GETTING DATA FROM 3RD PARTIES – PERILS AND CHALLENGES

SAMMY FORD, IV, *Houston*
Ahmad Zavitisanos Anaipakos Alavi & Mensing

PETER S. VOGEL
Gardere Wynne Sewell LLP
1601 Elm Street, Suite 3000
Dallas, Texas 75201
EMAIL: pvogel@gardere.com

State Bar of Texas
TECHNOLOGY FOR LITIGATORS
October 25, 2016
Houston

CHAPTER 6

Sammy Ford IV has tried over 20 cases before judges, juries, and arbitrators in the last five years. He represents companies and individuals around the country in all manner of civil matters, including business torts, securities and consumer class actions, and catastrophic personal injury cases. He is board certified in Personal Injury Trial Law by the Texas Board of Legal Specialization.

Mr. Ford currently works at Ahmad, Zavitsanos, Anaipakos, Alavi & Mensing. He previously worked at Susman Godfrey and Abraham, Watkins, Nichols, Sorrels, Agosto & Friend. He clerked for the Honorable Jerry E. Smith of the U.S. Court of Appeals for the Fifth Circuit.

He graduated with honors from the University of Texas School of Law in 2007. While there, he served as Development Editor of The Review of Litigation and as Chair of the Career Services Committee of the Thurgood Marshall Legal Society. Mr. Ford participated in the school's first Supreme Court Clinic and was on a team that convinced the U.S. Supreme Court to review a client's case during a term in which the Court agreed to hear only 78 of the 8,517 cases filed.

Mr. Ford is a native Houstonian who attended St. Thomas High School where he currently serves on the board. He attended Harvard University and graduated with high honors, magna cum laude, in 2004. At Harvard, he served as Historian of the Harvard Political Union, the College's debating society, and as Secretary of Harvard CHANCE, a group dedicated to mentoring and tutoring students from Cambridge Rindge and Latin School.

He is active in the community as a member of the local and state bar associations and the local, state, and national trial lawyer associations. Mr. Ford is a member of the State Bar's Computer and Technology Section Council, and numerous committees of the Houston Bar Association.

PETER S. VOGEL

GARDERE WYNNE SEWELL, LLP
1601 ELM STREET, SUITE 3000, DALLAS, TEXAS 75201
EMAIL: pvogel@gardere.com Telephone: 214-999-4422 TWITTER: @PETERSVOGEL Blog: VogelITlawBlog.com

As a lawyer for the more than 30 years, Peter S. Vogel combines his technical and business background with his legal expertise to help companies with IT, Cyber intrusion, and Internet litigation, dispute resolution, and contract negotiation. Peter has been involved with the IT industry, Internet, and electronic data for his entire career. Prior to practicing law he worked as a mainframe programmer, systems analyst and management consultant for companies acquiring IT and related services, and received a Masters in Computer Science.

Peter's clients often seek his advice about practical business issues relating to IT and the Internet, which often include cyber intrusions, colocation sites, cloud solutions, ERP implementation projects, website business management, outsourcing, software patents, copyrights, and trade secret protection. Because he is a seasoned IT professional with an accounting and marketing background, Peter also often advises clients about financial and marketing issues regarding IT and the Internet. His experience as an Adjunct Professor in the Law of eCommerce keeps him current on the fast moving evolution of the cyber intrusions and the Internet. He writes a monthly legal column for www.eCommerceTimes.com, and is often quoted in the media about Internet issues and crises. Peter's blog on the Internet, IT, and eDiscovery is widely recognized for timely topics and thought-provoking ideas: www.vogelitlawblog.com.

Peter chairs both the Electronic Discovery Group and the Internet, eCommerce, & Technology Team at GARDERE– where he guides clients through the legal, technology and business mazes of electronic evidence, cyber security & insurance, intellectual property, contracts, government regulation, and litigation. He assists many clients with ESI (Electronically Stored Information) issues and related creation, development and implementation of records retention policies.

Because of his unique background and expertise, Peter is often appointed as a Special Master to assist Courts throughout the US with eDiscovery & ESI, Internet, eCommerce, Intellectual Property, and IT matters. Peter is a Co-Founder of the American College of e-Neutrals and a Board Member and Fellow of the Academy of Court Appointed Masters. The Judges in the US District Court for the Western District of Pennsylvania appointed Peter to the E-Discovery Special Master Panel. He also serves as a court ordered Mediator in eDiscovery & ESI, Internet, eCommerce, intellectual property, and computer technology litigation. For more than 20 years Peter has served as an Arbitrator for technology disputes.

Peter has also devoted a substantial amount of time and energy serving government agencies and non-profit organizations by addressing their computer, Social Media, and Internet issues. Peter:

- Served as Founding Chair for 12 years of the TEXAS SUPREME COURT Judicial Committee on Information Technology whose mission is to put Internet on the desktops of all 3,200 judges in Texas and implement state eFiling. www.courts.state.tx.us/jcit
- Served on the Texas Task Force for the Uniform Electronic Transaction Act (UETA)
- Examined computer election systems for 13 years for the Texas Secretary of State

In 1994 Peter was President of the DALLAS BAR ASSOCIATION and also served on the Board of Directors of the STATE BAR OF TEXAS, where he served as Founding Chair of the Computer & Technology Section. Peter teaches courses on eDiscovery and the Law of eCommerce as an Adjunct Professor at the SMU DEDMAN LAW SCHOOL, and is on the founding Board of Advisors of the SMU Computer Law Review and Technology Journal.

The STATE BAR OF TEXAS gave Peter the Gene Cavin Award for Excellence in Continuing Legal Education in 2013, and a Lifetime Achievement Award for Promoting Technology in the Law in 2004. In addition, Peter is regularly recognized as one of America's Leading Business Lawyers in CHAMBERS, a Best Lawyer in America, a Top Lawyer in Dallas, and a Texas Super Lawyer.

Below is a listing of some recent presentations by Peter S. Vogel
Internet, Information Technology, and eDiscovery Speeches, Webcasts, and Podcasts:

"Internet Privacy and Cybersecurity in 2016," AAA-CPA South Texas Chapter, September 2016, Houston.

PANEL: "Cyber Risk for Clients and Lawyers," State Bar of Texas, August 2016, WEBCAST.

"Internet Privacy and Cybersecurity in 2016," AAA-CPA North Texas Chapter, August 2016, Dallas.

"Legal Ethics to Help Clients (and Law Firms) Deal with Cyber Attacks," Dallas Bar Association, July 2016, Dallas.

"Ethics & Honesty in IT & IP," AITP Dallas Chapter, July 2016, Dallas.

"How Special Masters Can Help in Complex Cases- Particularly IT & eDiscovery Dispute," Dallas Area Paralegal Association, June 2016, Dallas.

PANEL: "Responding to Data Breaches to Minimize Impact," Legal Tech West, ALM, June 2016, San Francisco.

"Internet Privacy and Cybersecurity in 2016," Stonebriar Mens Breakfast Club, June 2016, Frisco.

"eDiscovery from 3rd Parties," 29th Annual Advanced Evidence & Discovery Course, State Bar of Texas, May 2016, San Antonio.

"Cyber Legal Risks are Everywhere!," Dex Media Lunch and Learn, May 2016, DFW Airport.

THOUGHT LEADER: Digital Transformation, Cloud Security Challenges in 2016, & Threats to Digital Assets, Private Sector CISO & CIO Assembly, The Millennium Alliance, May 2016, Dallas.

"Data Breach: Not if, but When," Gardere, April 2016, WEBCAST.

PANEL: "Cybersecurity for Hotels," Gardere, April 2016, WEBCAST.

"Ethical Issues for Lawyers using the Internet - Including Social Media and the Cloud," Dallas Association of Law Librarians, April 2016, Dallas.

"eDiscovery from 3rd Parties," 29th Annual Advanced Evidence & Discovery Course, State Bar of Texas, April 2016, Dallas.

PANEL: "The Challenge of Enterprise Security Today and Into the Future," CIO Executive Leadership Summit, HMG, April 2016, Dallas.

PANEL: "2015 Rule Changes: Impact on e-Discovery (and e-Neutrals)," Annual Meeting, Academy of Court Appointed Masters, March 2016, Atlanta.

"Legal Issues facing the CIO in 2016 and Beyond," IT Leadership Business Technology Breakfast, March 2016, Dallas and Fort Worth.

PANEL: "The Challenge of Enterprise Security Today and Into the Future," CIO Executive Leadership Summit, HMG, March 2016, Houston.
PANEL: "eDiscovery: What Every Arbitrator Needs to Know," Panel Conference, American Arbitration Association, February 2016, New Orleans..

"2016 Update - Helping Clients Do Business on the Internet Ethically," Gardere, February 2016, Dallas & Houston.

PANEL: "Cybersecurity and Privacy Impacts to your Workforce - Risks to, and by, your Employees." Labor & Employment Law Section, Houston Bar Association, February 2016, Houston.

"2016 Update to Help Clients Do Business on the Internet," State Bar of Texas, January 2016, WEBCAST.

"Update on December 2015 Federal Rules Changes and e-Neutrals," State Bar of Texas, December 2015, WEBCAST.

"What Every Lawyer Needs to Know About Cybercrime," State Bar of Texas, November 2015, WEBCAST.

"Information Governance for General Counsel," bluesource, November 2015, Irving.

"Ethical Issues Regarding Cyber Security," Member Appreciation CPE Series, Dallas Chapter of the State Society of CPAs, October 2015, Dallas.

"Ethical Issues for Lawyers with Social Media and the Cloud," Computer Law Section, Dallas Bar Association, October 2015, Dallas.

"How Special Masters Can Help in Complex Cases, Particularly IT & eDiscovery Disputes," Business Litigation Section, Dallas Bar Association, October 2015, Dallas.

PANEL: "A Year of Increased Cyber Risks," Southern Law Network, 16th Annual General Counsel Conference, October 2015, Washington.

"Ethical Concerns for Paralegals When You and Your Company Find a Cyber Intrusion," Texas Advanced Paralegal Annual Seminar, State Bar of Texas, October 2015, Fort Worth.

PANEL: "Arbitrating in a Digital World - An eDiscovery Course for AAA Neutrals," AAA & American College of eNeutrals, September 2015, Washington.

PANEL: "Using Information Rights Management for Secure Collaboration in the Legal Industry," ALM * Intralinks, August, Webcast.

"International Data Privacy," Intellectual Property Section, Annual Meeting of the State Bar of Texas, June 2015, San Antonio.

PANEL: “Arbitrating in a Digital World - An eDiscovery Course for AAA Neutrals,” AAA & American College of eNeutrals, June 2015, New York.

“Legal Ethics in Negotiating and Litigating IT Contracts,” bluesource, June 2015, Irving.

“Ethical Issues for eDiscovery Including Admissibility for Social Media and Internet,” 28th Annual Advanced Evidence & Discovery Course, State Bar of Texas, May 2015, San Antonio.

“What Lawyers Need to Know About eEvidence in the Internet of Things (IoT),” State Bar of Texas, April 2015, WEBCAST.

KEYNOTE: “Ethical Concerns about Cyber Threats and the Internet,” Oregon Law Review Symposium on Disruptive Innovation in Law and Technology, April 2015, Portland.

“Ethical Issues for eDiscovery Including Admissibility for Social Media and Internet,” 28th Annual Advanced Evidence & Discovery Course, State Bar of Texas, April 2015, Houston.

PANEL: “Arbitrating in a Digital World - An eDiscovery Course for AAA Neutrals,” AAA & American College of eNeutrals, April 2015, Chicago.

“Legal Ethics for General Counsel and Trial Lawyers in eDiscovery,” bluesource, March 2015, Irving.

“Ethical Concerns for General Counsel When You and Your Company Find a Cyber Intrusion,” Corporate Counsel Section, Dallas Bar Association, March 2015, Dallas.

“Ethical Advice About Entering Into Internet Contracts and Privacy Protection,” Gardere, February 2015, Dallas & Houston.

“IT Legal Issues in 2015 and Beyond,” IT Leadership Business Technology Breakfast, February 2015, Dallas & Fort Worth.

PANEL: “Insulate Your Company From a Cyber Breach,” AIG*Jordan Lawrence*Gardere, February 2015, Dallas.

PANEL: “Cyberintrusions: Ethical Consideration for lawyers to protect attorney-client privilege, confidentiality from the latest Internet threats,” Symantec and CDW, LegalTech, February, New York.

“Internet Law 102,” Information Systems Audit and Control Association and Institute of Internal Auditors, January 2015, Dallas.

“2015 Update to Help Clients Do Business on the Internet,” State Bar of Texas, January 2015, WEBCAST.

“Ethics in an Age of Cyber Intrusions and Social Media,” State Bar of Texas, December 2014, WEBCAST.

“Ethics Issues with eDiscovery and Social Media,” Last Chance Winning with the Masters Speakers, Louisiana Association for Justice, December 2014, New Orleans.

“Ethical Issues for Lawyers with Social Media and the Cloud,” Holiday Ethics, Austin Bar Association, December 2014, Austin.

“Legal and Ethical Risks of Cybersecurity,” 16th Annual Conference of the General Counsel Forum, November 2014, San Antonio.

“Ethics for Lawyers with the Internet of Things,” State Bar of Texas, November 2014, WEBCAST.

“The 10 Commandments of IT Contracts,” IS Consulting Course, Business Information Systems, Texas Christian University, November 2014, Fort Worth.

PANEL: “Insulate Your Company From a Cyber Breach,” AIG*Jordan Lawrence*informatica*Gardere, November, 2014, Dallas.

“Ethical Concerns about Cybersecurity for Lawyers,” 38th Page Keeton Civil Litigation Institute, UT Law CLE, October 2014, Austin.

“How to Avoid Legal Disasters in the Internet Age,” Cornell Hospitality Research Summit, October 2014, Ithaca.

“Ethical Considerations and eDiscovery Issues with the Internet, Social Media, & Cybersecurity,” Annual Meeting, National Association of Paralegals, October 2014, Dallas.

“Legal and Ethical Risks of Internet Cloud Services for In-House Counsel,” Tech Summit, Texas Lawyer, September 2014, Dallas.

“The 10 Commandments of IT Contracts,” Alphaworks, September 2014, Frisco.

PANEL: “Data Protection and Privacy in the U.S. and Abroad,” eDiscovery Program, Driven, September, 2014, Houston.

“Legal and Ethical Risks of Internet Cloud Services for In-House Counsel,” Fidelity Investments, July 2014, Westlake..

“eDiscovery Cost Control by Using Defensible Deletion,” Gardere, July 2014, WEBCAST.

PANEL: “Cases in eDiscovery ,” Commercial Arbitration Training for Arbitrators and Counsel, NYSBA & Cardozo School of Law, July, 2014, New York.

“Innovations in ADR: Finding Areas Ripe For Neutrals,” Annual Meeting, Greater NY Chapter - Association for Conflict Resolution, June 2014, New York.

“Legal Risks for Cyber Attack,” 2014 Sponsor Forum, Center for Retailing Studies, Mays Business School, Texas A&M, May 2014, Houston.

PANEL: “Sharpening the Saw – All Things Legal that a CIO May Encounter,” BravoTech & Alvarez & Marsal, May 2014, Dallas.

Workshops:

"Social Media Workshop," Cooperative Processing Resources, April 2010, DFW Airport.
"eCommerce Legal Issues and Web 2.0," American Petroleum Institute, General Committee on Information Management and Technology, May 2009, Dallas.
"eGovernment and the Future of Government Services," Arizona County Treasurers Association Conference, April 2009, Safford.
"Legal Implications of the Internet for Medical Boards," Federation of State Medical Boards, September 2003, Seattle.

Information Technology Videos on WatchIT.com:

"Cyber Ethics: A Growing Business Challenge," "Perspectives on Net Neutrality," "Protecting Your Business: From Social Media to Cyber Threats," "BYOD: When You Are Left to Your Own Devices," "Privacy Policies: What You Don't Know Can Hurt You," "10 Commandments of IT Contracts," "Social Media 2011 Update," "5 Big Bang Theory of the Internet," "From ERP to Cloud Computing," "Legal Issues for Virtual Worlds,""Are You on the Software Police's Most Wanted List?" and "E-Discovery Investigations: What IT Professionals Need to Know!"

TABLE OF CONTENTS

GETTING DATA FROM 3RD PARTIES – PERILS AND CHALLENGES

INTRODUCTION

In 2016 every virtually all of our individuals and businesses use computers and the Internet to send emails, participate in Social Media, and conduct business. As a result the proliferation of Electronically Stored Information (ESI) will undoubtedly continue to grow in the future. With the social changes brought about by the evolution of Social Media more sources of ESI have become part of the evidence in litigation throughout the world. This paper will provide advice about how lawyers can get ESI from third parties, and related admissibility at trial.

I. WHAT IS ELECTRONICALLY STORED INFORMATION (ESI)?

With the advent of ESI in litigation a group called the Sedona Conference was founded in 2002. (https://thesedonaconference.org/) Since then has been provided a wealth of information about ESI. Of course much of the impetus for courts to get a handle on ESI was the incredible volume of ESI and its ubiquitous nature, not to mention that a number of US District Judges issued significant Order for the destruction of ESI which penalized many litigants. As a result of much discussion and public vetting the in 2006 Federal Rules of Civil Procedure were amended specifically to deal with ESI. Since the US District Courts hear both criminal and civil matters it seems pretty clear that the impact on the federal judiciary will never be the same.

One of the benefits we have today is that in 2012 the Federal Judicial Center published "Managing Discovery of Electronic Information: A Pocket Guide for Judges, Second Edition" (the "Pocket Guide") (http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt2d_eb.pdf/$file/eldscpkt2d_eb.pdf)

All Federal District Judges and Magistrate Judges have attended training regarding ESI and have copies of the Pocket Guide. Conveniently the Pocket Guide gives the following explanation about ESI:

> What Is Electronically Stored Information and How Does It Differ from Conventional Information?
>
> ESI currently includes e-mail messages, word processing files, web pages, and databases created and stored on computers, magnetic disks (such as computer hard drives), optical disks (such as DVDs and CDs), and flash memory (such as "thumb" or "flash" drives), and increasingly on "cloud" based servers hosted by third parties that are accessed through Internet connections. The technology changes rapidly, making a complete list impossible. Federal Rules of Civil Procedure 26 and 34, which went into effect on December 1, 2006, use the broad term "electronically stored information" to identify a distinct category of information that, along with "documents" and "things," is subject to discovery rights and obligations.
>
> ESI differs from conventional, paper-based information in several ways that affect discovery. The volume of ESI is almost always exponentially greater than that of paper information, and ESI may be located in multiple places that are widely dispersed. For example, draft and final versions of a single memorandum may be stored electronically in multiple places (e.g., on the computer hard drives of the document's creator, reviewers, and recipients; on the company server; on laptops and home computers; on backup tapes; and on local network servers and third-party hosted servers). Market research has found that the average employee sends or receives more than 100 electronic messages per working day, which translates into more than 2,400,000 messages a year for an organization of 100 employees.
>
> Although the possibility that paper documents or things could be damaged, altered, or destroyed has always been a concern, the dynamic and mutable nature of ESI presents new challenges. Computer systems automatically recycle and reuse memory space, altering potentially relevant information without any specific direction from, or even the knowledge of, the user. Merely opening a digital file changes information about that file, and e-mail messages may be automatically deleted after a certain period unless steps are taken to avoid it.
>
> Some aspects of ESI have no counterpart in print media, metadata being the most obvious example.1 Metadata, which most computer users never see, provide information about an electronic file, such as the date it was created, its author, when and by whom it was edited, what edits were made, and, in the case of email, the history of its transmission. Another example is those computer-based transactions that do not result in printable text-based documents, but instead are represented in specially formatted databases. Even less complex ESI may be incomprehensible and unusable when separated from the system that created it. For example, financial projections developed using spreadsheet software may be useless if produced in

> portable document format (PDF) rather than in the format of the spreadsheet software because embedded information, such as computational formulas, is not retained in the PDF file.
>
> Unlike paper documents, ESI can be produced in different forms, such as PDF and TIFF (tagged image file format). Some forms may not be compatible with the requesting party's computer system, may hide metadata and embedded data, and may not be as easy to search as the requesting party would like. If ESI was created on a system or with a program that is no longer used, either because it is obsolete or because the party does not have access to it, the information may be difficult to retrieve in a form that is useful. Deleting an electronic document does not necessarily get rid of it, as throwing away or shredding a paper document would. An electronic document may be recovered from the hard drive or server, to the extent it has not been overwritten, and may be available on the computers of other people or on archival media or backup tapes used for disaster recovery purposes. The costs and efforts required to retrieve and restore such information, however, can be very high and extensive.
>
> These and other differences between ESI and paper information have important implications for discovery. For example, the dynamic nature of ESI makes it vital that a litigant or potential litigant institute a "litigation hold" to preserve information that may be discoverable, whenever litigation is reasonably anticipated—and that can be well before a complaint is filed or an answer is served. The volume and multiple sources of ESI increase costs and burdens, which in turn leads to more disputes about whether discovery is relevant or proportional to the needs of the case. A review to identify and segregate privileged information is more difficult, increasing the likelihood of inadvertent production even when the producing party has taken reasonable steps to avoid it. Because deleted or backup information may be "relevant" under the discovery rules, parties may request its production, even though restoring, retrieving, and producing it may require expensive and burdensome computer forensic work that is disproportionate to the reasonable discovery needs of the requesting party. The choice of the form of production was not an issue with paper discovery, but it can lead to disputes in ESI discovery. Judges should be alert to the ways in which these differences may affect the discovery issues and management needs in their cases.

Pocket Guide, pp2-4.

II. SOCIAL MEDIA INCREASES ESI SOURCES AND VOLUMES

In 2016 one would have to be living under a rock to have missed the social changes that Social Media have wrought on virtually everyone in the world. Social Media has been involved with virtually every business and part of government revolutions around the world. So it is no wonder that Social Media has created new sources of ESI.

Although Facebook statistics when this paper is being written claims a +1 billion daily active users, there have higher estimates to be sure. (http://newsroom.fb.com/Key-Facts). But perhaps more important is the Facebook statistic that 'More than 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month.' How much of these billions of pieces of content will end up in litigation is unknown precisely, but assuredly some percentage will be part of future litigation.

The business Social Media site LinkedIn currently claims to have more than 400 million users as of February 2016 (http://www.linkedin.com/about-us). Given the increased business uses of LinkedIn there can be little question that LinkedIn ESI will also be a facet of litigation in many lawsuits in the future.

Of course there are dozens of important Social Media businesses including Wikipedia, Google, and Yelp to name a few. It takes little imagination to foresee that ESI from these Social Media sites will be a part of litigation for the foreseeable future.

III. STORED COMMUNICATIONS ACT (1986)

In 1986 Congress passed the Stored Communications Act (18 U.S.C. §§ 2701-2712) to deal with telephone records. With the advent and proliferation of the Internet the Stored Communications Act as been applied to Social Media and email.

In June 2010 the US Supreme Court voted 9-0 interpreting text messages under the Stored Communication Act in *City of Ontario et al v. Quon*. http://www.supremecourt.gov/opinions/09pdf/08-1332.pdf .

The Ontario, CA Police Department (OPD) did not violate the 4th Amendment by reviewing text messages sent from a work pager. Apparently the OPD's warrantless audit found Officer Quon had sent or received 456 messages, but only 57 were work-related. The OPD Computer Policy included the following provisions that the OPD "reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources." The Court ruled that the

"warrantless review of Quon's pager transcript was reasonable … because it was motivated by a legitimate work-related purpose, and because it was not excessive in scope." Today so many employees use cell phones and PDA provided by employers that surely the Supreme Court's ruling will impact all employees, not just government employees.

A Judge ruled that Facebook wall postings and MySpace comments may not be subpoenaed based on the 1986 Stored Communications Act which is the same statute before in *Quon*. US District Judge Margaret Morrow's May 26, 2010, 37 page Order in *Buckley H. Crispin v. Christian Audigier, Inc. et al* reversed a ruling from an US Magistrate Judge that defendants in a copyright infringement case could not subpoena private message on Facebook MySpace. Clearly courts will be vexed by these complex issues as social media continues to grow and change communications. http://smu-ecommerce.gardere.com/crispin%20order.pdf

The Second Circuit ruled in July 2016 that under the SCA that Microsoft was not in contempt of court for failing to produce records about an alleged drug dealer that were stored in Ireland in the case of In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation. Microsoft Corporation, Appellant, v. United States of America, Appellee. https://scholar.google.com/scholar_case?case=16465853205355950871&q=%22microsoft%22&hl=en&as_sdt=2006&as_ylo=2016

IV. THIRD PARTY ESI

Without trying to reinvent the wheel I recommend that you rely on Stephen Orsinger's excellent Chapter 19 of the *Essential of E-Discovery* entitled "Discovery of ESI from Nonparties" published by the State Bar of Texas in 2014 and edited by Judge Xavier Rodriguez (http://texasbarbooks.net/essentials-of-e-discovery/).

TEXAS RULES

Under the Texas Rules of Civil Procedure a party my serve a Rule 205 Subpoena to a third party for a deposition or production of ESI for a reasonable amount of time. Depending on the facts in the case there may be no need for the deposition and the only purpose is to obtain the ESI. However the rules for cost shifting differ for a non-party that the requesting party must reimburse all of the non-party's reasonable costs of production.

Of course Rule 196.4 was interpreted in *In Re Weekley Homes* (295 S.W.3d 309 (Tex. 2009)) 2009 under the Federal Rules which requires the requesting party to specify exactly what format the ESI should be produced. (https://scholar.google.com/scholar_case?case=15908085835515547296&q=in+re+weekley+homes&hl=en&as_sdt=2006)

Also in a presuit deposition under Rule 202 a party investigating a claim may request a deposition which requires a hearing with notice to the adverse party.

Under Rule 196.7 ESI may be involved in a request for entry on property for examination.

FEDERAL RULES

Federal Rule of Civil Procedure 45 is much like Texas Rule 205, but the costs are borne by the third party. Under a relatively recent change the Rule 45 subpoenas are under the authority of the court for the case rather than where the third party resides. Also Federal Rule 27 to perpetuate testimony is much like Texas Rule 202.

V. COMPUTER CRIMES (PENAL CODE, CHAPTER 33)

In 1985 the Texas legislature established the Computer Crime statute (http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.33.htm), however since the law was enacted there have not been many charges brought. But as you can image that is likely to change with the increased use of computer technology, the Internet, and the need to protect minors.

Since 1985 computer technology has changed as has Chapter 33 and currently here are a summary of the offenses:

Section 33.02 BREACH OF COMPUTER SECURITY.

(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner. …

(b-1) A person commits an offense if with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

Section 33.021 ONLINE SOLICITATION OF A MINOR.

(b) A person who is 17 years of age or older commits an offense if, with the intent to arouse or gratify the sexual desire of any person, the person, over the Internet, by electronic mail or text message or other electronic message service or system, or through a commercial online service, intentionally:

(1) communicates in a sexually explicit manner with a minor; or
(2) distributes sexually explicit material to a minor.

(c) A person commits an offense if the person, over the Internet, by electronic mail or text message or other electronic message service or system, or through a commercial online service, knowingly solicits a minor to meet another person, including the actor, with the intent that the minor will engage in sexual contact, sexual intercourse, or deviate sexual intercourse with the actor or another person.

(d) It is not a defense to prosecution under Subsection (c) that:

(1) the meeting did not occur;
(2) the actor did not intend for the meeting to occur; or
(3) the actor was engaged in a fantasy at the time of commission of the offense.

(e) It is a defense to prosecution under this section that at the time conduct described by Subsection (b) or (c) was committed:

(1) the actor was married to the minor; or
(2) the actor was not more than three years older than the minor and the minor consented to the conduct.

Sec. 33.05. TAMPERING WITH DIRECT RECORDING ELECTRONIC VOTING MACHINE.

(b) A person commits an offense if the person knowingly accesses a computer, computer network, computer program, computer software, or computer system that is a part of a voting system that uses direct recording electronic voting machines and by means of that access:

(1) prevents a person from lawfully casting a vote;
(2) changes a lawfully cast vote;
(3) prevents a lawfully cast vote from being counted; or
(4) causes a vote that was not lawfully cast to be counted.

(c) An offense under this section does not require that the votes as affected by the person's actions described by Subsection (b) actually be the votes used in the official determination of the outcome of the election.

Sec. 33.07. ONLINE IMPERSONATION.

(a) A person commits an offense if the person, without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person to:

(1) create a web page on a commercial social networking site or other Internet website; or
(2) post or send one or more messages on or through a commercial social networking site or other Internet website, other than on or through an electronic mail program or message board program.

(b) A person commits an offense if the person sends an electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any person:

(1) without obtaining the other person's consent;
(2) with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication; and
(3) with the intent to harm or defraud any person.

As courts will likely see more charges brought under the Computer Crime statutes it seems reasonable that Judges, prosecutors, and defense counsel all get a better understanding of electronic evidence.

In order for

VI. ADMISSIBILITY OF ELECTRONIC EVIDENCE

In 2007 US Magistrate Paul Grimm in Maryland issued a 101 page Memorandum Order which outlined the admissibility of ESI in *Lorraine v. Markel Am. Ins. Co.*, 241 FRD 534 (D. Md. 2007) (Memorandum Order). (http://www.mdd.uscourts.gov/Opinions/Opinions/Lorraine%20v.%20Markel%20-%20ESIADMISSIBILITY%20OPINION.pdf).

Exhibit A to this paper highlights Judge Grimm's Order about admissibility of ESI.

VII. WHAT ARE THE STANDARDS FOR WARRANTS INVOLVING ESI?

As the previous sections help to address the scope of ESI, the question remains as to the proper methods of searching and seizing evidence with a warrant. Under the Fourth Amendment, the act of a search and seizure must be balanced against the protected interests of liberty, property, and privacy. In the context of ESI, the diversity of data types and sources has led to a variety of methods among the courts as to the elements necessary to satisfy a "reasonableness" standard for a proper search and seizure. Depending on the jurisdiction, device, data, or investigation a court may choose a different standard of detail required in the warrant. However among this uncertainty there are certain guideposts to be aware of in understanding the bottom line as well as the more extensive parameters.

One of the first distinctions to make is whether the data sought after is "inside" or "outside" a device. For this discussion the term "device" will broadly refer to desktops, laptops, cell phones, tablets, external hard drives or memory storage, or any other computer related technologies that could store or transmit data. The distinction between "inside" and "outside" helps to establish who possess the data and what laws may regulate. Further the "expectation of privacy" that is important to the evaluation of a reasonable search is also impacted by the location of the data. For instances, if data is on a computer device used for personal matters there is a greater expectation of privacy and protection rather than a device used for a business or government purpose where the data may be available for some public access or greater scrutiny.

If the data is "inside" the device, then are issues of verifying who was using the device when the crime occurred, locating the device, obtaining the search warrant or consent to search, and forensic analysis of the device. If the data is "outside" the device, then collecting the data probably invokes the Stored Communications Act, the Wiretap Act (18 U.S.C. §§ 2510-2522), or the Pen Register Act (18 U.S.C. §§ 3121-3127). The Stored Communications Act would apply where data or records about a service subscriber are sought from an Internet service provider (ISP). These types of requests are often used to help identify anonymous accounts, verify user information, logs of service use, and other data held by the third party. The Wiretap Act would apply in instances where the content was sought from the transmission to or from a known account or subscriber such as phone calls, text messages, emails, or other communications. Similarly, the Pen Register Act would cover to the log activity of the previous mentioned transmissions, but would not cover the content. Although there is law in place for whether data is "inside" or "outside" the device, this is still a developing statutory area and should be carefully observed as it progresses.

As to the regulation and review of warrants, there is the "plain view" and the "special view" that are used by the courts. Under the "plain view" the scope of the search is determined by the "objects" sought in the warrant. This requires a (1) prior valid intrusion, (2) observing the object in plain view, and (3) the incriminating character of the object is immediately and creates a probable cause. As described in *U.S. v. Brooks* (427 F.3d 1246, (10th Cir. 2005)), the government was not, "…required to describe its specific search methodology," because the," court has never required warrants to contain a particularized computer search strategy… [because the court has] simply held that officers must describe with particularity the object their search."

On the other hand the "special view" to searching devices seeks to limit the "plain view" by distinguishing tangible writings from digital data. Thus the "special view" requires (1) search limitations such as file names, extension, and date range, (2) warrants sets out search methodology such as key words and terms, (3) possible use of technical search engine software, (4) possible second warrant for intermingled documents, and (5) limits what is in the plain view during a search. As a result, once you have seized a large amount of media the proper review may require a Special Master, Magistrate review, a Taint team that consists of a prosecutor and investor with no connection to the case, or technological restrictions on the scope of the search.

The "special view" was addressed 2010 in *U.S. v. Comprehensive Drug Testing* (621 F.3d 1162 (9th Cir. 2010)), in which there was a warrant seeking drug tests of 10 players.

Held:

1. Magistrates "should insist" government waive reliance upon plain view doctrine.
2. Segregation and redaction must be either done by specialized personnel or an independent third party.

    a. "if done by government computer personnel, must agree in warrant application that computer personnel will not disclose to investigators any info other than that which is the target of warrant.

3. Warrants/subpoenas must disclose actual risks of destruction of info and prior efforts to seize the info in the other judicial fora.
4. Search protocol must be designed to uncover only info for which government has probable cause and only that info may be examined by case agents.
5. The government must destroy or, if recipient may lawfully possess it, return non-responsive data, keeping issuing magistrate informed about when it has done so and what is has kept.

VIII. CONCLUSIONS

Judges, prosecutors, and lawyers need to know about IT in order to best deal with ESI. One way to learn more is to attend more educational programs such as this. As well the State Bar of Texas puts on a number of excellent CLE programs dealing with e-Discovery and many materials are on the State Bar CLE website: http://www.texasbarcle.com/CLE/

EXHIBIT A

SUMMARY:
LORRAINE V. MARKEL
241 F.R.D. 534 (D.Md. May 4, 2007).

BASIC EVIDENCE

Whether ESI is admissible into evidence is determined by a collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible. Whenever ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered: (1) is the ESI relevant as determined by Rule 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant under 401, is it authentic as required by Rule 901(a) (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it hearsay as defined by Rule 801, and if so, is it covered by an applicable exception (Rules 803, 804 and 807); (4) is the form of the ESI that is being offered as evidence an original or duplicate under the original writing rule, of if not, is there admissible secondary evidence to prove the content of the ESI (Rules 1001-1008); and (5) is the probative value of the ESI substantially outweighed by the danger of unfair prejudice or one of the other factors identified by Rule 403, such that it should be excluded despite its relevance.
Id, at 538.

RELEVANCE:

The relationship between Rule 104(a) and (b) can complicate the process by which ESI is admitted into evidence at trial, or may be considered at summary judgment. The rule states, in relevant part:

> (a) Questions of admissibility generally. Preliminary questions concerning the qualification of a person to be a witness, the existence of a privilege, or the admissibility of evidence shall be determined by the court, subject to the provisions of subdivision (b) . . . . In making its determination it is not bound by the rules of evidence except those with respect to privileges.
>
> (b) Relevancy conditioned on fact. When the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition.
> FED. R. EVID. 104 (a) and (b).
> ***Id, at 539.***

For example, if an e-mail is offered into evidence, the determination of whether it is authentic would be for the jury to decide under Rule 104(b), and the facts that they consider in making this determination must be admissible into evidence. In contrast, if the ruling on whether the e-mail is an admission by a party opponent or a business record turns on contested facts, the admissibility of those facts will be determined by the judge under 104(a), and the Federal Rules of Evidence, except for privilege, are inapplicable.
Id, at 540.

AUTHENTICATION

Although courts have recognized that authentication of ESI may require greater scrutiny than that required for the authentication of "hard copy" documents,21 they have been quick to reject calls to abandon the existing rules of evidence when doing so. For example, in *In Re F.P. , A Minor* the court addressed the authentication required to introduce transcripts of instant message conversations.

In rejecting the defendant's challenge to this evidence, it stated:

> Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages. The argument is that e-mails or text messages are inherently unreliable because of their relative anonymity and the fact that while an electronic message can be traced to a particular computer, it can rarely be connected to a specific author with any certainty. Unless the purported author is actually witnessed

> sending the e-mail, there is always the possibility it is not from whom it claims. As appellant correctly points out, anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person. However, the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen. We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of PaR.E. 901 and Pennsylvania case law . . . We see no justification for constructing unique rules of admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity.
> 878 A.2d at 95-96.

Indeed, courts increasingly are demanding that proponents of evidence obtained from electronically stored information pay more attention to the foundational requirements than has been customary for introducing evidence not produced from electronic sources.

As one respected commentator on the Federal Rules of Evidence has noted:
In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues. If a computer processes data rather than merely storing it, authentication issues may arise. The need for authentication and an explanation of the computer's processing will depend on the complexity and novelty of the computer processing. There are many states in the development of computer data where error can be introduced, which can adversely affect the accuracy and reliability of the output. Inaccurate results occur most often because of bad or incomplete data inputting, but can also happen when defective software programs are used or stored-data media become corrupted or damaged.
The authentication requirements of Rule 901 are designed to set up a threshold preliminary standard to test the reliability of evidence, subject to later review by an opponent's cross-examination.

See also MANUAL FOR COMPLEX LITIGATION at § 11.447 ("In general, the Federal Rules of Evidence apply to computerized data as they do to other types of evidence. Computerized data, however, raise unique issues concerning accuracy and authenticity. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy. The judge should therefore consider the accuracy and reliability of computerized evidence, including any necessary discovery during pretrial proceedings, so that challenges to the evidence are not made for the first time at trial.").
Id, at 542-43.

Although Rule 901(a) addresses the requirement to authenticate electronically generated or electronically stored evidence, it is silent regarding how to do so. Rule 901(b), however, provides examples of how authentication may be accomplished. It states:

(1) Testimony
(2) Non expert opinion on handwriting
(3) Comparison by trier or expert witness
(4) Distinctive characteristics
(5) Voice Identification
(6) Telephone Conversations
(7) Public Records or Reports
(8) Ancient documents or data collection
(9) Process or system
(10) Methods provided by statute or rule.

The ten methods identified by Rule 901(b) are non-exclusive. FED. R. EVID. 901(b) advisory committee's note ("The examples are not intended as an exclusive enumeration of allowable methods but are meant to guide and suggest, leaving room for growth and development in this area of the law."); WEINSTEIN at §901.03[1] ("Parties may use any of the methods listed in Rule 901(b), any combination of them, or any other proof that may be available to carry their burden of showing that the proffered exhibit is what they claim it to be."); *Telewizja Polska USA*, 2004

WL 2367740 (authentication methods listed in Rule 901(b) are "non-exhaustive")
Id, at 544-545.

EMAIL

One well respected commentator has observed:

> [E]-mail messages may be authenticated by direct or circumstantial evidence. An email message's distinctive characteristics, including its "contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances" may be sufficient for authentication.

Printouts of e-mail messages ordinarily bear the sender's e-mail address, providing circumstantial evidence that the message was transmitted by the person identified in the e-mail address. In responding to an e-mail message, the person receiving the message may transmit the reply using the computer's reply function, which automatically routes the message to the address from which the original message came. Use of the reply function indicates that the reply message was sent to the 40 sender's listed e-mail address.

The contents of the e-mail may help show authentication by revealing details known only to the sender and the person receiving the message.

E-mails may even be self-authenticating. Under Rule 902(7), labels or tags affixed in the course of business require no authentication. Business e-mails often contain information showing the origin of the transmission and identifying the employer company. The identification marker alone may be sufficient to authenticate an e-mail under Rule 902(7). However, the sending address in an e-mail message is not conclusive, since e-mail messages can be sent by persons other than the named sender. For example, a person with unauthorized access to a computer can transmit e-mail messages under the computer owner's name. Because of the potential for unauthorized transmission of e-mail messages, authentication requires testimony from a person with personal knowledge of the transmission or receipt to ensure its trustworthiness.

WEINSTEIN at § 900.07[3][c]; *see also* EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS § 4.03[4][b] (LexisNexis 6th ed. 2005)(hereinafter "IMWINKELRIED, EVIDENTIARY FOUNDATIONS.")
Id, at 554.

INTERNET WEBSITE POSTINGS

Courts often have been faced with determining the admissibility of exhibits containing representations of the contents of website postings of a party at some point relevant to the litigation.

The issues that have concerned courts include the possibility that third persons other than the sponsor of the website were responsible for the content of the postings, leading many to require proof by the proponent that the organization hosting the website actually posted the statements or authorized their posting. *See United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000) (excluding evidence of website postings because proponent failed to show that sponsoring organization actually posted the statements, as opposed to a third party)

One commentator has observed "[i]n applying [the authentication standard] to website evidence, there are three questions that must be answered explicitly or implicitly. (1) What was actually on the website? (2) Does the exhibit or testimony accurately reflect it? (3) If so, is it attributable to the owner of the site?"32 The same author suggests that the following factors will influence courts in ruling whether to admit evidence of Internet postings:

> The length of time the data was posted on the site; whether others report having seen it; whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g. financial information from corporations); whether the owner of the site has elsewhere published the same data, in whole or in part; whether others have published the same data, in whole or in part; whether the data has been republished by others who identify the source of the data as the website in question?33

The authentication rules most likely to apply, singly or in combination, are 901(b)(1) (witness with personal knowledge) 901(b)(3) (expert testimony) 901(b)(4) (distinctive characteristics), 901(b)(7) (public records), 901(b)(9) (system or process capable of producing a reliable result), and 902(5) (official publications).

Id, at 555.

TEXT MESSAGES AND CHAT ROOM CONTENT

Many of the same foundational issues found encountered when authenticating website evidence apply with equal force to text messages and internet chat room content; however, the fact that chat room messages are posted by third parties, often using "screen names" means that it cannot be assumed that the content found in chat rooms was posted with the knowledge or authority of the website host. SALTZBURG at § 901.02[12]. One commentator has suggested that the following foundational requirements must be met to authenticate chat room evidence:

(1) [e]vidence that the individual used the screen name in question when participating in chat room conversations (either generally or at the site in question);
(2) [e]vidence that, when a meeting with the person using the screen name was arranged, the individual . . . showed up; (3) [e]vidence that the person using the screen name identified [himself] as the [person in the chat room conversation]; evidence that the individual had in [his] possession information given to the person using the screen name; (5) [and] [e]vidence from the hard drive of the individual's computer [showing use of the same screen name].

Id. at § 901.02[12]. Courts also have recognized that exhibits of chat room conversations may be authenticated circumstantially.

Id, at 556.

COMPUTER STORED RECORDS AND DATA

The least complex admissibility issues are associated with electronically stored records. "In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues." WEINSTEIN at § 900.06[3]. That said, although computer records are the easiest to authenticate, there is growing recognition that more care is required to authenticate these electronic records than traditional "hard copy" records. MANUAL FOR COMPLEX LITIGATION at § 11.447;

> 34Computerized data, however, raise unique issues concerning accuracy and authenticity. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy. The judge should therefore consider the accuracy and reliability of computerized evidence . . . .
>
> 35"In the past, many courts have been lax in applying the authentication requirement to computer records; they have been content with foundational evidence that the business has successfully used the computer system in question and that the witness recognizes the record as output from the computer. However, following the recommendations of the Federal Judicial Center's *Manual for Complex Litigation*, some courts now require more extensive foundation. These courts require the proponent to authenticate a computer record by proving the reliability of the particular computer used, the dependability of the business's input procedures for the computer, the use of proper procedures to obtain the document offered in court, and the witness's recognition of that document as the readout from the computer." (citation omitted).

In *United States v. Meienberg*, the defendant challenged on appeal the admission into evidence of printouts of computerized records of the Colorado Bureau of Investigation, arguing that they had not been authenticated because the government had failed to introduce any evidence to demonstrate the accuracy of the records.

In contrast, in the case of *In Re Vee Vinhnee*, the bankruptcy appellate panel upheld the trial ruling of a bankruptcy judge excluding electronic business records of the credit card issuer of a Chapter 7 debtor, for failing to authenticate them. 336 B.R. 437.

As the foregoing cases illustrate, there is a wide disparity between the most lenient positions courts have taken in accepting electronic records as authentic and the most demanding requirements that have been imposed.

Lawyers can expect to encounter judges in both camps, and in the absence of controlling precedent in the court where

an action is pending setting forth the foundational requirements for computer records, there is uncertainty about which approach will be required.

The methods of authentication most likely to be appropriate for computerized records are 901(b)(1) (witness with personal knowledge), 901(b)(3) (expert testimony), 901(b)(4) (distinctive characteristics), and 901(b)(9) (system or process capable of producing a reliable result).
Id, 556-59.

COMPUTER ANIMATION AND COMPUTER SIMULATIONS

Computer generated evidence is an increasingly common form of demonstrative evidence. If the purpose of the computer evidence is to illustrate and explain a witness's testimony, courts usually refer to the evidence as an animation. In contrast, a simulation is based on scientific or physical principles and data entered into a computer, which is programmed to analyze the data and draw a conclusion from it, and courts generally require proof to show the validity of the science before the simulation evidence is admitted.

Thus, the classification of a computer-generated exhibit as a simulation or an animation also affects the evidentiary foundation required for its admission.
Id, at 559.

Courts generally have allowed the admission of computer animations if authenticated by testimony of a witness with personal knowledge of the content of the animation, upon a showing that it fairly and adequately portrays the facts and that it will help to illustrate the testimony given in the case.

Computer simulations are treated as a form of scientific evidence, offered for a substantive, rather than demonstrative purpose. WEINSTEIN at § 900,03[1] (p. 900-21); IMWINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.09[4][a],[c]. The case most often cited with regard to the foundational requirements needed to authenticate a computer simulation is *Commercial Union v. Boston Edison*, where the court stated:

> [W]e treat computer-generated models or simulations like other scientific tests, and condition admissibility on a sufficient showing that: (1) the computer is functioning properly; (2) the input and underlying equations are sufficiently complete and accurate (and disclosed to the opposing party, so that they may challenge them); and (3) the program is generally accepted by the appropriate community of scientists.
> 591 N.E.2d 165, 168 (Mass. 1992) (citation omitted).

*[In *State v. Swinton*,847 A.2d 921, 942 (Conn. 2004)]
In that regard, the court* noted that the following problems could arise with this type of computer evidence: (1) the underlying information itself could be unreliable; (2) the entry of the information into the computer could be erroneous; (3) the computer hardware could be unreliable; (4) the computer software programs could be unreliable; (5) "the execution of the instructions, which transforms the information in some way—for example, by calculating numbers, sorting names, or storing information and retrieving it later" could be unreliable; (6) the output of the computer—the printout, transcript, or graphics, could be flawed; (7) the security system used to control access to the computer could be compromised; and (8) the user of the system could make errors.
Id, at 559-60.

DIGITAL PHOTOGRAPHS

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. *Id.* If a question is raised about the reliability of digital photography in general, the court likely could take judicial notice of it under Rule 201. *Id.* For digitally converted images, authentication requires an explanation of the process by which a film photograph was converted to digital format. This would require testimony about the process used to do the conversion, requiring a witness with personal knowledge that the conversion process produces accurate and reliable images, Rules 901(b)(1) and 901(b)(9)-the later rule implicating expert testimony under Rule 702.

For digitally enhanced images, it is unlikely that there will be a witness who can testify how the original scene looked if, for example, a shadow was removed, or the colors were intensified. In such a case, there will need to be proof, permissible under Rule 901(b)(9), that the digital enhancement process produces reliable and accurate results, which gets into the realm of scientific or technical evidence under Rule 702. *Id.*

Id, at 561-62.

CONCLUSION

To prepare properly to address authentication issues associated with electronically generated or stored evidence, a lawyer must identify each category of electronic evidence to be introduced. Then, he or she should determine what courts have required to authenticate this type of evidence, and carefully evaluate the methods of authentication identified in Rules 901 and 902, as well as consider requesting a stipulation from opposing counsel, or filing a request for admission of the genuineness of the evidence under Rule 36 of the Federal Rules of Civil Procedure. With this analysis in mind, the lawyer then can plan which method or methods of authentication will be most effective, and prepare the necessary formulation, whether through testimony, affidavit, admission or stipulation. The proffering attorney needs to be specific in presenting the authenticating facts and, if authenticity is challenged, should cite authority to support the method selected.
Id, at 562.

The discussion above highlights the fact that there are five distinct but interrelated evidentiary issues that govern whether electronic evidence will be admitted into evidence at trial or accepted as an exhibit in summary judgment practice. Although each of these rules may not apply to every exhibit offered, as was the case here, each still must be considered in evaluating how to secure the admissibility of electronic evidence to support claims and defenses.
Id, at 585.