Center *for* Research Libraries

Human Rights Electronic Evidence Study

ADMISSIBILITY OF ELECTRONIC DOCUMENTATION AS EVIDENCE IN U. S. COURTS

Lucy L. Thomson, Esq.*

December 1, 2011

I. HUMAN RIGHTS DOCUMENTATION: THE CHANGING DIGITAL EVIDENCE LANDSCAPE

In October 2011 international human rights groups called for an independent investigation of the circumstances surrounding the killing of former Libyan dictator Moammar Gaddafi on the streets of Sirte, Libya. According to cell phone videos that surfaced the day he was killed, Gaddafi was found alive and may have been taunted and beaten by his captors. Evidence that will be scrutinized to determine whether brutality before his killing constitutes a war crime are cell phone videos taken by observers -- revolutionaries and Gaddafi supporters -- in the heat of the battle for control of Libya and its future.[1] Small snatches of videos that were posted on YouTube and played on Arab language television provided graphic illustrations of Gaddafi's capture and killing by revolutionaries. Several days later, the Global Post obtained another video showing other evidence of abuse as Gaddafi was captured. [2] In response, organizations ranging from the United Nations Human Rights Council in Geneva, representatives of the new Libyan government, the U.S. State Department, and international human rights organizations, including Human Rights Watch and Amnesty International, announced plans to investigate.

---

* This report was prepared by Lucy L. Thomson, a consultant for the Center for Research Libraries Human Rights Electronic Evidence Study. For further information, please contact James Simon at simon@crl.edu or Sarah Van Deusen Phillips at svandeusen@crl.edu.

Ms. Thomson is an attorney and a senior engineer at a global technology company where she focuses on cybersecurity and global data privacy. A former career federal criminal prosecutor at the U.S. Department of Justice, she pioneered the use of electronic evidence at trial in complex white-collar crime and landmark civil rights cases. Ms. Thomson is Chair-Elect of the American Bar Association (ABA) Section of Science & Technology Law, widely regarded as the global authority on science and technology law. She founded and co-chairs the ABA e-discovery and digital evidence committee, and is editor of the best-selling *Data Breach and Encryption Handbook* (ABA 2011). Ms. Thomson earned a master's degree from Rensselaer Polytechnic Institute (RPI) in 2001, and holds a J.D. degree from the Georgetown University Law Center.

[1] Sheridan, Mary Beth, Groups seek probe of Gaddafi's death, The Washington Post, October 22, 2011, page A1.

[2] Sheridan, Gaddafi buried in secret desert grave, Libyan official say, The Washington Post, October 26, 2011, page A10.

Evidence central to an international inquiry such as this has been created over the course of several weeks, months, and even years by observers on the scene in Libya, as well as individuals representing a broad range of organizations, including news reporters, people involved in both the Gaddafi government and revolutionaries, members of human rights organizations, government officials and military forces from diverse countries as well as NATO, law enforcement and police, and numerous others with a variety of perspectives, educational backgrounds, cultures and languages – all potential witnesses in possible upcoming cases before international tribunals or in extra-judicial proceedings.

In the digital age, evidence in human rights cases has become not only richer but also more complex. As human rights events unfold around the world, observers on the scene are documenting the details with photographs and video and audio recordings from their cell phones and cameras, and posting real-time commentary and photos (often transmitted through their mobile devices) on websites such as YouTube, global social media sites, and Twitter and in e-mail and text messages -- previously unavailable real-time, up-to-the-minute recordings. Now in court proceedings, traditional eyewitness testimony can be greatly enhanced and corroborated by introducing digital evidence of videos, photographs, audio recordings, and real-time commentary on critical human rights events. These live recordings by observers supplement the more carefully documented evidence that is often available in human rights proceedings, including interviews, government records, reports, and databases.

The graphically depicted death of dictator Moammar Gadaffi, the revolution in Libya, as well as the upheaval across the Middle East – with reported widespread violations of the human rights of hundreds of individuals – highlights the importance of addressing the legal sufficiency of the many means by which these incidents have been recorded, including those recorded in digital form. The judicial system has both principles and rules that govern the admissibility of evidence – and both advocates and the courts are struggling to determine how to address the myriad of evidentiary issues that arise when digital images and other computer generated information is presented in court.

This report focuses on the uses of various types of electronic evidence by organizations involved in the judicial process or extra-judicial proceedings in the United States. The analysis and recommendations are designed to facilitate the use and admissibility of digital documentation, and to ensure that necessary information about the creation, use, storage, and chain of custody is maintained for authentication of the evidence in human rights cases. In this report, the principles of admissibility, the relevant federal rules of procedure and evidence, recent cases, and observations made by commentators will be addressed. In additional, to assist human rights advocates, a number of recommendations will be made to facilitate the gathering of "evidence" by electronic means.

Over many years, human rights information has been used for a variety of important purposes:

- Awareness, activism, education, and policy advocacy
- Prosecution of human rights cases
- Obtaining reparations

- Preserving information, not only for history, but also for prosecution

The widespread use of information technology by individuals and organizations has created unprecedented challenges in legal proceedings as the courts decide how to properly authenticate digital information under the current judicial rules and procedures. While the basic legal requirements for establishing a foundation for admissibility in U.S. courts are well-established, their applicability to digital data and devices from which electronic evidence is generated raise complex issues and questions.

Admissibility versus Protection of Personal Privacy

While the goal of this report is to facilitate the use and admissibility of digital documentation in courts and extra-judicial proceedings, it is important to emphasize that in some circumstances, introducing personal information into evidence or otherwise publicizing it is not appropriate. This may mean not offering the information into evidence, when, for example, its use would result in a violation of personal privacy, security, or informed consent. Issues to consider include whether there would be a Constitutional violation if the evidence was acquired illegally or in violation of the rights of an accused, *e.g.* torture, or it would be used a purpose different from what the individual consented to.[3]

It is important to evaluate potential security risks to individuals. If a crowd scene, gathering, or individual is captured on videotape, individuals are tracked by GPS, or other personal information is stored digitally, public dissemination on the Internet may create risks of endangering people's safety. In short, it may not be safe for personal information to be posted on the Internet.

Admissibility in U.S. courts will be determined in accordance with the legal requirements for evidentiary privileges [4] and the Constitution and laws applicable in the court or state where the proceeding is taking place. Evidence may be excluded if it does not meet Constitutional and evidentiary requirements. In some cases, steps would be required to ensure that personal data are redacted, de-identified, aggregated, or protected under court rules such as entry of a protective order. Information governance best practices should include a requirement to document the privacy requirements of each type of information and protect confidential information of individuals appropriately.

Advanced Technology Trends

The nature of the evidence that is available in human rights cases has changed and expanded significantly in the digital age. Much of today's information is created in electronic form ("born digital"), and a large percentage is never printed. The Internet has revolutionized communications and made global information systems a reality. Information technology has caused a paradigm shift in the way individuals and organizations communicate -- and create, collect, share, and store data and information. As a result, the availability of observations and

[3] See Witness, *Cameras Everywhere*, *available at* http://blog.witness.org/2011/01/cameraseverywhere.

[4] United States courts recognize these privileges: (1) Privileges for Confidential Relations - Lawyer-Client; Psychotherapist-Patient; Husband-Wife; Penitent-Clergy Communications; (2) Attorney Work Product; (3) Government Privileges - Political Votes; Trade Secrets; Military and State Secrets; and Informant's Identity.

documentation of human rights events as they unfold is ever-increasing, resulting in an expansive collection of invaluable records.

Advanced technologies ranging from satellites to smart phones are providing new and sophisticated ways to document human rights incidents and potential violations. Thus, volumes of digital data and information are available instantaneously – and often transmitted widely and posted on websites for the world to see. Court rules require that for digital evidence to be admissible, it must be authenticated – in the simplest terms, this means that data and information must be shown to be what the proponent claims that it is. To authenticate digital evidence, the focus must be on the three key aspects of information technology: People – Process – Technology. Factors to be considered in evaluating the integrity of digital data include who created the evidence, what processes and technology were used, and what was the chain of custody throughout the entire digital evidence lifecycle. Because digital information can be created easily and without any verifiable record of who did so, and it can be changed, often without detection, courts are grappling with ways to authenticate digital evidence under these circumstances. Consider the challenges to authentication presented by each of the technology developments – highlighted below – that have taken place in recent years.

- The "mobile revolution" is upon us. Individuals are becoming more mobile, and they are creating and accessing data through a variety of mobile devices, including laptops, smart phones and tablets. The proliferation of mobile devices results in the creation and transmission of huge amounts of digital information. The new functionalities of these devices, expanding by the day, also change significantly the types of data and information that are created, including digital photographs, video and audio recordings, and text messages of various types. In many cases, e-mail and social media have become predominant means of communication, along with text messages, chat groups, and blogs. Thus, with the availability of mobile devices, millions of people are now creating documentation that may become "evidence" in human rights cases around the world.

- Digital information important for human rights cases is created in many different ways and in a myriad of settings. For example, according to a Pew Research Center study**,** cell phone owners are likely to use their mobile phones in the following ways, most of which involve the creation and transmission of digital data: [5]

    - Take pictures—76% of cell phone owners do this
    - Send or receive text messages—72% do this
    - Access the internet—38% do this
    - Send or receive e-mail—34% do this
    - Record a video—34% do this
    - Play music—33% do this
    - Send or receive instant messages—30% do this

[5] Smith, Aaron, *Mobile Access 2010*, Pew Research Center, *available at* http://www.pewinternet.org/Reports/2010/Mobile-Access-2010.aspx.

- Networking is a business reality. Most government and private sector organizations maintain web sites with myriad functions including chat rooms, wikis, blogs, and news feeds. Business locations may include cities, states, and countries, as well as campuses, sites, buildings, and rooms. In addition, employees may be allowed to work from home offices with complete access to company databases and communications tools. Remote users with portable computers, smartphones and wireless access may not have any fixed location. Law enforcement officials are utilizing new technologies from thermal imaging to GPS tracking. [6]

- The trend toward *consumerization* of information technology means that organizations are beginning to encourage individual users to connect their personal consumer devices, including laptops and handheld devices, to company networks to access applications and professional information for their jobs, as well as for personal use. Thus, in the computing environments of the future, networks will have fewer clearly-defined boundaries. Mobile devices will be used for both business and personal work and communication to access web sites, business applications, e-mail, and social networking sites.

- Social media sites are transforming the way people communicate. Complex relationships between and among individuals and businesses are documented in a constantly changing tapestry of text, audio, and photographic images. Few rules govern the attribution of these data to their sources, and changes to the information are often not logged or documented. Hundreds of thousands of people are members of social networks, creating volumes of digital information. [7]

  The world's largest and most popular social networks are truly global. [8]

  Ameba – Japan (a popular blogging site similar to Wordpress in the U.S.)
  Badoo – Global (based in central London, the company has 118 million members in 180 countries; may appeal particularly to Hispanics)
  BlackPlanet – *African-American*
  Copains d'avant – France (popular among students)
  Douban – China (popular Chinese site for book lovers, movie enthusiasts and music fans)
  hi5 – Global (hi5 describes itself as "the world's leading social play network" and is present in more than 200 countries)
  Hyves – Netherlands (includes blogs, events, photos and chat, and games)
  Ibibo – India (popular site for social games)
  iWiW – Hungary (its name stands for "International Who Is Who." Similar to

---

[6] *Kyllo v. United States*, 533 U.S. 27 (2001); *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010) cert. denied, 131 S. Ct. 671 (2010) and *cert. granted* by *United States v. Jones*, 131 S. Ct. 3064 (2011).

[7] The ten most popular social networks are considered to be *Facebook, MySpace, Twitter, LinkedIn, Classmates, MyLife, Ning, LiveJournal, Tagged*, and *Last.fm*, *available at* http://webtrends.about.com/b/2010/03/15/the-top-10-most-popular-social-networks.htm.

[8] *See*, http://blog.hubspot.com/blog/tabid/6307/bid/15931/The-Ultimate-List-24-of-the-World-s-Largest-Social-Networks.aspx

Facebook, members may log in to other sites with their iWiW credentials)
Mixi - Japan **(**the dominant social networking site in Japan; it offers check-ins and tagging information in real-time through mobile devices)
Muxlim – *Muslim* **(**world's largest Muslim lifestyle network)
Netlog - Belgium (a social networking website targeted at European youth; available in 34 languages with more than 77 million members throughout Europe, but disproportionately from Middle Eastern countries)
Nexopia - Canada ("Canada's largest social networking site for youth")
Odnoklassniki – Russia (a popular social network; appealing because users enter their educational institution; the site provides a list of people from there who are members).

- In our networked and virtual worlds, challenges for authentication arise with popular collaboration and social networking sites because they are designed to facilitate ever-changing information. Posting and broadcasting updates and creating links among thousands and millions of members of social media sites results in significant challenges to proving the authors of particular content.

- "Wiki," a Hawaiian term that means "quick," is a workspace that allows many people to create, modify, and organize web pages. Originally designed so that "anyone" could create, edit, or remove pages easily, wikis are becoming commonly used tools for business communication and collaboration, useful in creating "dynamic" content that changes frequently. Wikis can be hosted on an organization's server or by a third party. Sections of a wiki website can be private or hidden. Similarly, "team rooms" provide collaborative workspaces for creating and storing documents, and communicating with instant messaging (IM).

- Because of technological advances, the format and platforms on which individuals create and store their information are becoming more diverse, and digital information is changing frequently. Information originally created in paper form may be scanned or entered into a database, thus creating digital surrogates. Outsourcing in modern business creates efficiencies by contracting services or functions to an external third party. Because of cost reductions and ease of administration, many organizations are outsourcing their information technology to cloud service providers, resulting in the storage of digital information in cloud environments. Similarly, individuals are using cloud services for e-mail, social media, and storage of a broad array of digital data from documents to photographs.

- Globalization and industrial consolidation means that information systems are international in scope. Organizations operate in more locations, national and international, than ever before. Different laws, markets, and spoken languages are reflected in the digital information that is created around the globe.

- Technology developments are greatly expanding the use of data mining and business intelligence, creating many new types of data. The push towards the creation and use of electronic health records is greatly expanding the types of data available about individuals. Advances in medicine are being reflected in medical records, from digital

MRIs, CAT scans, etc. to bioinformatics. Telemedicine is creating data about remote diagnosis and treatment provided to patients. In life science, biotechnology and nanotechnology are even creating new life forms.

- Electronic commerce is well-established in every country, among both developed and developing nations, and in every business sector. Through e-commerce transactions, new data are created, transmitted and stored. These include point-of-sale purchasing, and financial transactions (e.g., brokerage and banking; contracts are being entered into electronically and sometimes without the involvement of a human being), etc.

- Geospatial images are being used by human rights organizations to rapidly gather, analyze, and disseminate authoritative satellite imagery, especially during times of crisis. They also provide compelling, visual proof to corroborate on-the-ground reporting of conflicts and natural disasters affecting human rights.

- Human rights organizations are developing strategies to systematically collect and preserve electronic information, creating websites that enable the collection of human rights evidence from investigators in the field and massive web archives that preserve significant records of events and communications. These developments show great promise for exposing human rights atrocities and creating a rich body of information that can be used for human rights cases and extra-judicial proceedings.

All of these sources and types of information can be important for human rights purposes and proceedings. However, the new technologies create significant complexities and questions for authentication and admissibility of the material in court. Strategies for facilitating admissibility of digital evidence require advance planning to systematically document key aspects of the evidence.

II. MODERN EVIDENTIARY FOUNDATIONS

This report addresses the evidentiary issues associated with a variety of types of digital information and reviews the approaches U.S. courts have used to authenticate the evidence in judicial proceedings, a critical factor in admitting evidence in a judicial proceeding. The *Federal Rules of Civil Procedure*, and the *Federal Rules of Evidence* govern the admissibility of digital evidence in federal court. State court rules of procedure and evidence (which may differ by State) govern admissibility in state courts.

Electronic evidence can be a key part of proving a case in a legal proceeding. The foundations for digital evidence in most legal proceedings are based on established principles of authentication and admissibility that originated with the use of "paper" evidence. [9]

Five Evidentiary Issues

In order to be admissible, separate "foundations" may be required to show the evidence is: [10]

[9] One court stated that there was no justification for creating a whole new body of law for construing admissibility of electronic communications. *In re F.P.*, 878 A.2d 91 (Pa. Super. Ct. 2005).

- ***Relevant*** – the evidence must be relevant to the claims asserted i.e., it must have "any tendency" to prove or disprove a consequential fact in the litigation.
- ***Authentic*** – a process for establishing that digital data or a document is what it is represented to be.
- ***Hearsay*** – an out-of-court statement introduced for the truth of the matter asserted; it applies if the proponent plans to use the record's contents as substantive evidence. The evidence must not be hearsay or it must be admissible under a hearsay exception.
- ***Best Evidence*** – applies if the document's terms are at issue; there are no "originals" of digital evidence.
- ***Probative value must outweigh any prejudicial effect*** -- Even if the evidence is "logically relevant," a court may exclude it under Rule 403 if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.

Federal Rules of Evidence 104(b) [11] and 901-903 govern authentication of evidence. Fed. R. Evid. 901(a) states:

> "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."

The standard for the admissibility of evidence generally has a low bar under Fed. R. Evid. 901(a). It is only necessary to establish a foundation from which the fact-finder (a jury) could legitimately infer that the evidence is what the proponent claims it to be; for example, that the letter is genuine or the photograph is accurate. The trial judge looks only to the proponent's evidence to assess the rational sufficiency of the foundational evidence, a question of law. The opponent may have controverting evidence. Thus, for digital evidence to be admissible, it must be shown only to be *arguably or colorably* authentic.

In sum, for any evidence to be admissible in a legal proceeding it must meet certain well established criteria, of which authenticity is but one, yet a critical factor. Although the bar for admissibility of evidence is low, each criteria of admissibility must be addressed when seeking to admit any evidence into a legal proceeding.

---

[10] Federal Rules of Evidence that apply to this analysis include Rules 401, 403, 803, 804, 807, 901(a), and 1001-1008. In *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 554 (D. Md. 2007), U.S. Magistrate Judge Paul Grimm stated that admissibility of electronic information as evidence is determined by a collection of evideniary rules that present themselves like a series of "hurdles" to be cleared by the proponent of the evidence -- five distinct but interrelated evidentiary issues that govern whether electronic evidence will be admitted into evidence. The five issues may not apply to every exhibit, but each must be considered.

[11] Fed. R. Evid. 104(b) covers preliminary matters decided by the judge.

Authentication Methods

The federal rules provide a number of authentication methods; these rules are the ones used most often for digital evidence:

Fed. R. Evid. 901(b)(1) – Witness with personal knowledge
Fed. R. Evid. 901(b)(3) – Comparison/ expert testimony
Fed. R. Evid. 901(b)(4) – Distinctive characteristics
Fed. R. Evid. 901(b)(7) – Public records or reports
Fed. R. Evid. 901(b)(8) – Data compilations; "ancient documents"
Fed. R. Evid. 901(b)(9) – System or process capable of producing a reliable result

More specifically, these rules provide as follows:

Rule 901(b)(1) – Witness with Personal Knowledge

A witness provides testimony that a matter is what it is claimed to be. The proponent has a light burden of proof for the evidence to be admitted.

Rule 901(b)(3) – Comparisons

Authentication or identification of the evidence is made by comparison with specimens that have been authenticated.

Rule 901(b)(4) – Distinctive Characteristics

Exhibits can be authenticated or identified by appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstance. Rule 901(b)(7) is use frequently to authenticate e-mail, text messages, and the content of websites.

Rule 901(b)(7) – Public Records or Reports

There is no requirement to show that the computer system producing public records was reliable or the records are accurate. Reports or records produced by governmental entities are generally "self-authenticating," and require no further foundation or testimony.

Rule 901(b)(8) – Data Compilation and Ancient Documents

Evidence that a document or data compilation in any form:

(A) is in such condition as to create no suspicion concerning its authenticity,

(B) was in a place where it, if authentic, would likely be, and

(C) *has been in existence more than 20 years at the time it is offered*. (e.g., 1992 and earlier)

is admissible.

Rule 901(b)(9) – Process or System

Authentication by evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result is permitted under this rule.. [12]

Rules 702 and 703 – Corroborate or prove an expert opinion

Geographic intelligence and satellite images have been admitted into evidence under this rule.

Hearsay

Rule 801 - Hearsay

Even if a piece of digital evidence has been found to be authentic, there are still additional barriers to admissibility. Hearsay can be a significant impediment. The Hearsay Rule bars out of court statements that are offered for the truth of their contents – unless an exception to the rule exists. For example, in general, witnesses are not permitted to testify to what other persons have told them or other statements, oral or written, by other individuals.

In U.S. courts, these five questions must be answered to determine whether a piece of digital evidence is hearsay.

(1) Does the evidence constitute a statement? Fed. R. Evid. 801(a)

(2) Was the statement made by a declarant? Fed. R. Evid. 801(b)

(3) Is the statement being offered to prove the truth of its contents? Fed. R. Evid. 801(c)

(4) Is the statement excluded from the definition of hearsay by Fed. R. Evid. 801(d)?

(5) If the statement is hearsay, is it covered by one of the exceptions in Fed. R. Evid. 803, 804 or 807?

The Hearsay rule is narrow in scope. [13] If the proponent does not offer a statement for its truth, or if the declaration is logically relevant on some other theory, the hearsay rule does not apply. [14]

---

[12] For example, in a case alleging deceptive trade practices by a website-based business, defendants produced a reconstruction from backup tapes of screenshots of their website on a particular day in the past. This process used "technology to create [the Intelius] site at that given time and ... rendered the [ ] pages as they were on that date…"; documents which plaintiff claimed were not authentic. *Hook v. Intelius*, 2011 WL 119630 (M.D. Ga., March 28, 2010).

To authenticate a process or system according to Rule 901(b)(9), the defendants must present "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result." Moreover, " '[i]t is not necessary that the computer programmer testify in order to authenticate computer-generated documents.' ... A computer printout may be authenticated by 'one who has knowledge of the particular record system.' " *U– Haul Int'l. v. Lumbermans Mut. Cas*. 576 F.3d 1040, 1045 (9th Cir.2009).

[13] *New York v. Microsoft Corp*., 2002 WL 649951 (D.D.C., April 12, 2002). (Multiple e-mails excluded as hearsay because they (1) were offered for the truth of the matters asserted, (2) were not shown to be business records under Rule 803(6), and (3) contained multiple levels of hearsay for which no exception had been established.

For what purpose is the electronic evidence being offered?

Decisions about admissibility will usually turn on the purpose for which the evidence is being offered. [15] The complexities of modern business information systems and global communications technology make it essential that litigators and the courts understand the context in which each piece of digital data is created, stored and transferred. Purposes for which digital evidence may be offered include:

- For the truth of the matter asserted
- To show knowledge, notice or intent
- Habit
- Motive, Intent, Scheme or Plan [16]
- Whether the alleged acts actually occurred
- Mental state
- Attitude
- Exact numbers or patterns, probabilities and trends

Exceptions to the Hearsay Rule

Certain types of digital records may constitute hearsay when offered for their substantive truth but may be admitted under a hearsay exception. Here are some examples of these exceptions:

Rule 803 – Availability of Declarant Immaterial

- Present Sense Impression [17] - A statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter.

---

[14] *United States v. Hamilton*, 413 F.3d 1138 (10th Cir. 2005). On appeal of a conviction for transporting child pornography in interstate commerce in violation of federal law, the U.S. Court of Appeals held that the District Court had correctly found that computer-generated header information (also known as metadata) on images defendant had allegedly uploaded to a newsgroup did not constitute hearsay under Fed. R. Civil P. 801. The Court reasoned that the header information did not fall within the Rule 801(c) definition of hearsay because "the header information was automatically generated by the computer hosting the newsgroup each time the defendant uploaded a pornographic image to the newsgroup."

[15] In *Foreward Magazine, Inc., v. OverDrive,,* 2011 WL 5169384 (W.D. Mich., October 31,2011) the court analyzed whether evidence of an Internet chat was hearsay. The court observed that if [the exhibit] was being offered to prove the truth of the matter asserted, then it is hearsay. If it was is offered only to show the sequence of events leading up to plaintiff's decision to decline defendant's offer, then it is not hearsay. Thus the court concluded, like many other items of evidence, that the exhibit is admissible for some purposes and not others.

[16] *State v. Wagner*, 2004 WL 1672200 (Ct. App. Ohio, July 26, 2004) (Pornography found on the defendant's computer was admissible to show the defendant's motive, intent, scheme, or plan in committing sexual abuse).

[17] *United States v. Ferber*, 966 F. Supp. 90 (D. Mass. 1997) (e-mail held admissible under the present sense impression exception to the hearsay rule).

- Excited utterance - A statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by the event or condition.
- Business records
- Public records
- Vital Statistics

Rule 803(6) - Business Records

If a company prints out data and offers a printout at trial as proof of the truth of the data, or provides an electronic copy of the evidence, the printout constitutes hearsay. The proponent must lay a foundation for a hearsay exception such as under Rule 803(6). [18]

Business records are admissible if they are:

- A memorandum, report, record or data compilation, in any form
- Of acts, events, conditions, opinions or diagnoses
- Made at or near the time
- By a person with knowledge
- Kept in the course of a regularly conducted business activity, and
- It was the regular practice of that business activity to make the record or data compilation.

A Custodian or other qualified witness must testify to each of these items, or by certification.

Business records are generally considered by courts to be genuine or truthful. The circumstantial guarantee of trustworthiness is (1) the entry is routine, and (2) business employees have developed habits of precision in gathering and reporting the data helps ensure the reliability of the report. Records kept in the normal course of business are considered reliable evidence because an employee will not remember a particular transaction from among thousands of similar transactions a year.

[18] *Hardison v. Balboa Ins. Co*., 4 Fed. Appx. 663 (10th Cir. 2001). (computer business records are admissible under Rule 803(6) "if the offeror establishes a sufficient foundation in the record."); *United States v. Catabran,* 836 F.2d 453 (9th Cir. 1988). (General ledger computer printouts admissible as business records under Fed. R. Evid. § 803(6), provided that proper foundational requirements are first established; "[a]ny question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility."); *United States v. Vela*, 673 F.2d 86 (5th Cir. 1982) (computerized telephone bills admitted under the business records exception where a telephone company employee laid a proper foundation for the reliability of the telephone bills record-keeping process;. computer data compilations are to be treated as any other records of regularly conducted activity; computerized reports "would be even more reliable than… average business record(s) because they are not even touched by the hand of man.")

Rule 801(d)(2) - Admission of a Party Opponent

Rule 801(d)(2) says an admission of a party opponent, generally a defendant, is *not hearsay*; and it does not require establishing reliability of the statement. [19]

Rule 803(16) – Statements in Ancient Documents

Statements in documents that are 20 years or more old are admissible pursuant to the ancient document rule. [20]

Rule 1006 - Voluminous or Bulky Records

Rule 1006 provides that the contents of voluminous records that cannot be conveniently examined in court may be presented in the form of a chart, summary, or calculation (this includes demonstrative charts). The originals, or duplicates, shall be made available for examination or copying, or both, to the other parties at a reasonable time and place. The court may order that they be produced in court. [21]

Scientific Evidence - Geographic intelligence and satellite images have been admitted into evidence under this rule.

III. EVIDENTIARY FRAMEWORKS FOR COMMON TYPES OF ELECTRONIC EVIDENCE

Challenges for Digital Evidence in Legal Proceedings

Judges and lawyers must have a common understanding of the elements of a foundation for the admissibility of digital evidence in court. The legal framework is the same in most respects as the one courts have traditionally applied when a party is seeking to offer a paper document into evidence. [22] Applying the basic legal principles for establishing a foundation for admissibility to digital data and devices from which electronic evidence is generated presents complex layers of authentication requirements.

The failure to understand how to appropriately and effectively authenticate electronic evidence has resulted in adverse rulings by federal courts. For example, in *Lorraine v. Markel American Insurance Co*., 241 F.R.D. 554 (D. Md. 2007), the court denied a motion for summary judgment due to the failure to provide admissible evidence and properly authenticate computer-generated evidence). In *Vinhnee v. American Express Travel Related Services Company, Inc.,* 336 B.R. 437 (9th Cir. BAP 2005), the court of appeals affirmed the trial court's decision not to

---

[19] *People v. Stone*, 2006 WL 2893777 (Cal. App., Oct. 12, 2006). (documents authored by the defendant and found on his laptop by a computer forensics expert admissible as an admission by a party opponent).

[20] *LG Display Co. Ltd. v. AU Optronics*, 265 F.R.D. (D. Del. 2010) (Paper memoranda (more than 20 years) were held admissible under "ancient document" exception to hearsay exclusionary rule).

[21] *Phoenix v. Com/Systems, Inc*., 706 F.2d 1033 (9th Cir. May 26, 1983) (A computer summary of work orders and parts requisitions was admissible as a summary; underlying documents were admissible under the business records exception); *Ford Motor Co. v. Auto Supply Co.,* 661 F.2d 1171 (8th Cir. Oct. 14, 1981) (Summary of spreadsheets was admissible; spreadsheets were completed in the ordinary course of business).

[22] *Lorraine v. Markel American Insurance Co*., 241 F.R.D. 554 (D. Md. 2007).

admit computerized records because of the lack of foundation for business records and an authentication foundation to assure the accuracy of the records).

In general, there are three primary challenges that are usually made to the authenticity of digital records:

- ***Identity management challenge – Who is the author of the records?*** – Courts look for ways to tie the author to the digital information offered into evidence. Whether a message, document, video, or photo was included in e-mail or posted on a website, it is important for the proponent to provide testimony or as much proof as possible about who the author is.

- ***Is the computer program that generated the records reliable?*** – Was the output of the computer what it is purported to be?

- ***Were the records altered, manipulated, or damaged after they were created?*** – There are numerous examples of how easy it is to alter digital records, often without any evidence of detection. Changes to photographs and videos can be made using Photoshop or graphic design programs, while hackers can alter websites, change databases, and other electronic media. Often they cover their tracks by changing audit log records.

To address these issues, the courts have created three approaches to determine the admissibility of digital evidence. [23] While the standards, ranging from strict to lenient, are discussed in the context of website evidence, the principles apply to all digital evidence. There appears to be no uniformity as to which standard will be applied – it often depends on the jurisdiction of the court and its knowledge of technology, as well as the likelihood the evidence had been altered from the version that was originally created. While the Fed. R. Evid. specify a "low bar" to admissibility of evidence, Non-Governmental Organizations (NGOs) should develop strategies to collect and preserve digital evidence so that it can meet the strictest test of admissibility.

Incompleteness and Integrity - Digital evidence may also be challenged on the basis of "completeness," e.g., is the evidence the entire record or conversation? In a recent case, a federal court held that where a challenge to the authenticity of e-mail transcripts, "instant messages," and "chats" raised an issue of gaps and anomalies in electronic evidence, the question goes to its weight. "There are obvious omissions in some of the communications. However, the Court finds that those omissions do not support excluding the communications. The omissions go

---

[23] ***Strictest*** – A witness with personal knowledge must testify that the information can be attributed to a particular person or organization. The testimony must address who maintained a website where information was posted and who authored the document

Somewhat Strict - Whether linking the information to the website's sponsor is required depends on the circumstances, such as the proponent's incentive and ability to falsify evidence -- in some cases, it is necessary to prove that the website owner actually posted the information.

Lenient - A web page is introduced through a screen shot -- testimony from the person who created the screenshot is required stating that the image "accurately reflects the content of the website and the image of the page on the computer at which the [screen shot] was made." The party seeking to introduce the evidence does not need to show who authored or sponsored the information.

to the weight rather than the admissibility of the evidence." *U.S. v. Lebowitz*, 647 F. Supp.2d 133 (N.D. Ga. 2009).

However, a Nebraska federal court excluded entirely a "cut-and-paste" version of chat room conversations, finding that because several important portions of conversations were omitted, the evidence was "not authentic" and the transcript was not the best evidence because it did not provide an accurate reflection of the original's content of chat room conversations. [24]

21st Century Foundations of Digital Evidence

While U.S. courts have been admitting computer records into evidence since the mid-1970's when computer systems were first used by individuals and organizations, "traditional" foundations for electronic evidence have focused on the relationship between the information and the computer. [25] Documents were admitted based on the assumption that the information produced from a computer is inherently reliable. Consistent with the Federal Judicial Center's *Manual for Complex Litigation*, many courts have required authentication of computer records by proving: [26]

- Reliability of the computer used.
- Dependability of the business's input procedures for the computer.
- Use of proper procedures to obtain the document offered in court.
- Witness's recognition of that document as the readout from the computer.

These foundations for computer records may no longer be adequate to address the complexities of modern information systems from which electronic evidence is generated. In order to demonstrate that digital evidence is what the proponent claims it to be, the foundation must take into account the legal requirements of procedure and evidence (addressing relevance, authentication, best evidence, hearsay, and related issues).

21st century foundations must focus more broadly on the key components of an information system:

- ***People***
- ***Process***
- ***Technology*** (hardware and software)

---

[24] *United States v. Jackson*, 2007 WL 1381772 (D. Neb. 2007).

[25] Imwinkelried, *Evidentiary Foundations*, § 4.03[2], page 59. Questions based on this foundation for computer records for different types of electronic evidence can be found in Professor Imwindelried's book: Computer Records § 4.03[2], "Faxed" Documents § 4.03[3]; e-Mail § 4.03[4]; Information Posted on a Business Website § 4.03[5]; Self-Authenticating Business Records § 4.03[6]; Official Records § 4.04; Caller Identification § 4.04[5]; and Tape Recordings § 4.0. *See, Larry P. v. Riles*, 343 F. Supp. 1306 (N. D. Cal. 1972) (order granting preliminary injunction), aff'd 502 F. 2d 963 (9th Cir. 1974) (per curiam); further opinion 495 F. Supp. 926 (N.D. Cal. 1979) aff'd. 502 F. 2d 963 99th Cir., 1984).

[26] Federal Judicial Center, *Manual for Complex Litigation*, (4th Ed. 2004).

People are instrumental in designing the system, building the ***technology***, and developing the ***processes*** that the system supports, and that make the system operate. Organizations adopt technology in order to improve or streamline their business processes. ***People*** design and build information systems according to an architecture framework – all systems have architectures that make it possible for them to run. People also create the data and information that is stored and processed in the system. ***Information technology*** is a contemporary term that describes the combination of ***computer technology*** (hardware and software) with ***telecommunications technology*** (data, image, and voice networks). Data and information are the central focus of an information system; this is the electronic evidence that proves or disproves the facts at issue in the litigation.

Authentication Questions

Questions related to admissibility must be considered in light of the fact that digital data may be falsely created, changed, or falsified without detection. It can be forged by a hacker, developer, or a lay person. When forwarding an e-mail, the sender can edit the e-mail. Such alterations are often not detectible by the recipient. It will be necessary to show that the information system was correctly designed, configured (firewalls, audit and logging) and maintained (patches). The chain of custody of each piece of evidence must be carefully documented.

The analysis must be tailored to the specific allegations and facts of each case and the types of electronic evidence to be introduced. The rigor with which an evidentiary foundation must be established depends on the purpose for which the electronic information is being offered into evidence, whether there is any reason to believe the evidence is not authentic, and the extent to which the data and information can be corroborated.

Has the authenticity of the electronic information been challenged and on what basis? Do the reason(s) for the challenge undermine the authenticity of the evidence? Do they undermine the validity of the purpose for which the information was offered into evidence?

How can the electronic evidence be corroborated? Corroboration is an essential tool for the successful presentation of electronic evidence in both civil and criminal cases. This can be done through a combination of witness testimony and documentary and physical evidence that address particular points in the case. In presenting electronic information, there are many ways to corroborate data, information, and communications through the content and context of the evidence. Consistent testimony by unrelated witnesses about a particular human rights event can indicate reliability. Actions taken in response to or consistent with an e-mail, text message or social media post can provide indicia of reliability. If it can be shown that purported author/sender was the only one likely to know the information in a message, it may be assumed to be accurate. The corroboration needed depends on the type of system from which the information was produced.

If fraud, forgery, destruction of evidence and similar issues are a central issue in the case, then a jury would decide issues about electronic evidence just as it would in a similar case involving paper documents.

With regard to use of the digital information about events such the killing of Gaddafi, questions that come immediately to mind are:

- Who created the videos of the event?
  - What is the date, time, and place where each video was made? Some of this information may be obtained from the metadata produced with the videos.
- What devices(s) were used to create each video? What information security controls were in place to prevent hacking?
- What is the chain of custody of the digital information?
  - For the video(s) posted on YouTube, who posted them? Where did s/he obtain the videos? For the videos obtained by the television and the news organization, what is the source of the videos?

    Who can testify that the scenes depicted on the videos accurately represent the actual events that occurred?
  - How were the videos transmitted from the devices on which they were created to the websites where they were posted or to the organizations where they were published? Was the digital information sent over the Internet? Was it encrypted or otherwise protected during transmission?

Foundation questions for specific evidence to be introduced in court will be tailored to the data and information to be introduced. [27] Examples of questions to be asked to establish a foundation for admission of human rights records include:

- Description of data/information in the system (what is it, how was it created and how is it maintained)
- Credentials of individuals who designed and operate the system
- Enterprise architecture of the system (hardware, software, logical/ physical/ data flow diagrams)
- Security controls (security plan and security risk assessments, certification and accreditation; vulnerability scanning, password compliance, configuration checking of firewall configuration, open ports, etc., audit and logging, backup tapes)
- Measures to ensure proper functioning of the system: performance monitoring
- Is the evidence a business record?
- How was the exhibit generated?
- What analysis was done? How? For what purpose?

[28] *See* Introduction to Security Issues in Email – PGP, S/MIME and SSL, *available at* http://www.oucs.ox.ac.uk/email/secure/.

- Different foundations for various types of documents (e-mail, printouts, PDF, faxes, information a web site, etc.)
- Chain of Custody
- Why a person is credible or not
- Who are the people who can testify about an incident
- If someone is recording a video, what should they be speaking about?

Establishing a Foundation for Various Types of Digital Evidence

In order to demonstrate that digital evidence is what the proponent claims it to be, the foundation must take into account not only the legal requirements of procedure and evidence (addressing relevance, authentication, best evidence, hearsay, and related issues), but must also include an evaluation of each of the components of the information system from which the evidence was generated. A number of courts have emphasized this essential need, and suggested approaches to establishing an appropriate foundation.

Authentication of Electronic Mail

Electronic mail is used widely for office and personal communication. While people using e-mail may believe that e-mail is secure, it can be easily spoofed and may be read or tampered with during transmission. In order to make e-mail secure, it is necessary to either (1) encrypt the messages using e-mail encryption software, or (2) send the e-mail using a secure connection such as SSL. [28] The underlying assumption in ABA Ethics Opinion 99-413 that transmission of e-mail affords a reasonable expectation of privacy from a technological and legal standpoint, may no longer be valid. [29]

An e-mail may be self-authenticating under Rule 902(7) and courts have routinely admitted e-mails into evidence. [30]

Commentators have reviewed various theories under the rules for the admissibility of e-mails. For example, Professor Imwinkelreid has posited several doctrines that can be used to

---

[28] *See* Introduction to Security Issues in Email – PGP, S/MIME and SSL, *available at* http://www.oucs.ox.ac.uk/email/secure/.

[29] *See* ABA Formal Opinion 99-413 Protecting the Confidentiality of Unencrypted E-Mail (March 10, 1999), *available at* http://www.abanet.org/cpt/nosearch/99-413.pdf ("A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint").

[30] *United States v. Safavian*, 2006 U.S. Dist. LEXIS 32284 (D.D.C. May 23, 2006) (e-mails were properly authenticated by the government); *People v. Downin*, 828 N.E.2d 341 (Ill. App. Ct., April 29, 2005) (trial court did not abuse its discretion in admitting e-mails containing admission of guilt; victim's testimony and other circumstantial evidence sufficiently established the authenticity of the e-mails); *Kearley v. Mississippi*, 843 So. 2d 66 (Miss. Ct. App. October 22, 2002) (Victim's testimony that she had received and printed the e-mails on her computer was sufficient authentication under the Federal Rules of Evidence.); *also see*, *Fenje v. Feld*, 2003 LEXIS 24387 (N.D. Ill., December 8, 2003) (discussion of standards for authentication of e-mail messages).

authenticate e-mail. [31] The professor argues that when a proponent presents an e-mail obtained from a reliable source and received a reply, there is an indicia of reliability. In addition, the argument for admissibility is strengthened when the proponent can show that only the purported author/sender was likely to know the information in the message. Furthermore, when the purported sender takes action consistent with the content of the message, authenticity of the e-mail message is further enhanced. If encryption was used in transmitting the message, this security safeguard is yet further evidence of the reliability of the message and that it has not been changed or tampered with. [32]

Finally, a more traditional method of demonstrating authenticity of e-mail messages would identify the chain of custody or the handling of the e-mail by the computer server and method of transmission and receipt.

Authentication of Information from a Website

Many web pages, formerly "static" and often archived, are now "dynamic," changing in response to different contexts or conditions. Interactivity can be created in two ways: (1) within a presentation in response to behavior by a user, generated on a client's computer; or (2) on a server that adjusts the sequence and reload of web pages or web content supplied to a browser. Server responses may be determined by such conditions as parameters in a URL, the type of browser being used, the passage of time, or a database or server state. From the standpoint of e-discovery, dynamic web pages will likely be different for each user, and the sequence may not be recorded.

The courts have created three approaches to admissibility:

1. A web page or information from a website -- A webmaster or witness with personal knowledge must testify that the information from the website was posted by a person or organization to which it is attributable. The testimony must address who maintained the website and who authored the documents.

2. Information linked to a website -- Whether linking the information to the website's sponsor is required depends on the circumstances, such as the proponent's incentive and ability to falsify evidence -- in some cases, it is necessary to prove that the website owner actually posted the information; a witness may be required.

3. A web page is introduced through a screen shot -- Testimony from the person who created the screenshot is required stating that the image "accurately reflects the content of the website and the image of the page on the computer at which the [screen shot] was made." The party seeking to introduce the evidence does not need to show who authored or sponsored the information.

---

25 Imwindelreid, *Evidentiary Foundations*, Lexis Nexis 6th Ed. section 4.03 [4][b], p. 71.

32 Encryption raises many associated issues, including the standard the encryption reflects, e.g., strong and professionally recognized or weak and ineffective. Also, the "key" or method of decrypting the secure message must, itself, be secure and unavailable to hackers or other malicious actors.

Under these or other theories courts are admitting website evidence. [33] However, information copied from a website it inherently unreliable. The content of a web site can be forged by saving the web site with the "File-Save Page As" command to a local computer hard drive. This will create a local copy of the web page on a computer hard drive. [34] The content can be redisplayed in a browser, modified by a text editor, and printed from a substituted URL.

Witnesses called to authenticate website pages or information obtained from a website can be challenged in the following ways:

1. Web sites are dynamic and may display different content to different users. Web sites that have been infected with a virus may display malicious content to the user only once. In these circumstances, the witness may be challenged to demonstrate that what the witness saw was actually depicted on the website.

2. The web site may change its content slightly in seconds, so it may not be possible for the witness to preserve every word of the page. If the content is copied to a Word document, it must be authenticated separately.

3. A web administrator may testify about the web content. However, this testimony could be challenged by allegations of hacking or the suggestion that a JavaScript DOM injection dynamically changed or modified the website content. If hackers can make websites statically or dynamically display any contents they want testify about the contents of the Internet Archive website would be highly relevant.

In the often-cited case of *Lorraine v. Markel*, 241 F.R.D. 554 (D. Md. 2007), Judge Grimm cited a commentator who presented a number of factors to consider:

- the length of time the data was posted on the site
- whether other persons report having seen it
- whether the data has remained on the website for the court to verify
- whether the data are of a type ordinarily posted on the website or websites of similar entities (e.g., financial information from a corporation)

---

[33] *Hutchens v. Hutchens-Collins*, 2006 LEXIS 87187 (D. Ore. Nov. 30, 2006) (Documents of plaintiff found by defendant's attorney on an Internet site with public access were sufficiently authenticated to use in support of defendant's summary judgment motion.); *St. Luke's Cataract & Laser Institute, P.A. v. Sanderson*, 2006 LEXIS 28873 (M.D. Fla. May 12, 2006) (Evidence of the appearance of web pages on various dates was denied; affidavit of administrative director for Internet Archive submitted two years earlier did not meet the requirements for authentication of evidence); *Telewizja Polska USA, Inc, v. Echostar Satellite*, 2004 WL 2367740 (N.D. Ill. Oct. 15, 2004) (Even though the "Internet Archive is a relatively new source for archiving websites," the website satisfied the threshold requirement of evidentiary reliability under Fed. R. Evid. 901 -- plaintiff could argue the issue of reliability to the jury); *Perfect 10, Inc. v. Cybernet Ventures*, 213 F. Supp.2d 1146 (C.D. Cal. 2002) (printouts from a website properly authenticated under Fed. R. Evid. 901(a) where plaintiff's CEO testified the exhibits attached to his declaration were "true and correct copies of pages printed from the Internet that were printed by [him] or under his direction."); *St. Clair v. Johnny's Oyster & Shrimp*, Inc. 76 F. Supp.2d 773 (S.D. Tex. 1999) (information from the Internet is inherently untrustworthy).

[34] http://www.depo.com/E-letters/TheDiscoveryUpdate/2008/October/Artices/website_authentication.htm.

- 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 have been republished by others who identify the source of the data as the website in question

Finally, web pages can be generated from official government websites. Under these circumstances, they may be considered to be self-authenticating. As such, these sites will be deemed authentic and admitted as evidence. [35]

In sum, while the courts continue to grapple with the admissibility of websites and website information, most courts – on whatever grounds – have found the information admissible. Indeed, notwithstanding the genuine risk of unreliability due to hacking or other malicious changes, the courts continue to admit such information into evidence.

Authentication of Photographs

Digital photographs are typically admitted into evidence to illustrate testimony under Fed. R. Evidence 901. Photographs are classified as "writings" in the rules. As such, they require authentication. Tampering with photographs, *i.e.*, changing relevant features is the issue. However, courts have responded with skepticism that images taken digitally and stored on computers are untrustworthy.

When a photograph is used to "illustrate" testimony, the rules are "relaxed." Little attention is paid to authentication and chain of custody. If a witness can testify that the photograph is an accurate depiction of the scene that the witness is to testify about, the photograph will be readily admitted into evidence. Here, a witness need not have taken the photograph or know any of the circumstances under which it was taken.

When the photograph is offered to prove the existence of an allegedly depicted condition – an ultimate fact, or used as the basis for the testimony of an expert witness, the photograph will be held to a higher standard to demonstrate its authenticity.

Digital Cameras

Modern digital cameras store metadata that can be used to authenticate digital photographs. Metadata is internally stored information about the creation and alteration of any electronic file. For modern digital cameras, the file will typically show the camera model, time and date of the photograph, focal length, and other characteristics.

It is also important to use the digital camera's setup menu to set the camera for normal sharpness, contrast, and color. The idea is to set the camera to settings that will produce photographs that depict what the human eye would have seen when the photograph was taken. [36]

---

[35] *Williams v. Long*, 2008 WL 4848362 (D. Md., November 7, 2008) (case search results printed from official government websites admitted).

Metadata may show when a digital photograph has been changed. Photos that are underexposed can be sharpened; latent detail can also be enhanced using Photoshop and other commercially available software. All these changes will need to be documented and explained. Any change that could lead to an allegation of deception should be carefully considered.

Digital photographs employed to prove ultimate facts require a witness who can testify that the scene depicted is an accurate representation of what the witness saw and be equipped to defend by the use of metadata any challenge to the authenticity of the photograph.

Authentication of Information from Social Media Sites

The explosion of participants in social networking venues such as Facebook, MySpace, and LinkedIn, including the creation of business and professional groups hosted on these sites, has resulted in information creation that is outside the knowledge and control of any specific organization. Because collaborative technologies transform the way individuals exchange information, litigators will be required to address their impact in creative ways.

Courts generally apply a stricter standard to information from a social networking site, because of the absence of restrictions on who may create or update a profile. Anyone can create a social network profile anonymously, using a pseudonym, or in someone else's name. Since one or many people may post messages on a social networking site, courts cannot necessarily attribute a particular message to the person who owns the site. Determining who made a post is particularly difficult if the person made the post from a public computer such as in a library or a hotel. [37]

Authentication of Instant Messenger/Messages

Courts have likewise admitted "instant messages." For example*, in In re F.P.*, 878 A.2d 91 (Pa. Super. Ct. 2005), the defendant appealed from an assault conviction, asserting the trial court erred in admitting improperly authenticated computerized instant messages into evidence. The defendant argued the messages should have been authenticated by either the source Internet Service Provider or computer forensic expert testimony. Rejecting this argument, the appellate court declared the circumstantial evidence properly rendered the instant messages admissible.

The court noted the defendant's argument would require it to create a whole new body of law just to deal with e-mails or instant messages. The court further stated it found no justification for constructing unique rules for admissibility of electronic communications such as instant messages. In this case, the instant messages were properly authenticated based on the following factual circumstances: the defendant referred to himself by name, his testimony mirrored some of

---

[36] *See, State of Connecticut v. Swinton* , 847 A.2d 921 (S. Ct. Conn. 2004) (requiring an adequate foundation for enhancements of photographs had been presented).

[37] *See, Griffin v. Maryland*, 2011 WL 1586683 (D. Md., April 28, 2011) (the potential for manipulation of social networking site evidence required greater scrutiny of the foundational authentication requirements than that of traditional records).

the comments in the instant messages, and he referenced one of the instant messages in a conversation with school authorities.

Authentication of Official Records

Some computer records have been treated as self-authenticating based on the assumption that information produced by a computer is inherently reliable. [38] Sometimes web pages are generated from official government websites. Under these circumstances, they may be considered self-authenticating, and will be considered authentic and admitted as evidence. [39]

The Government Printing Office (GPO) is responsible for providing permanent public access to authentic U.S. Government publications. GPO has launched an initiative [40] to assure users that information provided on its website is official and authentic and that trust relationships exist between all participants in electronic transactions. The GPO provides authenticated Adobe Portable Document Format (PDF) files for the 110th and 111th Congresses. Public and private laws are published by the Office of the Federal Register (OFR), National Archives and Records Administration (NARA). They are available as authenticated PDF files that have been digitally signed and certified by GPO using Public Key Infrastructure (PKI). Public laws for earlier years are not authenticated and digitally signed.

Authentication of State Official Records - In a major report published in 2007, the American Association of Law Libraries (AALL) addressed the question: How trustworthy are state-level primary legal resources on the Web? [41] This report examined the results of an online state survey that investigated which government-hosted legal resources on the Web are official and capable of being considered authentic. This report casts serious doubt on the authenticity of official records obtained from state web sites.

Official status demands appropriate authentication procedures. Standard methods of authentication may include encryption, digital signature and public key infrastructure, but other methods to adopt best practices are also possible. Certification or other types of formal endorsement of legal resources are a vital link in the "chain of custody" involved in dissemination, maintenance, and long-term preservation of digital materials. That chain may contain a link to computer technologies that guarantee the very copy delivered to one's computer screen is uncorrupted and complete or it may be part of other archival methods.

---

[38] Self-Authenticating Business Records: Federal Rules of Evidence -- Rules 902(11) and Domestic Business Records and (12)) Foreign Business Records.

[39] *Williams v. Long*, 2008 WL 4848362 (D. Md., April 7, 2008) (case search results printed from official government websites admitted on the basis that they are self-authenticating).

[40] GPO Authentication Initiative, Public and Private Laws Beta Application, Authenticated Public and Private Laws, available at http://fdlpdev.gpo.gov/plaws/index.html (last accessed July 11, 2007). *See* NIST Special Pub. 800-63, Electronic Authentication Guideline, available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

[41] American Association of Law Libraries, *State-By-State Report on Authentication of Online Legal Resources* (March 2007), *available at* http://www.aallnet.org/aallwash/authenreport.html.

Online legal resources are increasingly the sole official published source. Laws addressing those resources and other online official sources are seriously deficient, failing to require certification as to completeness and accuracy for online resources comparable to that required for print official sources. In 2011, the Uniform Law Commission passed the Uniform Electronic Legal Material Act (UELMA) to address these shortcomings – it will not be until states pass UELMA, and official publishers authenticate online legal material, that this problem is fully addressed.

Authentication of Metadata

Metadata provides information about data that "describes how, when, and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information)." [42] There are system and application metadata. Presently there are approximately 120 different types of metadata in the applications and systems used by organizations and individuals. [43] Authentication of metadata requires proof about how it was generated, and why it is accurate. There are many ways to change metadata as documents, databases, and data in other repositories are viewed, edited, updated, and otherwise changed.

Authentication of Business Records

In a well-designed information system, information technology offers the opportunity to collect and store enormous volumes of data, process business transactions with great speed and accuracy, and provide timely and relevant information for management. In many organizations, information has become a managerial resource equal in importance to property, facilities, employees, and capital. Many organizations consider information systems and computer applications as essential to their ability to compete or gain competitive advantage.

Authentication of Computer Printouts and other Computer Information

Computer printouts are commonly authenticated by a witness who testifies that the printout constitutes a complete record of all the relevant transactions or events. [44] Similar testimony will result in the authentication of other computer records. [45] The use of encryption on a computer will strengthen the authenticity of the relevant information and reduce the burden on

---

[42] The Sedona Conference: *Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age,* (2005) *available at* http://www.thesedonaconference.org/content/miscFiles/TSG9_05.pdf (last viewed July 15, 2007).

[43] Sedona Conference, *Id*.; *see* ABA Standing Committee on Ethics and Professional Responsibility, Formal Opinion 06-442, *Review and Use of Metadata* (August 5, 2006).

[44] *United States v. Melenberg*, 263 F.3d 1177 (10th Cir. 2001) (printouts were a record of all transactions and reflected the underlying records); *People v. Markowitz*, 721 N.Y.S.2d 758 (Sup. Ct. February 9, 2001) (testimony of a company employee who prepared the databases was sufficient foundation for admission of the electronic evidence);
Bank v. Eurich, 831 N.E. 2d 909 (S.J.C Mass., August 3, 2005) (Computer printouts admitted; bank routinely accessed and relied upon the accuracy of the information).

[45] *Vinhnee v. American Express Travel Related Services Company, Inc.,* 336 B.R. 437 (9th Cir. BAP 2005) (computerized business records not admitted due to lack of foundation); *People v. Rivera*, 537 N.E. 2d 924 (App. Ct. Illinois, April 4,1989) (enunciated standards for the admissibility of computer records).

the litigant in introducing the information into evidence. [46] Other issues focused on the admission of computer records or other information generated by a computer can be addressed by a computer forensics expert. [47]

Authentication of Information from a Web Archive

Web archives are being created by human rights organizations. Regular captures are being made of web sites; the material is being saved and preserved for the future. Web archiving is a new and important trend toward preserving human rights electronic evidence. Material from websites is being saved and preserved for the future. [48] Archived information from websites is being admitted into evidence just as information from active sites is being admitted. [49]

The Columbia University Center for Human Rights Documentation & Research has created a *Human Rights Web Archive* to select, preserve, and provide access to freely available human rights resources, specifically addressing at-risk websites in the area of human rights. These resources were created mainly by non-governmental organizations, national human rights institutions, and individuals. See http://library.columbia.edu/indiv/humanrights/hrwa.html.

Archive-It is a subscription service developed in 2005 by the Internet Archive, a Digital Library founded in 1996. Internet Archive has the largest public web archive in existence, compromising 200 billion pages, and over 85 million websites in 40 languages. *See* http://www.archive-it.org/public/collection.html?id=1068. Archive IT partners with over 160 institutions, including state archives and libraries, university libraries, federal institutions, NGOs, museums, public libraries, historical societies, and independent researchers.

Because web archives consist of collections of many web sites with material created in the past, they present significant challenges for establishing a foundation for admissibility. A foundation for each "layer" of evidence must be provided separately, including the chain of custody. The principles outlined above should be applied to each type of digital information in the web archive to be offered into evidence. For example, this should include testimony about who created the material, where the evidence was originally created or posted, and address how

---

[46] *State v. Levie*, 695 N.W.2d 619 (Minn. Ct. App. June 10, 2005)(admission of testimony of a computer forensic expert about defendant's computer usage and the presence of an encryption program on his computer deemed admissible).

[47] *Galaxy Computer Services, Inc. v. Baker,* 2005 WL 2171454 (E.D.Va. 2005) (testimony of a computer forensics expert concerning files deleted from a computer hard drive); *Kupper v. State of Texas*, 2004 WL 60768 (Ct. Ap. Texas, January 14, 2004) (testimony of a computer forensics expert concerning chain of custody and examination of a computer hard drive); *Inventory Locator Service, LLC* v. *PartsBase, Inc*., 2006 LEXIS 39521 (W.D. Tenn. 2066) (expert analysis that a party fabricated electronic evidence warranted appointment of a special master to determine that authenticity of allegedly altered server-logs).

[48] In April 2010 Twitter donated its entire archive of public tweets to the Library of Congress, so that it becomes part of the "historical record of communication, news reporting, and social trends – all of which complement the Library's existing cultural heritage collections." It contains a record of important events such as the 2008 United States presidential election and the "Green Revolution" in Iran. It also serves as a news feed with minute-by-minute headlines from major news sources. At the same time, it is a platform for citizen journalism with many significant events being first reported by eyewitnesses.

[49] *Telewizja Polska USA, v. Echostar Satellite Corp*., 2004 WL 2367740 (N.D. Ill. Oct. 15, 2004) (admission of material in internet archive).

the evidence was collected and maintained in the archive web site.

Authentication of Geospatial Technologies – Satellite Images

The Center for Resource Libraries - Global Resources Network Human Rights Archives and Documentation Project (HRADP) "supports the gathering, preservation, and appropriate accessibility of archives and documentation regarding human rights and legal proceedings in all world regions. [50] The American Association for the Advancement of Science (AAAS) has partnered with human rights organizations to provide them with technical assistance in using geospatial technologies to strengthen advocacy campaigns, support legal cases, and enhance response coordination and prevention efforts. Human Rights Watch used high-resolution imagery and other geospatial data to understand how and why civilians were killed or injured during Operation Iraqi Freedom, and made use of an archive of high-resolution imagery to document the systematic destruction of homes by Israeli Defense Forces in the Gaza Strip.

These are just a few examples of the uses organizations are making of satellite images to documents potential human rights violations. Geovisualization is an emerging field that draws upon approaches from several disciplines such as cartography, information and scientific visualization, and geographic information systems (GIS) to provide theories, tools, and methods for the presentation of geographic - or spatial - data. In some cases this may mean creating data with coordinates from global positioning systems (GPS) and then using the established methods and tools to display them in print or digital form. [51]

Validation of Scientific Evidence

The courts have long been suspicious of scientific evidence. In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993) the U.S. Supreme Court held that the trial judge must ensure that testimony qualifies as "scientific knowledge." A proponent must demonstrate that the theory is the product of sound scientific methodology – considering such factors as (1) whether the proposition is testable, (2) whether it has been tested, (3) the validity rate attained in any tests, (4) whether the research has been peer reviewed, and (5) whether the findings are generally accepted. This will often require two expert witnesses: a person with academic credentials and a technician. Images from satellites often record human rights abuses and, as such, can constitute valuable evidence.

Two potential avenues for admitting geographic intelligence are as demonstrative evidence under Rule 1006 of the Federal Rules of Evidence, or as scientific evidence under Rule 702 and 703. An argument can be made that a geographic intelligence exhibit is essentially "a chart, summary, or calculation" and thus admissible under Fed. R. Evid. 1006, which provides that "[t]he contents or voluminous writings, recordings, or photographs which cannot

---

[50] This documentation may include:
- The records of official tribunals, courts, truth commissions, and investigations of human rights violations
- Records of NGOs devoted to preventing, monitoring, and documenting human rights violations, including reports and documentation generated for advocacy and awareness
- Evidence and documentation collected by those official and NGOs, and gathered by others.

[51] Shadrock Roberts, What It Means to Think Spatially, US AID Frontlines, June/July 2011, *available at* http://www.usaid.gov/press/frontlines/fl_jun11/FL_jun11_ST.html

conveniently be examined in court may be presented in the form of a chart, summary, or calculation." [52]

Evidence such as maps, reports, and three-dimensional images is created from a geographic information system (GIS) and remote sensing tools. They use complex and voluminous data to present an illustrative and scientifically accurate chart for the court. Courts have long held that illustrative charts may be used to summarize complex computations in order to make the evidence "more enlightening to the jury." [53] For example, graphic computer presentations have been found to be "more akin to a chart or diagram than a scientific device. Whether a diagram is hand draw or mechanically drawn by means of a computer is of no importance." [54] A New York state court stated it directly. The court, the first to admit a graphic computer presentation at a criminal trial, expressly recognized (476 N.Y.S.2d at 722-23) that:

> "[c]omputers are simply mechanical tools … When the results are useful, they should be accepted, when confusing, they should be rejected. What is most important is that the presentation be relevant… that it fairly and accurately reflect the oral testimony offered and that it be an aid to the jury's understanding of the issue."

The more ways a party can show that the information is reliable all the way through the chain, from the satellite, to the computer, to the processing, to the final product, the greater the confidence the court will have in it. The same guiding principles apply to geographic intelligence figures and remotely sensed imagery when introduced as demonstrative evidence under Rule 1006. Under Rules 702 and 703, the proponent of the evidence would be guided by the *Daubert* standard, specified above.

IV. RECOMMENDATIONS - HUMAN RIGHTS DOCUMENTATION BEST PRACTICES

Outlined below are some principles NGOs should consider when determining ways to maximize the likelihood that digital evidence will be authenticated and admitted into evidence. The initial focus should be on the questions courts have traditionally asked when a party is seeking to offer a document into evidence (outlined in sections II and III above). Some of these principles go to the weight of the evidence.

This report has identified the practical legal issues related to the admissibility of electronic evidence for court cases, *e.g.*, rules of evidence, standards of review, and relevant precedent for accepting or rejecting certain formats and reasons. NGOs responsible for or involved in human rights cases should anticipate in advance the admissibility and authentication issues that could arise in a judicial or extra-judicial proceeding, so they will be able to present the evidence systematically. In the digital age, there are many ways to cast doubt on the authenticity of electronic evidence. Sound and informed practices must be adopted to determine whether the evidence fulfills the legal requirements for authenticity, reliability and integrity.

In sum, to be authenticated by a court, an advocate must assume the proposed evidence will be challenged. In this circumstance, detailed documentation should be maintained recording

---

[52] *See generally,* Hodge, "Satellite Data and Environmental Law: Technology Ripe for Litigation Application," 14 Pace Envtl.L.Rev.691, 718 (1997).
[53] *McDaniel v. United States*, 343 F.2d 785, 789 (5th Cir.), cert. denied, 382 U.S. 826 (1965).
[54] *People v. McHugh*, 124 Mis.2d 559, 560, 476 N.Y.S.2d 721, 722 (1984).

key facts about the evidence. With documentation, challenges – or questions about the evidence – can be addressed.

1. Documentation About Essential Aspects of Evidence – Content and Context - Must be Kept

The proliferation of electronic devices means that huge amounts of digital information are being created every day. Of significance for human rights incidents, numerous disparate individuals are recording the details of events in pictures and vivid descriptions as they unfold. In some other situations, "official" records are being created by government organizations, such as police, of treatment of individuals.

Much of these "on-the-scene" recordings of events are *ad hoc*, created with personal mobile devices such as smart phones, cameras, and tablets. The material is usually posted on a web site such as YouTube, a social media site, or is sent to a news organization. What should NGOs do to collect and preserve this material for possible use in a human rights proceeding? Along with the information, NGOs should collect as much data as possible about the context surrounding the events. In addition, they should collect any devices that are available with the recordings of human rights incidents. Data created by organizations and stored in databases or information systems should be collected and preserved by NGOs. In short, NGOs must organize available data systematically and identify witnesses with personal knowledge who can testify about the circumstances of its creation and the substance of its content.

Documentation is crucial to recall and demonstrate, at a later stage, the initial status of the scene and what was done, when, how and by whom. Chronological and careful documentation is important to ensure the "traceability" and "continuity" of the evidence throughout the process. The following documentation should be obtained about each piece of digital information that may be used in court or an extra-judicial proceeding.

- ***Who*** -- who produced a video, wrote an e-mail, tweet, or made a social network posting?
- ***What*** -- what is the video/ message/ post about; describe the scene, who is in it, what is the setting?
- ***When*** -- when was it taken or posted, date and time?
- ***Where*** -- where was it taken or posted?
- ***Why*** -- why was it taken, what is the background and context?
- ***How*** -- details of the device used to produce the data

2. Keep Information About Devices on Which the Evidence Was Created

To authenticate digital data, it is important to have as many details as possible about the device that was used to create the information, and detailed records of every person who handled, accessed, examined, or used the device.

For example, owner and contact information, device manufacturer, model, serial number, operating system, date the information was created, date the device was acquired by the

custodian identified in the log. The device properties and metadata will provide a wealth of identifying information that should be retained for whenever the information is used in a human rights proceeding. If the device contains an audit logging capability, audit records should be obtained as well.

3. Document Essential Facts Regarding Digital Evidence during Its Entire "Lifecycle"

A useful way to analyze best practices for digital evidence is to look at the "digital information lifecycle" [55] and determine for each stage what should be done to maximize the likelihood that the information will be admitted as evidence:

- Creation of Digital Evidence
- Physical Evidence – Collection and Storage
- "Transmission" of Digital Evidence
- Storage, Archiving and Preservation of Digital Evidence
- Chain of Custody

Documentation should be created and maintained to record each step in the digital evidence lifecycle to the extent practicable. In addition, information governance best practices must include a requirement to document the privacy requirements of each type of information and protect confidential information of individuals appropriately.

Thereafter, practical issues relating to chain of custody and the need to maintain careful documentation of the collection and maintenance of digital information must be addressed. Finally, as an example, the steps or questions needed of obtain the authenticity of digital evidence are set forth in section III,

4. Record the Chain of Custody of all Physical and Digital Evidence

The concept of chain of custody is derived from criminal law and requirements for the handling of physical evidence. Its principles apply to much of digital evidence because the integrity of the evidence can be challenged because the digital evidence can be changed.

The value of even carefully recovered and preserved evidence can be lost if the chain-of-custody is not maintained. "Chain of custody" refers to the "chronological and careful documentation of evidence to establish its connection to an alleged crime or incident. From the beginning to the end of the process, it is crucial to be able to demonstrate every single step undertaken to ensure "traceability" and "continuity" of the evidence from the incident to the courtroom. [56]

---

[55] The "lifecycle of human rights documentation" consists of multiple (and often overlapping) steps from the creation of documentation related to a human rights violation to the final stages of long-term preservation and maintenance of the evidence.

[56] *See*, United Nations Office on Drugs and Crime (UNODC), Crime scene and physical evidence awareness (New York, 2009),

In criminal cases, this information is recorded in a detailed evidence log. The purpose of this record is to enable the proponent to be able to prove that the proffered evidence had not been changed from that originally created.

5. Information Security – Ensure Lifecycle Evidence Not Changed or Falsified

Record what *controls* are built into the information system to ensure integrity, accuracy, reliability, and authenticity. Many computer systems have sophisticated audit logging systems to track and record the information about users and their transactions, as well as integrity checks and information security built in to ensure the data are accurate.

Illustration - E-Mail – Indicia of Reliability

In order for e-mail to be admissible, individuals and organizations should create a business-like form and format for e-mail, with the following clear indicia of ownership:

- Name of e-mail account, name of sponsoring organization
- Name and identification/affiliation of author; e-mail address
- Business labels: signature block with identifications, name
- Signature
- Further identification such as photograph of author
- Place where the e-mail is stored
- e-mail hosting service; Internet service provider
- Metadata

CONCLUSION

The report suggests some principles NGOs should consider when determining ways to maximize the likelihood that digital evidence will be authenticated and admitted into evidence. The initial focus should be on the questions courts have traditionally asked when a party is seeking to offer digital information into evidence. With the increasing collection and use of digital evidence, NGOs must be ever-vigilant to document the sources of the information they gather and the devices used to create digital evidence.

V. REFERENCES

United States Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2001), updated version, *available at* http://www.neiassociates.org/searchmanual.htm

United Nations Office on Drugs and Crime (UNODC), Crime scene and physical evidence awareness (New York, 2009), *available at* http://www.unodc.org/documents/scientific/Crime_scene_awareness__Ebook.pdf

Smith, Aaron, Mobile Access 2010, Pew Research Center, *available at* http://www.pewinternet.org/Reports/2010/Mobile-Access-2010.aspx

