WORKING PAPER

AN OVERVIEW OF THE USE OF DIGITAL EVIDENCE IN INTERNATIONAL CRIMINAL COURTS

SALZBURG WORKSHOP ON CYBERINVESTIGATIONS

This paper was prepared by Aida Ashouri '14, Caleb Bowers '15, and Cherrie Warden '15, students from the International Human Rights Law Clinic and the Samuelson Law, Technology & Public Policy Clinic at the University of California, Berkeley, School of Law, under the supervision of Professors Laurel E. Fletcher, Chris Hoofnagle, Eric Stover, and Jennifer Urban

October 2013

Table of Contents

Abstract

As digital evidence becomes more prevalent, it poses challenges to the International Criminal Court. This paper reviews some of the leading international criminal cases involving digital evidence, with a particular focus on the ICC, and identifies four types of evidentiary considerations specific to digital evidence: (1) authentication; (2) hearsay; (3) provenance (chain of custody); and (4) preservation of evidence. Using these four considerations, this paper aims to contribute to discussion on how best to respond to the challenges of digital evidence. The paper concludes with several questions raised by this analysis.

I. Introduction

Digital evidence poses particular challenges to the International Criminal Court ("ICC" or "Court"). Defined as information transmitted or stored in a digital format that a party to a case may use at a proceeding,[1] digital evidence may come in the form of photographs, video and audio recordings, emails, blogs, and social media (e.g. Facebook, Twitter). As digital evidence becomes more prevalent, the ICC must consider how to respond to its use. To assist in this effort, this paper reviews how judges have viewed the admissibility and probative value of digital evidence presented in proceedings at international criminal courts, with a particular focus on the ICC.[2]

The increasing use of digital evidence in proceedings offers new opportunities and challenges. Evidence of e-mail, a satellite intercept, or a video may help establish linkage evidence between the defendant and the commission of an international crime. Depending on the technology, digital evidence can also provide information on the time, place, and manner of an event to supplement *viva voce* evidence or live testimony. But digital evidence can also be altered or degraded. In addition, digital evidence is divorced from its source; for example, a photograph captures only one perspective of a location at a specific time, and e-mail does not capture the demeanor or tone of voice of the author.

This paper analyzes selected cases from the ad hoc International Criminal Tribunal for the former Yugoslavia (ICTY), the ad hoc International Criminal Tribunal for Rwanda (ICTR), the Extraordinary Chambers in the Courts of Cambodia (ECCC), the Special Court for Sierra Leone (SCSL), and the Special Tribunal for Lebanon (STL). We identified this pool of cases based on secondary literature, interviews with current or former court staff, and experts knowledgeable about the use of digital evidence in international criminal courts. This paper identifies four types of evidentiary considerations specific to digital evidence: (1) authentication; (2) hearsay; (3) provenance (chain of custody); and (4) preservation of evidence. The paper concludes with observations and questions raised by this analysis.

---

[1] *See* EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME (3d ed. 2011).

[2] The evidentiary standards at the International Criminal Court (ICC) reflect "current developments of the procedural models adopted by the international criminal tribunals," specifically those of the International Criminal Tribunal for the former Yugoslavia (ICTY) and the International Criminal Tribunal for Rwanda (ICTR) therefore making consultation with jurisprudence from these and similar tribunals appropriate. See Prosecutor v. Bemba Gombo, Case No. ICC-01/05-01/08, Decision on the admission into evidence of materials contained in the prosecution's list of evidence, ¶ 25 (Nov. 19, 2010).

This paper is not exhaustive of all potentially relevant cases. Trial transcripts, pleadings, and other public records of the cases presented here are not incorporated into this analysis. Such materials may identify additional concerns and questions regarding digital evidence. Nevertheless, this paper identifies the key cases and issues regarding the introduction of digital evidence and serves as background for a fuller discussion of the challenges and opportunities in this area.

II. Legal Standard of Admissibility of Evidence

The use of digital evidence in international criminal courts must be understood in light of the general approach to the admission of evidence in trial proceedings. International criminal courts incorporate elements of the common law and civil law traditions to varying degrees. Generally, the common law system contains more prohibitions and rules on excluding evidence that is irrelevant or unreliable, while in the civil law system all evidence is admitted and judges subsequently assess its probative value.[3] The Rome Statute created a system that "eschew[s] generally the technical formalities of the *common law* system of admissibility of evidence in favour of the flexibility of the *civil law* system."[4]

Rule 69(4) of the ICC Rules of Procedure and Evidence ("Rules") directs judges to admit evidence, "taking into account, *inter alia*, the probative value of the evidence and any prejudice that such evidence may cause to a fair trial or to a fair evaluation of the testimony of a witness."[5] In accordance with Rule 63(2), ICC judges determine the probative value and the "appropriate weight" of admitted evidence at the end of a case, when they are considering the evidence as a whole.[6] There are only two situations where there is a specific duty for judges to make a ruling

[3] Id. at ¶ 17 fn.28.
[4] Id. at ¶ 17.
[5] Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Decision on Confirmation Charges, ¶ 100 (Jan. 29, 2007).
[6] Id. at ¶ 9; *see also* Bemba Gombo, ICC, "Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute" of 6 September 2012, ¶ 11 (Oct. 8, 2012). Probative value refers "to the reliability and weight to be attached to the evidence concerned." Id. at ¶ 8. In order to be considered relevant, evidence must have the potential to influence the determination on at least one fact. Id. The Chamber must consider all the evidence "'submitted' before it and 'discussed' at trial in making its final determination regardless of the type of evidence presented." Bemba Gombo, ICC, Decision on the admission into evidence of materials contained in the prosecution's list of evidence, ¶ 15 (Nov. 19, 2010).

on the admissibility of evidence.[7] These provisions are drafted narrowly and do not provide for automatic exclusion of evidence.[8]

Similarly, the ICTY and ICTR have largely avoided common law rules of evidence exclusion as such rules were developed to limit evidence considered by juries and therefore are inapplicable to trials in the inquisitorial tradition.[9] Evidence must satisfy "minimum standards of relevance and reliability" to be admitted.[10] Since the bar for admissibility is low, admission of evidence does not in of itself signal that the evidence is accurate; judges separately evaluate its weight.[11] Thus, in considering evidence, the ad hoc tribunals do not focus on whether evidence is admissible, but rather what weight the evidence holds.

While the threshold of admission of evidence may be low, international criminal courts still have preferences for types of evidence introduced. The ICC generally favors *viva voce* evidence, or oral testimony.[12] When evidence other than direct oral testimony is challenged, the ICC Chamber "must ensure that the evidence is *prima facie* relevant to the trial, in that it relates to the matters that are properly to be considered by the Chamber in its investigation of the charges against the accused and its consideration of the views and concerns of participating victims."[13]

The ICC has developed standards specific to digital evidence. Digital evidence and material must conform to an "e-Court Protocol," even before it is submitted at the Confirmation Hearing.[14] The Protocol is designed to "ensure authenticity, accuracy, confidentiality and preservation of the record of proceedings."[15] The Protocol requires metadata to be attached,

---

[7] The only exceptions to this broad standard are provided in Article 69(7) of the Rome Statute and 71 of the ICC Rules. Article 69(7) of the Rome Statute prohibits evidence acquired by means that violate the Rome Statute or human rights if "the violation casts substantial doubt" on the reliability of the evidence or its admission would be "antithetical" and would "seriously damage the integrity of the proceedings." Rule 71 prohibits the admission of evidence of prior or subsequent sexual conduct of a victim or witness. Bemba Gombo, ICC, Decision on the admission into evidence of materials contained in the prosecution's list of evidence, ¶ 9 (Nov. 19, 2010); Rome Statute of the International Criminal Court, Article 69(7); International Criminal Court, Rules of Procedure and Evidence, Rule 71; *see also* Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Decision on Confirmation Charges, ¶ 87 fn.98 (Jan. 29, 2007).

[8] Id. at ¶ 84.

[9] Prosecutor v. Brdanin & Talic, Case No. IT-99-36-T, Order on the Standards Governing the Admission of Evidence, ¶ 14 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 15, 2002).

[10] Id. at ¶ 13; Case 001, Case No. 18-07-2007/ECCC/TC, Decision on Admissibility of Materials in the Case File, ¶ 7 (May 26, 2008).

[11] Brdanin & Talic, ICTY, Order on the Standards Governing the Admission of Evidence, ¶ 18 (Feb. 15, 2002); Prosecutor v. Boškoski & Tarčulovski, Case No. IT-04-82, Trial Judgment, ¶ 10 (Int'l Crim. Trib. for the Former Yugoslavia July 10, 2008).

[12] There are several exceptions to the preference of live testimony, including the permission to give recorded testimony, or to introduce documents or written transcripts. Bemba Gombo, ICC, Decision on the admission into evidence of materials contained in the prosecution's list of evidence, ¶ 14 (Nov. 19, 2010).

[13] Id. at ¶ 10 fn.23 (quoting Lubanga, ICC, Trial Chamber I, ¶¶ 26-27 (June 13, 2008)).

[14] Prosecutor v. Callixte Mbarushimana, Case No. ICC-01/04-01/10, Decision Amending the e-Court Protocol, 4 (Apr. 28, 2011).

[15] International Criminal Court e-Court Protocol at ¶ 1, ICC-01/04-01/10-87-Anx 30-03-2011, *available*

including the chain of custody in chronological order, the identity of the source, the original author and recipient information, and the author and recipient's respective organizations.[16] While the Protocol offers some guidance to facilitate the use of digital evidence, it is limited to harmonizing the format of digital evidence, and how it is stored in the Court's systems, and does not address issues of probative value of digital evidence. These challenges are discussed further below and how courts have addressed them in trial.

III. Evidentiary Considerations of Digital Evidence

Research for this paper found that international criminal courts rarely admitted digital information as direct evidence, but more commonly admitted it as corroborating evidence. Digital evidence is often introduced with other evidence that, in the opinion of the court, held a higher probative value, including *viva voce* evidence. This section will review the techniques used to assess digital evidence and its probative value.

A. Authentication

Authentication refers to a legal concept that promotes the integrity of the trial process by ensuring tendered evidence establishes what it is offered to prove.[17] Courts are particularly concerned with authentication of digital evidence because digital evidence can be easily manipulated. For example, video footage may be altered or metadata (internal digital information that describes characteristics of the data) may be changed; therefore some degree of authentication is required to ensure the veracity of the evidence.

Authentication and reliability are related, but distinct concepts. The purpose of authentication is to ensure that the admitted evidence has not been manipulated or tampered with, while the purpose of reliability is to establish whether a piece of evidence is what it purports to be. For example, the Sri Lankan government questioned the reliability of video footage taken on a soldier's cell phone in 2009 that allegedly depicted the killing of Sri Lankan prisoners. The Sri Lankan government argued the killings were staged. Even if the footage was authentic, meaning it was not manipulated, the prosecutor must prove the video was reliable, i.e. the footage actually depicted the killing of Sri Lankan prisoners.[18]

The ICC does not require that a judge rule separately on the authenticity of evidence.[19] If the parties agree that the evidence is authentic or if the evidence is prima facie reliable, then

---

at http://icc-cpi.int/iccdocs/doc/doc1049623.pdf

[16] International Criminal Court e-Court Protocol, ICC-01/04-01/10-87-Anx 30-03-2011, *available at* http://icc-cpi.int/iccdocs/doc/doc1049623.pdf. Although the Protocol does not establish substantive guidance on evidentiary standards, it may help identify potential issues for introduction of evidence simply by increasing visibility of the digital evidence at issue.

[17] *See* Prosecutor v. Popovic, et al., Case No. IT-05-88-T, Decision on Admissibility of Intercepted Communications in Trial Chamber II, ¶ 4, 22, 26, 33-35 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 7, 2007).

[18] Robert Mackey, *Video of Sri Lankan Executions Appear Authentic UN Says,* Jan. 8, 2010, http://thelede.blogs.nytimes.com/2010/01/08/sri-lanka-atrocity-video-appears-authentic-un-says/

[19] Prosecutor v. Jean- Pierre Bemba Gombo, Case No. ICC-01/05-01/08, Decision on the Prosecution's

judges may treat the evidence as authentic.[20] If the evidence does not meet the prima facie standard, a party may provide additional information to show authenticity.[21]

The ICC reiterated its flexible approach to authenticity of digital evidence in *Prosecutor v. Jean-Pierre Bemba Gombo.*[22] The prosecution sought to introduce into evidence ten audio recordings of broadcasts that provided background information about the conflict, the identity of those involved, as well as accounts from eyewitnesses and victims.[23] The defense questioned the authenticity of the recordings.[24] The judges ruled that "recordings that have not been authenticated in court can still be admitted, as in-court authentication is but one factor for the Chamber to consider when determining an item's authenticity and probative value."[25]

Judges at the ad hoc tribunals also may determine authenticity and reliability of evidence as part of their assessment of its probative value.[26] As most evidence is admitted, the threshold objections of the parties are to its authenticity.[27]

The ad hoc tribunals generally favor corroboration of digital evidence through external indicators.[28] External indicators include testimony or source identity information whereas internal indicators consist of timestamps and metadata. For example, in *Prosecutor v. Karemera* the prosecution submitted video evidence of a rally along with a transcript of the corresponding radio broadcast.[29] The ICTR held that the broadcast transcript authenticated the date of the video, which proved that the accused attended the rally.[30] Similarly, in *Prosecutor v. Bagosora* the combination of video footage with a transcript led the ICTR to find that the accused was

---

Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute, ¶ 9 (Oct. 8, 2012).

[20] Id.

[21] Id.

[22] Id. at ¶¶ 80-122.

[23] Id.

[24] Id.

[25] Id. at ¶120. Ultimately, the court excluded the evidence in this case because it preferred admission of whole recordings rather than excerpts. Id. at ¶122.

[26] Proof of authenticity is not a pre-condition to admissibility since to do so would impose a more stringent standard than intended by the rule of probative value, ICTY Rules of Evidence 89(c). Prosecutor v. Popovic, et al., Case No. IT-05-88-T, Decision on Admissibility of Intercepted Communications, ¶ 4, 22, 26, 33 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 7, 2007) (The nexus between authentication and the 89(c) Rule of Evidence on probative value is that reliability is an implicit component of a determination of probative value; authenticity may be a factor of reliability.).

[27] International Criminal Tribunal for the Former Yugoslavia, Rules of Procedure and Evidence, 89(c); International Criminal Tribunal for Rwanda, Rules of Procedure and Evidence, 89(c).

[28] *See* Prosecutor v. Karemera, et al. Case No. ICTR-98-44-T, Judgment, ¶¶ 169-173, 205 (Int'l Crim. Trib. for Rwanda Feb. 2, 2012); Prosecutor v. Bagosora, Case No. ICTR-98-41-T, Trial Judgment and Appeals Judgment, ¶¶ 2029-2031, 460 (Int'l Crim. Trib. for Rwanda Dec. 8, 2008; Dec. 14, 2011); Prosecutor v. Galic, Case No. IT-98-29-AR73.2, Appeals Judgment, ¶¶ 443, 549 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 30, 2006).

[29] Karemera, ICTR, Judgment ¶¶ 169-173, 205 (Feb. 2, 2012).

[30] Id.

acting as the Minister of Defense and therefore exercised control over the army.[31] The corroboration of digital evidence in both cases provided the ICTR with linkage evidence to support a conviction.[32]

Several international courts have authenticated digital evidence, such as a video, through other external indicators such as expert testimony or the use of multiple types of evidence. [33] For example, the ICTR held that radio announcements, which called for the apprehension of Tutsis, were authentic after an expert witness testified that following the announcements, people actively sought out Tutsis. [34] Two additional witnesses corroborated the experts' testimony by describing the events that preceded and succeeded the radio announcements.[35] Similarly, the ICTY found that radio intercepts were authentic because they were corroborated by other intercepts and expert testimony.[36]

Once digital evidence is authenticated, it may impeach testimonial evidence.[37] The ICTY, in *Prosecutor v. Krstic* found the accused guilty, in part, based on his own testimony in which he states that he was unaware of the presence of the army, despite the fact that a video depicted him walking past soldiers wearing uniforms belonging to his own unit.[38]

International courts have favored admissibility of evidence that is challenged on grounds of authenticity. For example, after the prosecution objected to the authenticity of redacted emails in *Prosecutor v. Lubanaga* the ICC stated that it would discern probative value on a case-by-case basis.[39] In *Prosecutor v. Milutinovic* the ICTY limited the scope of the digital evidence to victim identification rather than excluding such evidence altogether. In *Prosecutor v. Blagojevic* the court evaluated the evidence from a holistic lens stating that it did not consider unsigned, undated or unstamped documents, *a priori*, to be void of authenticity." [40]

---

[31] Bagosora, ICTR, Judgment and Appeals ¶¶ 2029-2031, 460 (Dec. 8, 2008; Dec. 14, 2011).
[32] Id.; *see also* Galic, ICTY, Appeals ¶¶ 443, 549 (Nov. 30, 2006)(The ICTY prosecutors offered photographs, ballistics reports, video, and testimony for authentication purposes. The court held that the evidence was admissible because each piece of digital evidence was corroborated by another piece of evidence leading the court to find the evident authentic.).
[33] *See* Prosecutor v. Rutaganda, Case No. ICTR-96-3-T, Judgment, ¶ 357 (Int'l Crim. Trib. for Rwanda Feb. 13, 1996); Prosecutor v. Tolimir, Case No.IT-05-88/2-T, Judgment, ¶ 63 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 12, 2012), Decision on Intercepts, ¶ 67 ((Int'l Crim. Trib. for the Former Yugoslavia Jan. 20, 2012).
[34] Rutaganda, ICTR, Judgment ¶¶ 357, 370 (Feb. 13, 1996).
[35] Id. (The timeline of events was as follows: announcement that the president died; father of the accused stated Tutsis had to be killed at a local meeting; radio announcement which called for the apprehension of Tutsis; individuals actively began to seek Tutsis; propaganda messages started to spread; Tutsis were killed and their homes looted.).
[36] Tolimir, ICTY, Judgment ¶ 63 (Dec. 12, 2012), Decision on Intercepts ¶ 67 (Jan. 20, 2012).
[37] Prosecutor v. Krstic, Case No. IT-98-33-T, Judgment, ¶ 278 (Int'l Crim. Trib. for the Former Yugoslavia Aug. 2, 2001).
[38] Id.
[39] Prosecutor v. Lubanaga, Case No. ICC-01/04-01/06-803-tEN, Decision on Confirmation Charges ¶¶ 131-32 (May 14, 2007).
[40] Prosecutor v. Milutinovic, Case No. IT-05-87-T, Judgment Vol. 2, ¶¶ 588, 617, 621, 683 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 26, 2009); Prosecutor v. Blagojević & Jokić, Case No. IT-02-60-T,

Summary Analysis

Regardless of the type of indicators used (internal or external), the cases suggest that international criminal courts establish authenticity in two distinct ways. Either the prosecution uses an indicator to establish the authenticity of digital evidence or the prosecution uses digital evidence to establish the authenticity of an indicator. For example, a prosecutor may use a transcript (indicator) to prove the authenticity of a video (digital evidence).[41] Conversely, the prosecution may use a photograph (digital evidence) to prove the authenticity of testimonial evidence (indicator).[42] Nevertheless, courts appear to favor authenticity of digital evidence through external indicators, such as a transcript or testimony.[43] Corroboration of digital evidence is thus critical to proving its authenticity.

B. Hearsay

Hearsay evidence is evidence of facts outside the direct knowledge of the testifying witness.[44] Digital evidence may raise hearsay concerns because it is not live testimony, and is removed from the originating source. The ICC, unlike the ad hoc tribunals, has no explicit rule on hearsay evidence.[45] The ICC prefers live witness testimony,[46] but its rules allow for alternatives in limited circumstances.[47]

Judgment ¶ 29 (Int'l Crim. Trib. for the Former Yugoslavia Jan. 17, 2005); *see also* Robert Mackey, *Video of Sri Lankan Executions Appear Authentic UN Says*, Jan. 8, 2010, http://thelede.blogs.nytimes.com/2010/01/08/sri-lanka-atrocity-video-appears-authentic-un-says/ (Sri Lankan government denied authenticity causing the UN Special Rapporteur to employ a forensic pathologist, video analyst, and firearms and ballistics expert to analyze the atrocities as a whole).

[41] *See* Prosecutor v. Karemera, et al. Case No. IT-98-44-T, Judgment, ¶¶ 169-173, 205 (Int'l Crim. Trib. for Rwanda Feb. 2, 2012)(transcript of radio broadcast authenticated the date of the video of rally and corroborated evidence that the accused was in attendance); Prosecutor v. Bagosora, Case No. IT-98-41-T, Trial Judgment and Appeals Judgment, ¶¶ 2029-2031, 460 (Int'l Crim. Trib. for Rwanda Dec. 8, 2008; Dec. 14, 2011)(transcript authenticated video footage corroborating evidence that the accused was acting as Minister of Defense and exercised control over the army).

[42] Prosecutor v. Nyiramasuhuko, et al., Case No. ICTR 98-42AR73.2, Decision on Pauline Nyiramasuhuko's Appeal on the Admissibility of Evidence, ¶ 7 (Int'l Crim. Trib. for Rwanda Oct. 2004)(photographs used to authenticate the witness' testimony, yet ultimately deemed inadmissible because of inconsistencies between the testimony and indictment timeline).

[43] Id.

[44] Prosecutor v. Blagojević & Jokić, Case No. IT-02-60-T, Trial Judgment, ¶ 21 (Int'l Crim. Trib. for the Former Yugoslavia Jan. 17, 2005).

[45] Instead, "the drafters of the [Rome] Statute framework have clearly and deliberately avoided proscribing certain categories or types of evidence, a step which would have limited - at the outset - the ability of the Chamber to assess evidence 'freely'. Instead, the Chamber is authorised by statute to request any evidence that is necessary to determine the truth, subject always to such decisions on relevance and admissibility as are necessary, bearing in mind the dictates of fairness." Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Judgment pursuant to Article 74 of the Statute, ¶ 107 (Mar. 14, 2010).

[46] Lubanga, ICC, Redacted Decision on the defence request for a witness to give evidence via video-link, ¶ 2 (Feb. 9, 2010).

[47] ICC Rule 67 allows for a witness to provide testimony by audio or video link, providing that the technology permits the Prosecutor, the defense, and the Chamber to examine the witness. Rules of Evidence and Procedure of the International Criminal Court, Rule 67. Rule 68 allows for testimony that

Since the ICC does not consider hearsay as a class of evidence in and of itself, examples of hearsay evidence being admitted by the Court are sparse. An example of the ICC's approach toward digital evidence hearsay is through its admission of anonymous hearsay. The ICC does not consider hearsay from anonymous sources inadmissible *per se*.[48] The Court has admitted e-mails as anonymous hearsay, notwithstanding objections from the defense regarding their truthfulness and authenticity.[49] As a general rule, the ICC has held that such anonymous hearsay could be admitted, but its use was limited to "corroborate other evidence."[50]

The ad hoc tribunals have a formal rule allowing for the admission of hearsay. Rule 92*bis* allows for the admission of written statements and transcripts in lieu of oral testimony when their admission goes to prove a matter other than the acts and conduct of the accused as charged in the indictment.[51] Still, hearsay is subject to the requirement of reliability for admissibility, and as such has less probative value than live witness testimony.[52]

Generally, ad hoc tribunals have admitted digital evidence that is hearsay when it is accompanied by live testimony explaining the methods by which the digital evidence was obtained.[53] In *Prosecutor v. Tolimir*, the ICTY admitted evidence of intercepted communications

---

has been previously recorded to be introduced, in accordance with article 69 paragraph 2, if both the Prosecutor and the defense had a prior opportunity to examine the witness, or if the witness is present before the Chamber, that he or she does not object to the previously recorded testimony, and the Prosecutor and the defense have an opportunity to examine the witness. Rules of Evidence and Procedure of the International Criminal Court, Rule 68. These alternatives to live testimony are available in instances where the witness has refused to attend court, is unable to do so, or if it is in the best interest to protect the psychological well-being and dignity of the witness. Lubanga, ICC, Redacted Decision on the defence request for a witness to give evidence via video-link, ¶ 15 (Feb. 9, 2010).

[48] Lubanga, ICC, Pre-Trial Chamber I, Decision on Confirmation Charges, ¶ 101 (Jan. 29, 2007). This also includes redacted versions of witness statements. Id. Objections to the use of anonymous hearsay have gone to the probative value of the evidence, and not its admissibility. Id. at ¶ 103.

[49] Id. at ¶ 99.

[50] Id. at ¶ 106.

[51] International Criminal Tribunal for Yugoslavia, Rules of Evidence and Procedure, Rule 92*bis*; Prosecutor v. Blagojević & Jokić, Case No. IT-02-60-T, Trial Judgment, ¶ 26 (Int'l Crim. Trib. for the Former Yugoslavia Jan. 17, 2005) (The court admitted hearsay when it found that each "written statement or transcript did not go to the acts and conduct of the Accused; was relevant to the present case; had probative value under Rule 89(C) of the Rules; and was cumulative in nature."); Prosecutor v. Stakić, Case No. IT-97-24, Judgment, ¶ 196 (Int'l Crim. Trib. for the Former Yugoslavia Mar. 22, 2006). The hearsay inquiry balances factors for and against admission laid out in 92*bis*(A)(i) and 92*bis*(A)(ii), respectively. Factors in favor of admitting hearsay include its relevancy, whether there exists corroborating testimony, and whether it includes general or statistical analysis. Factors against admitting hearsay include an "overriding public interest" for oral testimony, a showing that the evidence is unreliable or prejudicial, or there is a need for cross-examination. International Criminal Tribunal for Yugoslavia, Rules of Evidence and Procedure, Rev. 49, May 22, 2013, pp. 96-97.

[52] Prosecutor v. Brdanin & Talic, Case No. IT-99-36-T, Order on the Standards Governing the Admission of Evidence, ¶ 24 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 15, 2002); Prosecutor v. Stanišić & Župljanin, Case No. IT-08-91-T, Judgement, ¶ 16 (Int'l Crim. Trib. for the Former Yugoslavia Mar. 27, 2013), http://icty.org/x/cases/zupljanin_stanisicm/tjug/en/130327-1.pdf.

[53] Prosecutor v. Tolimir, Case No. IT-05-88/2, Trial Judgment, ¶ 63 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 12, 2012).

after the intercept operators and related personnel testified.[54] The reliability of the hearsay testimony was strengthened by establishing a chain of custody in the presentation of the evidence; the printouts of the intercepts submitted to the ICTY conformed to the original notebooks of the intercepted communications.[55] The evidence was also independently corroborated by evidence with a higher probative value, through notes of U.N. officials, telephone books, and aerial images, as well as by prior statements made by others, increasing the total weight of the evidence.[56]

Of interest in the *Tolimir* case is the decision to admit digital evidence hearsay without testimony regarding the methods by which it was obtained,[57] and still retaining its credibility.[58] In *Tolimir* the prosecution introduced aerial photos into evidence that it obtained from the United States, which came with instructions not to discuss the procedures through which the evidence was obtained.[59] The defense unsuccessfully challenged the reliability of the images, which the judges found to be credible despite the lack of direct evidence about its collection.[60] Instead of presenting testimony of those involved in obtaining the evidence, the prosecution presented testimony of investigators from the Office of the Prosecutor who had experience obtaining such evidence. These witnesses testified to the authenticity of the aerial images, in addition to providing corroboration by the testimony of additional witnesses.[61] The court found the hearsay evidence to be generally reliable.[62]

Summary Analysis

Factors that improve the probative value of digital evidence hearsay include corroborating evidence, such as live testimony, and explanations of the procedures by which the digital evidence was obtained, including testimony of those involved in obtaining it.[63] Reliability is also strengthened by creating a chain of custody in the presentation of the evidence.[64] The evidence can also be further corroborated by the presentation of other evidence that has a higher probative value, increasing the total weight of the evidence.[65] Yet to be assessed is whether digital evidence hearsay can ever be admitted on its own, or for the truth of the matter. Such situations could include digital documents of communications of deceased persons. An unresolved issue is

[54] Id. at ¶ 64 (evidence was shown to be reliable in the practices followed by the interceptors).
[55] Id. at ¶ 64, fn.165.
[56] Id. at ¶ 65.
[57] Id. at ¶ 68 (admitting into evidence aerial imagery investigators received from the U.S. on agreement that the methods used to obtain the images would not be disclosed at trial).
[58] Id. at ¶ 70.
[59] Id. at ¶ 68.
[60] Id. at ¶ 69.
[61] Id. at ¶ 70.
[62] Id.; *see also* Prosecutor v. Stanišić & Simatović, Case No. IT-03-69, Trial Judgment Part I, ¶ 880 (Int'l Crim. Trib. for the Former Yugoslavia May 30, 2013) (witness testimony corroborated a video showing an operation rounding up individuals to a location where they were later killed).
[63] Prosecutor v. Tolimir, Case No. IT-05-88/2, Trial Judgment, ¶ 64 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 12, 2012) (evidence was shown to be reliable in the practices followed by the interceptors).
[64] Id. at ¶ 64, fn.165.
[65] Id. at ¶ 65.

also to what extent is the presentation of chain of custody and expert testimony about digital evidence sufficient for it to be reliable.

C. Provenance (Chain of Custody)

Chain of custody, or provenance, is defined as "[t]he movement and location of real evidence, and the history of those persons who had it in their custody, from the time it is obtained to the time it is presented in court."[66] Establishing provenance requires both "testimony of continuous possession" and testimony "that the object remained in substantially the same condition" during each individual's possession.[67] This information provides a "complete history of hosting and possession" of who controlled the electronic information, which "is important in determining whether evidence has been modified or tampered with" when the court assesses the accuracy of the digital evidence.[68] A strong chain of custody increases the weight judges accord to the evidence because "[f]actors such as . . . proof of authorship will naturally assume the greatest importance in the Trial Chamber's assessment of the weight to be attached to individual pieces of evidence."[69]

Research has not revealed a consistent definition of "authorship" in international criminal courts. However, authors have been considered to be persons on whom the court may rely for testimony regarding the origins of the evidence. Courts have accepted the testimony of persons note-taking and monitoring radio intercepts,[70] recording audio,[71] or even those who obtain aerial images originally taken by others,[72] in order to find reliability and probative value in the evidence.

Lack of author testimony usually will not preclude the admission of evidence. In the ICC, "nothing in the Statute or the Rules expressly states that the absence of information about the chain of custody . . . affects the admissibility or probative value of Prosecution evidence."[73] When the defense does "nothing more than raise a general objection to the admissibility of . . . evidence for which no information pertaining to the chain of custody . . . ha[s] been provided, without addressing specific items or providing the reasons for its objection," reasonable doubt is not cast upon the authenticity of the evidence such that it should be excluded.[74] This rule is similar to that of the ICTY, which has held that evidence will not necessarily be barred from

---

[66] BLACK'S LAW DICTIONARY 260 (9th ed. 2009).
[67] Id.
[68] CENTER FOR RESEARCH LIBRARIES, HUMAN RIGHTS ELECTRONIC EVIDENCE STUDY 51 (2012), *available at* http://www.crl.edu/grn/hradp/electronic-evidence.
[69] Prosecutor v. Brdanin and Talic, Case No. IT-99-36-T, Order on the Standards Governing the Admission of Evidence, ¶ 18 (Int'l Crim. Trib. for the Former Yugoslavia, Feb. 15, 2002).
[70] Prosecutor v. Popovic et al., Case No. IT-05-88-T, Judgement Volume I, ¶¶ 64-66 (Int'l Crim. Trib. for the Former Yugoslavia June 10, 2010).
[71] Prosecutor v. Renzaho, Case No. ICTR-97-31-T, Decision on Exclusion of Testimony and Admission of Exhibit, ¶¶ 1-2 (Mar. 20, 2007).
[72] Prosecutor v. Tolimir, Case No. IT-05-88/2-T, Judgement, ¶¶ 67-70 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 12, 2012).
[73] Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Decision on Confirmation Charges, ¶ 96 (Jan. 29, 2007).
[74] Id. at ¶ 98.

initial admission because of an absence of the author's testimony.[75] The ICTR, however, has refused to admit evidence absent the author's testimony.[76]

The ICC does require precautions when submitting digital evidence. Digital evidence and material must conform to an "e-Court Protocol," even before submissions at the Confirmation Hearing.[77] This Protocol, combined with the considerations of authorship articulated by other international courts, highlights the overall importance of provenance when courts assess admissibility and evidentiary weight later in the proceedings.

The record of how international courts have evaluated the evidentiary weight of provenance indicates a spectrum of responses. On one end, testimony of the author—which establishes the foundation of the chain of custody—can give the evidence significant weight.[78] For example, after the *Popovic* Trial Chamber heard testimony from intercept operators and analysts, it concluded that there were no chain of custody issues.[79] At the other end of the spectrum, inconsistencies in testimony regarding the provenance of evidence may lead the court to discount the evidence.[80] In the *Milutinovic* case the court did not give weight to a chain of custody author's testimony when the author's written and oral testimony (as to whom he gave video evidence) contradicted his testimony on cross-examination.[81]

Other cases fall in between these cases. Here, witness corroboration of the evidence is helpful. In the *Brdanin* case identification by a witness of his own and others' voices on intercepts helped establish reliability of the digital evidence, despite an imperfect chain of custody and the fact that the intercept evidence had been edited.[82] The prosecution was allowed to admit these intercepts as Compact Disks, despite the fact that they contained information that

---

[75] Brdanin and Talic, ICTY, Order on the Standards Governing the Admission of Evidence, ¶ 20 (Feb. 15, 2002); Prosecutor v. Delalic, Case No. IT-96-21, Decision on the Motion of the Prosecution for the Admissibility of Evidence, ¶ 22 (Int'l Crim. Trib. For the Former Yugoslavia Jan. 19, 1998) ("It is clear from the relevant provisions of the Rules that there is no blanket prohibition on the admission of documents simply on the ground that their purported author has not been called to testify in the proceedings.").

[76] Prosecutor v. Renzaho, Case No. ICTR-97-31-T, Judgement and Sentence, ¶ 841 (July 14, 2009); Renzaho, ICTR, Decision on Exclusion of Testimony and Admission of Exhibit, ¶¶ 1-2 (Mar. 20, 2007) (Chamber denied requests to admit audio evidence "due to lack of information about the recording and its provenance," despite four witnesses claiming to identify the accused's voice on an incriminating audiotape. The tape was subsequently admitted when the prosecution offered the testimony of the journalist who recorded the audiotape.).

[77] Prosecutor v. Callixte Mbarushimana, Case No. ICC-01/04-01/10, Decision Amending the e-Court Protocol, 4 (Apr. 28, 2011), e-Court Protocol *available at* http://icc-cpi.int/iccdocs/doc/doc1049623.pdf.

[78] Popovic, et al., ICTY, Judgement Volume I, ¶¶ 64-66 (June 10, 2010).

[79] Id.

[80] Prosecutor v. Milutinovic et al., Case No. IT-05-87-T, Judgement Volume 3 of 4, ¶545 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 26, 2009).

[81] Id.

[82] Prosecutor v. Brdanin, Case No. IT-99-36-T, Judgement, ¶ 34, n.38 (Int'l Crim. Trib. for the Former Yugoslavia Sept. 1, 2004).

had been originally recorded on cassettes and then erased.[83] Additionally, in *Tolimir* ICTY prosecutors successfully offered provenance testimony regarding the source of aerial photo evidence and a witness' receipt of it, even though the methods used to obtain the evidence remained undisclosed.[84] At this point on the spectrum, evidence will not necessarily be excluded for defects in provenance, [85] although it can be if the defects are serious enough (such as the author's failure to testify).[86]

Summary Analysis

At the admissibility stage, there is no typical amount of author testimony required, and the bar for admission is usually low.[87] Cases from the ad hoc tribunals offer different approaches to the question of whether it is necessary for the author of digital evidence to testify to establish provenance: some have not *automatically* refused evidence submitted without author testimony, while others have refused to admit even corroborating witness testimony without testimony from the author.[88] However, international courts appear to prefer the prosecution to provide testimony from a live witness, usually the author, before admitting or giving weight to digital evidence.

When courts assign evidentiary weight to digital evidence, the record suggests that the greatest evidentiary weight is given to live witness testimony that establishes the chain of

---

[83] Prosecutor v. Brdjanin, Case No. IT-99-36-T, Decision on the Defence "Objection to Intercept Evidence", ¶ 13 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 3, 2003) (finding the "disks produced [we]re incomplete" and the "same documents ha[d] different dates.").

[84] Prosecutor v. Tolimir, Case No. IT-05-88/2-T, Judgement, ¶¶ 67-70 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 12, 2012) (Investigators received aerial imagery from U.S. on agreement that the methods used to obtain the images would not be disclosed at trial. Although "evidence [wa]s lacking on the method of creation of these images," general credibility of the images was not impaired, as investigators identified and located gravesites based upon them, and witnesses corroborated authenticity of the images. The court found the evidence to be reliable and to have probative value.).

[85] See Prosecutor v. Blagojevic and Jokic, Case No. IT-02-60-T, Judgement, ¶ 29 (Int'l Crim. Trib. for the Former Yugoslavia, Jan. 17, 2005) (Chamber did not consider unsigned, undated, or unstamped documents to be void of authenticity. Chamber also allowed intercept evidence over Defense objections relating to unknown operating personnel, inexperienced operators lacking sufficient training, and substandard equipment.). See also Brdjanin, ICTY, Decision on the Defence "Objection to Intercept Evidence" (Feb. 15, 2002) (Court admits intercepts despite challenges to provenance of storage tapes for incomplete and unsupervised chain of custody.).

[86] See Prosecutor v. Renzaho, Case No. ICTR-97-31-T, Decision on Exclusion of Testimony and Admission of Exhibit, ¶¶ 1-2 (Mar. 20, 2007).

[87] Blagojevic and Jokic, ICTY, Judgement, ¶ 30, n.72 (Jan. 17, 2005) (Handwritten notebooks of radio intercept recordings accepted without complete audiotape recordings when accompanied by testimony of intercept operators. This was despite Defence objections to unreliable transcriptions, lack of operator training, and substandard equipment, and the Prosecution's failure to admit original recordings.); Prosecutor v. Blagojevic and Jokic, Case No. IT-02-60-T, Decision on the Admission Into Evidence of Intercept-Related Materials, ¶ 2 (Int'l Crim. Trib. for the Former Yugoslavia, Dec. 18, 2003) (The Court concluded the operators described procedures with sufficient similarity and "took their task seriously.").

[88] Brdanin and Talic, ICTY, Order on the Standards Governing the Admission of Evidence, ¶ 20 (Feb. 15, 2002). But see Prosecutor v. Renzaho, Case No. ICTR-97-31-T, Judgement and Sentence, ¶ 841 (July 14, 2009); Renzaho, ICTR, Decision on Exclusion of Testimony and Admission of Exhibit, ¶¶ 1-2 (Mar. 20, 2007).

custody. The author's testimony should play the lead role here. When author testimony is unavailable or imprecise, other testimony can give weight to the evidence. Such testimony includes witness corroboration (or sometimes, corroboration by multiple witnesses), as well as testimony of other parties (such as investigators who obtained information).[89]

Overall, the case law demonstrates that authorship, although it is not concretely defined, is the most prevalent consideration when determining the weight of the evidence based on provenance.

D. Preservation

"Digital preservation refers to long-term, error-free storage of digital information, with means for retrieval and interpretation, for the entire time span" for which the information is required.[90] Proper preservation of digital evidence is necessary to provide courts and parties with a complete and accurate record of the evidence. Once stored (or archived), digital evidence can remain an authentic and effective tool for justice over a long period of time.[91] For example, journalist Nick Hughes used a digital camera to record footage of the Gikonda massacre in Rwanda; the footage showed the murder of a father and daughter and others, and was distributed to world news organizations.[92] These news organizations stored the footage, and it later contributed to identification of victims, perpetrators, and promoted general public awareness of the genocide in Rwanda.[93]

The ICC is evaluating ways to ensure complete and accurate preservation of digital evidence.[94] For example, the e-Court Protocol aims to achieve consistency of digital evidence submitted to the Court; yet, standardized formatting can sometimes degrade the quality of evidence and require a lengthy process of compiling metadata for each piece of evidence.[95] Aside from the ICC's efforts to ensure consistent methods of formatting and storing digital evidence, international courts appear not to have discussed preservation of digital evidence. This is especially true for the periods prior to investigators' acquisition of digital evidence from authors or from other parties that have obtained the evidence.

International criminal courts appear to focus more on preservation when its deficiencies detract from evidentiary quality, rather than on establishing affirmative standards for

---

[89] See Tolimir, ICTY, Judgement, ¶¶ 64-70 (Dec. 12, 2012); Prosecutor v. Brdanin, Case No. IT-99-36-T, Judgement, ¶ 34, n.38 (Int'l Crim. Trib. for the Former Yugoslavia Sept. 1, 2004). But see Renzaho, ICTR, Decision on Exclusion of Testimony and Admission of Exhibit, ¶¶ 1-2 (Mar. 20, 2007).

[90] *Digital Preservation* Definition, U.S. LEGAL, http://definitions.uslegal.com/d/digital-preservation (last visited Sept. 29, 2013).

[91] CENTER FOR RESEARCH LIBRARIES, HUMAN RIGHTS ELECTRONIC EVIDENCE STUDY 7, 147 (2012), *available at* http://www.crl.edu/grn/hradp/electronic-evidence. (discussing reporter's Gikonda film footage of Rwandan genocide and its impact on identifying victims and perpetrators, and on bringing those perpetrators to justice).

[92] Id. at 147.

[93] Id.

[94] Prosecutor v. Callixte Mbarushimana, Case No. ICC-01/04-01/10, Decision Amending the e-Court Protocol, 4 (Apr. 28, 2011).

[95] Id. (Prosecutor objected to following the e-Court Protocol in this case for these two reasons.).

preservation.[96] Furthermore, proper preservation of digital evidence has been considered as unnecessary to meet the "best evidence" rule.[97] An example is *Popovic*, where the ICTY allowed handwritten notes that had been entered into digital documents to replace what would have been the "best evidence" of audio recordings. The tribunal allowed the notes because the prosecution did not have the full and complete set of audio recordings, and it did not require the prosecution to produce the full set of recordings.[98]

The ICTY has admitted altered evidence under certain circumstances. In one case, the defence (unsuccessfully) challenged the reliability of aerial images provided by the United States government and offered by the prosecution.[99] While one witness had testified he "did not believe the aerial images could be altered by anyone," another "explained why he had added and removed dates on certain aerial images."[100] The defence also argued the images were not linked with particular locations because none had site codes or coordinates.[101] A similar challenge was made in *Tolimir*, where aerial images were challenged "on the grounds that no evidence was presented on their origin, the method of their creation, the manner of their editing, how to interpret them or whether they were delivered to the Prosecution in their original form or previously modified."[102] Although the Trial Chamber acknowledged the lack of information on the creation of the images, it found these deficiencies did not impair the "credibility of the aerial images in general."[103]

When the best evidence has not been fully preserved, the ICTY has admitted alternative forms of evidence.[104] In *Popovic*, the ICTY prosecution possessed only a few audiotape recordings of intercepts. The prosecutor's analyst also acknowledged the "possibility that the intercepts were tampered with or fabricated."[105] The prosecution nonetheless sought to admit transcripts and notes in place of the full set of recordings. The defence objected to the transcripts as incomplete.[106] Nonetheless, the Trial Chamber admitted the transcripts, noting that procedures

---

[96] Prosecutor v. Callixte Mbarushimana, Case No. ICC-01/04-01/10, Decision on the Confirmation of Charges, ¶¶ 63-65 (Dec. 16, 2010) (Defence challenges to admissibility of seized hard drives because of breaking of seals on containment bags was "unsubstantiated and speculative" and did not warrant exclusion of the hard drives.)

[97] Prosecutor v. Popovic, et al., Case No. IT-05-88-T, Decision on Admissibility of Intercepted Communications, ¶ 39 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 7, 2007).

[98] Id.

[99] Prosecutor v. Popovic et al., Case No. IT-05-88-T, Judgement Volume I, ¶¶ 72-75 (Int'l Crim. Trib. for the Former Yugoslavia June 10, 2010).

[100] Id. at ¶¶ 73.

[101] Id.

[102] Prosecutor v. Tolimir, Case No. IT-05-88/2-T, Judgement, ¶¶ 69-70 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 12, 2012).

[103] Id.

[104] Prosecutor v. Popovic, et al., Case No. IT-05-88-T, Decision on Admissibility of Intercepted Communications, ¶ 39 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 7, 2007).

[105] Id. at ¶¶ 22, 52 (Ultimately, the witness stated she had no "serious questions about the authenticity or the reliability of the intercepts as a whole.").

[106] Id. Similar objections have been made in other cases, such as when the prosecution failed to submit original recordings. Prosecutor v. Blagojevic and Jokic, Case No. IT-02-60-T, Judgement, ¶ 29 (Int'l Crim. Trib. for the Former Yugoslavia, Jan. 17, 2005).

had been used to preserve accurate and standardized transcripts, which ensured their authenticity.[107]

Summary Analysis

These examples indicate the lack of strict preservation standards in the ad hoc tribunals. Completeness and accuracy of preservation was not a prerequisite to admission when the ICTY could consider other factors to find reliability and authenticity.[108] Likewise, the court allowed digital evidence that was not in its original form; it also admitted this evidence despite several inaccuracies.[109] Yet, the ICC is developing ways to standardize and preserve digital evidence, such as the e-Court Protocol.[110] This brings consistency to digital evidence submitted to the Court, although it raises questions about the degradation of data quality and can require a lengthy process of compiling metadata on individual pieces of evidence.[111] Furthermore, these methods are limited. Investigators do not have control over digital evidence before it comes into their possession. Therefore, the protocol may minimize preservation problems once investigators secure digital evidence, but it may not reduce the risks to degradation of digital evidence quality before that time.

IV. Conclusion

Generally, case law on digital evidence matters is sparse, largely because it is an emerging form of evidence at international criminal courts. In its analysis of the limited case law, this paper made specific findings and found several unresolved issues. The following section summarizes these findings and provides recommendations for further research.

Authentication

Based on the review of relevant cases, it appears that international criminal courts place a high priority on live testimony of an expert who can corroborate the authenticity of digital evidence. Courts also accept documentary evidence, such as a transcript of an audio recording, in lieu of or in addition to live testimony. The need for external corroboration raises several questions. For example, what procedures should be considered during the collection of digital evidence so as to ensure eventual authentication in proceedings? Digital evidence provided by non-governmental actors in the course of an investigation may pose challenges to protect the identities of

[107] Popovic, et al., ICTY, Decision on Admissibility of Intercepted Communications, ¶ 39 (Dec. 7, 2007) (The court detailed that intercept operators followed "general procedures" with "near uniformity" to eavesdrop on radio communications, recorded the conversations onto audiotapes, and then transcribed the conversations into handwritten notebooks. The notebooks were then typed onto computers and sent to command.).
[108] See id. at ¶¶ 22, 52; Blagojevic and Jokic, ICTY, Judgement, n.72 (Jan. 17, 2005).
[109] See Popovic, et al., ICTY, Decision on Admissibility of Intercepted Communications, ¶¶ 22, 52 (Dec. 7, 2007); Blagojevic and Jokic, ICTY, Judgement, n.72 (Jan. 17, 2005).
[110] Prosecutor v. Callixte Mbarushimana, Case No. ICC-01/04-01/10, Decision Amending the e-Court Protocol, 4 (Apr. 28, 2011).
[111] Id.

individuals with direct knowledge of the evidence. Therefore, how can courts balance authenticity needs with identity protection?

Hearsay

Due to the lack of a formal rule on the acceptance of hearsay, the ICC has not explicitly dealt with its admission in many cases. Still, both the ICC and the ad hoc tribunals generally admit hearsay when it is corroborating other evidence that has a higher probative value. To strengthen the probative value of digital evidence hearsay, prosecutors have presented live testimony from those who were involved in gathering the digital evidence, explaining their methods, as well as presenting a strong chain of custody. This testimony improves the reliability and credibility of the evidence. There does not seem to be a bar to admitting hearsay, as the ICC has already admitted anonymous hearsay. However, questions remain as to whether hearsay can be introduced for the truth of the matter. As well, it is not clear whether hearsay can be admitted without testimony regarding how it was obtained, and if testimony is necessary, 1) to what extent this testimony has to be from a party that was directly involved in gathering the evidence; and 2) how much testimony would be sufficient for the court to consider the evidence credible.

Provenance

Case law demonstrates that, when courts assign weight to the evidence, authorship is the most prevalent and important consideration. However, there are situations where authorship may be difficult to determine. For example, NGOs and other non-governmental actors may possess important digital evidence, such as video footage, where the author may not be identified or locatable. Proper verification of the identities of those who have had control of information before it reached investigators may be required, or the evidence may be at risk of exclusion. The importance of proof of authorship also raises questions about digital evidence in forms where digital transmissions may be difficult to link to an author, such as email. In this scenario, courts could potentially require verification of electronic signatures or other linkage to an author, or could require corroborating evidence.

Preservation

So far, international criminal courts have provided little guidance on the best means of preserving digital evidence. Additionally, the ICC does not appear to take measures to ensure digital information has been properly preserved *before* investigators obtain it. Therefore, questions arise as to what methods should be used to ensure evidence is preserved in a manner that will satisfy Chambers. It is especially uncertain what methods of preservation are proper for evidence obtained from unverifiable sources, such as videos uploaded to the Internet without identity information of the owner.

V. Appendix

Cases Consulted

International Criminal Court (ICC)
Prosecutor v. Bemba Gombo, Case No. ICC-01/05-01/08
Prosecutor v.Lubanga, Case No. ICC-01/04-01/06
Prosecutor v. Callixte Mbarushimana, Case No. ICC-01-04-01/10
Prosecutor v. Banda and Jerbo, Case No. ICC-02/05-03/09

Extraordinary Chambers in the Courts of Cambodia (ECCC)
ECCC, Case(001) No. 001/18X07X2007/ECCC/TC

International Criminal Tribunal for Rwanda (ICTR)
Prosecutor v. Karemera, Ngirumpatse, and Nzirorera, Case No. ICTR 98-44-T
Prosecutor v. Musema, Case No. ICTR 96-13-T
Prosecutor v. Simba, Case No. ICTR 01-76-T
Prosecutor v. Nyiramasuhuko and Ntahobali, Case No. ICTR 98-42AR73.2
Prosecutor v. Rutaganda, Case No. ICTR 96-3-A
Prosecutor v. Bagosora et al., Case No. ICTR 98-41-T
Prosecutor v. Renzaho, Case No. ICTR-97-31-T

International Criminal Tribunal for the former Yugoslavia (ICTY)
Proscutor v. Delalic, Mucic, Delic, and Landzo, Case No. IT-96-21
Prosecutor v. Karadzic and Mladic, Case No. IT-95-5/18-T
Prosecutor v. Perišić, Case No. IT-04-81
Prosecutor v. Mladić, Case No. IT-09-92
Prosecutor v. Dordevic, Case No. IT-05-87/1-T
Prosecutor v. Milutinovic, Case No. IT-05-87-T
Prosecutor v. Sanovic, Case No. IT-01-47-T
Prosecutor v. Brdanin and Talic, Case No. IT-99-36-T
Prosecutor v. Popovic, Beara, Nikolic, Boroveanin, Miletic, Gvero, and Panderuvic, Case No. IT-05-88/2-T.27
Prosecutor v. Tolimir, Case No. IT-05-88/2
Prosecutor v. Galic et al., Case No. IT-98-29-AR73.2,
Prosecutor v. Milošević, Case No.IT-02-54-AR73.4
Prosecturo v. Stanišić & Župljanin, Case No. IT-08-91
Prosecutor v. Stakić, Case No. IT-97-24
Prosecutor v. Boškoski & Tarčulovski, Case No. IT-04-82
Prosecutor v. Blagojević & Jokić, Case No. IT-02-60
Prosecutor v. Stanišić & Simatović, Case No. IT-03-69
Prosecutor v. Krstić, Case No. IT-98-33
Prosecutor v. Haraqija and Morin, Case No. IT-04-84-R77-4A

Special Tribunal for Lebanon (STL)
Prosecutor v. Badreddine, Ayyash, Oneissi & Sabra, Case No. STL-11-01/I/PTJ

Special Court for Sierra Leone (SCSL)

Prosecutor v. Sam Hanga Norman et al., Case No. SCSL-04-14-AR65
Prosecutor v.Norman et al., Case No. SCSL-04-14-T
Prosecution v. Taylor, Case-No.SCSL-04-15-T 118
Prosecutor v. Sesay, et al., Case No. SCSL-04-15-T

WORKING PAPER

DIGITAL EVIDENCE AND THE AMERICAN SERVICEMEMBERS' PROTECTION ACT

SALZBURG WORKSHOP ON CYBERINVESTIGATIONS

This paper was prepared by Aida Ashouri '14 and Caleb Bowers '15, students from the International Human Rights Law Clinic and Samuelson Law, Technology, & Public Policy Clinic at the University of California, Berkeley, School of Law, under the supervision of Professors Laurel E. Fletcher, Chris Hoofnagle, Eric Stover, and Jennifer Urban.

October 2013

Table of Contents

Abstract

This paper provides background on the American Servicemembers' Protection Act (ASPA or Act) and examines the circumstances surrounding the passage of the Act, its key provisions and their exceptions, and how the Act affects investigations by the International Criminal Court (ICC or Court).

International criminal prosecutions increasingly rely on cyberinvestigations to uncover digital evidence that can be subsequently admitted in court proceedings. ASPA restricts U.S. cooperation with the ICC and its investigations within the United States. As the majority of e-mails and social media platforms are linked to U.S. entities, ICC cyberinvestigations will inevitably invoke ASPA in one way or another. This paper examines the current administration's increased engagement with the ICC within the scope of ASPA, as well as whether or not this engagement signals that revisions to the Act should be made. These questions serve as the starting point for examining the nexus of cyberinvestigations, ASPA, and the International Criminal Court.

I. Introduction

This background paper examines the American Servicemembers' Protection Act (ASPA or the Act), which was signed into law by then-President George W. Bush on August 2, 2002. The Act contains a broad prohibition on cooperation between the United States and the International Criminal Court (ICC or the Court), strictly prohibiting U.S. "support" to the ICC and limiting ICC "investigative activity" within the United States.[1] Notwithstanding these broad restrictions, the Act contains exceptions that allow for conditional assistance to the ICC. The most important of these is "the Dodd Amendment," which allows for U.S. cooperation with ICC prosecutions of foreign nationals on a case-by-case basis.[2]

As the ICC Office of the Prosecutor (OTP) increases its efforts to collect and introduce digital evidence in proceedings, it is necessary to understand how ASPA applies to digital information under the control, or within the territory, of the United States. Furthermore, knowledge of the Act's exceptions can assist in identifying possible avenues for U.S. cooperation with OTP investigations. This knowledge takes on an added importance in the context of digital information, given that the majority of this information is controlled by U.S. Internet Service Providers (ISPs).

Accordingly, this paper examines (1) the political environment at the time the Act was passed; (2) the Act's impact on the investigative abilities of the ICC; (3) the ways in which the U.S. is using the Dodd Amendment and other exceptions to support the OTP and the Court in general; (4) what penalties, if any, individuals and institutions might incur in connection with breaches of the Act; and (5) the unresolved questions regarding the functions of the Act and its reach.

[1] American Servicemembers' Protection Act, 22 U.S.C. §§ 2004(h), 2013(12) (2008), *available at* http://www.house.gov/legcoun/Comps/aspa02.pdf.
[2] ASPA § 2015.

This paper is based on limited research, and does not include classified or internal documents on the Act's operations. It sets out to provide a background and understanding of the framework of ASPA, as it is publicly known. Our findings are based on primary and secondary research on ASPA, as well as interviews conducted with government officials knowledgeable of ASPA's operations.

II. Legislative History

The United States was an initial supporter of the ICC, and it actively participated in the negotiations leading up to the final conference in Rome.[3] However, as the conference approached a final vote on the Court's statute (Rome Statute), U.S. officials realized certain critical negotiating objectives would not be achieved, and support for the Rome Statute quickly diminished.[4] David Scheffer, former Ambassador-at-Large on War Crimes Issues at the U.S. Department of State and U.S. lead negotiator in Rome, unsuccesfully attempted to buy time for U.S. reconsideration of the Statute before deliberations were pushed through to a vote.[5] On July 1, 2002, after receiving the necessary sixty ratifications for implementation, the Rome Statute of the International Criminal Court entered into force.[6]

American concerns about the new international court were multifold. After the Rome Statute vote, Ambassador Scheffer reported to Congress that the Rome Statute could potentially "inhibit the ability of the United States to use its military to meet alliance obligations and participate in multinational operations, including humanitarian interventions to save civilian lives."[7] The U.S. had two principal concerns. First, the ICC's possible exercise of jurisdiction over non-party nationals prompted sovereignty concerns related to the prosecution of U.S. troops and civilians serving abroad.[8] Second, the possibility for politicized prosecutions and an unaccountable prosecutor raised concerns about the targeting of Americans.[9] Although the U.S.—during the waning days of the Clinton Administration—ultimately signed the Rome Statute in 2000, it subsequently notified the United Nations Secretary General in May 2002 that it did not intend to become a party.[10] The U.S. thereby relieved itself of an obligation not to

---

[3] DAVID SCHEFFER, ALL THE MISSING SOULS: A PERSONAL HISTORY OF THE WAR CRIMES TRIBUNALS 192 (Princeton University Press 2012).
[4] Id. at 207.
[5] Id.
[6] See Rome Statute of the International Criminal Court, *entered into force* July 1, 2002, 2187 U.N.T.S. 90.
[7] *American Service-Members' Protection Act*, U.S. DEPARTMENT OF STATE, BUREAU OF POLITICAL AND MILITARY AFFAIRS, http://www.state.gov/t/pm/rls/othr/misc/23425.htm (last visited Sept. 11, 2013).
[8] JENNIFER K. ELSEA, CONG. RESEARCH SERV., CRS REPORT FOR CONGRESS: U.S. POLICY REGARDING THE INTERNATIONAL CRIMINAL COURT 5-6 (2006), *available at* http://congressionalresearch.com/RL31495/document.php?study=U.S.+Policy+Regarding+the+International+Criminal+Court.
[9] Id. at 7-8. Other U.S. concerns included the fact that fewer due process guarantees existed under the Rome Statute than the U.S. Constitution, as well as an American belief that the ICC would interfere with U.N. Security Council operations. Id. at 8-11.
[10] WILLIAM H. TAFT, IV ET AL., AMERICAN SOCIETY OF INTERNATIONAL LAW, U.S. POLICY TOWARD THE INTERNATIONAL CRIMINAL COURT: FURTHERING POSITIVE ENGAGEMENT 30-31 (2009). John Bolton, former U.S. Ambassador to the United Nations, described his rescinding of the American

defeat the Statute's "object and purpose."[11] U.S. concerns then set the stage for subsequent legislation targeting the ICC in the American Servicemembers' Protection Act.

The American Servicemembers' Protection Act became law in August 2002. Senator Jesse Helms introduced the legislation,[12] which the Senate adopted as an amendment to the Supplemental Defense Appropriations Act of 2002.[13] Senator Helms and other legislators argued that the legislation was necessary because the ICC threatened U.S. sovereignty.[14] Therefore, they included a provision allowing the President to use "all means necessary and appropriate" to release U.S. personnel detained on behalf of the Court, as well as other provisions restricting cooperation with the ICC.[15] Senator Christopher Dodd, however, managed to add language to the Act that expressly permited a certain degree of U.S. cooperation with the ICC.[16] This mixed result reflected divided Congressional opinions as to whether there should be cooperation with the Court with respect to cases involving individuals accused of committing serious international crimes.

III. Functions and Operation

ASPA currently prohibits U.S. cooperation with ICC investigations in three ways. First, the term "support" limits the extent of U.S. assistance to the ICC. Second, a prohibition on ICC "investigative activity" is included in the Act to prevent ICC investigations "within the United States." Third, the Act bars the sharing of intelligence and law enforcement information with the ICC or with any States Parties to the Rome Statute.[17]

A. Defining "Support"

The prohibition on "support" can be broadly interpreted to limit virtually any U.S. governmental "agency or entity of the United States Government or of any State or local government, including any court" from cooperating in any manner with the ICC.[18] Therefore, essentially all public entities are prohibited from providing support to the ICC.

The Act defines support as "assistance of any kind, including financial support, transfer of property or other material support, services, intelligence sharing, law enforcement cooperation, the training or detail of personnel, and the arrest or detention of individuals."[19]

---

intention to ratify the Rome Statute as "the happiest moment in my government service." Carla Anne Robbins, *Disarming America's Treaties*, WALL STREET JOURNAL, July 19, 2002.

[11] See Vienna Convention on the Law of Treaties art. 18, *opened for signature* May 23, 1969, 1155 U.N.T.S. 331.

[12] 147 CONG. REC. 24,377 (2001).

[13] 148 CONG. REC. 14,051 (2002).

[14] 148 CONG. REC. 9589 (2002).

[15] ASPA § 2008.

[16] 148 CONG. REC. 9590 (2002).

[17] Id.

[18] ASPA §§ 2004(e), (h), 2013(12).

[19] ASPA § 2013(12). As Senator Warner explained, "no Federal or State entity, including courts, may cooperate with the ICC in law enforcement matters," including: arrest, extradition, search and seizure,

Furthermore, "[n]o classified national security information can be transferred directly or indirectly to the ICC."[20] Senator John Warner, discussing ASPA on the Senate floor in 2002, elaborated that the prohibition included "searches and seizures, discovery, asset seizure … [and] otherwise render[ing] services to the ICC."[21]

B. Defining "Investigative Activity within the United States"

The Act's "Prohibition on Investigative Activities of Agents" limits the ICC's activities in the United States. It provides that "[n]o agent of the International Criminal Court may conduct, in the United States or any territory subject to the jurisdiction of the United States, any investigative activity relating to a preliminary inquiry, investigation, prosecution, or other proceeding at the International Criminal Court."[22]

Although an authorative interpretation of the statute from the Office of Legal Counsel, Department of Justice,[23] has not been made public, a restrictive reading of "investigative activity" could prohibit virtually any ICC activity within the United States. Both the clauses "investigative activity" and "within the United States" could prohibit ICC personnel from conducting any activities in support of either their examination of witnesses or their investigations on U.S. soil. The restrictions could extend to a smaller scale of activity than one might initially assume from reading the plain text of the Act. For example, this reading may even prohibit investigative activity involving an ICC investigator contacting a witness located in the United States. Because the call is pursuant to an ICC investigation, ASPA could be interpreted to require the witness to relocate outside the U.S. before speaking with an ICC agent about anything of substance regarding the individual's potential testimony. These examples demonstrate the extent of ASPA's interference on ICC investigative activity with a restrictive reading of the Act.

A more liberal reading could instead center on the location of the ICC investigator. The investigative activity provision of ASPA then would not be implicated until the ICC investigator actually enters U.S. territory, and so a phone call to a potential witness may not be prohibited as "investigative activity within the United States." Or, if the phone call is not investigatory in nature, the call itself may be exempt. The reading of what is "investigative" and what is considered "within the United States" goes to the heart of issues with cyberinvestigations and ASPA.

---

discovery, asset seizure, financial support, transfer of property, personnel details, intelligence sharing, or otherwise rendering services to the ICC. 148 CONG. REC. 9589 (2002).

[20] ASPA § 2006; 148 CONG. REC. 9589 (2002).

[21] 148 CONG. REC. 9589 (2002).

[22] ASPA § 2004(h).

[23] The Office of Legal Counsel at the Department of Justice is charged with "provid[ing] authoritative legal advice to the President and all the Executive Branch agencies." OFFICE OF LEGAL COUNSEL, DEPARTMENT OF JUSTICE (last visited October 12, 2013), http://www.justice.gov/olc/.

C. Obtaining Digital Evidence from Service Providers

The extent to which considerations related to ASPA limit the ICC's ability to gather digital evidence from U.S. service providers remains unclear. This is important for investigations, as the amount of information flowing through U.S. service providers is very high. As described below, there is nothing in ASPA's statutory language to suggest that U.S. service providers that hold digital evidence[24] are bound by its restrictions. However, service providers may be reluctant to cooperate for practical, political, or other reasons. Further, establishing the location of data can be relatively difficult. Overall, as described in the working paper "Digital Evidence: Investigatory Principles," ICC investigators will need to develop protocols for accessing digital evidence from service providers. Moving forward, it would be helpful to identify whether United States service providers consider themeselves restricted by ASPA or related considerations, and what might prevent these actors from cooperating with the ICC.

i. ASPA's Jurisdiction and Private Companies

On its face, ASPA restricts only the actions of public entities, not private companies such as Internet Service Providers (ISPs or service providers). Specifically, the Act states that "no United States Court, and no agency or entity of any State or local government, including any court, may cooperate with the International Criminal Court in response to a request for cooperation submitted by the International Criminal Court pursuant to the Rome Statute."[25] However, a question remains as to whether or not private U.S. entities would want to cooperate with the ICC, or feel obligated to do so, given that the United States is not bound by the Rome Statute.

There do exist important threshold questions as to how companies might respond to such requests. There is the possibility of a chilling effect, where private entities may be unwilling to cooperate because of political considerations surrounding ASPA, and related fears of governmental retribution for cooperating. This effect appears with other complex statutes, such as when a statute imposes sanctions for prohibited conduct with a foreign entity, and companies may restrict conduct beyond that specified in the statute for fear of being in violation.

[24] As set forth in the "Digital Evidence: Investigatory Principles" working paper for this meeting, digital evidence is "data that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the proceeding." For the purposes of the discussion, the "Digital Evidence: Investigatory Principles" working paper divides "digital evidence" into three categories. The first category includes data that investigators acquire from a physical device such as a hard drive or wireless phone. The second category includes data divorced from a device, but accessible from a service provider. For example, a video that is stored in a publicly available online service, such as YouTube, or evidence emailed to an investigator from the scene of a crime, would each fall into this category. The third category includes evidentiary data held by a service provider, and not otherwise available. Email messages held by a service such as Gmail or Yahoo! Mail and photographs held in a cloud storage service such as Dropbox are each examples of data in this category.

[25] ASPA § 2004.

ii. Location of Data in Cyberinvestigations

Data relevant to investigations may be located solely within the United States, solely outside of the United States, or in multiple locations at the same time. U.S. service providers have located their data centers worldwide, in order to gain efficiency, speed up user access to data, and to comply with local requirements. Accordingly, data may be available without access to a server located within the United States. Complications, however, can arise in terms of where the data is stored and what jurisdiction governs access to that data.

Data may be stored outside of the United States, or may be available in multiple jurisdictions. For example, if an American student travels to Europe to attend a workshop, her Gmail cloud-based e-mail service may copy the archive of her email to servers in Europe to improve access. Obtaining data located in a foreign jurisdiction like this may involve identifying and following that country's local rules and procedures. These may be straightforward to follow or not, depending on the situation at hand.

However, the greatest difficulty may actually be pinpointing the location of the data, which has to be conducted on a case-by-case basis and may be constantly changing. Section III of the workshop paper "Digital Evidence: Investigatory Principles" further elaborates on indentifying the location of the data and processes for obtaining data from U.S. service providers.

In theory, digital evidence should be obtainable from service providers, but a variety of factors may complicate any particular investigation. Outstanding questions include whether service providers consider themselves to be bound or limited by ASPA's restrictions, locating the data, and developing protocols for obtaining data from U.S.-based or foreign servers owned by U.S.-based service providers.

IV. Special Exceptions to ASPA's Prohibitions

There are some statutory exceptions to the prohibitions on U.S. cooperation with the ICC. First, the Dodd Amendment allows U.S. agencies to share information with the Court.[26] Second, the President may cooperate with or transfer national security information to the ICC when the cooperation is pursuant to his duties as Commander in Chief of the Armed Forces.[27] Third, the President may waive restrictions, for one-year periods, on both U.S. participation in U.N. peacekeeping operations and on U.S. military assistance to States Parties.[28] All of these exceptions, however, are accompanied by limitations and are examined in this section.

[26] *The State Department's Rewards Programs: Performance and Potential: Hearing Before the Subcomm. on Terrorism, Nonproliferation, and Trade*, 112th Cong. 1 (2012) [hereinafter *Rewards Programs Hearings*] (statement of Stephen Rapp, Ambassador-at-Large, Office of Global Criminal Justice).
[27] ASPA § 2011.
[28] ASPA §§ 2003, 2005, 2007.

A. The Dodd Amendment

Section 2015 of the Act, also known as the Dodd Amendment, counteracts ASPA's otherwise broad prohibition on ICC support. Because the Amendment applies to ICC investigations of *foreign* nationals, it can serve, in the view of some commentators, as a "catch-all exception authorizing the U.S. government to participate in a wide range of international justice efforts"[29] so long as U.S. persons are not at risk of prosecution. The Amendment, which is contained in a section entitled "Assistance to International Efforts," provides:

> Nothing in this title shall prohibit the United States from rendering assistance to international efforts to bring to justice Saddam Hussein, Slobodan Milosovic, Osama bin Laden, other members of Al Qaeda, leaders of Islamic Jihad, and other foreign nationals accused of genocide, war crimes or crimes against humanity.[30]

The Amendment ensures that U.S. cooperation with the ICC is possible when (1) the ICC has jurisdiction over an international crime, (2) when a foreign national (as opposed to U.S. national) is being investigated or prosecuted, and (3) when there is no U.S. objection to that jurisdiction (such as when U.S. nationals—or, potentially, U.S. allies—could be prosecuted).[31]

At this time, the Dodd Amendment is the primary exception the United States has invoked to directly assist the investigative efforts of the ICC. The Amendment operates on a case-by-case basis. For each ICC request for information that is within the control of a United States public entity, the ICC submits a request to the U.S. embassy at The Hague. The embassy then transmits the requests to the State Department, where they are reviewed internally and within an interagency process.[32] For a typical request, an internal memorandum will be circulated to relevant agencies, allowing for an opportunity to object to case-specific information sharing. Absent objection, the request will be approved. For atypical requests, the relevant agencies and authorities may meet face-to-face to weigh competing policy considerations. Though limited in scope, this approach permits U.S. cooperation with the ICC, while also allowing the U.S. to retain control over the the extent of its cooperation.

B. Presidential Waivers

Various Presidential waivers exist that circumvent prohibitions of ASPA. Section 2011 of ASPA permits the President, pursuant to his powers as Commander in Chief, to share information in his control with the ICC.[33] According to the research for this paper, the President has not yet invoked this waiver. However, members of Congress have already spoken to how this waiver would be implemented. Speaking on the floor of the House of Representatives in 2002, Senator Henry Hyde, who introduced ASPA in the House, explained that this exception turns on the

---

[29] 148 CONG. REC. 15,659 (2002). Recall that the purpose of ASPA is to protect against ICC prosecutions of *U.S.* nationals.
[30] ASPA § 2015.
[31] 148 CONG. REC. 15,659 (2002).
[32] *Rewards Programs Hearings*, *supra* note 26.
[33] 148 CONG. REC. 14,050 (2002).

"parameters of the President's authority under the Constitution,"[34] and is decided on a "case-by-case basis" by the President.[35] He also clarified that this waiver can be used to facilitate the transfer of foreign nationals to the ICC.[36] Importantly, he noted that this provision also allows the President to provide classified national security information to the ICC.[37] However, this waiver cannot be used by the President to order state and local governments to undertake any action vis-à-vis the ICC, a power not within the President's executive authority.[38] In his remarks, Representative Hyde also stated that there may be other situations, not yet explored, where this presidential waiver could be used.[39]

Other waivers also exist in ASPA that govern the participation of U.S. Armed Forces in peacekeeping missions. First, a waiver in section 2003 authorizes the President to waive restrictions on peacekeeping in section 2005. This waiver also applied to section 2007, before it was removed in the 2008 amended version of ASPA.[40] Second, section 2003 also waives prohibitions in sections 2004 and 2006 that govern United States cooperation with an investigation or prosecution of a named individual by the International Criminal Court.[41] However, the entire section 2003 waiver may not be executable on its face. The waiver requires that the ICC enter into a binding agreement with the United States "that prohibits the [ICC] from seeking to exercise jurisdiction" over U.S. personnel.[42] Such a binding agreement could be non-achievable in practice, given it would require the ICC to relinquish its own jurisdiction.

In regards to peacekeeping efforts, section 2005 still allows for U.S. participation if the President obtains a "national interest certification."[43] This certification requires that U.S. Armed Forces participating in peacekeeping efforts be immunized from risk of criminal prosecution or other assertion of the jurisdiction of the ICC,[44] and it relies on "factual judgments made by the President."[45] A sample of such an agreement is attached in the Appendix of this paper. Both Presidents Bush and Obama have obtained national interest certifications to allow U.S. Armed Forces to participate in U.N. peacekeeping efforts.[46]

---

[34] Id. at 14,049.
[35] Id.
[36] Id.
[37] Id.
[38] Id. at 14,050.
[39] Id. at 14,050.
[40] ASPA §§ 2001-2015.
[41] ASPA § 2003.
[42] ASPA § 2003(a)(2).
[43] ASPA § 2005(c), (2008); 148 Cong. Rec. 14,049 (2002).
[44] ASPA §§ 2003-2005 (2008).
[45] 148 CONG. REC. 14,049 (2002).
[46] President Bush authorized the participation of U.S. Armed Forces in the United Nations-African Union Mission in Darfur (UNAMID), while also declaring U.S. Forces immune from ICC jurisdiction. Memorandum from the President to the Secretary of State, *Certification Concerning U.S. Participation in the United Nations-African Union Mission in Darfur Under Section 2005 of the American Servicemembers' Protection Act* (March 26, 2008), http://georgewbush-whitehouse.archives.gov/news/releases/2008/03/print/20080327-1.html. See Appendix A (Sample

Before the 2008 amendment to ASPA, section 2007 restricted military aid to parties to the Rome Statute.[47] Article 98 waivers were obtained to waive the restriction on military assistance.[48] These agreements immunized U.S. personnel from ICC prosecution in exchange for a waiver on restrictions to U.S. military aid.[49] However, the 2008 amendment to ASPA removed section 2007 and the restrictions on military aid.[50]

C. Unresolved Questions Regarding Penalties for Breach

Currently, there are no explicitly defined penalties for breach of ASPA in the text, or stated through Congressional interpretation of the Act. Neither intra-governmental penalties nor penalties for private individuals or institutions exist within the text. Further, to the best of our knowledge, no breaches of ASPA have been found, or penalties for breach imposed.

V. The Current Extent of U.S. Cooperation with the ICC

The current U.S. administration is increasing cooperation with the ICC, while still maintaining reservations and control over information it shares. On March 23, 2010, at a meeting of the Assembly of States Parties in New York, Ambassador Stephen Rapp, the Ambassador-at-Large on War Crimes Issues at the U.S. Department of State,[51] delivered a speech in which he indicated that the United States wished to strengthen and improve its relationship with the ICC.[52]

Presidential Waiver). In 2012, President Obama authorized U.S. participation in the United Nations Mission in South Sudan. Memorandum from the President to the Secretary of State, *Certification Concerning U.S. Participation in the United Nations Mission in South Sudan Consistent with Section 2005 of the American Servicemembers' Protection Act* (January 10, 2012), http://www.whitehouse.gov/the-press-office/2012/01/10/presidential-memorandum-certification-concerning-us-participation-united. Additionally, national interest certifications have been used to authorize the involvement of U.S. Armed Forces in the United Nations Stabilization Mission in Haiti (MINUSTAH) and the United Nations Mission in Liberia (UNMIL). Memorandum from the President to the Secretary of State, *Certification Concerning U.S. Participation in the United Nations Stabilization Mission in Haiti Consistent with Section 2005 of the American Servicemembers' Protection Act* (June 14, 2004), http://georgewbush-whitehouse.archives.gov/news/releases/2004/06/20040614-10.html; Memorandum from the President to the Secretary of State, *Certification concerning U.S. participation in the U.N. mission in Liberia consistent with Section 2005 of the American Servicemembers' Protection Act* (October 20, 2003), http://georgewbush-whitehouse.archives.gov/news/releases/2003/10/20031020-9.html.

[47] ASPA § 2007 (2002).

[48] A list of the waivers can be found at Georgetown Law Library, *International Criminal Court - Article 98 Agreements Research Guide*, http://www.law.georgetown.edu/library/research/guides/article_98.cfm.

[49] Id.

[50] Office of the Press Secretary, *President Bush Signs H.R. 4986, the National Defense Authorization Act for Fiscal Year 2008 into Law*, (January 28, 2008); ASPA §§ 2001-2015 (2008).

[51] Biography, U.S. DEPARTMENT OF STATE, Stephen J. Rapp, http://www.state.gov/r/pa/ei/biog/129455.htm (last visited Oct. 9, 2013).

[52] Stephen J. Rapp, *Statement by Stephen J. Rapp, U.S. Ambassador-at-Large for War Crimes, Regarding Stocktaking at the Eighth Resumed Session of the Assembly of States Parties of the International Criminal Court* (March 23, 2010), *available at* http://usun.state.gov/briefing/statements/2010/138999.htm.

President Obama has since taken steps toward improving relations with the ICC. In March 2010, President Obama affirmed his commitment to "support[] the ICC's prosecution of those cases that advance U.S. interests and values, consistent with the requirements of U.S. law."[53] Further, in October 2012, Susan Rice, then-U.S. Ambassador to the United Nations, said the U.S. had "actively engaged with the ICC Prosecutor and Registrar" to support "specific prosecutions already underway" and has "responded positively to informal requests for assistance."[54]

The Obama Administration has also taken direct action to improve cooperation with the ICC. The President signed into law a State Department program that issues rewards for information regarding certain ICC suspects-at-large.[55] Ambassador Rapp stated the program "would be *crime*-specific, not court-specific and would allow the United States to engage more fully in pursuit of . . . foreign nationals."[56] In May 2013, the State Department announced that it was offering monetary rewards for information leading to the arrest and surrender of Joseph Kony and other commanders of the Lord's Resistance Army—all of whom have been indicted by the ICC.[57] The U.S. has also facilitated the transfer of ICC suspect Bosco Ntaganda to The Hague when he appeared at the U.S. embassy in Kigali, Rwanda.[58] These actions fall within the scope of the Dodd Amendment as they concern ICC prosecution of foreign nationals.

The Obama Administration has also taken actions apart from direct cooperation with the ICC (and outside of ASPA's reach) that may align with the interests of the Office of the Prosecutor. On August 4, 2011, President Obama issued Presidential Study Directive 10, establishing an interagency Atrocities Prevention Board ("the Board").[59] According to the Directive, the "primary purpose of the Atrocities Prevention Board shall be to coordinate a whole of government approach to preventing mass atrocities and genocide."[60] Further, the Board ensures increased monitoring and capacity to prevent and respond to atrocities.[61] Importantly, it will examine protocols to share intelligence with institutions in response to atrocities.[62] In a

---

[53] United States National Security Strategy, THE WHITE HOUSE, (May 27, 2010), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
[54] Susan E. Rice, Ambassador, U.S. Permanent Representative to the United Nations, *Remarks at a UN Security Council Debate on Peace & Justice, with a Special Focus on the Role of the International Criminal Court New York, NY* (October 17, 2012), http://usun.state.gov/briefing/statements/199261.htm.
[55] Department of State Rewards Program Update and Technical Corrections Act of 2012, on January 15, 2013 (S.2318A), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112s2318enr/pdf/BILLS-112s2318enr.pdf. See Statement by the President on Enhanced State Department Rewards Program (January 15, 2013), http://www.whitehouse.gov/the-press-office/2013/01/15/statement-president-enhanced-state-department-rewards-program.
[56] *Rewards Programs Hearing*, *supra* note 26, at 112-129.
[57] *U.S. offers $5 million for information leading to Joseph Kony, top associates*, CNN (Apr. 4, 2013, 5:23 AM), http://www.cnn.com/2013/04/03/us/kony-reward-money/index.html. See *Wanted: Joseph Kony*, U.S. DEPARTMENT OF STATE, OFFICE OF GLOBAL CRIMINAL JUSTICE, http://www.state.gov/j/gcj/wcrp/206078.htm (last visited Oct. 6, 2013).
[58] Id.
[59] Presidential Study Directive/PSD-10, Presidential Study Directive on Mass Atrocities (August 4, 2011).
[60] Id.
[61] Id.
[62] Id.

recent fact sheet on the Board, an affirmation of support for "national, hybrid, and international mechanisms (including, among other things, commissions of inquiry, fact finding missions, and tribunals)" was made.[63] As well, it detailed actions like "the passage of UN Security Council Resolutions 1970 and 1973, which authorized—in an unprecedented combination of measures—referral of the situation in Libya to the International Criminal Court," and the support to capture "priority figures wanted by international tribunals (including Goran Hadzic and Ratko Mladic)."[64]

VI. Conclusion

The Obama Administration has increased efforts to cooperate with the ICC, as well as to improve U.S. responses to atrocity crimes. This increased American openness to aiding in the prosecution of crimes at the international level suggests that a thorough review should be undertaken, in order to consider how public and private entities in the United States can lawfully respond to digital information requests from the ICC. In particular, U.S.-based ISPs can review their responses to the sharing of data with the ICC, although the ICC may not be able to directly request information from private entities.

ASPA already provides some tools for increased responsiveness to the ICC. First, the Dodd Amendment can continue to be invoked in the case-by-case manner in which it is currently used to share information and otherwise support particular cases proceeding before the ICC. Second, the President can invoke the section 2011 waiver, which allows use of executive Commander in Chief powers. This waiver could potentially be used to assist in the apprehension of suspects and their subsequent transfer to the control of the ICC. It could also be used to provide relevant, classified national security information to the ICC. Third, the President can increase usage of section 2005 to further U.S. participation in U.N. peacekeeping operations. The President need only provide to Congress the "national interest certification" that ensures the operation aligns with U.S. interests and that U.S. personnel will not be subject to prosecution by the ICC. Finally, cooperation external to the ICC can be expanded, such as through development of the Atrocities Prevention Board and the State Department's Rewards Program.

Changes to or clarifications of internal interpretations of ASPA could make the extent of its reach regarding digital evidence much clearer. This would include defining any application of ASPA to private entities, such as ISPs, since it appears ASPA currently only extends to public entities. Clarity is also needed regarding whether or not the Act extends to data outside of the U.S. that is controlled by U.S.-based companies, especially considering that U.S. companies control the vast majority of digital information. Furthermore, any potential penalties for breach of ASPA should be made clear.

As Senator Dodd has stated, ASPA is very complex, and "[t]here are waivers within waivers which turn out not to be waivers at all because the conditions of the waivers are

[63] The White House, *Fact Sheet: A Comprehensive Strategy and New Tools to Prevent and Respond to Atrocities* (Apr. 23, 2012), *available at* http://www.whitehouse.gov/the-press-office/2012/04/23/fact-sheet-comprehensive-strategy-and-new-tools-prevent-and-respond-atro.
[64] Id.

unattainable in many instances."[65] Futher clarification is required to understand how the Act applies to digital evidence and the circumstances surrounding increased U.S. engagement with the ICC.

[65] 148 CONG. REC. 9591 (2002).

VII. Appendix

SAMPLE PRESIDENTIAL WAIVER

> Consistent with section 2005 of the American Servicemembers' Protection Act (Public Law 107-206; 22 U.S.C. 7421 et seq.), concerning the participation of members of the Armed Forces of the United States in certain United Nations peacekeeping and peace enforcement operations, I hereby certify that members of the U.S. Armed Forces participating in the United Nations-African Union Mission in Darfur (UNAMID) are without risk of criminal prosecution or other assertion of jurisdiction by the International Criminal Court (ICC) because the United Nations Security Council has permanently exempted members of the U.S. Armed Forces participating in UNAMID from criminal prosecution or other assertion of jurisdiction by the ICC for actions undertaken by them in connection with UNAMID by deciding, in Resolution 1593 (2005), that "personnel from a contributing state outside Sudan which is not a party to the Rome Statute of the International Criminal Court shall be subject to the exclusive jurisdiction of that contributing State for all alleged acts or omissions arising out of or related to operations in Sudan established or authorized by the Council or the African Union, unless such exclusive jurisdiction has been expressly waived by that contributing State."

Memorandum for the Secretary of State, Certification Concerning U.S. Participation in the United Nations-African Union Mission in Darfur Under Section 2005 of the American Servicemembers' Protection Act (March 26, 2008), http://georgewbush-whitehouse.archives.gov/news/releases/2008/03/print/20080327-1.html.

WORKING PAPER

DIGITAL EVIDENCE: INVESTIGATORY PROTOCOLS

SALZBURG WORKSHOP ON CYBERINVESTIGATIONS

This paper was prepared by Tommy Umberg '15 and Cherrie Warden '15, students from the International Human Rights Law Clinic and the Samuelson Law, Technology & Public Policy Clinic at the University of California, Berkeley, School of Law, under the supervision of Professors Laurel E. Fletcher, Chris Jay Hoofnagle, Eric Stover, and Jennifer M. Urban

October 2013

Table of Contents

Abstract

The purpose of this paper is to assist the Office of the Prosecutor ("OTP") at the International Criminal Court ("ICC") by discussing cyberinvestigation protocols that enable strategic mobilization and acquisition of digital evidence.

This paper discusses cyberinvestigation protocols relevant to three types of digital evidence: data that is on a device; data that is not on a device or is accessible online; and data that is held privately by a service provider. The first section addresses how an investigator should acquire and authenticate physical devices that may have evidentiary value. The protocols demonstrate methods that reduce the risk of inadmissibility and manipulation. The second section addresses situations where the investigator obtains evidence independent of a physical device, for instance, a video that is posted on a publicly available website. Since this type of digital evidence is not forensically acquired, this section aims to help investigators determine its reliability. Additionally, this section explains how prosecutors might authenticate such evidence by corroboration or testimony. The third section turns to data held by service providers that is not available without their cooperation. This data may be acquired by a direct request from a prosecutor. For United States service providers, the U. S. Stored Communications Act ("SCA") sets forth procedures for domestic law enforcement access to this data. It is silent on foreign law enforcement access. The Mutual Legal Assistance Treaties ("MLAT") process addresses foreign law enforcement access to this data; however, this process is lengthy and may be subject to other legal requirements, such as dual criminality. Please note that protocols in all three sections are based on standards that reflect the current technological landscape and therefore should be updated when necessary. Furthermore, the basic procedures discussed here are derived from lengthy treatments of forensic analysis in source documents. In all three types of investigations, situational factors arise in which deviation from the protocols discussed is appropriate. Therefore, each investigation will need to employ specific procedures that are context-dependent.

I. Introduction

Cyberinvestigation protocols help investigators gather digital evidence in a forensically valid way. This paper presents the existing landscape, presents challenges and opportunities, as well as provides a framework to aid prosecutors in strengthening linkage evidence in cyberinvestigations.

Digital evidence is "data that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the proceeding."[1] For purposes of this paper, we have divided "digital evidence" into three categories. The first category includes data that an investigator acquires from a physical device such as a hard drive or wireless phone. The second category includes data divorced from a device, but accessible from an online service. For example, a video that is stored in a publicly available online service, such as YouTube, or evidence emailed to an investigator from the scene

[1] STEPHEN MASON, BRITISH INSTITUTE OF INTERNATIONAL AND COMPARATIVE LAW, INTERNATIONAL ELECTRONIC EVIDENCE (2008).

of a crime. The third category includes evidentiary data held by a service provider, and not otherwise available. Email messages held by a service such as Gmail or Yahoo! Mail and photographs held in a cloud storage service such as Dropbox are each examples of this category of data.

The protocols illustrate digital evidence practices employed by investigators throughout the international community; however, this paper does not claim to set out minimum standards required to gather evidence or to offer precise procedures for how the ICC will evaluate different forms of digital evidence. Individual investigations are context and fact-specific, thus they may be affected by resource limitations as well as situational factors. As such, this paper sets out the basic procedures in order to provide some foundational information to aid the workshop discussion and the ICC's efforts in further developing its cyberinvestigation practices. Finally, the entirety of relevant investigative practices cannot be summarized in a treatment of this length.

II. Evidentiary Protocols for Devices Possessed by Investigators

This section addresses situations for investigators who encounter or directly obtain a physical device, such as a hard drive, that may have evidentiary value. The handling of the device affects admissibility of evidence and its probative value. Consideration of the described protocols will enhance the veracity of the evidence.

These protocols are a compilation of the U.S. Department of Justice [2] and the Association of Chief Police Officers ("ACPO")[3] practice guides for computer-based electronic evidence. These guidelines were chosen because they are based upon current technologies and are referenced throughout the cyberinvestigation community; however, the guidelines should be updated as new technologies emerge.

A. Acquisition

To maximize the integrity of an investigation, the investigator should identify the device, determine its setup, and make a forensic copy of the data. Investigators should document their actions by keeping a log that describes persons who handled the evidence, actions taken which could potentially alter the evidence, and the physical storage of the evidence from the point of discovery to its introduction. Capturing the entire process on video[4] is highly recommended.[5] Thorough documentation of the acquisition process will aid in establishing the chain of custody and the overall credibility of evidence.

---

[2] US DEPARTMENT OF JUSTICE, FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT, (2012), *available at* https://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

[3] ASSOCIATION OF CHIEF POLICE OFFICERS, GOOD PRACTICE GUIDE FOR COMPUTER-BASED ELECTRONIC EVIDENCE, (2003), *available at* http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

[4] If possible, disable audio component because conversations or reactions by investigators may become an issue during trial.

[5] MARJIE T. BRITZ, COMPUTER FORENSICS AND CYBER CRIME 317 (2013).

Furthermore, the documentation log should include a diagram or a photograph depicting the device's setup, including all cables and ports, so it may be reassembled if necessary. If disassembling the device for relocation, all items should have signed exhibit labels attached. Failure to do so may create difficulties with chain of custody leading to defense challenges. Additionally, it is common for individuals to keep their passwords in written form and in close proximity to their computer; therefore investigators should search surrounding areas and document all potentially valuable pieces of evidence.

Upon discovery[6], the investigator should determine whether the device is powered on or off. A device in sleep mode or with a powered-off monitor may mislead the investigator in this determination.[7] To check if a computer is truly off, the investigator should switch the monitor on and move the mouse slightly. If there is no change in the screen, then the device may be powered off.[8]

i. Discovery of a Powered-Off Device

A powered-off device should be forensically imaged on site or in a forensic lab.[9] A forensic image ensures that analysts do not inadvertently alter data during the examination. Retaining an unaltered version strengthens the evidence's probative value by alleviating best evidence[10] concerns. Ideally, an image of the entire device should be made, however, partial or selective file copying may be considered as an alternative when the amount of data to be imaged makes complete copies impracticable.

As part of the forensic imaging process, the investigator should compare the internal clock of the device in its BIOS against the actual time. Often, the internal clock differs from the actual date and time causing file metadata[11] to be inaccurate. Information regarding the difference between the internal clock and the actual time is useful in authentication of the evidence, establishing its chain of custody, and may aid in creating linkage between the

---

[6] Storage drives may be located on a wired or wireless network, thus a thorough investigation would trace the physical wired network and search for wireless links to network storage. Furthermore, if available, then investigators should always seize back-ups of the data.

[7] US DEPARTMENT OF JUSTICE, ELECTRONIC CRIME SCENE INVESTIGATION: AN ON-THE-SCENE REFERENCE FOR FIRST RESPONDERS (2001), *available at* http://www.ncjrs.org.

[8] Id.

[9] For a detailed explanation of currently available tools for "forensic imaging" *See* PETER SOMMER, INFORMATION ASSURANCE ADVISORY COUNSEL, DIGITAL EVIDENCE, DIGITAL INVESTIGATIONS AND E-DISCLOSURE: A GUIDE TO FORENSIC READINESS FOR ORGANISATIONS, SECURITY ADVISERS AND LAWYERS 40, *available at* *http://www.iaac.org.uk/_media/DigitalInvestigations2012.pdf?goback=%2Egde_37008_member_157854004#%21.*

[10] "Best evidence" issues arise when the evidence submitted is a copy of an original and the original was accessible to the party proffering such evidence

[11] "Metadata" is "data about data," and includes the dates and times the files were viewed or altered.

defendant and the evidence.[12] To establish the accurate metadata time stamps, examiners can photograph the computer time in the BIOS screen next to an external clock.

At this point the hard drive and its forensic copy should be brought to a secure location for examination and analysis. Proper ways to transport and store the equipment are discussed below.

ii. Discovery of a Powered-On Device

A powered-on device presents special challenges. If the device has encryption, powering it off may cause volumes to automatically encrypt such that investigators can never recover the data.[13]

An inexperienced investigator, who discovers a hard drive, should leave it on until the appropriate personnel arrive to assess the situation. Once the investigator arrives, two decisions exist. First, whether to immediately shut down the device or gather evidence prior to doing so. Second, whether it is more prudent to shut down the device by pulling the power cord or by internal commands. This section discusses the tradeoffs in both decisions.

In assessing whether to power-down or gather evidence, first, investigators must weigh whether a digital inspection will inadvertently alter evidence and raise authentication issues later.[14]

Alternatively, some data may be destroyed or encrypted if the device is immediately shut down. Data at risk of being lost is stored in the devices' Random Access Memory (RAM), which may contain active programs and passwords.[15] Ultimately, investigators should consider whether the value of the recoverable volatile data outweigh the potential risk of diminishing the credibility of other anticipated evidence.

---

[12] *See* Prosecutor v. Karemera, et al. Case No. IT-98-44-T, Judgment, ¶ 169-173, 205 (Int'l Crim. Trib. for Rwanda Feb. 2, 2012)(The date and time of a video of a rally submitted as evidence proved that the accused was in attendance).

[13] *In re Grand Jury Subpoena to Sebastien Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. 2009) (Investigators shut down a suspect's computer causing encryption of evidence that was unrecoverable without the suspect's password).

[14] The general rule for mobile phones is to block remote alteration by placing the phone in a faraday bag, which is a radio frequency shielding cloth, or by switching it to "airplane" mode or its equivalent. *See* Eric Katz, A Field Test of Mobile Phone Shielding Devices 8 (Dec. 10, 2010) (Ph.D dissertation, Purdue University). *available at* http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1033&context=techmasters. However, mobile forensics is becoming more complex as security on mobile devices improves. New features allowing the user to remotely wipe data (such as Apple iPhone's "Find My Phone") require mobile devices to be quickly isolated from the network to prevent the user from destroying data. On the other hand, network isolation can trigger data destruction. For instance, Blackberry devices will automatically wipe all data after being disconnected from the network for a certain number of days, thus requiring forensic analysis to occur shortly after the device is seized.

[15] Examples of "running processes" that are typically more valuable to investigations are, instant messaging conversations, financial statements, active remote data storage, or data encryption.

If an investigator decides to gather evidence prior to shutting down the device, then the investigator should consider making the evidence visible on the screen and photographing it. All actions taken in the attempt to bring the relevant information onto the screen should be documented.

The recommended method for powering down the computer is dependent upon the target device's operating system.[16] It is generally advocated to pull the power cord or battery out of the device rather than from the wall socket. This prevents the hard drive from performing shut down processes that may alter the original hard drive.[17] However, some operating systems can be damaged by immediate power failure and should be shut down through the regular internal shut down commands. To aid in making this decision, appendix V lists operating systems and their corresponding preferred shut down method.

Once the device is shut down, it should be forensically imaged.

B. Authentication

Authentication demonstrates that the investigation has not altered the digital evidence. The authentication process seeks to determine that the forensic image is an exact replica of the original device in question. Even a slight difference between the forensic image and the original will have a deleterious affect on the evidence's ultimate probative value.[18]

Typically, investigators authenticate evidence originating from a hard drive through an electronic fingerprinting process.[19] In this process, the original hard drive is subjected to a "checksum" of its contents through a mathematical process that produces a result unique to the specific hard drive in its current state.[20] The forensic image of the hard drive is subjected to the same fingerprinting test, with identical results between the original, which is exposed to the test early in the process, and the forensic image, which is exposed at a later stage, indicating with a high degree of probability that the two are truly identical.[21]

To improve the likelihood that the forensic image and the original hard drive are identical, investigators should pay attention to the transportation and storage of the device. As a general guideline, computer equipment should be stored at normal room temperature and free from magnetic influence such as radio receivers.[22] Also dust, smoke, sand, water, oil, and extreme humidity are harmful to electronic equipment.[23] Moreover, transporting digital evidence

---

[16] See Appendix IV for recommendations based on specific operating systems.
[17] ROBERT MOORE, CYBERCRIME: INVESTIGATING HIGH-TECHNOLOGY COMPUTER CRIME 215 (2010).
[18] *Prosecutor v. Bemba Gombo,* Case No. ICC-01/05-01/08, 19 November 2010 (holding that minor authentication issues does not prohibit admission into evidence, but does affect its final probative value).
[19] The most common tools for this are MD5 and SHA.
[20] Some forensic software, such as EnCase, can perform both the forensic imaging and digital fingerprinting process simultaneously.
[21] SOMMER, *supra* note 8 at 33.
[22] ASSOCIATE CHIEF POLICE OFFICERS, *supra* note 3 at 12.
[23] Id.

in the trunk of a police car is not recommended because of high temperatures and close proximity to other electronic communication equipment.[24]

C. Conclusion

In all cases, investigators should exercise diligence, carefully log their investigative actions, and document how the device is connected to other equipment. The principal investigation should be performed on a forensic copy of the device, rather than the original. Furthermore, every step of the forensic analysis conducted by the investigator should be capable of replication.

III. Evidentiary Protocols for Digital Evidence Not Recovered from a Device

Investigators sometimes obtain evidence that is divorced from a device or its creator. This may include a video emailed to an investigator or stored upon some publicly available internet service.

Typically, the device that captured the evidence, i.e. the hard drive or camera, does not accompany it, and in some situations the evidence may be sent anonymously, thus creating concern over its origins. With the increase in access to cameras and other recording devices, this type of evidence can be extremely useful in linking suspects to crimes perpetrated on large groups or in public view.[25]

As opposed to the previous section, evidence of this nature has few acquisition procedures because, by definition, it has already been either acquired by investigators or is in the public realm.[26] Thus, this section switches focus to techniques that prove that the proffered "divorced" evidence is what it purports to show, and thus authenticated.[27] Each individual case is unique and no universal practices can be applied to authenticating divorced evidence. However, an understanding of traditional approaches to authentication, coupled with the creativity to go beyond those approaches when untraditional situations present themselves, will increase the likelihood that valuable divorced evidence will be usable.

This section provides a non-exhaustive list of useful authentication techniques for divorced evidence, followed by a case study in which an investigation attempted to authenticate a video brought into the public realm through private submission to a news agency.

---

[24] ROBERT MOORE, CYBERCRIME: INVESTIGATING HIGH-TECHNOLOGY COMPUTER CRIME 223 (2010).
[25] *See* Prosecutor v. Karemera, et al. Case No. IT-98-44-T, Judgment, ¶ 169-173, 205 (Int'l Crim. Trib. for Rwanda Feb. 2, 2012)(Video evidence of rally and transcript of radio broadcast authenticated the date of the video and proved that the accused was in attendance); Prosecutor v. Bagosora, Case No. IT-98-41-T, Trial Judgment and Appeals Judgment, ¶ 2029-2031, 460 (Int'l Crim. Trib. for Rwanda Dec. 8, 2008; Dec. 14, 2011)(Video footage and transcript led the Court to conclude that the accused was acting as Minister of Defense and exercised control over the army).
[26] If the evidence is in the public realm, i.e. YouTube, then see section IV (a) for discussion on acquisition.
[27] *See Prosecutor v. Popovic*, et al., Case No. IT-05-88-T, Decision on Admissibility of Intercepted Communications, ¶ 4, 22, 26, 33-35 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 7, 2007)

A. General Authentication Techniques

Prosecutors and investigators often employ general techniques that are applicable to a wide variety of evidence when authenticating divorced evidence. These techniques include use of witness testimony, internal factors such as metadata, and comparison with other independently authenticated evidence.

If the divorced evidence involves personal communication, courts typically prefer it be introduced through testimony of an individual who was a party to the communication.[28] This method affords the defendant an opportunity to cross-examine. If the witness is not available to deliver in-person testimony, then a written statement can still be beneficial for authentication.[29] For divorced evidence, this technique typically requires the investigator to trace back the origins of the evidence until someone can be ascertained who is knowledgeable of its contents or creation. For instance, if the evidence is a YouTube video, a request can be made to YouTube to identify the information of the subscriber who uploaded it.[30]

Additionally, divorced evidence's metadata may be used to assist in its authentication.[31] The use of metadata is helpful in many ways, but in the authentication context it is most helpful in tracing the evidence's origins to a party who can testify to its accuracy.

Lastly, if divorced evidence is similar enough to other independently authenticated evidence, courts may determine that the divorced evidence is also authenticated based on its similarities.[32]

B. Sri Lanka Case Study[33]

Often authentication is not suited for divorced evidence; therefore, an investigator must use unconventional methods. Authentication scenarios requiring creative maneuvering vary dramatically, and thus, advisable techniques must adapt. The following case study describes one such situation that called for creative approaches to authentication.

---

[28] US DEPARTMENT OF JUSTICE, OBTAINING AND ADMITTING ELECTRONIC EVIDENCE 58 (2011) *available at,* http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf

[29] *Prosecutor v. Dordevic,* Decision on Prosecution's Oral Motion for Admission of Evidence Tendered Through Witness Philip Coo, Case No. IT-05-87/1-T, (Int'l Crim. Trib. for the Former Yugoslavia Oct. 1, 2009) (Holding that it is desirable that digital documents be submitted into evidence via oral testimony, but not required because courts discretion will take this into account when determining probative value).

[30] For details on how to submit such a request see section IV (c).

[31] *Lorraine v. Markel*, 241 F.R.D. 534, 560 (D. Md. 2007) (stating that metadata is a useful tool in authenticating digital evidence).

[32] *See United States v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (holding that email exchanges where authenticated based on their similarity to other previously authenticated emails between the same individuals).

[33] This section is predominantly compiled from, *Deeming Sri Lanka Execution Video Authentic, UN Expert Calls for War Crimes Probe,* UN News Centre, January 7, 2010, http://www.un.org/apps/news/story.asp?NewsID=33423

In August of 2009, during the Sri Lankan army's battle against the Liberation Tigers of Tamil Eelam, video footage purporting to show the execution of prisoners became public through private submission to a news agency.[34] No witnesses were willing to verify the video, nor was there any ancillary evidence to corroborate the video's authenticity. Furthermore, the Sri Lankan Government denied the allegations and labeled the video unreliable.[35]

Philip Alston, the UN special rapporteur on extrajudicial, summary or arbitrary executions, suspected that the video had evidentiary value and therefore sought to determine whether the video was authentic. Additionally, he set out to determine the video's reliability, i.e., that it depicted what it purported to show.

To prove that the video was authentic, Alston sent the footage to a digital editing forensic expert. The expert used software[36] to stabilize and enlarge vital parts of the footage. He concluded that there were no breaks in the film's continuity, indicating that the footage had not been edited or manipulated.

Subsequently, Alston sent the stabilized and enlarged footage to two other experts, a ballistic expert and a forensic pathologist. The ballistic expert sought to determine whether the guns and bullets shot during the video were real. He concluded that the weapons in the video were AK-47s and thus conducted experiments by shooting live and fake AK-47 ammunition. After comparing the tapes with the original video, he concluded that the recoil, the movement of the weapon and shooter, and the gasses emitted from the muzzle were consistent with the firing of live ammunition rather than blanks. The forensic pathologist analyzed the victims' body reactions and blood splatter from the video and determined that both were consistent with "what would be expected" in a close range shooting.[37]

While none of the experts' findings independently proves beyond all doubt that the video is authentic, working in conjunction, they serve as compelling evidence of the video's authenticity. Upon publishing these findings, the international community pressed the Sri Lankan Government to address the situation. In addition, Christof Heyns, a U.N. special rapporteur, stated at a press conference that the case should go to the next level of international investigation.[38] The results of the official investigation are pending.

The case study's methods shed sufficient light upon the accuracy of the video to warrant an official investigation. If resources permit, then similar techniques should be employed to aid in the authentication for other divorced evidence. Furthermore, the investigation's reliance upon

---

[34] Video can be viewed at http://www.liveleak.com/view?i=0a1_1311145191

[35] Office of the High Commissioner for Human Rights, United Nations, *UN Expert Concludes that Sri Lankan Video is Authentic, Calls for an Independent War Crimes Investigation*, (Jan. 7, 2010), http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=9706&LangID=E.

[36] The exact software used was "Cognitech"

[37] Office of the High Commissioner, *supra* note 35

[38] United Nations News Centre, United Nations, *Sri Lanka: UN Experts Calls on Government to Probe Executions Captured on Video*, (May 31, 2011), http://www.un.org/apps/news/story.asp?NewsID=38564#.UkyDJLyTaFM.

a wide array of experts suggests that it is advantageous for an investigative body such as the OTP to pursue and maintain a large network of diverse experts.

C. Conclusion

For evidence that is recovered independently of a device or from some anonymous source, investigators must proceed on a case-by-case basis. Investigators dealing with divorced evidence may be able to employ traditional authentication techniques, but at times are required to develop creative strategies similar to those depicted in the Sri Lanka case study.

IV. Evidentiary Protocols for Digital Evidence Stored with Service Providers

A. Acquisition and Preservation

Often a private-sector provider of communications or other services holds relevant information to an investigation. When seeking this data, U.S. law enforcement may make a direct request to a service provider to acquire user data. International law enforcement must "domesticate" requests through either a Mutual Legal Assistance Treaty (MLAT) process or through "letters rogatory".[39] Furthermore, international law enforcement may be able to use the Joint Investigation Team ("JIT") process. These are discussed below in section IV(D).

Major service providers publish guides for investigators on how to request data,[40] but as a first matter, it is important to identify the correct service provider to contact. This can be confusing, because even the unsophisticated can mask their IP address or disguise the provenance of an email.

Investigators often begin an inquiry by examining available IP addresses of suspects. Investigators can run certain commands to try to reverse-trace the owner of an IP address. Similarly, email headers can be carefully inspected to determine its route and origin.

In the United States, the Stored Communications Act ("SCA") regulates access to stored electronic records, and this law limits government requests for user data. The SCA is a complex statute and this discussion aims to introduce the main contours of the Act. The SCA is section II of the Electronic Communications Privacy Act ("ECPA") and is codified at 18 U.S.C. 121 §§ 2701-2712. It addresses voluntary and compelled disclosure of stored wire and electronic communications.[41] Furthermore, the SCA is silent on foreign law enforcement, but it suggests that any domestic law enforcement personnel can trigger a request.[42]

---

[39] Letters rogatory are the "customary method of obtaining judicial assistance from abroad in the absence of a treaty or executive agreement." http://travel.state.gov/law/judicial/judicial_683.html

[40] Apps. I-V.

[41] Stored Communications Act, 18 U.S.C. 121 §§ 2701-2712 (1986).

[42] United States Department of Labor, *Wage and Hour Division*, http://www.dol.gov/whd/regs/compliance/web/SCA_FAQ.htm, (last visited Oct. 10, 2013) (Furthermore, as discussed in *Digital Evidence and the American Servicemembers' Protection Act*, ASPA does not appear to directly apply to private entities).

The status of the service provider is a key determinant of legal protection for user data. If the service provider is a non-public provider, then it is exempt from many SCA obligations and therefore can voluntarily disclose non-content and content data to any person for any reason. If the service provider serves the public, then it is subject to SCA and must comply with its rules generally prohibiting disclosure of content. To determine the classification of a service provider as public or non-public, a prosecutor should ask whether the service provider affords service to the community at large.[43] A company that administers email only for its employees is most likely a private provider; whereas Google, Yahoo, or Microsoft mail are public providers.

There are two types of data categories: non-content and content data. Non-content data includes subscriber and traffic data; subscriber data[44] focuses on who owns the account whereas traffic data[45] focuses on who sent or received an email. Content data includes the actual substance of an email or telephone call such as subject lines or text in the body of an email. As a general framework, subscriber data requires a subpoena that shows the request is relevant to an ongoing investigation; traffic non-content data requires a 2703(d) order which states "specific and articulable facts" linking the data request to an ongoing investigation; and content data such as email content requires a 2703(c)(1) warrant.[46]

Importantly, a preservation request can be made under 2703(f) pending the court order.[47] For a 2703(f) request, a government entity need only send a fax requesting the service provider to preserve all data in relation to the investigation.

Lastly, if a statutory exception is applicable, then public service providers may voluntarily disclose non-content and content data to the government.[48] For example, if exigent circumstances exist such as a kidnapping, then the government's request will fall within the statutory exemption.[49]

B. Authentication and Chain of Custody

Authentication refers to a legal concept that promotes the integrity of the trial process by ensuring tendered evidence establishes what it is offered to prove.[50] To ensure chain of custody

---

[43] US DEPARTMENT OF JUSTICE, EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 135

[44] Subscriber data: the name and address associated with the account; usernames or screen names; session times and duration; IP addresses; means and source of payment; local and long distance telephone toll billing records; telephone number and type of service provided; and a temporarily assigned network address

[45] Traffic data: Data that is not basic subscriber information or content specific. Some examples include log files, IP logs, and identities of e-mail correspondents.

[46] Stored Communications Act, 18 U.S.C. 121 §§ 2702-2703

[47] Id. at 18 U.S.C. 121 §§ 2703(f)

[48] Id.

[49] Stored Communications Act, 18 U.S.C. 121 §§ 2702(5) (1986).

[50] *See* Prosecutor v. Popovic, et al., Case No. IT-05-88-T, Decision on Admissibility of Intercepted Communications in Trial Chamber II, ¶ 4, 22, 26, 33-35 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 7, 2007).

and thus the admissibility of the service provider data, the recipient of the data should date the creation of the document, write the name of the client or individual being served, describe the evidence being held, describe the reason for the transfer from point A to point B, complete a list of each person who had physical control over the evidence, and provide appropriate space for individuals to sign when they receive and release the evidence.[51]

C. Procedure on How to Request Service Provider Data [52]

Some major service providers such as Google and Facebook have corporate forms that require all data requests to be executed in the U.S. To ensure investigators do not duplicate efforts and to assist in later stages of the legal process, investigators may consider completing a data acquisition request form for internal planning of the request from the service provider.[53] The request form should identify the evidence being sought, methodological information, the date and time of the acquisition, the individual who collected the data whether it was from a physical device or divorced from a device, the location, and any other reasonable information.[54] Furthermore, many service providers publish a guide for law enforcement investigators with forms for data requests and specific information about procedures. These guides can be obtained by contacting the specific service provider's legal office, searching online, or looking at the Electronic Frontier Foundation's page that stores these documents.[55] Comcast is one of many service providers that provide step-by-step data acquisition guidelines as outlined below.

First, the requestor should verify that the IP address or e-mail address is registered to the service provider by using the reverse-trace mechanism. Second, the requestor should determine whether the data sought is subscriber, traffic, or content data and therefore whether it implicates a subpoena, 2703(d) order, or a 2703(c)(1) warrant respectively. Third, the requestors' inquiry should include the IP address, email address, street address, phone number and all other pertinent information that would allow the service provider to adequately respond. Fourth, the requestor should include the date and time of all incidents including seconds and time zone, i.e. 12 December 2007 @ 06:13:21 EST. Requestors should caution time synchronization stamps because if preserved inaccurately, then issues arise.[56] Fifth, the requestor should ensure that the required certifications and all applicable substantive and procedural requirements under the particular statutes or regulation authorizing the request have been satisfied. Sixth, the requestor should ensure that there is a complete explanation of the nature and circumstances of any potential serious injury or death to justify an emergency disclosure. Lastly, the requestor should ensure that all of the contact information is correct.

---

[51] Erik Laykin, INVESTIGATIVE COMPUTER FORENSICS 76-69, 83-85 (2013).
[52] COMCAST, LAW ENFORCEMENT GUIDE, http://cryptome.org/isp-spy/comcast-spy.pdf
[53] Erik Laykin, INVESTIGATIVE COMPUTER FORENSICS (2013).
[54] Erik Laykin, INVESTIGATIVE COMPUTER FORENSICS (2013).
[55] Electronic Frontier Foundation, https://www.eff.org
[56] Interview with Chris Hoofnagle, Director, Information Privacy Programs, Berkeley Center for Law & Technology (Oct. 1, 2013).

D. Mutual Legal Assistance Treaties and Joint Investigation Teams

Mutual Legal Assistance Treaties ("MLATs") and letters rogatory allow international evidence exchanges in criminal procedures.[57] The MLAT process is initiated when a treaty facilitating the evidence exchange exists and the letters rogatory process is used when a treaty does not exist to facilitate the exchange between courts. MLATs are negotiated by the Department of State in cooperation with the Department of Justice.

Google is one service provider that specifies a MLAT framework as well as other diplomatic arrangements to assist foreign entities in their data requests.[58] Google states that non-U.S. agencies can work through the U.S. Department of Justice to gather evidence for legitimate investigations. Furthermore if United States law is implicated in the investigation, then "a U.S. agency may open its own investigation and provide non-U.S. investigators with evidence gathered." Google may provide data on a voluntary basis if the request is consistent with international norms, U.S. law, and the requesting country's law. Given that an international agency goes through a diplomatic process, like MLAT, Google will divulge the same information to a non-U.S. agency, as it would produce if the request originated directly from a U.S. agency. The MLAT process takes significantly more time than that experienced by domestic law enforcement requesting data through the SCA.

Joint Investigation Teams ("JITs") are a response to the 21st century criminal landscape, which consists of highly mobile groups engaged in illegal activity across borders.[59] This trend demands strengthened transnational cooperation between competent authorities.[60] A JIT is an investigation team established for a specified time period, based on an agreement between two or more European Union ("E.U.") member states and/or competent authorities. If all parties are in agreement, then non-E.U. members may participate in a JIT.[61]

V. Conclusion

This brief paper has set forth strategies to acquire and authenticate digital evidence in a forensically valid manner. Careful cyberinvestigations can strengthen the prosecutions' case as well as provide linkage evidence connecting the accused to the alleged crime. Digital evidence acquisition is fundamental in all investigations within a modern law enforcement environment.

---

[57] U.S. DEPARTMENT OF STATE, BUREAU OF INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT AFFAIRS, INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT (Mar. 7, 2012)(It is unclear whether and how the OTP can use the MLAT or letters rogatory processes. Furthermore, it is ambiguous whether parties to the Rome Statute should initiate the MLAT or letters rogatory processes).

[58] GOOGLE, TRANSPARENCY REPORT, n.d., *available at* http://www.google.com/transparencyreport/userdatarequests/legalprocess/#how_does_google_respond

[59] EUROPEAN COMMISSION: JOINT INVESTIGATION TEAMS, *available at* http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/jit/index_en.htm

[60] *Id*. (It is unclear whether "authorities" means states or may include international criminal tribunals.)

[61] EUROPOL, JOINT INVESTIGATION TEAMS, 2013, *available at* https://www.europol.europa.eu/content/page/joint-investigation-teams-989

The collection of digital evidence is the "rule rather than the exception" in current investigations.[62]

Two key themes dominate each procedure: First, the goal of acquisition is to obtain an exact replica of the data to ensure validity and thus the highest probative value. Second, authenticity is critical and is attainable through corroboration or other means. This paper addresses data that is already in the possession of the OTP. Therefore, further points of discussion are warranted.

- What investments in training and equipment are necessary to enhance evidence gathering in a forensically valid way as well as increase the probative value of the evidence?

- Given the burdens of the MLAT and letters rogatory processes, should the ICC seek U.S. provider data on European servers or the JIT process?

[62] INTERNATIONAL CRIMINAL COURT, DIGITAL EVIDENCE REPORT, Oct. 2013

VI. Appendices I-VI

I. Sample Preservation Request Letter
II. Sample Language for Subpoenas, 2703(d) Court Orders, and Search Warrants
III. Sample Consent to Search Form
IV. List of Operating System and Preferred Methods
V. Electronic Frontier Foundation Law Enforcement Guide Overview

Appendix I: Sample Preservation Request Letter[63]

This letter serves as a formal request for the preservation of records and other evidence pursuant to 18 U.S.C. § 2703(f) pending further legal process. For the Yahoo! subscriber ID [*INSERT ID, email address, Group name, Flickr NSID, Flickr URL, or Profile URL*], you are hereby requested to preserve, for a period of 90 days, the records described below currently in your possession.

This request applies only retrospectively. It does not in any way obligate Yahoo! to capture and preserve new information that arises after the date of this request. This preservation request specifically applies to all records and other evidence relating to the subscriber(s), customer(s), account holder(s), or other entity(ies) associated with the subscriber(s) identified above, including, without limitation, [*include as may be relevant*]:

- Subscriber names, user names, screen names, or other identities;
- Mailing addresses, residential addresses, business addresses, email addresses, telephone numbers, and other contact information;
- Billing records;
- Information about length of service and the types of services the subscriber(s) or customer(s) used;
- Any other identifying information, whether such records are in electronic or other form;
- Connection logs and records of user activity for the subscriber(s) identified above, including log-in history and records identifying sent and received communications;
- All communications stored in the account(s) of the subscriber(s) identified above; and
- All files that are controlled by user accounts associated with the subscriber(s) identified above. At this time we are expecting to obtain formal legal process within 90 days. We acknowledge that if we do not serve legal process upon you in the next 90 days and do not request a 90-day extension, the preserved information may no longer be available.

[63] YAHOO!, COMPLIANCE GUIDE FOR LAW ENFORCEMENT 14, http://cryptome.org/isp-spy/yahoo-spy.pdf

Appendix II: Sample Language for Subpoenas, 2703(d) Court Orders, and Search Warrants[64]

Sample Subpoena Wording for Identification of a Yahoo! User

Any and all records regarding the identification of a user with the Yahoo! ID "_____" or Yahoo! email account "_____," to include name and address; Yahoo! email address; alternate email address; IP address and date and time of registration; account status; and log-in IP addresses associated with session times and dates.

Note: If Credit card numbers are sought, please identify any Yahoo! premium service used by the subscriber, if known, and insert: "credit card numbers used by the Yahoo! user to pay for Yahoo! premium services [or the name of the specific Yahoo! premium service used]."

Sample Subpoena Wording for Information About a Yahoo! Group and its Moderators

For the Yahoo! Group known as _____, email addresses for all moderators and members of the Group, the date the Group was created, the Group/List ID, and Group description.

Any and all records regarding the identification of the owners and/or moderators of the Yahoo! Group listed above, to include name and address; Yahoo! email address; alternate email address; IP address and date and time of registration; account status; and log-in IP addresses associated with session times and dates.

Sample Search Warrant Wording for Information Related to a Yahoo ID

Any and all information for Yahoo! ID "_____" or Yahoo! email account "_____," to include name and address; Yahoo! email address; alternate email address; IP address and date and time of registration; account status; and log-in IP addresses associated with session times and dates.
(If information related to email content is sought, add)

For the subscriber identified in Paragraph A above, the contents of any and all emails stored in the subscriber's Yahoo! account. [NOTE: Email content stored in domain-based email accounts hosted on Yahoo! or Flickr email must be requested explicitly.]
(If information is sought related to stored Yahoo! Briefcase files or Flickr photos, add)

Any and all contents of electronic files that the subscriber has stored in the subscriber's Briefcase and/or Flickr account.
(If Friends List information is sought, add)
Any and all Yahoo! IDs listed on the subscriber's Friends list.
(If information related to payments is sought, add)
Any and all methods of payment provided by the subscriber to Yahoo! for any premium services.

[64] YAHOO!, COMPLIANCE GUIDE FOR LAW ENFORCEMENT 15, http://cryptome.org/isp-spy/yahoo-spy.pdf

Sample Search Warrant Wording for Information about a Group and its contents

A. The identity of the moderators and members of the Yahoo! Group known as _____, including the date the Group was created, the Group ID, the dates that members joined the group, and the delivery options for the current members.

B. The current contents of the Files, Photos, Links, and Polls section of the Yahoo! Group known as _____ and the archived message posts, and all records relating to the activities of the Group members, as reflected in the Group Activity Log.

Appendix III: Sample Consent to Search Form[65]

(This request must be accompanied by a subpoena and a cover letter or fax bearing the official seal of the requesting agency)

I, _____ the account holder of the Yahoo! account with Yahoo! ID _____ understand that my account is being sought in connection with an official law enforcement investigation. As part of that investigation, I hereby grant my consent to authorize the following agency: _____, to receive, review, copy, and otherwise obtain access to all information of any kind held by Yahoo! relating to my accounts and any and all accounts that I have linked to the following Yahoo! ID _____, including but not limited to information about my identity, my online activities, and the contents of all electronic files or communications maintained by Yahoo! related to me or my ID.

Pursuant to the consent I hereby request that the following specific information be provided:
_____
In connection with this authority to release information, I do hereby agree to hold harmless and do forever hold harmless Yahoo! for the disclosure of such information and do forever waive on my behalf, and on behalf of my heirs and assigns, any and all claims resulting from Yahoo!'s disclosure of any information related to my account pursuant to this authorization.
The following information should be used by Yahoo! to verify my identity:
Login name/Yahoo! ID Yahoo! email address Alternate email address Birthday (as indicated on this account) Answer to secret question

(Contact Yahoo! Compliance for secret question) City, state, and zip Gender
_____ Yahoo! user's signature
_____ Date

[65] YAHOO!, COMPLIANCE GUIDE FOR LAW ENFORCEMENT 17, http://cryptome.org/isp-spy/yahoo-spy.pdf

Appendix IV: List of Operating System and Preferred Methods

This chart displays the generally recommended shut down method based on the operating system employed by the target device. The list of operating systems is not exhaustive, but instead lists only the popular operating systems investigators are likely to find.[66]

Pull plug From device	**Traditional method via internal commands**
Windows Version 3.11	Windows 2000 Server
Windows 95	All Macintosh operating systems
Windows 98	Linux/Unix
Windows 2000	
Windows XP	

[66] ROBERT MOORE, CYBERCRIME: INVESTIGATING HIGH-TECHNOLOGY COMPUTER CRIME 212-17 (2010).

Appendix V. Electronic Frontier Foundation Law Enforcement Guide Overview
*Extracted from Electronic Frontier Foundation; Full version available at https://www.eff.org/files/EFF_Social_Network_Law_Enforcement_Guides-sprdsht.pdf

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

Date	Facebook 2010
Date, length, link (if available) and other info	May 2010, 5 pages
How does Guide address Legal Process Requirements under Electronic Communications Privacy Act (ECPA)?	"we will provide records as required by law." (p.2)
How does site define and/or distinguish different types of user information	User ID number, email address, date/time account was created, most recent logins, registered mobile number (p. 4) "Expanded Subscriber Content (sometimes referred to as Neoprint)": Contact information, mini-feed, status update history, shares, notes, wall postings, friend listings (include friend IDs), group listings (including group member IDs), future and past events, video listings (p. 4)
What other info is available?	"User photos (sometimes referred to as User Photoprint)": User uploaded photos and photos tagged with user's name, group information, private messages (p. 4)
How does LE Guide address IP and other logs?	• IP logs contain same data as 2008/09 and also include Session Cookie -- HTTP cookie set by user session • Logs are often incomplete, but if available will be provided (p. 4)
How long is data generally retained? How long in reponse to preservation request?	90 days, but an extension can be made if necessary. "By default we will return data no older than 90 days prior to the date we receive the request." (p. 2)
Is content that has been changed or deleted by user (including private messages) still available?	If messages are retained by user, they are available (page 4)
Can law enforcement monitor user account without user knowledge?	Will normally disable account unless law enforcement clearly specify that doing so will hurt investigation (page 2)

Does site have exception for emergency disclosure?	Can provide upon answering 3 questions:Describe emergency? Provide ID of users involved? Provide location of evidence? (p. 5)
Does site charge law enforcement fees?	Does not say
What are the requirements to begin preserving records?	Request to preserve from law enforcement, with ID, name of agency, and contact info (p. 3)
Does site address fake accounts created by law enforcement?	Will "always disable accounts that supply false or misleading profile information or attempt to technically or socially circumvent site privacy measures." (p. 2)
Can user consent to data release?	Does not say
How will site deliver data?	Does not say
Other info?	"We are required to disable accounts engaged in illegal activity, even if that activity is brought to our attention through a request for records." (p.5)
Sample forms or sample language?	Emergency Disclosure Form