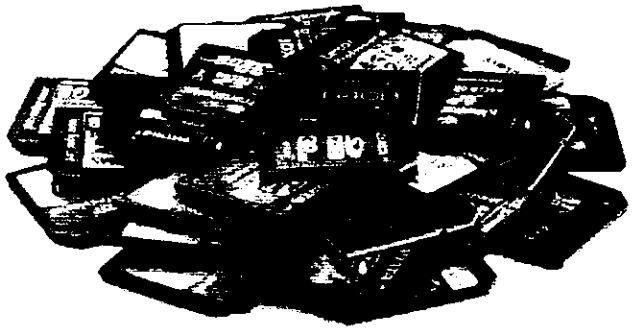




LOCATION TRACKING THROUGH PHOTOS TAKEN

- Use of photo metadata
- Filter by photos taken by device
- Extract date, time and location
- Use data to display on program

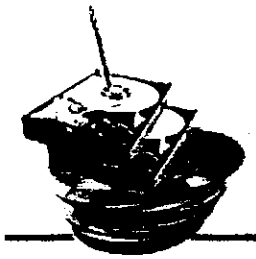




Camera:	Apple iPhone 6s
Date:	Tue 25th of July 2017
Address:	1141-1143 Co Hwy 53, Grand Lake CO 80447, USA
City:	Grand Lake , Colorado
Country:	United States
Location:	[illegible]

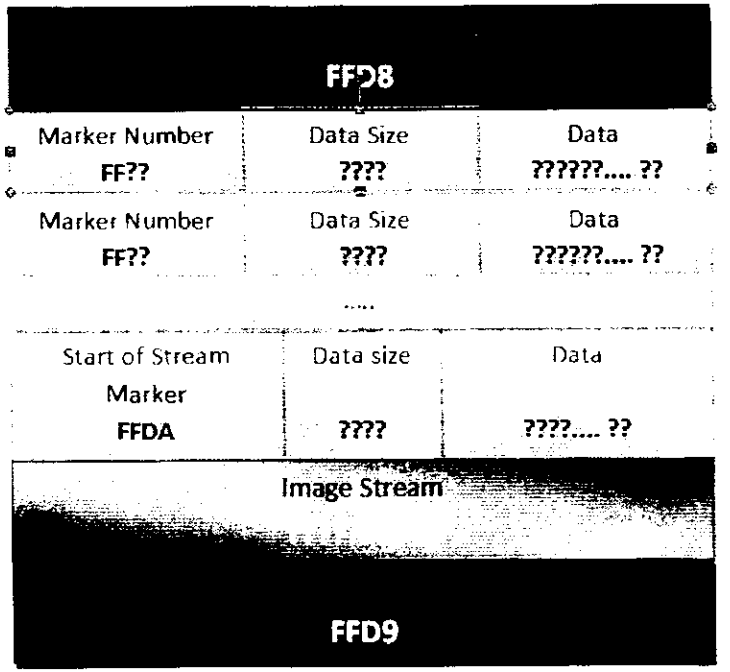
View More Details

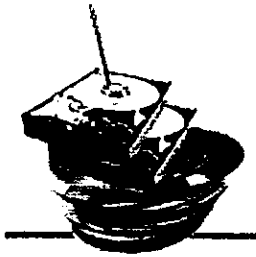
PHOTOS, EXIF METADATA



WHAT IS EXIF DATA?

- Metadata of an image file
- EXIF: EXchangeable Image Format
- Includes:
  - Make and model
  - Photo date and time
  - Lens: shutter speed, focal length, flash
  - GPS info: latitude, longitude, altitude, direction
  - Compression, file size, dimensions, ...





EXIF DATA EXAMPLE: FUGITIVE SOFTWARE TYCOON

- 11/11/2012: Neighbor death
  - "Person of Interest"
- 12/03/2012: Interview
- 12/03/2012: Article published
  - Twitter: iPhone 4s Raw Photo
- 12/05/2012: Arrested

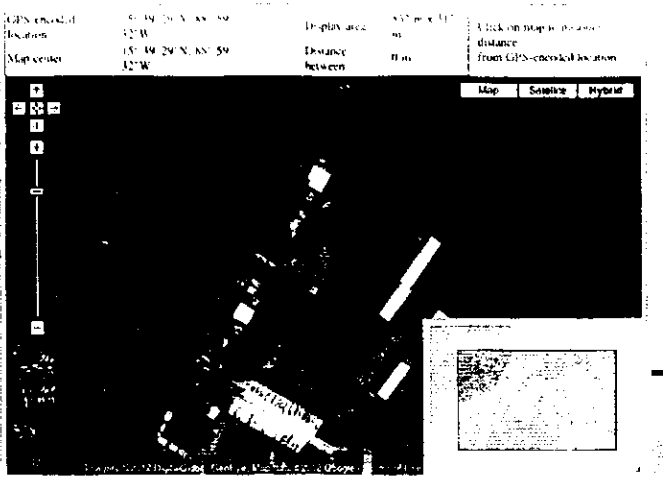
exif:GPSImgDirection: 54424/255

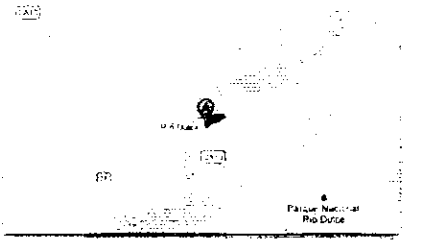
exif:GPSImgDirectionRef: T

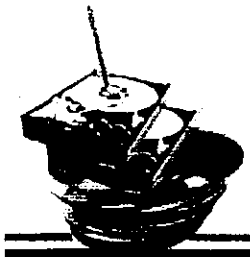
exif:GPSLatitude: 15,39,49N

exif:GPSLongitude: 88,59,53W

exif:GPSTimeStamp: 2012-12-03T18:25:26Z







EXIF EXAMPLE: HORSEBACK RIDING TRIP

PIC2MAP

Random Location | Upload Photo

Camera: Apple iPhone 7 Plus

Date: Tue 25th of July 2017

Address: Co Hwy 53, Grand Lake, CO 80447, USA

City: Grand Lake / Colorado

Country: United States

Location: 39° 58' 55.58" N, 105° 56' 19.75" W

View More Details

Map | Satellite

Map data ©2017 Google Imagery ©2017 , DigitalGlobe | 10 m | Terms of Use | Report a map error

CAMERA INFORMATION

Brand: Apple	**Model:** iPhone 7 Plus	**Lens Info:** iPhone 7 Plus back dual camera
Shutter: 1/212 (0.0047 seconds)	**F Number:** f/2.8	**ISO Speed:** ISO 20
Flash: Not Used	**Focal Length:** 6.6 mm	**Color Space:** Uncalibrat

FILE INFORMATION

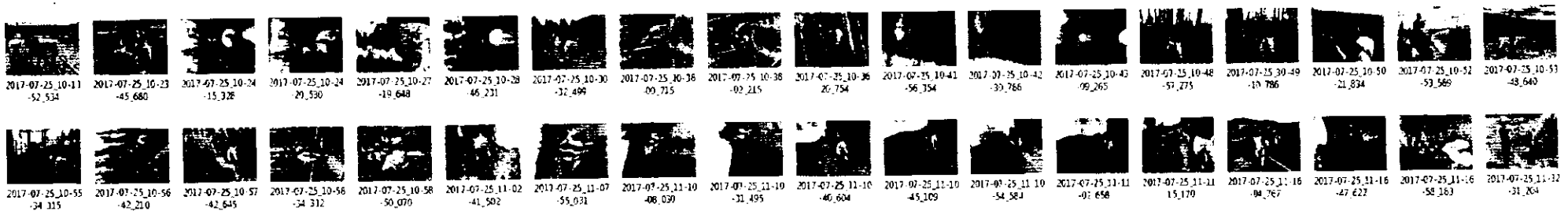
File Name: 2017-07-25_11-16-58_163.jpeg	**Image Size:** 1000 x 750 pixels	**Megapixels:** 0.8 megapixels
File Size: 167,649 bytes (0.17 MB)	**MIME Type:** image/jpeg	**Resolution:** 72 DPI

DATE & TIME

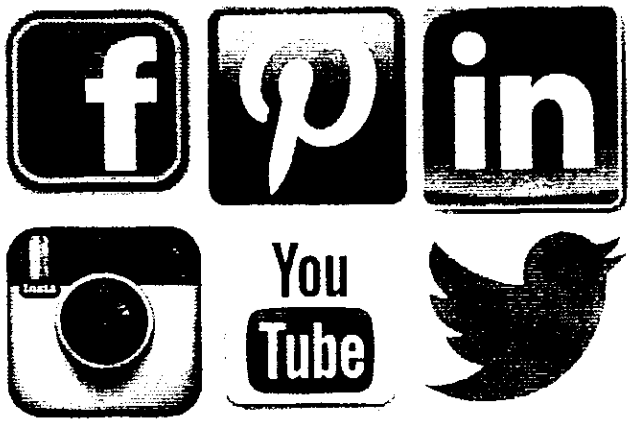
Date: 2017-07-25	**Time:** 11:16:58 (GMT -06:00)	**Time Zone:** America / Denver

GPS INFORMATION

Latitude: 39.982106	**Longitude:** -105.938819	**Lat Ref:** North
Long Ref: West	**Coordinates:** 39° 58' 55.58" N, 105° 56' 19.75"	**Altitude:** 2686m (Above Sea Level)
Direction Ref: True North	**Direction:** 167.53 Degrees	**Pointing:** South


2017-07-25_10-11
-52_534
2017-07-25_10-23
-45_680
2017-07-25_10-24
-15_328
2017-07-25_10-24
-29_530
2017-07-25_10-27
-19_648
2017-07-25_10-28
-46_231
2017-07-25_10-30
-32_499
2017-07-25_10-38
-09_715
2017-07-25_10-38
-02_215
2017-07-25_10-38
20_754
2017-07-25_10-41
-56_354
2017-07-25_10-42
-30_786
2017-07-25_10-43
-09_265
2017-07-25_10-48
-57_275
2017-07-25_10-49
-19_786
2017-07-25_10-50
-21_834
2017-07-25_10-52
-53_569
2017-07-25_10-53
-48_649
2017-07-25_10-55
-34_315
2017-07-25_10-56
-42_210
2017-07-25_10-57
-42_645
2017-07-25_10-58
-34_312
2017-07-25_10-58
-50_070
2017-07-25_11-02
-41_502
2017-07-25_11-07
-55_031
2017-07-25_11-10
-08_039
2017-07-25_11-10
-31_495
2017-07-25_11-10
-46_604
2017-07-25_11-10
-45_109
2017-07-25_11-10
-54_584
2017-07-25_11-11
-03_658
2017-07-25_11-11
15_170
2017-07-25_11-16
-04_767
2017-07-25_11-16
-47_622
2017-07-25_11-16
-58_163
2017-07-25_11-32
-31_804


20
21
22
19
16

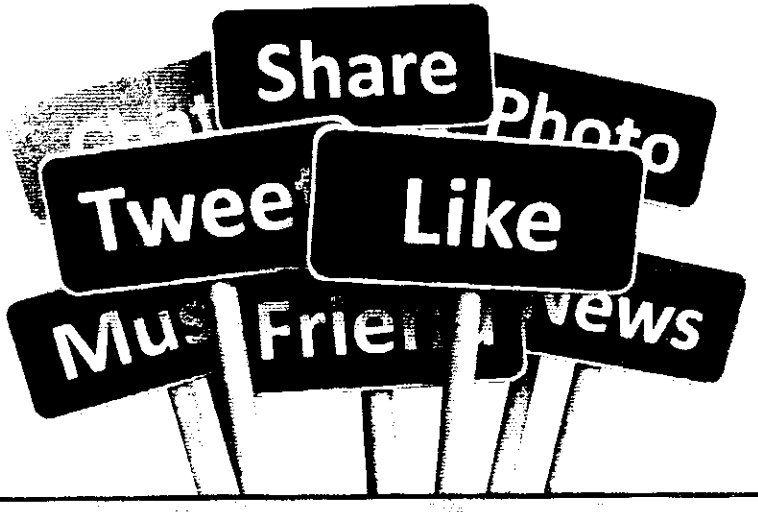


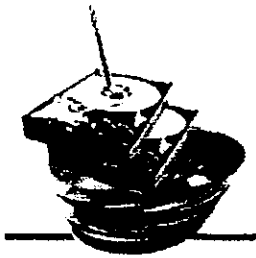
USING SOCIAL MEDIA IN DISCOVERY

What is "Social Media"?

- "Forms of electronic communication (such as websites) through which people create online communities to share information, ideas, personal messages, etc." *(Dictionary and Thesaurus | Merriam-Webster)*

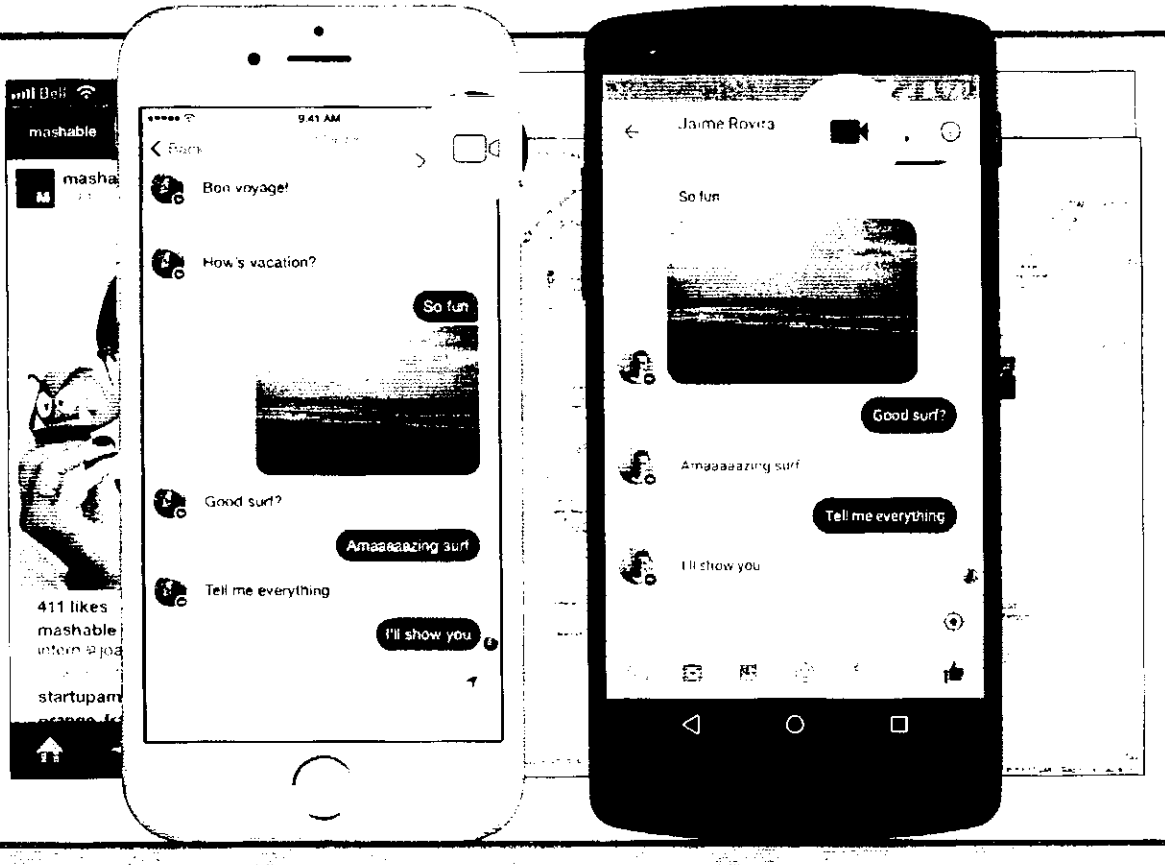
- Properties
  - Via online service
    - Facebook, Instagram, Twitter
  - Sharing content with others

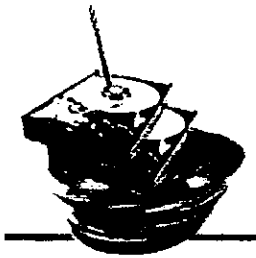




SOCIAL MEDIA EVIDENCE

- Friends
- Texts
- Photos & videos
- Location info
- Private messages





EXPECTATION OF PRIVACY

- Public
  - Profile photos
  - Comments to profile photos
- Friends of Friends
  - All photos, posts, comments
  - Timeline
- Friends
  - All photos, posts, comments
  - Timeline
- User Account
  - Hidden photos, posts, comments
  - Messages

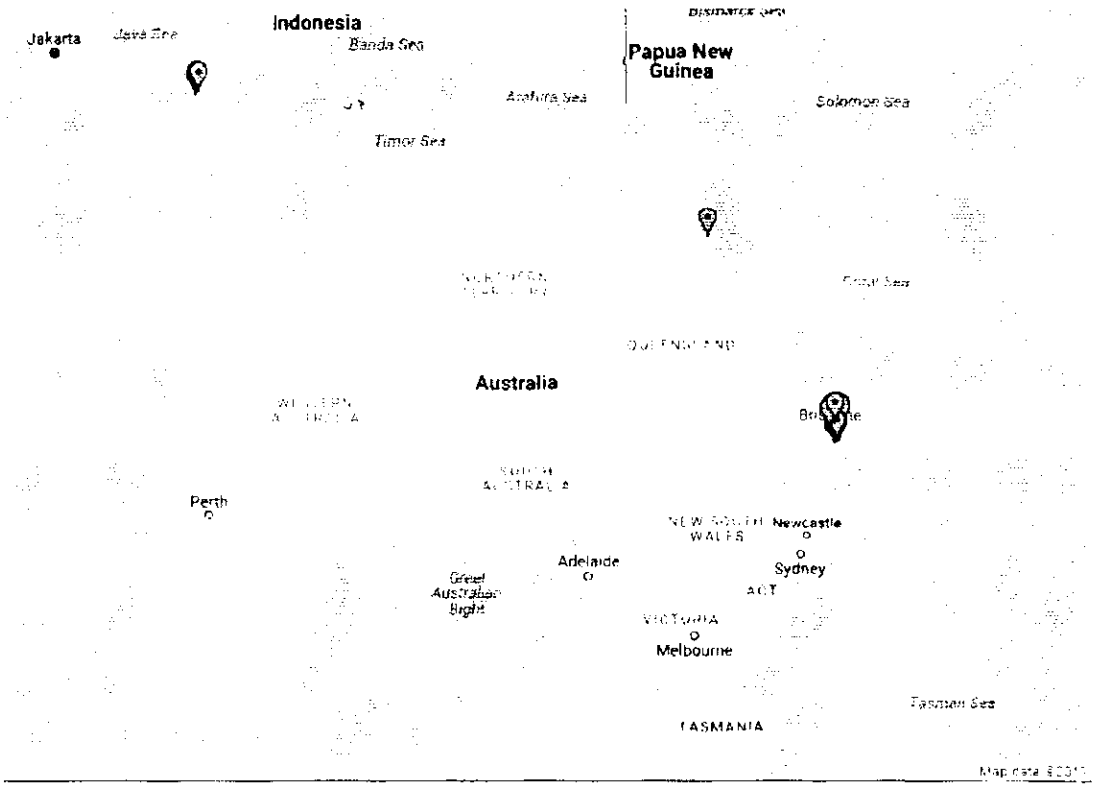
REAL LIFE EXAMPLES:
"THE ACHILLES TENDON GIRL"

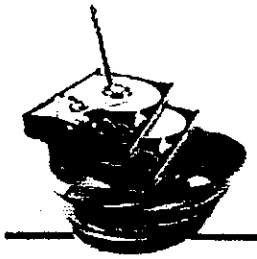
- Lifeguard
- Achilles tendon injury on the job
- Pain and suffering
- Unable to enjoy life
- Unable to move around

Social Media and Blog Posts:
"The Achilles Tendon Girl"

EMBEDDED PHOTO METADATA: *"THE ACHILLES TENDON GIRL"*

- Google Map showing travel locations, as well as dates/times the photos were taken
  - Embedded GPS coordinates in the photos on her blog





EXAMPLE OF FALSIFYING EVIDENCE

1. Go to website, e.g., Facebook
2. Go to page to be printed, e.g., wall posts
3. Print to PDF
4. Open PDF in Adobe Acrobat edit mode
5. Edit text to liking

Modified Post

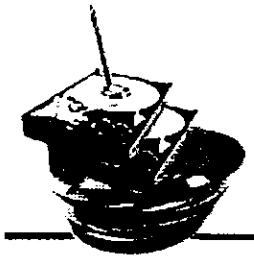
Mark Zuckerberg with Jim Shelton and Priscilla Chan.
Yesterday at 10:04am · Palo Alto, CA

Priscilla and I are excited to share with everyone that Jim Shelton is going to be moving in with us.

Last week I guaranteed Jim 1% of my Facebook stock to show appreciation for all his continuel support for his efforts in our various charitable initiatives. We look forward to providing him with other financial rewards that may include houses, cars or cold hard cash.

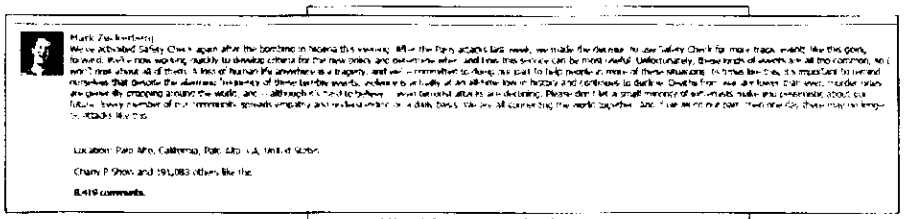
The Chan Zuckerberg Education Initiative is new, but it pulls together all...
Continue Reading

Original Post

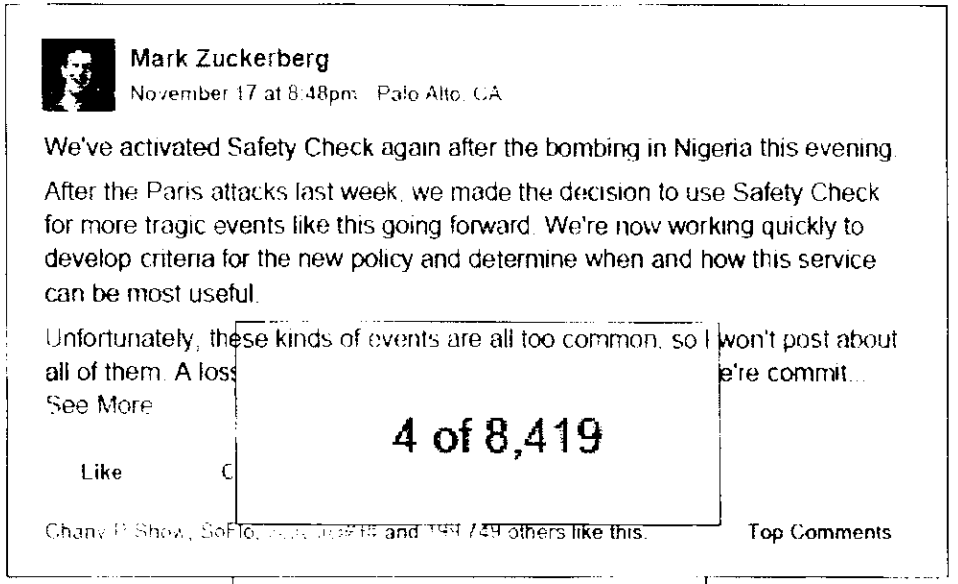


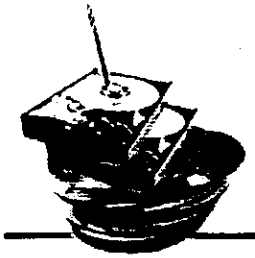
FACEBOOK PROFILE: FORENSIC VS "WEB SCRAPE"

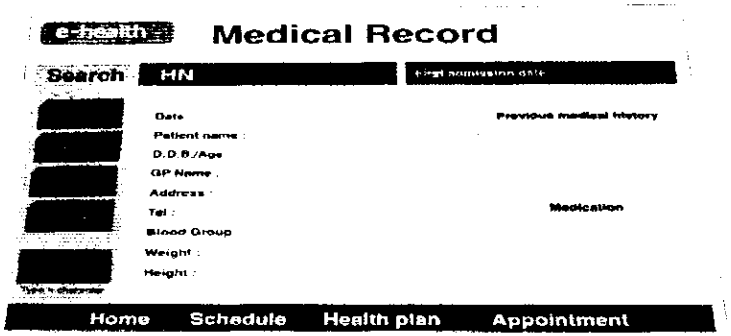
Forensic Collection

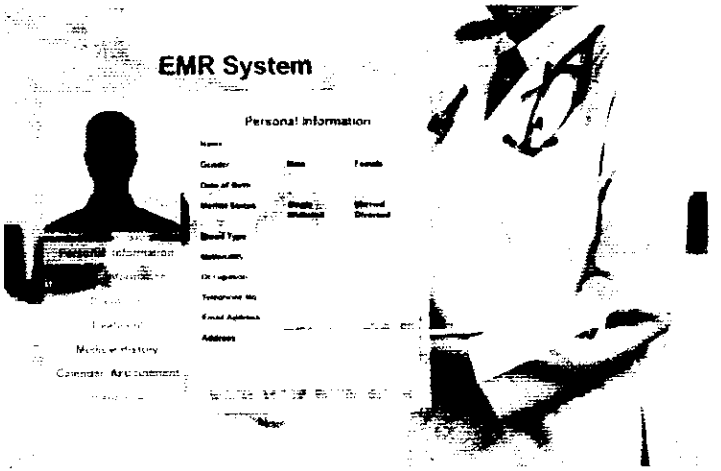


8.419 comments.

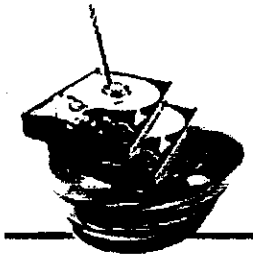






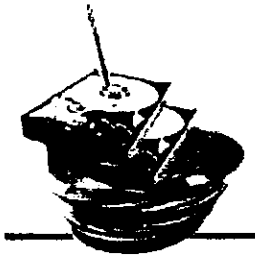


Electronic Medical Records (EMR)



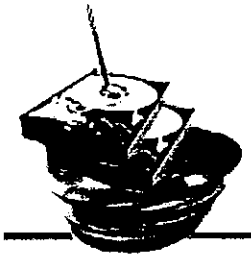
USE OF EMR META-DATA

- Submission of charts and notes
  - Back-dating, back-charting
- Viewing of records
  - Become aware of problem
- Editing of records
  - Editing, falsification
- Litigation holds
- Tracking copies of records shared



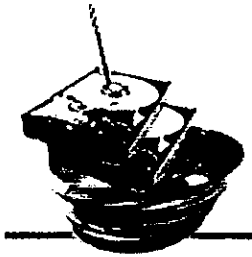
EMR METADATA

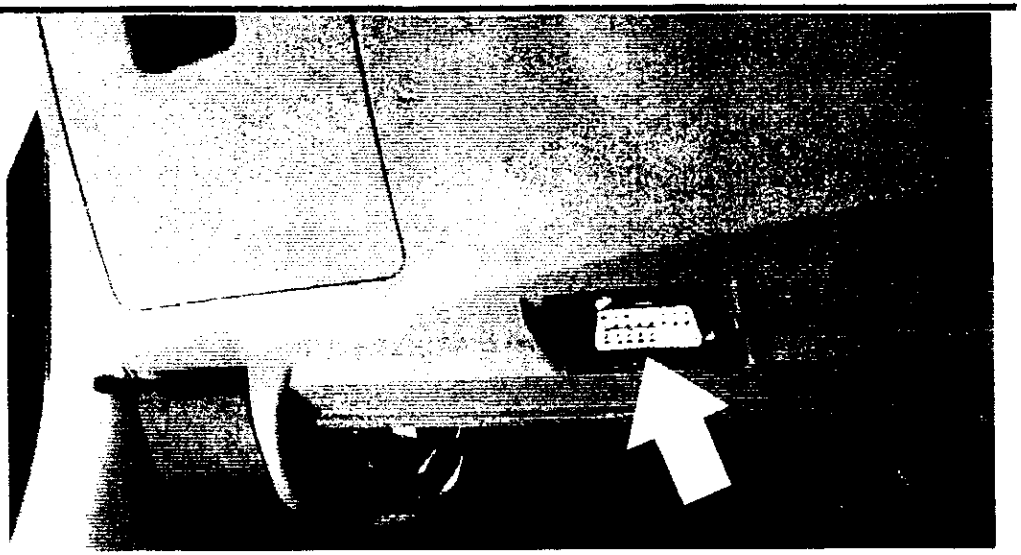
Application Metadata	Metadata Tag	Type	Length	
	Patient Account Number	Integer	9	
	Patient Last Name	Alpha	50	
	Patient First Name	Alpha	50	
	Date of Admission	Integer	10	
Document Metadata	**User name**	**Action**	**Date/time**	**Length of time**
	Smith212	View	01-13-13/0234	00:01.01
	Jones339	Create	01-14-13/1345	00:19:22
	Jones339	Edit	01-14-13/1543	00:04.43
	Corey112	Print	01-21-13/0901	00:01.16
File Metadata	**Name of Application**			
	Laboratory Information System			
	Imaging Information System			
	Radiation Information System			
Embedded Metadata				
	Versioning			
	Track Changes			



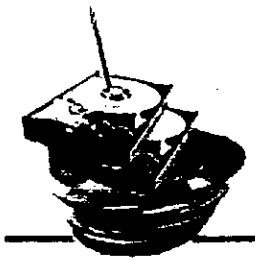
ALTERED RECORDS STORY

- Claim re: doctor's treatment of patient
- Defendant original production
  - Docs produced as PDF files and screenshots
- Plaintiff request for EMR metadata
- Evidence of viewing and modifying records after doctor became aware of potential claim



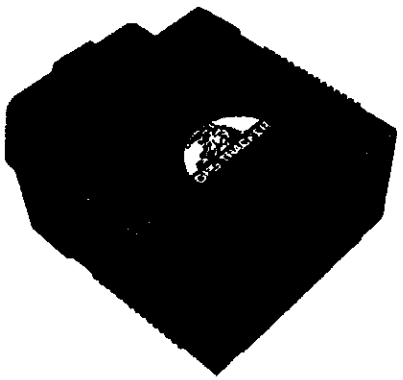


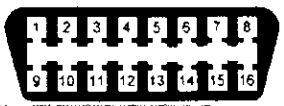
ON-BOARD DIAGNOSTICS (OBD)

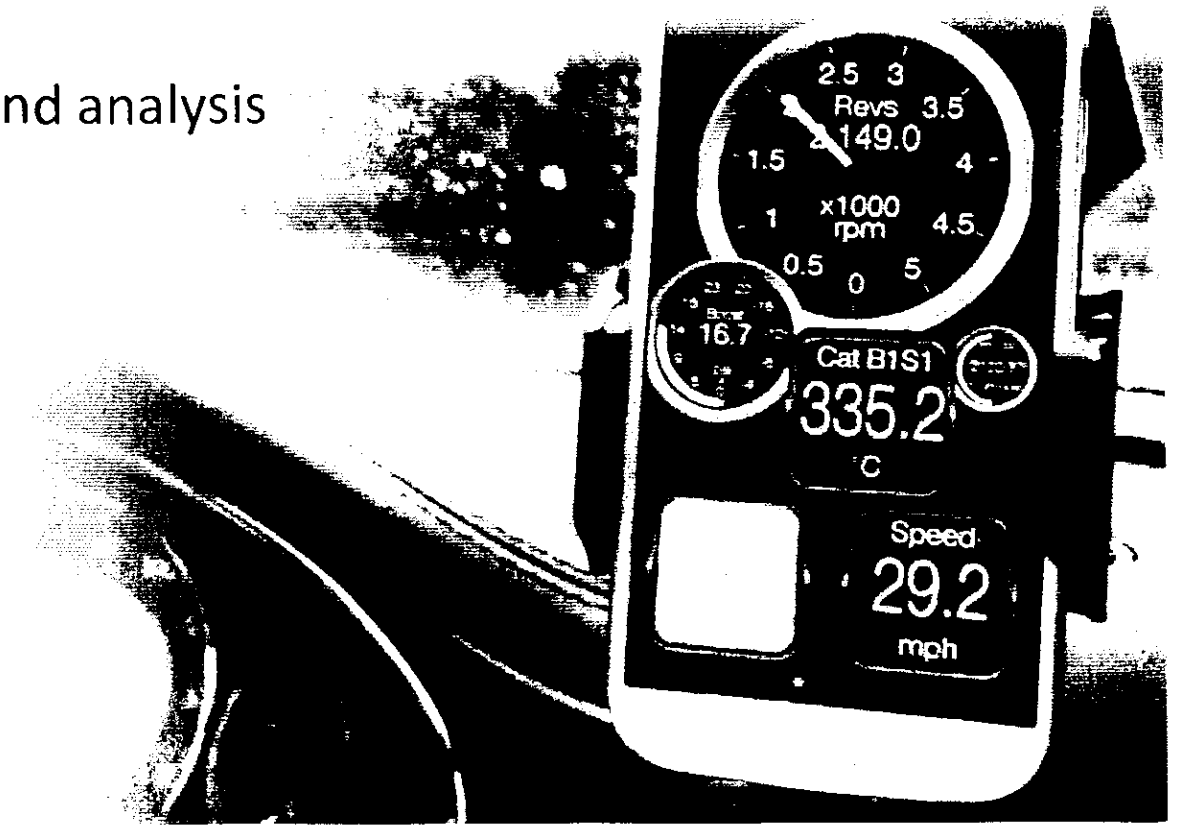


OBD APPLICATIONS

- Hand-scan tools
- Mobile device-based tools and analysis
- Emissions testing
- Data loggers
- Vehicle telematics

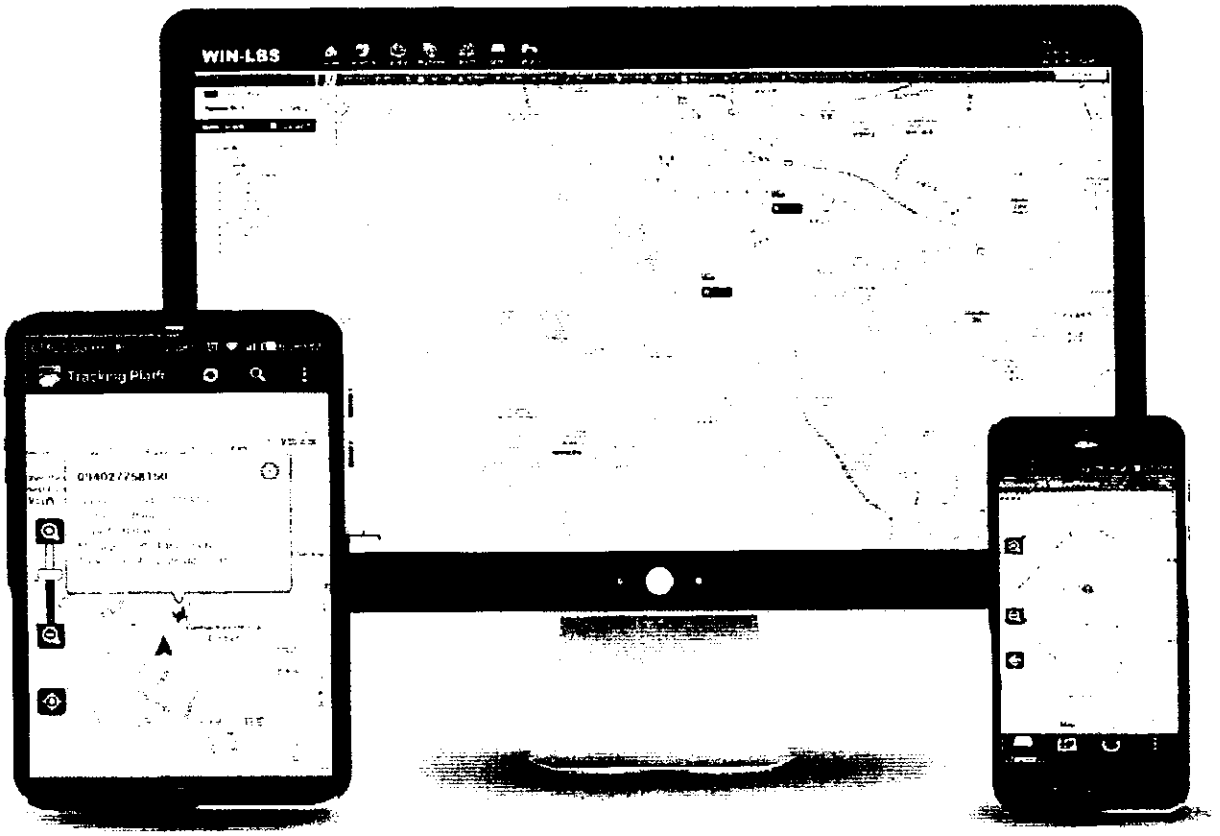


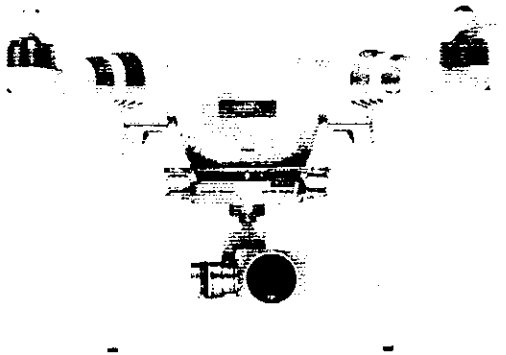




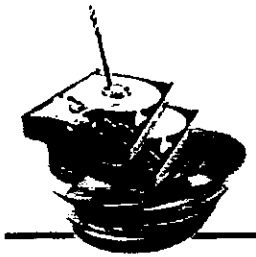
VEHICLE TELEMATICS

- Fleet tracking
- Monitor fuel efficiency
- Prevent unsafe driving
- Remote diagnostics
- Vehicle speed
- Idle times
- Over-revving



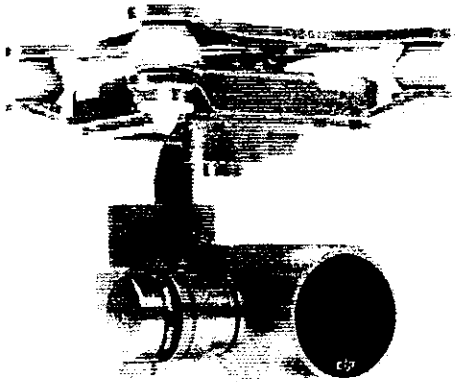


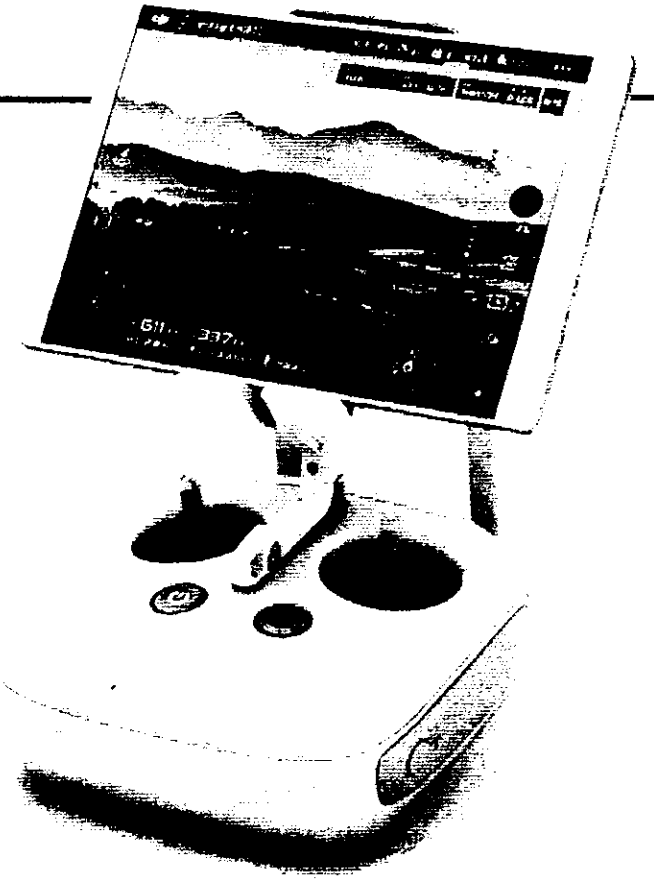
REMOTELY PILOTED VEHICLE (RPV)



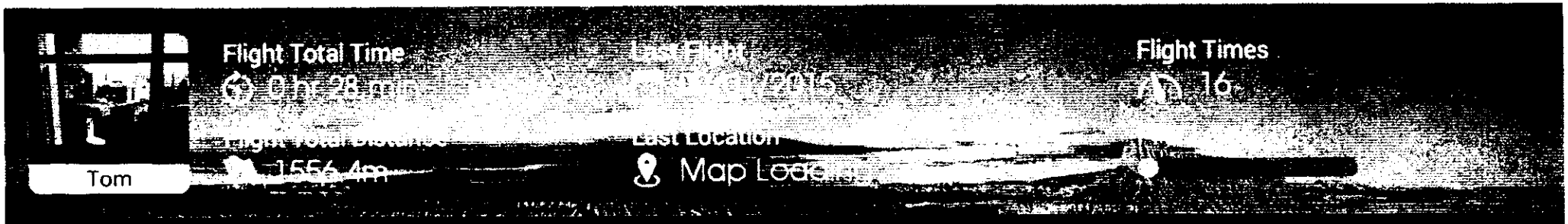
TYPES OF RPV DATA

- Telemetry flight data
- Flight path: longitude, latitude, altitude
- Pictures with EXIF data
- Video

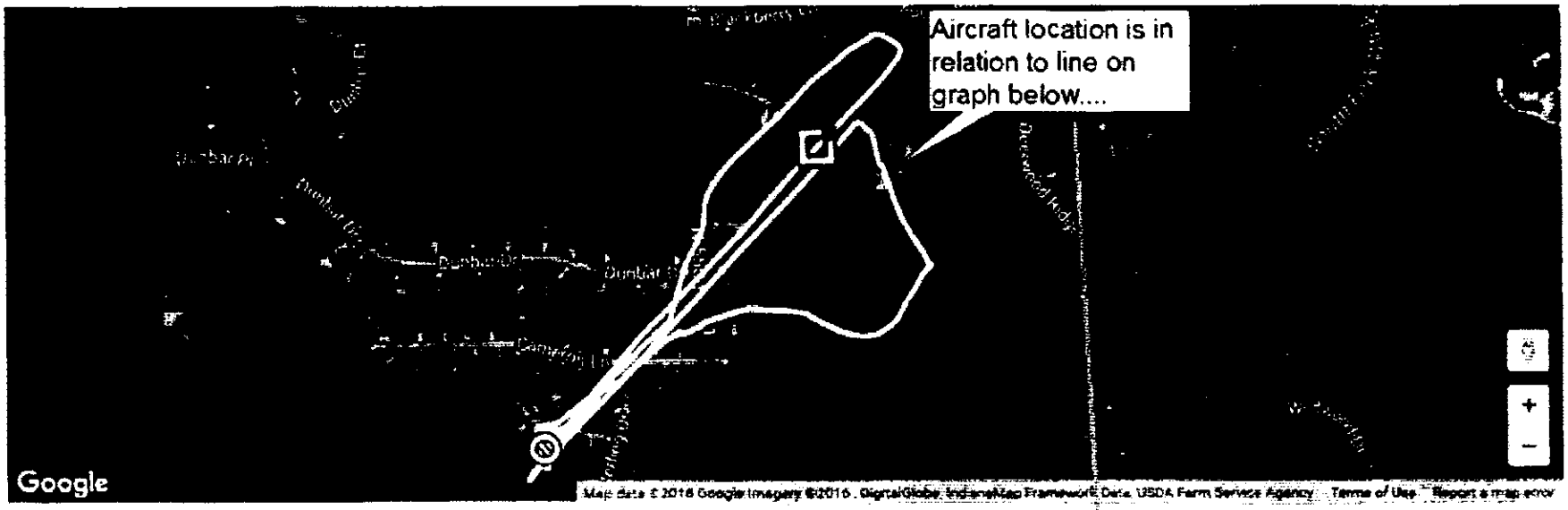




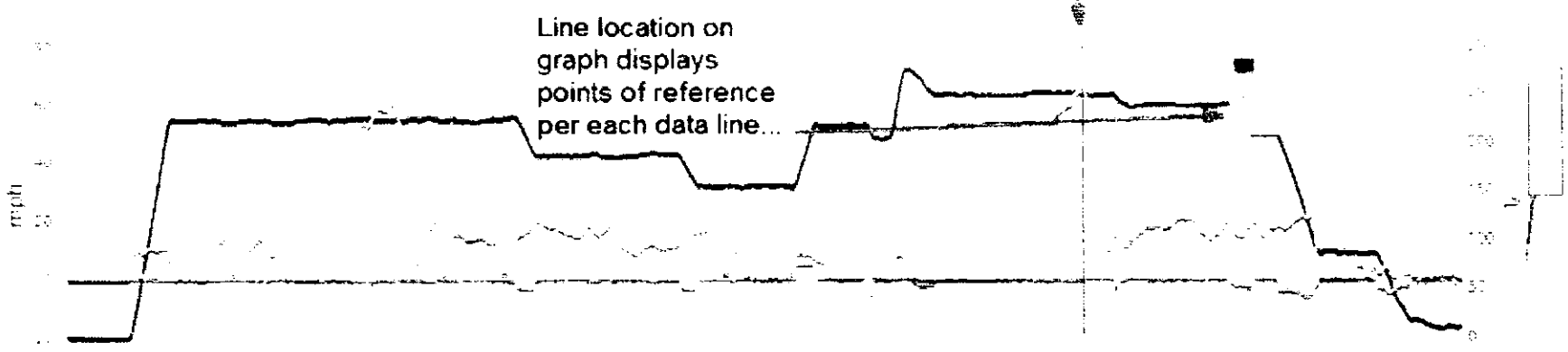
Flight Record



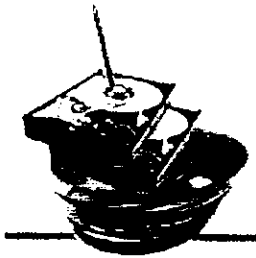
Favorite	Date	Location	Mileage	Time	Max Alt	Photos	Video	Moments
	09/01/2015	Map Loading	0.0m	14Min	31.4m	6	00:00	
	09/01/2015	ShenZhen	206.5m	1Min	18.3m	0	00:00	
	09/01/2015	ShenZhen	0.0m	1Min	18.3m	0	00:00	
	09/01/2015	ShenZhen	4.6m	1Min	25.2m	0	00:00	
	31/12/2014	Map Loading	1000.6m	12Min	226.0m	0	00:00	
	09/01/2015	HongKong	0.0m	1Min	37.4m	0	00:00	



Hide track (H) Play (K) Decrease speed (J) Normal speed (I) Increase speed (L) Loop (O)

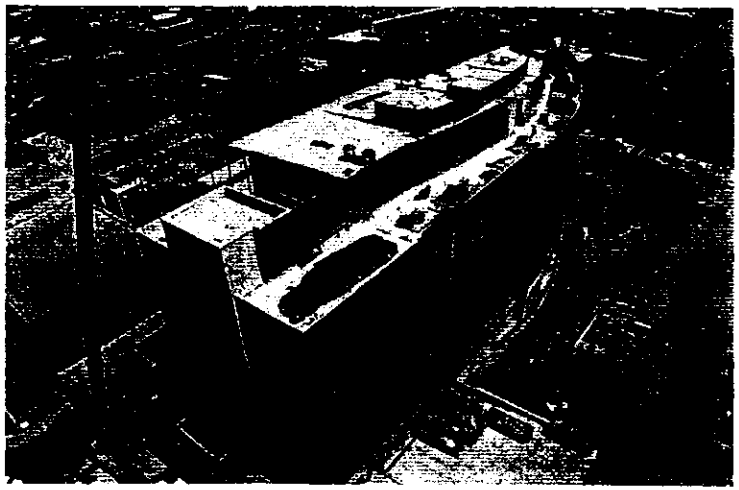


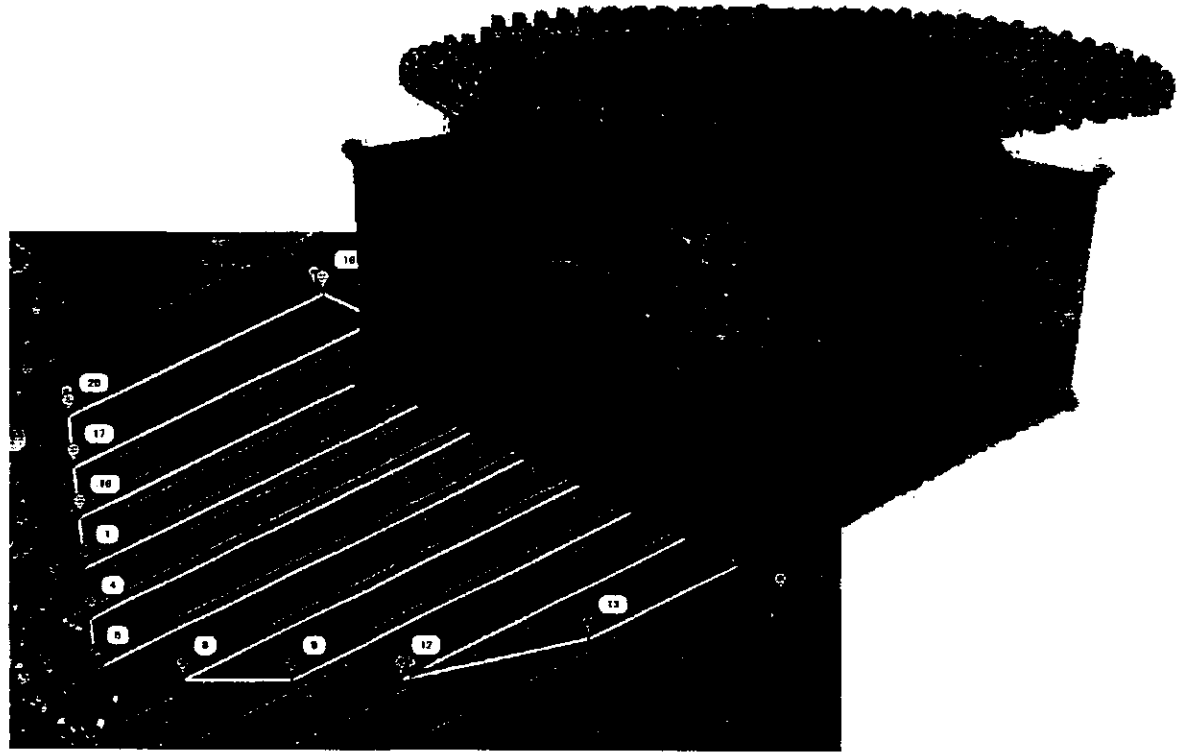
Average speed	Distance flown	Flight time	Max altitude	Max speed	Max distance
11.75 mph	19028.32 ft	00:00:35	275.62 ft	64.23 mph	2165.81 ft

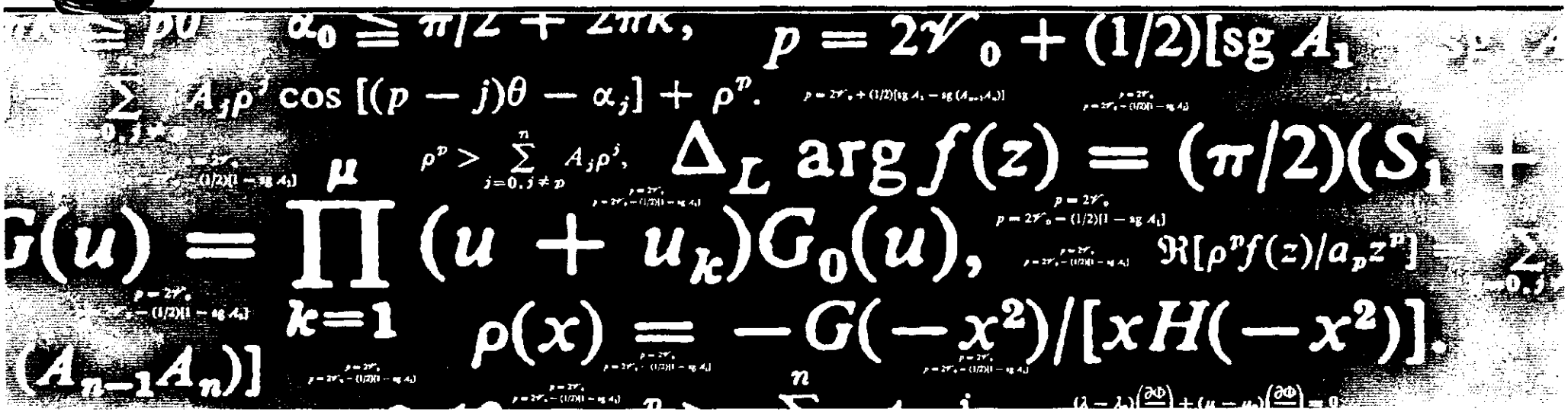


APPLICATION OF RPV CAPTURED DATA

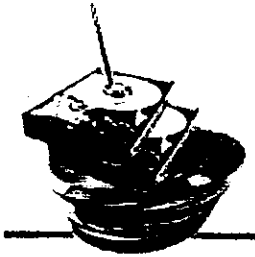
- Agriculture
- 3D Models
- Building Inspection







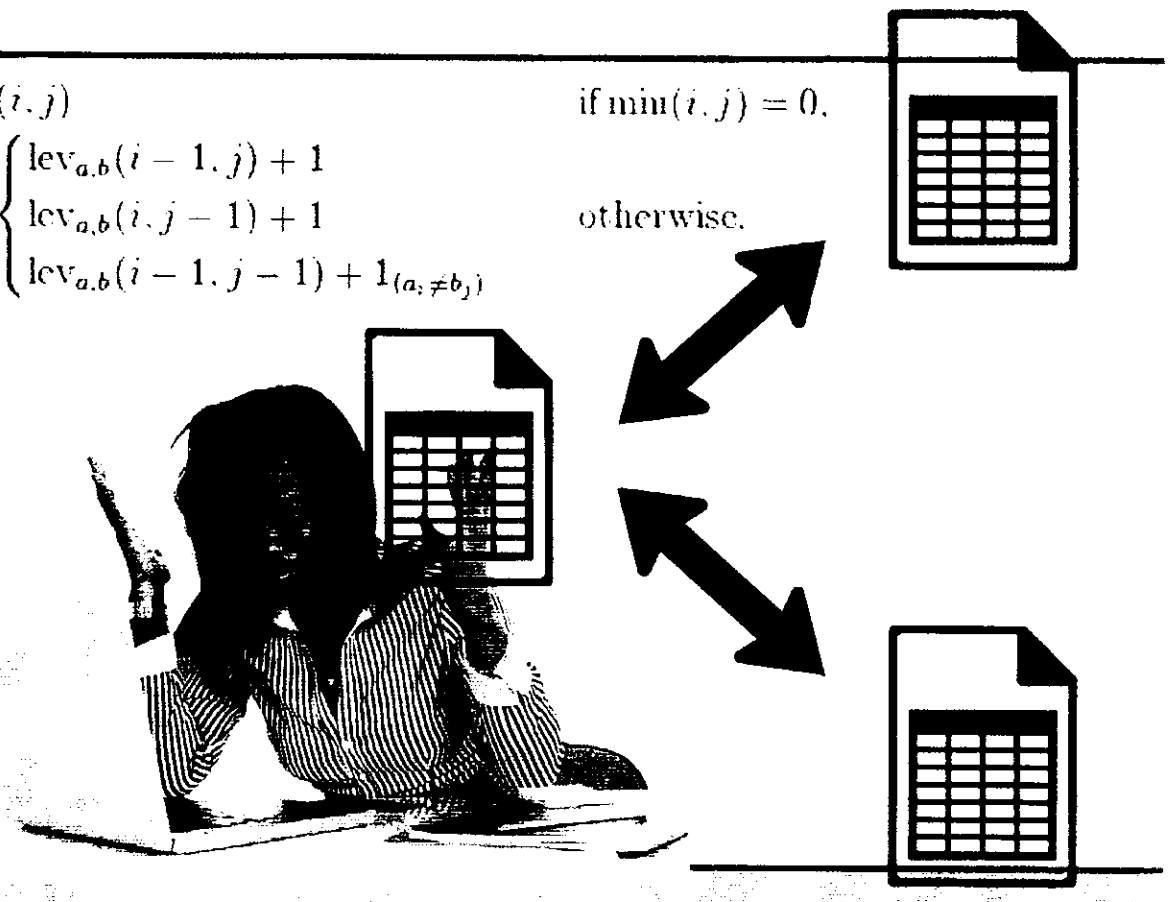
ALGORITHMIC TECHNIQUES



ALGORITHMIC TECHNIQUES

- Master List
- Customer List: A
- Customer List: B
- Challenges:
  - 1000s, spelling, abbreviations
- Options:
  - Individual search = X * Y
  - Technical solution

$$\mathrm{lev}_{a,b}(i,j) = \begin{cases} \max(i,j) & \text{if } \min(i,j) = 0, \\ \min \begin{cases} \mathrm{lev}_{a,b}(i-1,j) + 1 \\ \mathrm{lev}_{a,b}(i,j-1) + 1 \\ \mathrm{lev}_{a,b}(i-1,j-1) + 1_{(a_i \neq b_j)} \end{cases} & \text{otherwise.} \end{cases}$$



ALGORITHMIC TECHNIQUES

Master List	Closest Match	Score
3M Company	4M Company	1
A.G. Edwards Inc.	AG Edwards, Inc	0
Abbott Laboratories	John Laboratories	8
Abercrombie & Fitch Co.	Alamo & Fitchferal	23
ABM Industries Incorporated	Bob Industries	15
Ace Hardware Corporation	Ace Hardware	7
ACT Manufacturing Inc.	A.C.T. Manufacturing	3
Acterna Corp.	Acterna Corporation	6
Adams Resources & Energy, Inc.	Adams Resources Energy Inc	0
ADC Telecommunications, Inc.	Alphabet Telephone	18

DISCOVERABILITY: YOU HAVE TO KNOW HOW TO ASK

Do not bother with ESI requests that include the words: "any & all."

They are incompatible with the **proportionality rule** that was added in 2014. This rule is intended to prevent abuse & is frequently the dispositive consideration with ESI requests.

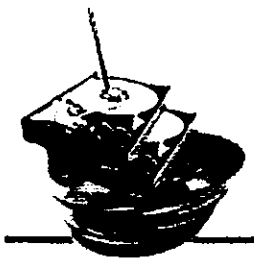
The court must determine whether the likely burden or expense of the ESI discovery outweighs the likely benefit, taking into account the amount in controversy, resources of the parties, importance of the issues to the litigation & in resolving the issues.

Ill.S.Ct. R.201(c)(3)(West 2014)

"PRESUMPTIVELY NONDISCOVERABLE"

Under the proportionality rule, the following categories of ESI are typically considered nondiscoverable:

- Deleted, "slack," "fragmented" or unallocated data on hard drives
- Random access memory (RAM)
- On-line access data;
- Data in metadata fields that are frequently updated automatically;
- Backup data that is duplicative of data available elsewhere;
- Legacy data;
- Other forms of ESI whose preservation/production requires extraordinary affirmative measures.

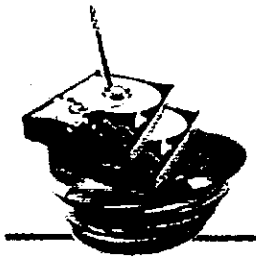


ALWAYS AN EXCEPTION

Because those categories of ESI have been declared "presumptively nondiscoverable," a party seeking such information bears the burden "to justify the making of an exception." *Carlson v. Jerousek, 2016 IL App (2d) 151248, ¶49.*

The following factors are relevant in this regard:

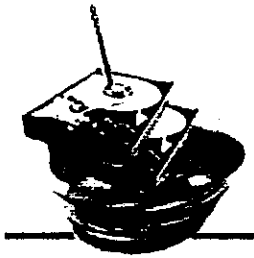
- A compelling need for the information;
- The information is not available from other sources;
- The requesting party is using the least intrusive means to obtain the information. *Id.*



DON'T FORGET ABOUT RULE 214

Supreme Court Rule 214 was also amended to require a party's production of ESI & to require the producing party to organize responsive documents "in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms."

BEWARE: Failure to organize documents in this way, or mixing nonresponsive materials with the requested documents, "constitutes a discovery abuse subject to sanctions under Rule 219." *Ill.S.Ct. R. 213, Committee Comments (West 2014).*

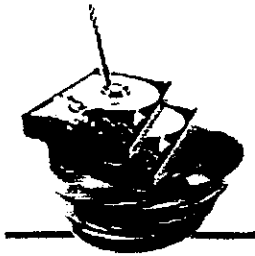


PRIVACY CONCERNS MAY BE UNPERSUASIVE

Parties frequently object based on privacy concerns when social media content is requested. However, this is largely a losing argument.

Why? Because there is no expectation of privacy when content is posted on social media platforms.

As a result, not all "invasions" of privacy are forbidden. Only *unreasonable* invasions of privacy are verboten. *Carlson v. Jerousek, 2016 IL App (2d) 151248, ¶ 35.*



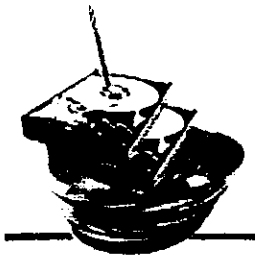
REASONABLENESS = RELEVANCE

"Reasonableness is a function of relevance."

Kunkel v. Walton, 179 Ill.2d 519, 538 (1997).

A party who wants an opponent's social media information must make a threshold showing of relevance, which simply means that the information is reasonably calculated to lead to the discovery of admissible evidence.

Although this is a liberal standard, fishing expeditions are not allowed & the rules "do not permit the requesting party to [aimlessly] rummage through...files for helpful information." *Carlson at ¶ 29.*



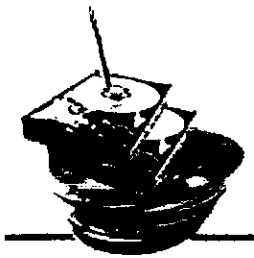
CARLSON V. JEROUSEK

YOU MUST KNOW THIS CASE!

It is the only reported case in Illinois interpreting the proportionality rule applicable to ESI.

FACTS: Auto accident case. Plaintiff claimed personal injuries, including cognitive deficits/loss of normal life. Defendants requested the following information:

- Name, web address & user name for all blogs, online forums & social networking sites to which plaintiff belonged since the accident;
- Internet/email, telephone & cell phone providers;
- Internet/email passwords & all login information;
- All ESI relating to issues in the lawsuit;
- Identification of any destroyed/deleted documents responsive to the requests.

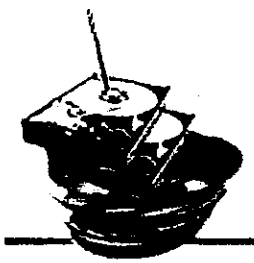


CARLSON V. JEROUSEK

Because plaintiff worked as a computer analyst, defendants also requested inspection of any computers or electronic devices he used, including his work computer, in order to assess his claims of cognitive impairment.

Due to suspicion plaintiff may have researched symptoms of brain injury on the Internet, defendants also requested ability to review his history of Internet searches since the accident, "time stamps" for work-related tasks & metadata.

Defendants also requested information about extent of plaintiff's computer gaming & games scores.

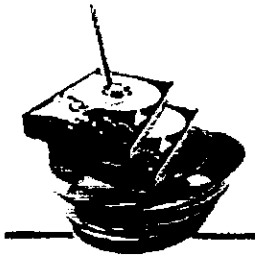


CARLSON V. JEROUSEK

The trial court ultimately ordered forensic imaging of several computers, including the work computer owned by plaintiff's employer. Defendants proposed having their expert search all hard drives, catalogue the results & prepare an executive summary of the findings.

REVERSED BY THE APPELLATE COURT

Illinois rules contain "no provision allowing the requesting party to conduct its own search of the responding party's files – regardless of whether those files are physical or electronic." *Id. at ¶ 53.*



EXCEPTIONS?

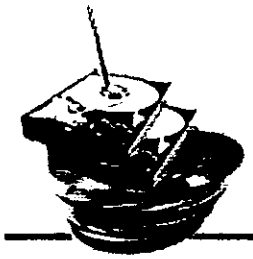
Although the Appellate Court characterized the forensic imaging order as an "inversion of traditional discovery protocol," it noted this "might be appropriate in rare circumstances," such as:

- Where the computer itself is directly involved in the litigation; or
- Where there has been a significant history of "demonstrated noncompliance." *Carlson at ¶ 55-56.*

ADMISSIBILITY

Must understand difference between computer-generated & computer-stored evidence. They have different foundational requirements.

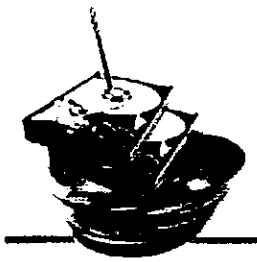
"Records directly generated by a compute are admissible as representing the tangible result of the computer's internal operations. In contrast, printouts of computer-stored records constitute statements placed into the computer by out-of-court declarants & cannot be tested by cross-examination and, therefore, are inadmissible absent an exception to the hearsay rule." *Anderson v. Alberto-Culver USA, Inc., 337 Ill.App.3d 643, 667 (1st Dist., 2003).*



EXAMPLES

Computer-generated: Cell phone records, GPS receiver records, black box readings, billing data generated instantaneously by a computer.

Because these records are not dependent on observations or reporting of a human declarant, evidentiary foundation only requires proof that the recording device was accurate & operating properly when evidence was created. *Bachman v. General Motors Corp., 332 Ill.App.3d 760, 789 (4th Dist., 2002).*

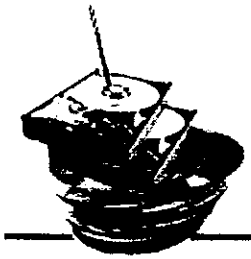


EXAMPLES

Computer-stored: Word processed documents, spreadsheets, etc.

Business records exception to hearsay rule can apply if 1) the electronic computing equipment is standard; 2) the input is entered in the regular course of business reasonably close in time to the event recorded; & 3) testimony establishes that the source of the information, method & time of preparation indicate trustworthiness & justifies its admission. *Aliano v. Sears, Roebuck & Co.; Ill.R.Evid. 803*

NOTE: If the evidence was produced by human input obtained from original documents, those documents must be made available & proponent must be able to provide testimony about the facts within them from a competent witness who has seen the originals.



DON'T FORGET: SILENT WITNESS RULE!

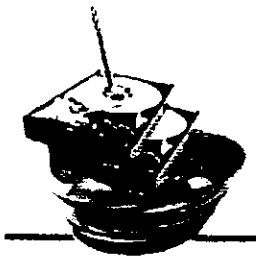
This rule is triggered where automatic devices such as cameras or surveillance systems are involved & produce videotapes, CDs or DVDs.

Holds that "a witness need not testify to the accuracy of the image depicted in the photographic or videotape evidence if the accuracy of the process that produced the evidence is established with an adequate foundation." *People v. Taylor, 2011 IL 110067, ¶ 32.*

WHAT IS ADEQUATE FOR SILENT WITNESS RULE?

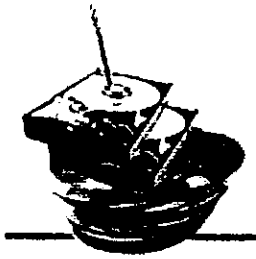
The Illinois Supreme Court approved these "nonexclusive" factors:

1) The device's capability for recording/general reliability;
2) Competency of the operator;
3) Proper operation of the device;
4) Showing the manner in which the recording was preserved (chain of custody);
5) Identification of the persons, locale or objects depicted; and
6) An explanation of any copying or duplication process.



LEGISLATIVE DEVELOPMENTS

- **Geolocation Privacy Protection Act** (HB 3449) – Passed on June 27, 2017 & awaiting Governor Rauner's signature. Requires notification to consumers that their geolocation data is being collected & used. Violations may be prosecuted by Attorney General or State's Attorneys under the Consumer Fraud & Deceptive Business Practices Act. Does not apply to actual contents of any communication.



LEGISLATIVE DEVELOPMENTS

- **Right to Know Act (SB 1502)** – Received 3rd reading in the Senate on May 4, 2017 & sent to the House, where it received 2nd reading. Re-referred to Rules Committee on July 8, 2017. Provides that operators of commercial websites/online services that collect personally identifiable information about customers who use/visit the site through the Internet must notify them of its information sharing practices & provide method to request specific information shared. Creates private cause of action to customers whose rights are violated under the Act.

THE HUNT FOR ESI: EVIDENCE HIDING IN PLAIN SIGHT

Presented By:

Judge Lynn M. Egan

Trent Walton CCE, ACE

National Director of Legal Technology

Phone: 720.878.3913

Email: twalton@uslegalsupport.com