

Fordham International Law Journal

Volume 41, Issue 2

Article 1

REGINA A. LOUGHRAN MEMORIAL ISSUE

Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials

Lindsay Freeman*

*

Copyright © by the authors. *Fordham International Law Journal* is produced by The Berkeley Electronic Press (bepress). <https://ir.lawnet.fordham.edu/ilj>

ARTICLE

DIGITAL EVIDENCE AND WAR CRIMES PROSECUTIONS:

THE IMPACT OF DIGITAL TECHNOLOGIES ON INTERNATIONAL CRIMINAL INVESTIGATIONS AND TRIALS

*Lindsay Freeman**

ABSTRACT

As technology develops, new tools are continually being introduced that alter the nature and availability of courtroom evidence. The proliferation, connectivity, and capabilities of camera-embedded and internet-enabled mobile devices, which record far more information about people's activities and communications than ever before, are transforming the way criminal investigators and prosecutors collect, evaluate, and present evidence at trial. This is particularly true in international criminal trials, where prosecutors must present a voluminous and varied body of evidence to prove multiple charges related to complex conflicts. It is the prosecutor's job to present evidence in a way that assists the fact-finder in evaluating its significance and understanding how it fits into the greater narrative. Advanced digital devices can now capture far more information about a situation than a witness can perceive, and innovative presentation tools allow lawyers to augment and strengthen the evidence in their cases by adding supplementary data and creating compelling visuals. In cases involving war crimes, crimes against humanity, and genocide, a large quantity and diversity

* JD (University of San Francisco School of Law), BA (Middlebury College); Research Fellow, Human Rights Center, UC Berkeley School of Law; former Assistant Research and Development Officer, Office of the Prosecutor, International Criminal Court. The author thanks Alexa Koenig and Colin Black for their invaluable feedback.

of evidence is necessary to explain the context of the conflict and to prove the requisite elements of crimes and modes of liability. By examining the evidence and presentation techniques used in recent cases before international criminal courts, this article illustrates how war crimes prosecutions are evolving to meet the challenges and advantages of modern times. Part II explains the applicable law and describes how the use of emerging types of evidence in international criminal cases has expanded and been refined over the years. Part III analyzes three exceptional, yet emblematic cases from 2016, which call attention to an important trend that is predictive of the future use of digital evidence in war crimes prosecutions. Part IV discusses cases on the horizon and what these technological developments mean for members of the international justice community.

ABSTRACT.....	283
I. INTRODUCTION.....	285
II. THE PRINCIPLES OF EVIDENCE IN INTERNATIONAL CRIMINAL LAW.....	291
A. The evolution of evidence in international criminal trials.....	298
III. RECENT INTERNATIONAL CRIMINAL CASES INVOLVING DIGITAL EVIDENCE.....	307
A. Evidence of a conspiracy to commit terrorist acts.....	307
1. Case Background.....	308
2. Digital Explosives Evidence.....	310
3. Telecommunications Evidence.....	312
B. Evidence of crimes against cultural heritage.....	314
1. Case Background.....	315
2. Open Source Evidence.....	316
3. Interactive Digital Platform.....	319
C. Evidence of offenses against the administration of justice.....	320
1. Brief overview of the Main Case.....	321
2. Case Background.....	322
3. Digital Financial Evidence.....	323
4. Telecommunications and Intercept Evidence.....	326
5. Digital Communications Evidence.....	327

IV. THE FUTURE OF EVIDENCE IN WAR CRIMES
 PROSECUTIONS329
 A. Considerations for international criminal law
 practitioners.....333
 V. CONCLUSION335

I. INTRODUCTION

In 1945, the four Allied powers—the United States, the United Kingdom, the Soviet Union and France—convened to establish the first international military tribunal for Nuremberg, and a new category of public international law was born. In the aftermath of World War II, international criminal law was created to deal with mass atrocities in a global forum. These atrocity crimes were later codified into three categories: war crimes, crimes against humanity, and genocide.¹ Around the same time, a movement was underway in national jurisdictions to increase the use of scientific evidence to solve crimes and achieve justice.²

Due to the nature of the cases at Nuremberg or, more precisely, the nature of the Nazi perpetrators as methodical record-keepers, the Chief Prosecutor moved away from a reliance primarily on witnesses to focus more on documentary evidence.³ The use of science and technology to efficiently and systematically wipe out the Jewish population was part of the modus operandi of the Nazis. They used early IBM computers to track lists of names.⁴ The very instruments the Nazis used to facilitate their crimes, along with other evidence, provided a record of information that would later be used to prove their guilt. In addition to the large volume of official government and

1. The Rome Statute is the treaty that established the International Criminal Court. It was adopted in 1998 and entered into force in 2002. Article 5 of the Statute lists the crimes within the jurisdiction of the Court, which includes the crime of genocide, crimes against humanity, and war crimes. *See* Rome Statute of the International Criminal Court art. 5, July 17, 1998, 2187 U.N.T.S. 90. Also listed is the crime of aggression, but that crime has not yet been adopted and therefore will not be discussed in this article. *See id.*

2. *See generally* Joseph Peterson & Ira Sommers, *The Role and Impact of Forensic Evidence in the Criminal Justice Process*, NATIONAL INSTITUTE OF JUSTICE (Sept. 2010), <https://www.ncjrs.gov/pdffiles1/nij/grants/231977.pdf> [https://perma.cc/GR99-NEMV] (archived Dec. 29, 2017).

3. Patricia M. Wald, *Dealing with Witnesses in War Crime Trials: Lessons from the Yugoslav Tribunal*, 5 YALE HUM. RTS. & DEV. L.J. 217 (2002).

4. *See generally* EDWIN BLACK, *IBM AND THE HOLOCAUST: THE STRATEGIC ALLIANCE BETWEEN NAZI GERMANY AND AMERICA’S MOST POWERFUL CORPORATION* (2001).

military records available in these cases, stacks of photographs and hours of film taken by war correspondents were also presented at trial.⁵ War photography went from a tool for government decision-makers and journalists to an important source of evidence in courts of law.

The Nuremberg trials laid the groundwork for future international criminal cases, but it was not until nearly fifty years later that the next generation of international criminal tribunals emerged with the creation of ad hoc courts for conflicts in the Balkans and Rwanda in 1993 and 1994, respectively. These new international courts, the International Criminal Tribunal for the Former Yugoslavia (“ICTY”) and the International Criminal Tribunal for Rwanda (“ICTR”), were established through United Nations Security Council Resolutions.⁶ During this period, the use of more advanced methods of forensic science, such as DNA profiling, facilitated by the advent of super computers with the capacity to analyze large data sets, became widespread within criminal justice systems.⁷ As forensic science developed as an increasingly effective tool for law enforcement, military forces were embracing the use of satellites, unmanned aerial vehicles and other cutting-edge remote sensing technologies for intelligence gathering and combat strategy.⁸ As the ICTY and ICTR cases progressed over two decades, forensic anthropology techniques became more precise and satellite imagery resolution got sharper. To identify mass graves and to provide before and after comparisons of towns destroyed by aerial bombardments, ICTY prosecutors introduced satellite imagery procured from the United States military as evidence against the perpetrators of the Srebrenica massacre.⁹ Satellite imagery went from an instrument of

5. See generally ERIC STOVER ET AL., *HIDING IN PLAIN SIGHT: THE PURSUIT OF WAR CRIMINALS FROM NUREMBERG TO THE WAR ON TERROR* (2016). See also History Documentary Films, *History Channel documentary Nuremberg Trials World War II Documentary*, YOUTUBE (Jan. 5, 2016), <https://www.youtube.com/watch?v=K5lslg1gjAds>.

6. See S.C. Res. 827, ¶ 2 (May 25, 1993) (establishing the International Criminal Tribunal for the former Yugoslavia); S.C. Res. 955 ¶ 21 (Nov. 8, 1994) (establishing the International Criminal Tribunal for Rwanda).

7. Lisa Calandro et al., *Evolution of DNA Evidence for Crime Solving – A Judicial and Legislative History*, FORENSIC MAGAZINE (Jan. 6, 2005).

8. Ben Yunmo Wang et al., *Problems from Hell, Solution in the Heavens?: Identifying Obstacles and Opportunities for Employing Geospatial Technologies to Document and Mitigate Mass Atrocities*, 2 STABILITY: INT’L J. OF SEC. & DEV. 2-3 (2013).

9. INT’L BAR ASS’N (IBA) CRIM. COURT PROGRAMME, EVIDENCE MATTERS IN ICC TRIALS 24-25 (Aug. 2016).

military strategists and private corporations to an important resource for war crimes investigators and prosecutors.

The cases at the ICTY and ICTR also depended to a large extent on the testimony of expert witnesses, including scientists, analysts, sociologists, psychologists, and historians. The conflicts in the former Yugoslavia and in Rwanda were incredibly complex, both stemming from long histories of feuding local populations and political turmoil. Unlike Nuremberg, where all the parties involved (and in a sense, the whole world) had an intimate knowledge of the conflict and its background, the international community (and the international judges and lawyers who arrived at the tribunals) did not necessarily come with a deep cultural understanding of the people and location in which these conflicts took place. As a result, experts who could provide proper background information and context played an important role in the proceedings. Social experts were used to provide background on the historical, cultural, and political context of the conflict; legal experts were used to explain intricate and specialized areas of the law; and forensic experts were used to describe the analytical and scientific methods employed in the field.¹⁰

A decade later came the third wave in the evolution of international criminal justice with the establishment of the first permanent international criminal tribunal, the International Criminal Court (“ICC”) in The Hague, Netherlands in 2002. At about the same time a handful of hybrid or ‘internationalized’ tribunals were set up to deal with specific situations in Sierra Leone (2002), Cambodia (2003), and Lebanon (2007).¹¹ The birth of these courts coincided with the popularization of the internet, particularly social media and

10. See generally Doris Buss, *Expert Witnesses and International War Crimes Trials: Making Sense of Large-Scale Violence in Rwanda*, in NARRATIVES OF JUSTICE IN AND OUT OF THE COURTROOM (Dubravka Zarkov & Marlies Glasius eds., 2014); Patricia M. Wald, *The International Criminal Tribunal for the Former Yugoslavia Comes of Age: Some Observations on Day-To-Day Dilemmas of an International Court*, 5 WASH. U. J.L. & POL’Y 87, 101 & 108. (2001).

11. See UN Security Council, *Statute of the Special Court for Sierra Leone*, 16 January 2002 establishing the Special Court for Sierra Leone (hereinafter “SCSL”); Law on the Establishment of the Extraordinary Chambers in the Courts of Cambodia for the Prosecution of Crimes Committed During the Period of Democratic Kampuchea (2001) (Cambodia), as amended by NS/RKM/1004/006 (Oct. 27, 2004) (unofficial translation) establishing the Extraordinary Chambers in the Courts of Cambodia (hereinafter “ECCC”); Statute of the Special Tribunal for Lebanon, S/RES/1757 (2007), establishing the Special Tribunal for Lebanon (hereinafter “STL”); see also CRYER, R. ET AL., AN INTRODUCTION TO INTERNATIONAL CRIMINAL LAW AND PROCEDURE 181-90 (3d ed. 2014).

other interactive web services, the proliferation of cellular phones and other mobile devices outfitted with cameras and global positioning systems, and the rise and spread of drone technologies.¹² In the span of only a couple decades, technologies that were once held solely in the domain of governments and militaries became more affordable and, as a result, more accessible to the public.¹³ With the proliferation of these technologies came an overabundance of data. Information that once would have disappeared into the ether was recorded and stored in our digital history.

While the early ICC cases relied heavily on witness testimony, which proved problematic in ways that will be discussed later in this article, there was some limited use of alternative types of evidence. The ICC's initial investigations began in the Democratic Republic of Congo and Uganda. Video evidence was introduced in the first trial, *Prosecutor v. Thomas Lubanga Dyilo* ("Lubanga"), for crimes committed during the 2002-2003 conflict in the Ituri Region of the Democratic Republic of Congo.¹⁴ In the second trial arising from the same conflict, *Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui* ("Katanga and Ngudjolo"), the Prosecution made a belated attempt to gather forensic evidence, although much of it was excluded due to its late disclosure.¹⁵ In Uganda, investigators collected audio-recordings of radio intercepts between members of the Lord's Resistance Army taken by national authorities. Years later, in anticipation of the first trial resulting from the Uganda investigation, *Prosecutor v. Dominic Ongwen* ("Ongwen"), which is currently underway as of this writing, the Prosecution performed forensic

12. In 2002 the first drone was used; in 2004 the term Web 2.0 was coined to describe the emergence of new social networking platforms in the early 2000s. See Digital Trends Staff, *The history of social networking*, DIGITAL TRENDS (May 14, 2016), <https://www.digitaltrends.com/features/the-history-of-social-networking/> [<https://perma.cc/NQ45-4UL8>] (archived Jan. 17, 2018).

13. For example, portable GPS devices, drones, infrared cameras, telephoto lenses, and satellite phones are all items ordinary citizens can purchase over the internet. See Wang et al., *supra* note 8.

14. *Prosecutor v. Lubanga*, Case No. ICC-01/04-01/06-2842, ¶ 107, https://www.icc-cpi.int/CourtRecords/CR2012_03942.PDF [<https://perma.cc/7ZNJ-S4NP>] (last visited Dec. 29, 2017).

15. See generally *Prosecutor v. Katanga*, Case No. ICC-01/04-01/07-1515, Decision on the disclosure of evidence material relating to the Prosecutor's site visit to Bogoro on 28, 29 and 31 March 2009 (Oct. 7, 2009) [hereinafter *Katanga*, Decision on the disclosure of evidentiary material], https://www.icc-cpi.int/CourtRecords/CR2009_07212.PDF [<https://perma.cc/TP5M-YYEP>] (archived Dec. 29, 2017).

analysis such as audio-enhancement and voice-identification on those recordings.¹⁶

However, it was not until after the Trial Chambers issued a few critical decisions and admonishments regarding the investigations conducted by the Office of the Prosecutor (“OTP”), citing weaknesses due to the overreliance on witnesses and under-reliance on other forms of evidence, that the OTP developed its internal capacity for forensic investigations.¹⁷ By 2011, the OTP was significantly better equipped to deal with cases in Kenya, Cote d’Ivoire, and Libya, where mobile phone use was widespread.¹⁸ Many of the videos shown during confirmation hearings and trials in those cases were taken with mobile digital devices such as cell phone cameras. In more recent cases, comprehensive satellite imagery collected from humanitarian organizations, private companies, and open source platforms has aided investigations in Sudan and Mali, and analysts have extracted useful leads in a number of other current investigations from websites such as Facebook and YouTube.¹⁹ Consequently, the more recent cases at the ICC have been significantly stronger from an evidentiary standpoint than the initial witness-focused cases advanced by the Prosecution. In the last few years, telecommunications data, such as call data records, cell site maps, and telephone intercepts, as well as

16. Prosecutor v. Ongwen, Case No. ICC-02/04-01/15-533, Prosecutor’s Pre-Trial Brief, ¶ 80 (Sept. 6, 2016), https://www.icc-cpi.int/CourtRecords/CR2016_06511.PDF [<https://perma.cc/WT4G-4Z5B>] (archived Dec. 29, 2017).

17. See generally Prosecutor v. Ngudjolo, Case No. ICC-01/04-02/12-3-tENG, Judgment pursuant to article 74 of the Statute (Dec. 18, 2012) [hereinafter *Ngudjolo*, Judgment], https://www.icc-cpi.int/CourtRecords/CR2013_02993.PDF [<https://perma.cc/3AQJ-SM6J>] (archived Dec. 29, 2017) (acquitting on all charges); Prosecutor v. Mbarushimana, Case No. ICC-01/04-01/10-465-Red, Decision on the confirmation of charges (Dec. 16, 2011), https://www.icc-cpi.int/CourtRecords/CR2011_22538.PDF [<https://perma.cc/B4DJ-85FB>] (archived Dec. 29, 2017) (declining to confirm the charges); Prosecutor v. Garda, Case No. ICC-02/05-02/09-243-Red, Public Redacted Version Decision on the Confirmation of Charges (Feb. 8, 2010) [hereinafter *Garda*, Decision on Confirmation of Charges], https://www.icc-cpi.int/CourtRecords/CR2010_00753.PDF [<https://perma.cc/BH3C-8RUB>] (archived Dec. 29, 2017) (declining to confirm the charges).

18. See U.C. BERKELEY SCHOOL OF LAW HUMAN RIGHTS CTR., DIGITAL FINGERPRINTS: USING ELECTRONIC EVIDENCE TO ADVANCE PROSECUTIONS AT THE INTERNATIONAL CRIMINAL COURT 5 (Feb. 2014); see also IBA, EVIDENCE MATTERS IN ICC TRIALS, *supra* note 9.

19. Humanitarian efforts to collect and analyze satellite imagery of atrocities in Darfur, Sudan include the Satellite Sentinel Project, the United States Holocaust Memorial Museum’s “Crisis in Darfur” Project in partnership with Google Earth, and Amnesty International’s “Decode Darfur” Project.

emails, social media posts, and records of financial transactions have all been used to further investigations, corroborate witness testimony, and strengthen prosecutions at the ICC. Digital information from user-generated online content, consumer data from communications service providers, and geolocation data are quickly becoming essential tools of the trade for international criminal investigators.

In order to demonstrate how newer types of digital and technologically derived evidence have been used, this article examines three recent international criminal cases: *The Prosecutor v. Salim Jamil Ayyash, Mustafa Amine Badreddine, Habib Merhi, Hussein Hassan Oneissi and Assad Hassan Sabra* (“*Ayyash et al*”);²⁰ *The Prosecutor v. Ahmad Al Faqi Al Mahdi* (“*Al Mahdi*”);²¹ and *The Prosecutor v. Jean-Pierre Bemba Gombo, Aimé Kilolo Musamba, Jean-Jacques Mangenda Kabongo, Fidèle Babala Wandu and Narcisse Arido* (“*Bemba et al*”).²² All three cases are, in their own way, unique and precedent setting, particularly with regard to the use of digital evidence.²³ In *Ayyash et al*, the defendants are the first before an internationalized tribunal to be charged with the crime of terrorism and are the first in recent history to be tried *in absentia*. In *Al Mahdi*, the accused is the first ICC defendant to be charged with the destruction of cultural heritage as a war crime and the first to plead guilty at the ICC. In *Bemba et al*, the defendants are the first to be charged with offenses against the administration of justice for interfering with witnesses in another ICC trial pursuant to Article 70 of the Rome Statute. In each case, the Prosecution relied on digital evidence in ways not previously seen in international proceedings. These cases illustrate how the types of evidence before international criminal courts are changing. Further, the decisions in these cases will serve as precedent (both persuasive and/or binding, depending on the jurisdiction) and thus contribute to the emerging jurisprudence on digital evidence for future mass atrocity cases.

20. Prosecutor v. Ayyash et al., Case No. STL-11-01, Special Tribunal for Lebanon [Spec. Trib. Leb.], <https://www.stl-tsl.org/en/the-cases/stl-11-01>.

21. Prosecutor v. al Madhi, Case ICC-01/12-01/15, <https://www.icc-cpi.int/mali/al-mahdi> [<https://perma.cc/9Z96-373H>] (last visited Dec. 29, 2017).

22. Prosecutor v. Bemba, Case ICC-01/05-01/13, <https://www.icc-cpi.int/car/bemba> [<https://perma.cc/5VSL-QXRX>] (last visited Dec. 29, 2017).

23. 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 proceedings.” BRIT. INST. OF INT’L AND COMP. L., INTERNATIONAL ELECTRONIC EVIDENCE xxxv (Stephen Mason ed., 2008).

II. THE PRINCIPLES OF EVIDENCE IN INTERNATIONAL CRIMINAL LAW

The law of evidence encompasses the rules and legal principles that govern the proof of facts in legal proceedings. In criminal cases, evidence law is designed to ensure that the rights of witnesses, suspects, and the accused are protected through the following of proper procedures.²⁴ The overriding purpose of evidentiary and procedural rules is to ensure that trials meet fundamental standards of fairness and justice.²⁵ For proceedings before international criminal courts, the applicable rules are derived from the founding instruments, as well as the case law and other relevant sources of international law. There are no uniform rules of procedure and evidence in international criminal law, since the ad hoc and hybrid tribunals have taken varied approaches. However, despite variations among these rules and procedures, certain common principles have emerged. Those common principles were incorporated into the formation of the ICC Rules of Procedure and Evidence, which serve as the main legal reference in this article.²⁶

At the international level, the already complex laws of evidence are further complicated by the differences in approaches to fact-finding and evidence across disparate legal traditions.²⁷ All international and internationalized criminal tribunals have taken, to varying degrees, a hybrid approach to institutional design and the rules of evidence and procedure, pulling features from both common and civil law systems.²⁸ The applicable law may be difficult to ascertain since pertinent rules are scattered throughout multiple

24. See generally Helen Brady, *The System of Evidence in the Statute of the International Criminal Court*, in *ESSAYS ON THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT* 279 (Flavia Lattanzi & William A. Schabas eds., 1999); see also *PRINCIPLES OF EVIDENCE IN INTERNATIONAL CRIMINAL JUSTICE* 231 (Karim A. A. Khan et al. eds., 2010).

25. KATRINA E. ANDERSON ET AL., *THE KHMER ROUGE TRIBUNAL* 82 (John Ciorciari ed., 2006).

26. See generally IBA, *EVIDENCE MATTERS IN ICC TRIALS*, *supra* note 9.

27. Common law is an adversarial system with the judge acting as referee, whereas civil law is an inquisitorial system with the judge acting as an investigator. See generally Geoffrey C. Hazard Jr. & Angelo Dondi, *Responsibilities of Judges and Advocates in Civil and Common Law: Some Lingering Misconceptions Concerning Civil Lawsuits*, 39 *CORNELL INT'L L.J.* 59 (2006).

28. See generally Colin B. Picker, *International Law's Mixed Heritage: A Common/Civil Law Jurisdiction*, 41 *VAND. J. TRANSNAT'L L.* 1083 (2008).

sources.²⁹ Significantly, the founding instruments for international courts tend to lack specificity on the rules of evidence, leaving substantial discretion to the judges. Evidentiary standards in international criminal law are generally more permissive than common law jurisdictions since there are no juries.³⁰ Further, international criminal courts and tribunals have mixed benches (judges from both legal traditions), which makes their decisions difficult to predict.

As a general rule, principles of evidence may be understood to fall into one of three broad categories, “power-based rules,” “rights-based rules,” and “procedural rules.”³¹ “Power-based rules” define the prosecutor’s authority to collect evidence or to request State authorities to collect evidence on their behalf. “Rights-based rules” require the prosecutor to accord certain privileges to suspects and witnesses during interviews and when collecting physical and documentary evidence. “Procedural rules” govern the techniques the prosecutor can use to gather and preserve evidence, such as the need to record interviews or maintain a chain of custody for physical items. International judges have broad discretion on deciding the consequences for violating any one of these rules, but a serious violation of any of these rules could potentially lead to the exclusion of evidence at trial.

In proceedings before the International Criminal Court evidence is vetted in three stages: (1) submission or identification; (2) admission; and (3) determination of weight. All items of evidence will be submitted, which means marked on the record before being officially admitted, unless they are *prima facie* unreliable.³² The Chambers have discretion to decide when they want to make a determination on the admissibility of the evidence – they can do it during trial as the evidence is presented by the parties or wait until

29. Amal Alamuddin, *Collection of Evidence*, in *PRINCIPLES OF EVIDENCE IN INTERNATIONAL CRIMINAL JUSTICE* 232 (Karim A. A. Khan et al. eds., 2010); *see generally* WILLIAM A. SCHABAS, *THE INTERNATIONAL CRIMINAL COURT: A COMMENTARY ON THE ROME STATUTE* (2010).

30. Brady, *The System of Evidence*, *supra* note 24, at 286.

31. Amal Alamuddin, *Collection of Evidence*, in *PRINCIPLES OF EVIDENCE IN INTERNATIONAL CRIMINAL JUSTICE* 231 (Karim A. A. Khan et al. eds., 2010).

32. Prosecutor v. Bemba, Case No. ICC-01/05-01/08-1386 OA 5 OA 6, Judgment on the appeals of Mr Jean-Pierre Bemba Gombo and the Prosecutor against the decision of Trial Chamber III entitled “Decision on the admission into evidence of materials contained in the prosecution’s list of evidence” (May 3, 2011), <https://www.icc-cpi.int/pages/record.aspx?uri=1066048>.

their final judgment.³³ The majority of Chambers have opted for the latter. Thus, when the parties close their cases, they do not know which items of evidence will be admitted and which, if any, will be excluded. Exclusion of evidence is infrequent since international judges have shown a preference to admit an item of evidence, but may nevertheless choose to give it little or no weight. There has, however, in recent years, been a notable increase in the exclusion of evidence, particularly for items of new media that have not been properly sourced.³⁴ While most Chambers choose to rule on admissibility in the final judgment, a few Chambers have made exceptions for certain items of evidence. Such exceptions have occurred when digital evidence is involved and it is central to the Prosecution's case. For example, in *Bemba et al*, despite its decision to wait until the final judgment to rule on admissibility, the Trial Chamber made an exception for items of evidence such as call data records, telephone intercepts by Dutch authorities, and financial records emanating from Western Union, since these newer types of evidence were unprecedented at the ICC.³⁵ Similarly, in *Ayyash et al* at the Special Tribunal for Lebanon, the judges have made multiple interlocutory rulings on the admissibility of telecommunications evidence early on in the proceedings.

33. *Id.* at ¶ 37. "The Trial Chamber has the power to rule or not on relevance or admissibility when evidence is submitted to the Chamber." *Id.* Accordingly, it may decide either (i) to make the ruling on relevance and/or admissibility of the evidence at the time of its submission and defer the determination of its probative value to the end of the trial, or (ii) to defer this ruling to the end of the proceedings, making it 'part of its assessment of the evidence when it is evaluating the guilt or innocence of the accused person.'" *Id.*

34. See, e.g., Prosecutor v. Ayyash, STL-11-01, Decision on the Admissibility of Documents Published on the Wikileaks Website (Spec. Trib. Leb., May 21, 2015) [hereinafter *Ayyash*, Wikileaks Documents Decision], <https://www.stl-tsl.org/en/the-cases/stl-11-01/main/filings/orders-and-decisions/trial-chamber/4031-f1955>; see also Prosecutor v. Bemba, Case No. ICC-01/05-01/08-2299-Red, Decision on the admission into evidence of items deferred in the Chamber's "Decision of the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute" (June 27, 2013), <https://www.icc-cpi.int/pages/record.aspx?uri=1609724> [https://perma.cc/KN2C-Y3QM] (archived Dec. 29, 2017).

35. Prosecutor v. Bemba, Case No. ICC-01/05-01/13-1854, Decision on Requests to Exclude Western Union Documents and other Evidence Pursuant to Article 69(7), (Apr. 29, 2016) [hereinafter *Bemba*, Decision to Exclude Western Union Documents], <https://www.icc-cpi.int/Pages/record.aspx?docNo=ICC-01/05-01/13-1854> [https://perma.cc/WC4G-6RLR] (archived Dec. 29, 2017); Prosecutor v. Bemba, Case No. ICC-01/05-01/13-1855, Decision on Requests to Exclude Dutch Intercepts and Call Data Records (Apr. 29, 2016) [hereinafter *Bemba* Decision on Requests to Exclude Dutch Intercepts], <https://www.icc-cpi.int/Pages/record.aspx?docNo=ICC-01/05-01/13-1855> [https://perma.cc/4MY2-8ZRM] (archived Dec. 29, 2017).

The main rules governing the admissibility of evidence before the ICC are Rule 64 of the Rules and Article 69 of the Statute. In particular, Article 69(4) states, “[t]he Court may rule on the relevance or admissibility of any 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, in accordance with the Rules of Procedure and Evidence.”³⁶ Thus, for any tendered item to be admitted into evidence, it must satisfy a three-part admissibility test. Under this test, the Chamber will examine whether the submitted materials (1) are relevant to the case; (2) have probative value; and (3) are sufficiently relevant and probative to outweigh any prejudicial effect that could be caused by their admission.³⁷

The exclusion of evidence is provided for in Article 69(7) of the Statute, which states that the Chamber must first consider whether the evidence was collected in violation of the Court’s statutory scheme or internationally recognized human rights. If such a violation has occurred, the Chamber must then consider whether this violation “casts substantial doubt on the reliability of the evidence” or whether the admission of the evidence “would be antithetical to and would seriously damage the integrity of the proceedings.”³⁸ While this seems to dictate mandatory exclusion of evidence, in practice the judges have broad discretion on how this provision is applied.³⁹ According to the Pre-Trial Chamber, “the judges have the discretion to seek an appropriate balance between the statute’s fundamental

36. See Rome Statute of the International Criminal Court art. 69(4), July 17, 1998, 2187 U.N.T.S. 90.

37. Prosecutor v. Bemba, Case No. ICC-01/05-01/08-2299-Red, Public Redacted Version of “Decision on the Prosecution’s Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute,” ¶ 7 (Oct. 8, 2012) [hereinafter *Bemba*, Public Redacted Version of Admission of Materials into Evidence] <https://www.icc-cpi.int/Pages/record.aspx?docNo=ICC-01/05-01/08-2012-Red> [https://perma.cc/PCW8-MNFA] (archived Dec. 29, 2017) (citing Prosecutor v. Bemba, First decision on the prosecution and defense requests for the admission of evidence, ¶ 13 (Dec. 15, 2011)).

38. See Rome Statute of the International Criminal Court art. 69(7), July 17, 1998, 2187 U.N.T.S. 90.

39. K.M. PITCHER, JUDICIAL RESPONSES TO PRE-TRIAL PROCEDURAL VIOLATIONS IN INTERNATIONAL CRIMINAL PROCEEDINGS, University of Amsterdam at 543-44 “[Article 69(7) of the ICC Statute] provide[s] for an exclusionary *discretion*, whereby the determination to be made thereunder is a matter of fact and degree, entailing consideration of the particular circumstances of the case”

values in each concrete case.”⁴⁰ The only internationally recognized human right defined in ICC case law to date is the internationally recognized right to privacy.

Evidence can be characterized in a number of ways.⁴¹ However, most evidence law textbooks identify four general categories of evidence: testimonial, documentary, physical, and forensic.⁴² While all evidence, regardless of category, goes through the same three-part test for admissibility, the determination of weight is more nuanced. The Chamber’s assessment of the weight to be attributed to any item of evidence depends on the type of evidence. The Chamber will identify each item of evidence either as direct or indirect, the latter encompassing hearsay evidence.⁴³ Direct evidence provides first-hand information that supports the truth of an assertion.⁴⁴ By contrast, indirect or circumstantial evidence requires an inference to connect the evidence to a conclusion of fact. The Chambers have stated that direct evidence has higher probative value than circumstantial evidence, which is of low probative value, although under the rules of the Court, circumstantial evidence is accepted.⁴⁵

The assessment as to how much weight to give an item of evidence will also vary based on the category of evidence. To assess testimonial evidence, the Court will evaluate the credibility of the witness and the reliability of his or her testimony. When evaluating

40. Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Decision on the Confirmation of Charges, ¶ 84 (Feb. 7, 2007), <https://www.icc-cpi.int/pages/record.aspx?uri=266175>.

41. Evidence may be testimonial, documentary, physical or forensic; scientific, digital or electronic; lay witness or expert; direct, indirect or circumstantial; hearsay; corroborative or conclusive; demonstrative; statistical; character; contextual; incriminating or exculpatory; or crime base or linkage.

42. Some people choose to look at physical and forensic evidence in one category. I have chosen to separate it here.

43. Prosecutor v. Muthaura, Kenyatta and Ali Case No. ICC-01/09-02/11-382-Red, Decision on the confirmation of charges, ¶ 82 (Jan. 23, 2012) [hereinafter *Muthaura et al.*, Decision], https://www.icc-cpi.int/CourtRecords/CR2012_01006.PDF.

44. *Id.* at ¶ 83.

45. “Nothing in the statutory framework prevents the Chamber from relying on circumstantial evidence.” See Prosecutor v. Bemba, Case No. ICC-01/05-01/08-3343, Judgment pursuant to Article 74 of the Statute, ¶ 39 (Mar. 21, 2016) [hereinafter *Bemba*, Judgment], <https://www.icc-cpi.int/Pages/record.aspx?docNo=ICC-01/05-01/08-3343>. Note: This is a slightly different approach than some national jurisdictions. For example, California Jury Instruction states that “Both direct and circumstantial evidence are acceptable types of evidence to prove or disprove the elements of a charge, including intent and mental state and acts necessary to a conviction, and neither is necessarily more reliable than the other. Neither is entitled to any greater weight than the other.” CALIFORNIA CRIMINAL JURY INSTRUCTIONS § 223 (CALCRIM 2017).

the oral testimony of a witness, the Chamber will consider “the entirety of the witness’s account; the manner in which he or she gave evidence; the plausibility of the testimony; and the extent to which it was consistent, including as regards other evidence in the case.”⁴⁶ The Chamber will evaluate the extent and seriousness of the inconsistency and its impact on the overall reliability of the witness.⁴⁷ When assessing the testimony of expert witnesses, the Chamber considers factors such as “the established competence of the particular witness in his or her field of expertise, the methodologies used, the extent to which the findings were consistent with other evidence in the case and the general reliability of the expert’s evidence.”⁴⁸

To assess documentary evidence, on the other hand, the Chamber will examine its “provenance, source or author, as well as their role in the relevant events, the chain of custody from the time of the item’s creation until its submission to the Chamber, and any other relevant information.”⁴⁹ The Chambers have explained that the burden of proof of the reliability of a document lies on the party seeking its admission.⁵⁰ If a document is determined to be authentic, it means it is what it purports to be, which is different from the determination as to whether its contents are reliable. It is important to note that a document may be authentic but nevertheless unreliable.⁵¹ There is no strict requirement that every document be authenticated officially or by a witness in court.⁵² The Chambers have explained that:

46. Prosecutor v. Lubanga, Case No. ICC-01/04-01/06-2842, Judgment pursuant to Article 74 of the Statute, ¶ 102 (Mar. 14, 2012) [hereinafter *Lubanga* Judgment], https://www.icc-cpi.int/CourtRecords/CR2012_03942.PDF [https://perma.cc/5P9G-7W5C] (archived Dec. 29, 2017).

47. *Id.* at ¶ 102.

48. *Id.* at ¶ 112.

49. *Bemba*, Judgment, at ¶ 247.

50. *Id.*

51. *Id.*

52. Documents may be admitted by the parties through a “bar table” motion, which provides for the situation where documents or other material are put into evidence directly, without being produced by or through a witness in the course of testimony. *See generally* Prosecutor v. Katanga, Case No. ICC-01/04-01/07-2290, Prosecution’s Submission of Material as Evidence from the Bar Table Pursuant to Article 64(9) of the Statute (July 16, 2010), <https://www.icc-cpi.int/pages/record.aspx?uri=909643> [https://perma.cc/BBQ7-F5W6] (archived Dec. 29, 2017). The “procedure of tendering materials from the bar table without it being introduced by a witness has been accepted by all the Trial Chambers” at the Court. Prosecutor v. Ruto and Sang, Case No. ICC-01/09-01/11-1219-Red, Public redacted version of the “Joint Defence Application for the Admission of Items related to the Testimony of P-0536 from the Bar Table,” ICC-01/09-01/11-1219-Conf, 13 March 2014 536, ¶ 7 (July 6, 2016),

items can also be (i) self-authenticating, if they are official documents publicly available from official sources; (ii) agreed upon by the parties as authentic; (iii) *prima facie* reliable if they bear sufficient indicia of reliability such as a logo, letter head, signature, date or stamp, and appear to have been produced in the ordinary course of the activities of the persons or organisations who created them; or (iv) in case the item itself does not bear sufficient indicia of reliability, shown to be authentic and reliable by the tendering party through provision of sufficient information to enable the Chamber to verify that the documents are what they purport to be.⁵³

Digital evidence is “information and data of value to an investigation that is stored on, received, or transmitted by an electronic device.”⁵⁴ Most digital evidence is considered documentary or forensic evidence, depending on whether any analysis or scientific procedure has been applied in order to validate or verify the digital item. Digital photographs, aerial and satellite images, digital audio- and video-recordings, call records, emails and other electronic communications or records are considered documentary evidence and are therefore evaluated based on the same criteria as paper documents. If forensic processes have been applied to digital information (i.e., audio enhancement or photograph augmentation) or an analytic product or expert report has been compiled using raw digital data (i.e., a geolocated photograph or call sequence table) that evidence may have to be introduced through an expert witness, which would require additional conditions to be met. Analytical products that are introduced as evidence should be distinguished from demonstrative evidence, such as visual representations or models, which are technically not evidence at all.

Based on the limited jurisprudence available to date, digital evidence may be excluded if its collection violated the Statute or an internationally recognized human right, such as the right to privacy, and digital evidence may be given little weight if the judges do not understand its significance or if it cannot be properly sourced or authenticated. While the overarching principles of how digital

https://www.icc-cpi.int/CourtRecords/CR2016_04873.PDF [https://perma.cc/M7VQ-4V4E] (archived Jan. 17, 2018).

53. *Bemba*, Public Redacted Version of Admission of Materials into Evidence, at ¶ 9.

54. ARIC W. DUTELLE, AN INTRODUCTION TO CRIME SCENE INVESTIGATION 374 (2016); U.S. DEP'T OF JUSTICE, DIGITAL EVIDENCE IN THE COURTROOM: A GUIDE FOR LAW ENFORCEMENT AND PROSECUTORS 72 (2007).

evidence will be evaluated are known, decisions are made on a case-by-case basis and there is still minimal guidance on how the Chambers will rule based on different sets of facts. To better understand the applicable rules and principles, the following Section discusses the most relevant jurisprudence on digital and technologically derived evidence in international criminal cases.

A. The evolution of evidence in international criminal trials

While, over many decades, national criminal trials have gradually evolved from cases based exclusively on the testimony of eyewitnesses to incorporating documentary and physical evidence, international criminal trials have been exceptional with a diverse body of evidence from the beginning because of the unique nature of the institutions, the perpetrators, and the crimes themselves. In order to understand the evidence and its significance in international criminal cases, the parties and judges need considerable background information and context on the historical, cultural, and political nature of the conflict. Thus, technologically derived evidence and innovative methods of evidence collection, preservation, and presentation have been an integral part of the international criminal justice story from start.

In addition to being the first court of its kind, the International Military Tribunal for Nuremberg was remarkable in a number of other ways. The cases were striking because of the large volume of documentary evidence, particularly official government and military records, Third Reich propaganda and public campaigns, and photographs and film produced by journalists covering the war, which were all used to prove the Nazi's organizational hierarchy, chain of command, and genocidal intent, as well as other criminal elements.⁵⁵

When facing the challenge of the first international military prosecution, the Chief Prosecutor at Nuremberg, Justice Robert Jackson, had concerns about a shortage of evidence.⁵⁶ Those fears were quickly laid to rest when a mountain of evidence arrived and he

55. See generally WHITNEY R. HARRIS, *TYRANNY ON TRIAL: THE EVIDENCE AT NUREMBERG* (Barnes & Nobel Inc. eds., 1995).

56. History.com Staff, *Nuremberg Trials*, HISTORY.COM (2010), <http://www.history.com/topics/world-war-ii/nuremberg-trials> [https://perma.cc/77D3-V8K5] (archived Dec. 29, 2017); see generally History Documentary Films, *History Channel Documentary Nuremberg Trials World War II Documentary* (Jan. 5, 2016), YOUTUBE, <https://www.youtube.com/watch?v=K5lslb1gjAds&t=5s>.

realized that the Nazi defendants, consistent with German cultural norms and practice in general, were orderly, fastidious record-keepers who documented every action they took and officially stamped each document.⁵⁷ Justice Jackson decided, against common wisdom, to switch his prosecution away from witnesses to what he referred to as a “documentation trial.”⁵⁸ One person who opposed this approach was General William Donovan, Head of the Office of Strategic Services during the war and a member of the trial staff. General Donovan believed that the trial would not have a great enough impact unless there were live witnesses on the stand being interrogated. Live testimony was necessary to capture public attention. In rejecting this approach, Justice Jackson demonstrated an important truth: that despite the grave and horrific nature of the crimes, a criminal case could be successful based on cold, hard facts and evidence rather than relying on the sympathetic testimony of victims to capitalize on human empathy as a response to atrocities. He presented a case that allowed for a decision based on reason, not emotion.

In addition to the large amounts of government and military records that served as evidence, photographs and film also played a significant role.⁵⁹ For over a century, war crime reporting through the use of photography and, more recently, film had developed as a way of educating government decision-makers and informing the public about war efforts abroad.⁶⁰ World War II was a large-scale, important global conflict and, as such, was well documented. With the creation of Nuremberg, war documentation found a new application as evidence in war crimes prosecutions. The large scale of the conflict and the amount of people it touched meant far more witnesses to the events than could ever actually be presented during a trial, especially one that was mandated to be expeditious. The abundance of evidence forced the prosecutors to make choices about which victims and witnesses to put on the stand, and gave them freedom and creativity in

57. See History Documentary Films, *supra* note 56 at 14:05 (“47 crates of binders, 3,000 pounds of Nazi party records, tons of diplomatic papers, 12 volumes of secret foreign policy conference records and miles of film poured in.”).

58. See *id.*

59. *Evidence from the Holocaust: How we know what we know*, UNITED STATES HOLOCAUST MEMORIAL MUSEUM, <https://www.ushmm.org/wlc/en/article.php?ModuleId=10007147> [<https://perma.cc/K49T-AGDU>] (last visited Dec. 29, 2017).

60. See generally JASON FRANCISCO, *War Photography*, in *ENCYCLOPEDIA OF TWENTIETH CENTURY PHOTOGRAPHY* 1636 (Lynne Warren ed., Routledge, 2005).

their approach to presenting evidence, educating the fact-finder, and telling the story.

Along with the advantages that came with trying cases based on a global event of this magnitude, there were a host of challenges that came with wielding justice on this scale and in an international environment. An obvious problem that arises immediately in an international trial is that the various participants will speak different languages and evidence may require cultural knowledge and interpretation to properly understand it. At Nuremberg the defense counsel and their clients spoke German, while the four judges and prosecution teams representing the Allied powers spoke English, Russian, or French.⁶¹ The tribunal had a mandate to provide “fair and expeditious” proceedings.⁶² To be fair, the accused had to be questioned in their native language, but to be expeditious, the Court could not rely on the existing technology of consecutive translation into all four languages. To solve this problem, the Head of interpreting systems at Nuremberg, Col. Leon Dostert, consulted with an old friend, Thomas Watson Sr., the CEO of IBM.⁶³ IBM offered to test out a new technology it had been working on and developed a system of microphones and headsets to transmit the cacophony of languages in real time.⁶⁴ Thus, simultaneous interpretation, which is still used today, was invented specifically for the Nuremberg Trials.⁶⁵ This partnership between IBM and the Nuremberg tribunal would be the first in a history of collaboration between technologists and

61. The Allied powers were English, American, Soviet and French and each had one judge and one prosecution team. See Roman A. Matasov, *Nuremberg: The Trial of Six Million Words*, AIIC, <https://aiic.net/page/7943/> [<https://perma.cc/WFK4-FPU7>] (last visited Jan. 22, 2018).

62. Richard May & Marieke Wierda, *Trends in International Criminal Evidence: Nuremberg, Tokyo, The Hague and Arusha*, 37 COLUM. J. OF TRANSNAT'L L. 727, 729, 735-36 (1999).

63. See generally Catherine Pilishvili & Charlotte Kelly, *Chief Interpreter at Nuremberg Trials Leaves His Mark on Georgetown*, SFS.GEORGETOWN.EDU (Nov. 2016), <https://sfs.georgetown.edu/chief-interpreter-nuremberg-trials-leaves-mark-georgetown/> [<https://perma.cc/6WGS-ZHLT>] (archived Dec. 29, 2017).

64. Even before the Nuremberg trials were over, Dostert had taken his system to the United Nations in New York. It is the same model used today. While technology has not yet replaced the interpreters themselves, one day it might. In the last year, multiple universal translation devices have come on the market such as Babelfish and Sismo. See generally Pilishvili & Kelly, *supra* note 63.

65. Nina Porzucki, *How the Nuremberg Trials Changed Interpretation Forever*, PRI.ORG (Sept. 29, 2014), <https://www.pri.org/stories/2014-09-29/how-do-all-those-leaders-un-communicate-all-those-languages> [<https://perma.cc/7XQ4-NXD6>] (archived Dec. 29, 2017).

international criminal justice professionals to solve problems unique to prosecuting cases of this magnitude in the international arena.

The second international criminal justice wave came in the early 1990s with the ICTY and ICTR. While witness and victim testimony was a significant part of the cases before both tribunals, non-oral evidence such as satellite imagery, forensic anthropology and expert reports, and radio broadcasts were offered as evidence. ICTR prosecutors pioneered the use of new forms of evidence to support innovative charges in what is now considered the landmark “media case,” *Prosecutor v. Nahimana et al.*⁶⁶ In this case, the Prosecution introduced radio broadcasts as evidence to support the charge of inciting genocide by encouraging violence through the public airwaves. Three individuals were convicted for incitement of genocide based primarily on recordings of radio broadcasts through which one of the accused incited violence against the Tutsi population. While radio itself was not new, more recent technology allowed for the availability of these recordings years after the broadcast made the case possible. They may not have been preserved as evidence without advancements in electronics that expanded data storage capacity.⁶⁷ It is also interesting to note that, just as in the Nuremberg trials, it was the tools utilized by the Accused that produced the best evidence of their criminal intent.

At the ICTY, aerial images offered by the Prosecution were admitted to show areas of disturbed earth that represented mass graves in the cases of *Krstić*, *Blagojević*, *Popović et al* and *Tolimir*.⁶⁸

66. *Prosecutor v. Nahimana*, Case No. ICTR-99-52-T, Judgment and Sentence (Dec. 3, 2003), <http://unictr.unmict.org/en/cases/ictr-99-52> [<https://perma.cc/33RR-QZT8>] (archived Dec. 29, 2017); see UNITED NATIONS, MECHANISM FOR INTERNATIONAL CRIMINAL TRIBUNALS, *Nahimana et al. (Media case) (ICTR-99-52)* (describing Nahimana et al. as the “media case”).

67. Zetta Staff, *History of Data Storage Technology*, ZETTA.NET (May 5, 2016), <https://www.zetta.net/about/blog/history-data-storage-technology> [<https://perma.cc/K8CK-XE5W>] (archived Dec. 29, 2017).

68. *Prosecutor v Tolimir*, Case No. IT-05-88/2-T, Trial Judgment, ¶¶ 65, 67–68, 70, 435, 454, 457, 478, 561, 564 (Int’l Crim. Trib. for Fmr. Yugo. Dec. 12, 2012), <http://www.icty.org/case/tolimir/4> [<https://perma.cc/6DTJ-YMLJ>] (archived Dec. 29, 2017); *Prosecutor v Popović et al.*, Case No. IT-05-88-T, Public Redacted Judgment, Volume I ¶¶ 73-75, (Int’l Crim. Trib for Fmr. Yugo. June 10, 2010), <http://www.icty.org/case/popovic/4> [<https://perma.cc/SZ6L-SV68>] (archived Dec. 29, 2017); *Prosecutor v Blagojević*, Case No. IT-02-60-T, Trial Judgment, n. 1397, 1398 (Int’l Crim. Trib. for Fmr. Yugo. Jan 17, 2005), http://www.icty.org/case/blagojevic_jokic/4 [<https://perma.cc/C4SC-9HRC>] (archived Dec. 29, 2017); *Prosecutor v Krstić*, Case No. IT-98-33-T, Trial Judgment, ¶¶ 114, 223, 229, 230, 238, 250, 253, 258 (Int’l Crim. Trib. for Fmr. Yugo. Aug. 2, 2001), <http://www.icty.org/>

The aerial images, which had been provided to the prosecution by the US government, also showed buildings, vehicles, large groups of prisoners and bodies which corroborated the testimony of witnesses and assisted the judges in comprehending relevant geographical relationships such as the proximity of the mass graves to Srebrenica.⁶⁹ The US government's stipulation on providing this information was that the sources and methods used to collect these digital images could not be discussed in the courtroom.⁷⁰ In response to the defense's objections, the Trial Chamber explained that without evidence to challenge the reliability of the images, they would not be excluded.⁷¹ This ruling remains significant today, since it places a burden on the Defense to make a showing that digital images lack reliability or are not authentic before allowing them to challenge the admissibility of the evidence on those grounds.

The first ICC Prosecutor's approach to cases diverged from his predecessors at the ICTY and ICTR in that the early cases were eyewitness-focused and relied almost entirely on testimonial evidence. In *Prosecutor v. Lubanga*, the first trial before the ICC, the Prosecution introduced evidence in oral, written and audio-visual form. There was no physical or forensic evidence.⁷² The evidence included testimony from sixty-seven witnesses, only one of whom was qualified as an expert.⁷³ Documents and other materials such as transcripts of interviews, videos, records from non-governmental organizations, letters, photographs and maps were either introduced through witnesses or by bar table motion.⁷⁴ Soon after the trial commenced, evidence emerged that some of the witnesses'

case/krstic/4 [https://perma.cc/FG5W-WPRP] (archived Dec. 29, 2017); IBA, EVIDENCE MATTERS IN ICC TRIALS, *supra* note 9.

69. Aerial imagery released by United States military intelligence has now also been used at the ICTY in criminal trials of members of the Bosnian Serb Army including Radislav Krstic and, most recently, the ongoing case against Ratko Mladic. These images were used to corroborate witness accounts of war crimes and crimes against humanity carried out in 1995 by identifying areas of disturbed earth indicating the presence of mass graves and by noting the presence of large groups of people and the vehicles witnesses described as those used to transport the victims. *See generally* IBA, EVIDENCE MATTERS IN ICC TRIALS, *supra* note 9.

70. *See generally Tolimir*, Judgment; IBA, EVIDENCE MATTERS IN ICC TRIALS, *supra* note 9.

71. *Tolimir*, Judgment, ¶ 69.

72. *Lubanga*, Judgment, ¶ 93.

73. *Id.* The expert was a psychologist called by the Chamber to give testimony on the psychological impact of a child having been a soldier and the effect of trauma on member. *See Lubanga*, Judgment, ¶ 105.

74. *Lubanga*, Judgment, ¶ 93.

testimonies had been tainted by the influence of corrupt intermediaries.⁷⁵ In particular, a recurring issue was whether some of the intermediaries used by the Prosecution encouraged witnesses to lie about their ages.⁷⁶ Lubanga was charged with the war crime of using, conscripting or enlisting child soldiers, and so the Prosecutor had to prove beyond reasonable doubt that “the perpetrator conscripted or enlisted one or more persons into the national armed forces or used one or more persons to participate actively in hostilities” and that “*such person or persons were under the age of 15 years.*”⁷⁷ Thus, lies about the age of alleged child soldiers were material to the case. While the testimony of the nine witnesses was admitted, the judges attributed almost no weight in their final decision.⁷⁸ Ultimately, the Chamber found the testimony of nine prosecution witnesses, all alleged child soldiers, unreliable because of witness coaching.⁷⁹

The conditions under which the investigators were operating in the Ituri region made it difficult to establish the age of the witnesses.⁸⁰ For the security of the alleged child soldiers, the investigators chose not speak to family members or members of the community, and could not easily access school records. The Chamber found that the Prosecution’s failure to investigate the children’s histories significantly undermined its case.⁸¹ To support the charge despite the witnesses’ lack of credibility, the Prosecution introduced video footage portraying Lubanga inspecting troops who appeared to be under the age of fifteen and presented an expert report relating to X-ray examinations of bones and teeth. Though the probative value of these additional pieces of evidence was minimal, they helped corroborate aspects of the witness testimony and, as a result, secure a conviction.⁸²

In *Prosecutor v. Katanga and Ngudjolo*, the second trial, which came out of the same initial investigation in the Democratic Republic

75. An “Intermediary” is an individual or organization who, upon request of an organ or unit of the Court of Counsel, conducts certain activities. See generally INT’L CRIM. CT., ICC CODE OF CONDUCT FOR INTERMEDIARIES (Mar. 2014).

76. *Lubanga*, Judgment, ¶ 169.

77. Int’l Crim. Ct., *Elements of Crimes*, art. 8(2)(b)(xxvi) (2011); *Prosecutor v. Lubanga*, Judgment pursuant to Article 74 of the Statute, ICC-01/04-01/06-2842 (Mar. 14, 2012), ¶¶ 1-8.

78. See generally *Lubanga*, Judgment.

79. See generally *Lubanga*, Judgment.

80. *Lubanga*, Judgment, ¶ 70.

81. *Lubanga*, Judgment, ¶ 75.

82. See generally *Katanga*, Decision on the disclosure of evidentiary material.

of Congo, the Prosecution's case faced similar issues with witness credibility and the use of corrupt intermediaries. Therefore, after the confirmation hearing, and even after the passage of disclosure deadlines, the Prosecution continued its investigation, sending an expert mission to examine the 'Institut de Borogo' in the Ituri region in March 2009, about seven months before the trial was scheduled to commence.⁸³ The examinations yielded additional materials which the Prosecutor sought to admit as evidence, which included a digital 360-degree visual representation of the 'Institut' with a report by the visual technician who created it and over 200 photographs taken by drone which were used for its production; a ballistic expert report accompanied by video of the crime scene investigation and related physical evidence such as shell casings; a forensic report concerning blood analysis and blood samples; and a forensic report about the exhumation and autopsy of human remains, as well as videos and hundreds of photographs of exhumation process and the human remains.⁸⁴ They also sought to add four experts to the witness list: a visual technician, a ballistics expert, an expert in morphologic analysis of blood traces, and a DNA expert.⁸⁵ The Prosecution justified the late submission, in part, on the security situation which, it argued, prevented them from taking these investigative steps earlier. The Defense challenged the validity of the Prosecution's justification for not having been able to conduct the examination earlier and argued that the complexity of the reports required a counter-expert.⁸⁶ In addition, since six years had passed since the alleged events, the Defense argued that there were serious concerns about the loss and alteration of the physical evidence collected.⁸⁷

The Chamber found that the photographic representation could assist it in visualizing the 'Institut' and its surroundings, but noted that it had very limited evidentiary value.⁸⁸ It also discussed the limited probative value of the conclusions in the reports due to the degradation of evidence upon which they were based. The Chamber

83. *Id.*

84. *See generally id.*

85. *See generally id.*

86. *See id.* at ¶¶ 8-9. The Chamber acknowledged that the ballistic report was relevant to the case, yet found that it did not offer particularly compelling information to aid it since the experts were not able to establish the projectile's origin or the time it was fired. Similarly, with the blood report and exhumation and autopsy report. *Id.* at ¶¶ 41-45.

87. *See Katanga*, Decision on the disclosure of evidentiary material, ¶ 10.

88. *See id.* at ¶ 39 ("It is simply a tool for orientation, just like a diagram or drawing.").

concluded that, given the rather limited pertinence of the information contained in the reports, it could only allow their late addition if the added value of the information outweighed the procedural implications to the fair trial rights of the Accused caused by the late disclosure.⁸⁹ The Chamber admitted the visual representation, but excluded the rest, acknowledging that while they were relevant, the Chamber was not convinced that the expert reports offered significantly more compelling evidence than what had been previously disclosed. In an interview in 2012, Judge Bruno Cotte, the presiding judge in *Katanga and Ngudjolo*, said that the Prosecution's cases would benefit from diversifying the kinds of evidence it presents at trial, noting as well that witness testimonies are "often fragile."⁹⁰

Additionally, in its decision, the Chamber admonished the Prosecution for selecting and instructing the experts unilaterally without properly informing or consulting the Defense. The Chamber was of the view that the opposing party should, to the extent possible, be invited to participate in the expertise from an early stage onward, and that the Defense should be able to comment on the working methods of experts.⁹¹ The Chamber explained that early involvement by all parties prevents them from being caught off-guard by the findings: "[t]his unfortunate situation could have been almost entirely avoided if the Prosecution had invited the Defense to take part in the expert mission to Bogoro from the beginning."⁹² It is likely that future judges might apply the same standard to complex digital forensics analysis as well as physical forensic missions. After the *Katanga* and *Ngudjolo* judgments, the consideration of conducting forensic missions early on has been part of all OTP investigation plans.

During the arrests of Jean-Pierre Bemba Gombo in 2008 and Callixte Mbarushimana in 2010, investigators seized electronic hardware such as laptops and cell phones from the Accused.⁹³ However, the Prosecution did not offer digital evidence from these sources in the hearings or at trial. This could be because they did not have the capacity and resources to do a thorough digital forensic

89. *See id.* at ¶ 56.

90. BERKELEY HUMAN RIGHTS CTR., DIGITAL FINGERPRINTS, *supra* note 18, at 5 (citing Franck Petite, "Interview with ICC judge Bruno Cotte, presiding judge at the second trial at the ICC," Radio Netherlands Worldwide, 20 June 2012).

91. *Katanga*, Decision on the disclosure of evidentiary material, ¶ 68.

92. *Id.* at ¶ 74.

93. BERKELEY HUMAN RIGHTS CTR., DIGITAL FINGERPRINTS, *supra* note 18.

investigation, or because they did not find relevant material of evidentiary value on the devices. The charges against Mbarushimana were not confirmed. On the other hand, Bemba was convicted after a lengthy trial, although evidence from his computer was not essential to the case. Interestingly, in his second trial for witness tampering which is discussed in detail in Part III, more digital evidence was seized and it did play an important role in building that case against him.

By 2011, the Office of the Prosecutor was investigating cases in which digital evidence was critical in Kenya, Cote d'Ivoire, and Libya. These new cases generated an increased demand for the storage, processing, and analysis of digital evidence. In response, the Court began to consider ways to build its cyber forensics capacity.⁹⁴ In cases originating from the atrocities committed in Darfur, Sudan, satellite imagery has played an important role in tracking the burning and destruction of villages, the movement of populations, and the location (absence or presence on the tarmac) of Antonovs, the aircrafts used by the Government of Sudan. The availability of this satellite imagery is, in part, due to the massive efforts and resources provided by various humanitarian non-governmental organizations to collect this material.⁹⁵ The Prosecution presented satellite imagery in the confirmation of charges hearings for the cases of *Prosecutor v. Abdallah Banda Saleh Jerbo Jamus* and *Prosecutor v. Bahr Idriss Abu Garda*, which involved an attack against an African Peacekeeping Mission at the Haskanita Military Group Site in Darfur.⁹⁶ The evidence in the other Darfur cases has yet to be presented, since the accused are still at large, but it is likely that satellite imagery will be an integral part of those cases as well.

In its tenure from 2002-2015, the ICC Chambers issued three trial judgments in the cases of *Lubanga*, *Ngudjolo*, and *Katanga*.⁹⁷ In

94. *Id.*; IBA, EVIDENCE MATTERS IN ICC TRIALS, *supra* note 9.

95. The Satellite Sentinel Project, Harvard Humanitarian Initiative, Amnesty International, and the Holocaust Memorial Museum in partnership with Google Earth have all worked on initiatives to analyze and utilize satellite images of human rights abuses and war crimes committed in Darfur, Sudan.

96. *See generally* *Prosecutor v. Banda*, Case No. ICC-02/05-03/09-121-Corr-Red, Public Redacted Version Corrigendum of the "Decision on the Confirmation of Charges" (Mar. 7, 2011), http://www.worldcourts.com/icc/eng/decisions/2011.03.07_Prosecutor_v_Banda.pdf [<https://perma.cc/TF8L-4HEK>] (archived Dec. 29, 2017); *Garda*, Decision on Confirmation of Charges.

97. *See generally* *Lubanga* Judgment; *Ngudjolo* Judgment; and *Katanga* Judgment. Please note that although *Katanga* and *Ngudjolo* originated as one case, the cases were later

2016, the number of trial judgments doubled with the issuance of judgments in *Bemba*, *Al Mahdi*, and *Bemba et al.* These cases, and the digital evidence used by the Prosecution to prove the respective charges, are examined in the following Part.

III. RECENT INTERNATIONAL CRIMINAL CASES INVOLVING DIGITAL EVIDENCE

This Part examines the different types of digital and technologically derived evidence offered by the Prosecution in three recent cases before international criminal courts. Since international criminal justice is still a rather new field of law, most cases deal with never before seen sets of facts and unprecedented legal issues. Outliers are the norm. Thus, all three case studies below are atypical and represent many “firsts” for the field, yet are nevertheless relevant because the way in which the judges rule on the admissibility and weight of these newer types of evidence will set the standard for future cases. The first case involves computer-facilitated analysis of an explosion (“digital explosives evidence”) and call data records (“telecommunications evidence”). The second case involves images from Google Earth and videos from YouTube (“open source evidence”) and an interactive platform created from visual representations (“interactive digital platform”). The third case involves records of wire transfers (“digital financial evidence”), call data records and telephone intercepts (“intercepts evidence”), and emails and social media posts (“digital communications evidence”).

A. Evidence of a conspiracy to commit terrorist acts

The main case before the Special Tribunal for Lebanon (“STL”), *Prosecutor v. Ayyash et al.*, is one of many firsts for international criminal justice, both legally and procedurally.⁹⁸ The STL is the first tribunal of an international character to have jurisdiction over the crime of terrorism and is uniquely set up with an independent Defense Office responsible for protecting and promoting the rights of the accused. It is also the first tribunal in recent history to hold trials with

severed and separate judgments were issued by the Trial Chamber. Ngudjolo was acquitted. Katanga was convicted on some charges and acquitted on other charges.

98. See generally *Ayyash*, Wikileaks Documents Decision.

the defendants *in absentia*.⁹⁹ The Prosecution's case is entirely circumstantial with no direct evidence, and includes the first use of telecommunications data as evidence. The terrorist attack upon which the case is based occurred in Lebanon in 2005 – a place and time when cellular phones were widely used and relied upon. The investigation began shortly after the attack and continued over many years leading to the creation of the STL in 2007 and the issuance of an indictment in 2011. The trial opened on January 6, 2014 and is ongoing.

1. Case Background

On February 14, 2005 at 12:55 p.m., an explosion in front of the St. Georges Hotel shook downtown Beirut. The blast destroyed a convoy of vehicles carrying the former Prime Minister of Lebanon, Rafik Hariri, killing him along with eight members of his entourage and 13 bystanders, as well as injuring over 200 others.¹⁰⁰ Shortly after the attack, two separate investigations commenced. Local police ran one investigation, while the other was directed by the United Nations.¹⁰¹ The United Nations poured millions of dollars into their investigation, focusing on the explosion and forensic evidence collected at the scene. While this provided investigators with a clearer picture of the events that occurred before, during, and after the attack, it did little in the way of identifying those responsible. By contrast, one of the local police officers, a young investigator with a computer engineering background named Wissam Eid, took a different approach: he decided to look at cellphone records.¹⁰² At Eid's request, a judge ordered Lebanon's main cellphone companies, Alfa and MTC Touch, to produce records of all calls and text messages in Lebanon in the four months preceding the bombing.¹⁰³ At the time, cell phone

99. Prosecutor v. Ayyash et al, Decision to hold trials in absentia, STL-11-01/1/TC, R109799. See generally International Bar Association, *Report on the 'Experts Roundtable on trials in absentia in international criminal justice'* (Sept. 2016). The Tribunal decided to hold an international trial in absentia for the first time since the Allied tribunal at Nuremberg in 1946 sentenced Hitler's aide Martin Bormann to death.

100. Ronen Bergman, *The Hezbollah Connection*, N.Y. TIMES MAGAZINE (Feb. 10, 2015), <https://www.nytimes.com/2015/02/15/magazine/the-hezbollah-connection.html>.

101. Rep. of the Int'l Indep. Investigation Comm'n Established Pursuant to S.C. Res. 1595 (Oct. 19, 2005).

102. Bergman, *The Hezbollah Connection*, *supra* note 100, at 13.

103. *Id.* (granting of such a request was rather exceptional – in the United States, for example, privacy laws and the requirement for specificity in search warrants would likely

evidence had been used infrequently in national jurisdictions, and law enforcement officials were less informed about the value of information that could be derived from examining cellphone use. Eid understood the potential for significant evidence extracted from cell phone metadata and meticulously analyzed the records, creating an algorithm that revealed a peculiar pattern.¹⁰⁴ He noticed that in October 2004, just after Hariri resigned, a cluster of cellphones began following him everywhere. Eid started with the location data from the phone of Hariri and known members of his entourage, and then eliminated them to isolate the phones in the same locations that were unknown. From plotting the movement of these phones, it was clear that Hariri was under constant surveillance by unidentified individuals for months preceding the attack. Eid worked backwards to attribute the phone numbers and identify their users.¹⁰⁵ Soon the investigation was blown wide open. As Eid honed in on the suspects, the United Nations took note of his work, eventually incorporating his methods and work product into their own investigation.¹⁰⁶

On May 30, 2007, the UN Security Council passed Resolution 1757 to establish the STL to prosecute the individuals responsible for committing the February 14 attack in Beirut. The founding instrument for the Tribunal specified that it must apply the Lebanese Criminal Code for crimes of terrorism, defined as “acts intended to cause a state of terror and committed by means liable to create a public danger such as explosive devices, inflammable materials, toxic or corrosive products and infectious or microbial agents.”¹⁰⁷ Despite this mandate, the Appeals Chamber issued an interlocutory decision holding that it could also apply international law related to the definition of terrorism to which Lebanon is bound.¹⁰⁸ After years

preclude such a broad request; later the Prosecutor’s Office received additional records for years of calls in the entire country).

104. Metadata is data about data and includes time stamps, geospatial information, or copyright information. *See generally* Bergman, *supra* note 100.

105. Bergman, *supra* note 100, at 13.

106. Bergman, *supra* note 100, at 15.

107. S.C. Res. 1757, art. 1-2 (May 30, 2007); Lebanese Crim. Code, art. 314; Michelle Flash, *The Special Tribunal for Lebanon Defines Terrorism*, HUMAN RIGHTS BRIEF (Oct. 10, 2011), <http://hrbrief.org/hearings/the-special-tribunal-for-lebanon-defines-terrorism/> [<https://perma.cc/V83W-V7QT>] (archived Dec. 29, 2017).

108. Prosecutor v. Ayyash et al., Case No. STL-11-01, Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, ¶ 113, 114 (Spec. Trib. Leb., Feb 16, 2011), <https://www.stl-tsl.org/en/the-cases/stl-11-01/main/filings/orders-and-decisions/appeals-chamber/534-f0936> (referencing the Arab Convention for the Suppression of Terrorism, articulated a customary international law

of investigation, the first indictment was confirmed on June 28, 2011 in which the four accused were charged with conspiracy to commit a terrorist act; committing a terrorist act by using explosive materials; premeditated intentional homicide by using explosive materials; and attempted premeditated intentional homicide by using explosive materials.¹⁰⁹ The trial began in January 2014 and, as of 2017, the Prosecution was still presenting its case. This is a complex case, so to aid the judges, the Prosecution divided its presentation of the evidence into three categories: (1) forensic evidence relating to the attack; (2) evidence of the preparatory acts of the Accused; and (3) the identity and roles of the Accused.¹¹⁰ These categories are discussed below.

2. Digital Explosives Evidence

The forensic evidence relating to the attack involves DNA profiling and analysis of human remains, as well as analysis of trace explosive materials and physical evidence such as the remnants of the Mitsubishi Canter van used to carry the bomb. Video footage from surveillance cameras in the square and surrounding area has been used to corroborate the findings of the forensic examinations and to establish a clear timeline of events leading up to the attack. During the Prosecution's opening statement, two detailed physical models of the square where the attack occurred—one representing the scene before the explosion and one representing the destruction afterwards—were placed in the center of the courtroom. In order to calculate the amount of explosives used and to pinpoint where the bomb was detonated, the Prosecution presented expert reports and testimony from two Argentinian civil engineering professors who used specialized computer programming and algorithms to input the data

definition of terrorism, and explained how the Tribunal is not limited by Lebanese case law as it applies the Lebanese Criminal Code related to terrorism).

109. The original indictment in *Ayyash et al.* was filed on January 17, 2011. See *Ayyash Indictments*, SPECIAL TRIBUNAL FOR LEBANON, <https://www.stl-tsl.org/en/the-cases/stl-11-01/main/indictments-6> (last visited Nov 19, 2017). It was amended on March 11, 2011, May 6, 2011, and June 10, 2011 to add new information and Accused, and confirmed by the Pre-Trial Judge on June 28, 2011. See *id.* Arrest warrants were issued for Messrs Salim Jamil Ayyash, Mustafa Amine Badreddine, Hussein Hassan Onessi and Assad Hassan Sabra the same day. See *id.*

110. *STL Bulletin – June 2017: The Prosecutor v. Ayyash et al. (STL-11-01) – Stages of Evidence*, SPECIAL TRIBUNAL FOR LEBANON (June 2017), https://www.stl-tsl.org/index.php?option=com_k2&id=9832_197ae81aefd245109078b7d3ca3ed287&lang=en&task=download&view=item.

and determine what it would take to cause the damage to the square. Explosion reconstruction is not a new science and has been applied in national cases, but this is the first time this technology has ever been used before an international criminal tribunal. Further, the amount of resources and manpower dedicated to this portion of the evidence is unprecedented.¹¹¹

The experts authored two reports, which presented and analyzed several scenarios explaining the size of the crater and the structural damage caused to the buildings. The analysis was carried out to determine whether the explosives were buried, sitting on the ground surface, or at some point above the ground.¹¹² They explained how they ascertained the quantity of the explosives as well as their location in terms of height above ground of the explosive mass, concluding that, given the parameters of the crater, the damage observed, measured and numerically modeled could have only been created by an above-ground explosion. The reports and testimony supported the Prosecution's theory of the case that the explosion was the work of a suicide bomber driving a van carrying explosives, and refuted the defense that the blast was caused by an underground bomb.

The amount of data points entered into the calculation and the ability to produce different scenarios could not have been done by a human being—it required machine intelligence. Thus, while the defense may present a counter-expert, it will be very difficult to challenge the findings of the computer program without the ability to truly understand how the algorithm works.¹¹³ The defense cannot cross-examine a computer program. In addition to the need for specialized knowledge to understand this evidence, the cost of these forensic examinations and calculations was incredibly high, posing an obstacle to the defense's ability to effectively counter the

111. As of 2015, before arrests had been made, the setting up of tribunal and investigation had cost \$500 million. See Adam Taylor, *The U.N.'s tribunal in Lebanon has cost millions and made no arrests. Now the journalists are on trial.*, THE WASHINGTON POST (Apr. 7, 2015), https://www.washingtonpost.com/news/worldviews/wp/2015/04/07/the-u-n-s-tribunal-in-lebanon-has-cost-millions-and-made-no-arrests-now-the-journalists-are-on-trial/?utm_term=.47802009e3b0.

112. *STL Bulletin – February 2015: The Prosecutor v. Ayyash et al. (STL-11-01)*, SPECIAL TRIBUNAL FOR LEBANON (Feb. 2015), https://www.stl-tsl.org/index.php?option=com_k2&id=5592_d5d1446d8ec69151079ac415c6320ac9&lang=en&task=download&view=item.

113. Rebecca Wexler, *When a Computer Program Keeps You in Jail*, N.Y. TIMES (June 13, 2017), <https://www.nytimes.com/2017/06/13/opinion/how-computers-are-harming-criminal-justice.html>.

Prosecution's claims. While the case is in progress and, therefore, no final judgment has been issued, the questions asked of the witnesses by the judges show just how difficult some of the technical aspects of the testimony are to grasp. When the testimony is this specialized and technical, judges are put in the difficult position of either rejecting it because they do not understand it or accepting the conclusions without qualification—both dangerous propositions for the interests of justice.

3. Telecommunications Evidence

The evidence of the preparatory acts of the accused and their identity and roles in the plot is based primarily on telecommunications evidence, including call data records (“CDRs”), cell site information, and subscriber records provided by Communication Service Providers (“CSPs”).¹¹⁴ CSPs collect CDRs for customer billing and systems management purposes.¹¹⁵ These records are generated and maintained in the usual and ordinary course of business, and were introduced through witnesses from the CSPs who could explain the record-keeping process.¹¹⁶ Since all CDRs are “without further analysis largely unintelligible,”¹¹⁷ the Prosecution extracted the relevant information and entered it into what it terms “call sequence tables” to make the raw data capable of presentation and analysis without altering it.¹¹⁸ The call sequence tables are chronological sequences of calls to or from a specific number over a specified period of time, organized by the Prosecution for forensic

114. *Primer on Telecommunications on Evidence: Guide to understanding the testimony in Ayyash et al.*, SPECIAL TRIB. FOR LEBANON (Aug. 24, 2017), <https://www.stl-tsl.org/en/media/stl-bulletin/5752-primer-on-telecommunications-evidence>.

115. Acknowledging the full complexity of the telecommunications evidence, the STL has published a guide to understanding the testimony in *Ayyash et al.* regarding this evidence, entitled *Primer on Telecommunications on Evidence: Guide to understanding the testimony in Ayyash et al.*

116. SPECIAL TRIB. FOR LEBANON, *Primer on Telecommunications on Evidence*, *supra* note 114.

117. Prosecutor v. Ayyash, Case No. STL-11-01/T/TC, Prosecution Motion for the Admission of Red Network-Related Call Sequence Tables and Related Statement, ¶ 13 (Spec. Trib. Leb., Jan. 28, 2015), <https://www.stl-tsl.org/en/the-cases/stl-11-01/main/filings/motions/office-of-the-prosecutor/3758-f1831>.

118. Prosecutor v. Ayyash, Case No. STL-11-01/T/TC, R273784, Decision on Five Prosecution Motions on Call Sequence Tables and Eight Witness Statements and on the Legality of the Transfer of Call Data Records to UNIIIC and STL's Prosecution, ¶ 2 (Spec. Trib. Leb., May 6, 2015), <https://www.stl-tsl.org/en/the-cases/stl-11-01/main/filings/orders-and-decisions/trial-chamber/3996-f1937>.

analysis.¹¹⁹ The call sequence tables were introduced through OTP analysts. Additionally, the Prosecution has called telecommunications experts to explain how cellular signal and cell tower sites are used to geolocate the cell phone user. The amount of witnesses and hours of testimony required to authenticate and understand the relevance and probative value of the telecommunications evidence is significant, because it refutes the notion that using this type of technologically derived evidence would be more efficient than eyewitnesses. At the same time, these witnesses are arguably at a lower security risk than victims and eyewitnesses.

In his opening statement, the Prosecutor explained, “the evidence demonstrating the identities of the Accused is, to a large extent, dependent on the variety of tools they themselves used – the telephones.”¹²⁰ He further stated that witness testimony, documents, contacts made to other phones, geolocation of the phones and SMS content place the phones used for aiding and abetting the crimes in the hands of the accused. The Prosecution alleged that the interconnected mobile telephone networks were involved in planning, preparing, and executing the attack. The Prosecution alleged that the Accused took considerable steps to use the telephones in a covert manner and under false names or no names, which showed that they were aware of the risk that telephone use could reveal their identity and their activities.¹²¹ However, they did not account for everything that investigators would be able to pull out of the metadata, such as their use of these covert network telephones in conjunction with the use of other telephones in their possession. The data showed that one of the accused, Badreddine, carried both his operational phone used for plotting Hariri’s assassination in one pocket and his personal phone used to call his girlfriends in the other.¹²² Two of the other accused, Oneissi and Sabra, used their covert network telephones for personal matters. With the application of logic, investigators were able to derive deep insights into the persons involved in the attack. The cost of the mobile phones used in the operation provided information about the group’s resources, and the pattern of calls revealed the

119. SPECIAL TRIB. FOR LEBANON, *Primer on Telecommunications on Evidence*, *supra* note 114.

120. Prosecutor v. Ayyash, Case No. STL-11-01/T/TC, Official Transcript, 41:20 (Spec. Trib. Leb., Jan. 16, 2014), <https://www.youtube.com/watch?v=PDIHgs7hqhk>.

121. *Id.*

122. Bergman, *supra* note 100, at 21, 22.

hierarchical command structure. The defense teams in this case have had the difficult task of pioneering how best to challenge this type of evidence without the resources of the Prosecution. They have had to employ their own experts and find ways to poke holes in the assumptions and conclusions drawn from the data, as well as question the data itself. One particular challenge that has come up on cross examination is the accuracy of using cell tower signals to predict a user's physical location. The way cellular signals work is not necessarily precise or predictable, and the defense teams have had some success at demonstrating this through questioning of the Prosecution's experts. Since this case is ongoing as of the time of writing, there is no judgment and no way to know what weight the judges will attribute to this evidence; but since this evidence is the crux of the Prosecution's case, there will not be a conviction unless the judges accept the authenticity, relevance, and probative value of the telecommunications evidence and related findings.

B. Evidence of crimes against cultural heritage

The next case, *Prosecutor v. Al Mahdi*, also involves many firsts for international criminal justice. The Accused is the first at the ICC affiliated with an Islamic terrorist group, the first at the ICC to be charged with the war crime of destroying cultural property, and the first to plead guilty before the ICC.¹²³ This case is one of the fastest to move through the stages of proceedings, with the issuance of an arrest warrant, confirmation of charges, and trial all within about a year period. The attacks on ten cultural heritage sites upon which the case is based took place in Mali in June and July 2012—a time and place where mobile phone and social media use was growing.¹²⁴ The investigation began in 2013, which led to the issuance of an arrest warrant and immediate arrest of the Accused in September 2015.

123. See generally Mark Kersten, *The al-Mahdi Case is a Breakthrough for the International Criminal Court*, JUSTICE IN CONFLICT (Aug. 25, 2016), <https://justiceinconflict.org/2016/08/25/the-al-mahdi-case-is-a-breakthrough-for-the-international-criminal-court/> [<https://perma.cc/QX5V-7J2T>] (archived Jan. 17, 2018). While some defendants at the ICTY were charged with the war crime of destroying cultural property in the context of the shelling of Dubrovnik, Al Mahdi is the first in an international criminal case to only be charged with this crime, as opposed to it being paired with additional and more traditional war crimes charges.

124. See generally INTERNATIONAL BAR ASSOCIATION, EVIDENCE MATTERS IN ICC TRIALS (Aug. 2016). The Arab Spring marked an increase in mobile phone and social media use generally in the region.

After the confirmation of charges, the Accused pled guilty. A year later, a three-day trial took place from August 22-24, 2016.

1. Case Background

In early 2012, an internal armed conflict broke out in northern Mali and, within a few months, Islamist militants groups Ansar Dine and Al-Qaeda in the Islamic Maghreb overtook Timbuktu.¹²⁵ Al Mahdi was appointed to lead Ansar Dine's morality brigade, *Hesbah*, which was entrusted with suppressing anything perceived to constitute "visible vice."¹²⁶ Timbuktu's mausoleums and mosques were an integral part of the religious life of its inhabitants, a part of their common heritage, and a perceived threat to Ansar Dine. In June 2012, the Ansar Dine leadership destroyed these cultural sites with Al Mahdi overseeing the effort. On July 18, 2012, the Malian Government referred "the Situation in Mali since January 2012" to the ICC pursuant to Article 53 of the Statute.¹²⁷ In January 2013, the Prosecutor opened an official investigation. After nearly three years of investigations into the situation in Mali, the Pre-Trial Chamber issued an arrest warrant for Al Mahdi and he was swiftly transported to the seat of the Court in The Hague, where he was charged with intentionally directing attacks against ten buildings of a religious and historical character in Timbuktu on or around June and July 2012.¹²⁸

Due to the overwhelming evidence against him, Al Mahdi admitted guilt. However, because the ICC does not have a full plea-bargaining scheme as in countries like the United States, the Prosecution was nevertheless required to present some evidence against the Accused to corroborate the admission. During a three-day trial, which opened with Al Mahdi's statement, the Prosecutor presented the main evidence in its case. To assess whether Al Mahdi's admission of guilt was supported by the facts of the case pursuant to Article 65(1)(c) of the Statute, the Trial Chamber heard three witnesses and considered over seven hundred items of documentary

125. Prosecutor v. Al Mahdi, Case No. ICC-01/12-01/15-171, Judgment and Sentence, ¶ 22 (Sept. 27, 2016) [hereinafter *Al Mahdi*, Judgment], https://www.icc-cpi.int/CourtRecords/CR2016_07244.PDF [<https://perma.cc/Z4BC-AGX9>] (archived Dec. 29, 2017).

126. *Id.* at ¶¶ 31 & 33.

127. INT'L CRIM. CT., SITUATION IN MALI, ARTICLE 53(1) REPORT ¶ 2 (Jan. 16, 2013), https://www.icc-cpi.int/itemsDocuments/SASMaliArticle53_1PublicReportENG16Jan2013.pdf [<https://perma.cc/PC4R-23VY>] (archived Dec. 29, 2017).

128. *Al Mahdi*, Judgment, at ¶ 10 (Arrest warrant issued September 18, 2015 and charging document filed December 2015).

evidence.¹²⁹ The Prosecution's evidence against Al Mahdi included documents and witness statements, as well as satellite images from before and after the destruction; archive photographs taken at different times; audio recordings found on the internet containing statements from members of armed groups; video recordings on the internet which show the destruction at the time of the attack; a geolocation report from an expert witness, which made it possible to "locate with certainty" each video with regard to a precise mausoleum; an expert report ascribing dates and a time frame to the videos; 360-degree panoramic photographs; and scientific police reports which have been carried out on the scenes of destruction by ICC teams.¹³⁰ The evidence was agreed upon by the parties and therefore not challenged by the Defense. As the Senior Trial Lawyer explained in his opening statement:

In view of the guilty plea entered, the public must understand, therefore, today that the Prosecution does not intend to deal with each of the 700 pieces of evidence that have been filed before the Court, we will deal only with specific aspects; namely, starting with an interactive platform, the Prosecution will use satellite images, photographs, videos and other materials gleaned from the Internet which are included on the list of our evidence material to show the situation of the mausoleums before, during and after the destruction, including the participation of the accused.¹³¹

The Chamber issued its verdict a month after the trial, finding beyond reasonable doubt that the admission of guilt, together with the additional evidence, satisfied the essential facts to prove the alleged crimes and sentenced Al Mahdi to nine years.¹³²

2. Open Source Evidence

Of particular note in the *Al Mahdi* case was the amount of open source evidence presented, including satellite images from Google Earth, videos from YouTube, and audio clips found on the internet. Open source evidence is information collected from publicly available

129. *Id.* at ¶ 29 (714 items of documentary evidence).

130. Prosecutor v. Al Mahdi, Case No. ICC-01/12-01/15-T-4-Red-ENG, Transcript, 28-29 (Aug. 22, 2016) [hereinafter *Al Mahdi*, Opening Transcript], https://www.icc-epi.int/Transcripts/CR2016_05767.PDF [<https://perma.cc/6AEN-9DFL>] (archived Dec. 29, 2017).

131. *Id.* at 41.

132. *Al Mahdi*, Judgment, ¶ 43.

sources for trial purposes.¹³³ Since the conflict occurred in 2012, a time when use of mobile phones, digital cameras, satellites and drones were pervasive, even in a locality as remote as Timbuktu, the criminal acts, resulting damage, and intent of the parties were well documented. Ansar Dine, a terrorist group who, like many others, skillfully utilized modern technologies as part of their recruitment strategy and aggression tactics, deliberately made public statements explaining their intent and reasoning for destroying the mosques and mausoleums. Al Mahdi himself agreed to be interviewed by the press and allowed journalists to video record his team taking sledgehammers to the buildings. These video recordings were broadcast on television and some were uploaded onto the internet. At the same time, Timbuktu residents, in an effort to memorialize their cultural heritage and its razing, either with the hope of accountability for the perpetrators or for future reconstruction efforts, used their own hand-held devices to record the destruction and they too shared that footage with the world by uploading the videos to public websites.¹³⁴ As part of their investigation, OTP investigators scoured the internet for relevant information from their desks in The Hague. This allowed the investigation to progress even at times when the unpredictable security situation in Mali prevented their physical presence. The videos served as tools for identifying the buildings and their locations, pinpointing locations the investigators should visit as part of their due diligence, as well as ascertaining the identities of the perpetrators and potential witnesses who investigators should locate and interview. Thus, the open source information helped investigators run a more efficient and targeted investigation.

The Defense did not challenge the authenticity of the videos, agreeing to their admission as part of the terms of the guilty plea. Therefore, the Chamber was not forced to rule on their admissibility.¹³⁵ The Chamber could have required a higher threshold for the Prosecution to admit these items, but did not do so in this case. Open source derived information, such as social media videos, has yet to be intensely challenged as evidence in an international courtroom. For the YouTube videos and publicly available digital images found on the internet, the Prosecution used internal investigators to verify

133. Alexa Koenig, Felim McMahon, and Shikha Silliman Bhattacharjee, *Open Source Fact-Finding in Preliminary Examinations*, CILRAP (forthcoming 2018).

134. *See generally Al Mahdi*, Judgment.

135. *See generally id.*

the authenticity of the images by geolocating the landmarks in the images.¹³⁶ While the Prosecution made an effort to geolocate some of the open source videos and photographs, limited forensic analysis was admitted alongside. To authenticate and verify open source videos, investigators must determine whether or not they are fake. Videos may be considered “fake” or inauthentic for a number of reasons – they could be doctored, staged, or misleading or attached to misinformation.¹³⁷ In this case, the Prosecution focused on ascertaining the date, time and location, but did not show concern that the images and videos may be doctored or staged. In sticking with the standard from the ICTY, without any indication of fraud, the Prosecution need not take extra steps to verify that an image has not been falsified.

In addition to videos and images taken by persons on the ground, the Prosecution also relied on satellite images found on Google Earth. While the images were not challenged in this case, it is important to note some of the legal issues that may have been raised if the Defense had offered a challenge. In fact, there exist valid grounds upon which to challenge the admission of Google Earth images, particularly in the format presented by the Prosecution—a screenshot. The Prosecution was not required to take the additional step of seeking out the raw images from Google, question employees of Google Earth about their process, or verify on the ground the accuracy of the satellites used by Google Earth in that location and time. This is problematic because Google Earth positional accuracy is not fixed but varies from one time to another.¹³⁸ Variations may be the result of the process by which Google Earth updates its images, which involves periodically replacing old images with more recent or better resolution images.¹³⁹ The three-dimensional mapping that Google Earth uses takes flat images and shapes them onto sphere, essentially creating a patch work quilt of images that are stretched and sewn together to create the

136. See Elliot Higgins, *A Beginner's Guide to Geolocating Videos*, BELLINGCAT (July 2014), <https://www.bellingcat.com/resources/how-tos/2014/07/09/a-beginners-guide-to-geolocation/> [https://perma.cc/N3C5-G5S4] (archived Dec. 29, 2017) (Geolocation is the identification of the real life geographic location of a person, building, object, signal, or event. It often involves the analysis of visual information in an image along with any available metadata in order to match those visual cues and data with a confirmed location).

137. Nikita Mehandru and Alexa Koenig, *Open Source Intelligence and its Use in International Criminal Law* (forthcoming 2018).

138. Dr. Nagi Zomrawi Mohammed et al., *Positional Accuracy Testing of Google Earth*, 4 INT'L J. OF MULTIDISCIPLINARY SCI. & ENGINEERING 6, 6-9 (2013).

139. See generally *id.*

seamless scrolling function.¹⁴⁰ Since Google Earth was not made for the courtroom and is not required to be forensically sound, there are a number of variables that could impact the reliability of these images. The reliability of Google Earth images and the extracted positional data should be supported with field checks of the locations and corroborated with other evidence. Additionally, it would be best practice to acquire the original images directly from the source rather than taking screenshots because it is more reliable to uncover potential tampering with the primary image file. The unchallenged admission in this case of Google Earth images will not bar future challenges in other cases, but it may cause everyone from activists to criminal investigators to rely on this type of material when they should be taking a more critical stance against its admission as evidence.

3. Interactive Digital Platform

In addition to the source of the digital evidence in this case, the way it was presented is also noteworthy. In addition to mining photographs, satellite imagery, and video footage from the internet, the Prosecution sent a team to Timbuktu to produce their own images of the area.¹⁴¹ They used specialized technology to create 360-degree visuals. The imagery from all sources was compiled and used to create an interactive platform presentation.¹⁴² The platform was presented to the judges by the senior trial lawyer during his opening statement and then submitted to the Trial Chamber as evidence so that the judges could further explore the interactive platform in their own time. The creators of the platform were not called to testify to their process or methodology even though they handled the evidence. The senior trial lawyer explained that this interactive platform allowed the Prosecution to provide an optimal presentation of the various videos that were found on the internet.¹⁴³ Because they were dealing with so many different locations, the interactive platform presentation assisted the judges in seeing what occurred at each and every one of the

140. *See generally id.*

141. *See generally Al Mahdi*, Opening Transcript.

142. The creation of the interactive digital platform was outsourced to Situ Research, who provided its services pro bono. *See* Liz Stinson, *The Hague Convicts A Tomb-Destroying Extremist With Smart Design*, WIRED (Aug. 25, 2016) <https://www.wired.com/2016/08/hague-convicts-tomb-destroying-terrorist-smart-design/> [<https://perma.cc/F6L3-T3CS>] (archived Jan. 17, 2018).

143. *Al Mahdi*, Opening Transcript, at 44.

relevant locations.¹⁴⁴ This platform was demonstrative, so even though it was admitted as a separate item of evidence in addition to its individual components (i.e., images and videos), it was not necessarily attributed with evidentiary value. Demonstrative evidence, which includes diagrams, maps, drawings, graphs, animation, simulations, and models, is information to help the judges better understand the evidence, not evidence per se. While it was not an issue in this case because of the guilty plea, intentional or inadvertent bias in the presentation of these type of demonstrative visual representations raise significant fair trial issues, as does the exorbitant cost of creating such intricate presentation tools.¹⁴⁵ This platform was far more sophisticated than the visual representation created of the Institut of Bogoro in 2009. The interactivity of the platform is interesting, as it forces judges to engage with the evidence rather than being passive observers, which is a new development. Lawyers should be paying attention to the advantages that come with new digital tools for presenting evidence at trial while at the same time remaining wary of any potential biases in the software.¹⁴⁶

C. Evidence of offenses against the administration of justice

The final case, *Prosecutor v. Bemba et al*, is, again, a case of firsts for the International Criminal Court.¹⁴⁷ It is the first case involving the charge of offenses against the administration of justice.¹⁴⁸ It is also the first investigation to use an anonymous

144. *Al Mahdi*, Opening Transcript, at 69.

145. Interactive digital platform created by Situ Research and presented by the Senior Trial Lawyer in his opening statement for *Prosecutor v. Al Mahdi*. See *International Criminal Court, Case Against M. Al. Mahdi*, <http://icc-mali.situplatform.com/> [https://perma.cc/CA8Q-69DD] (last visited Jan. 17, 2018). In this particular case, the platform was from for the OTP, because Situ provided its services pro bono. However, the cost of this technical and labor-intensive work is generally high, and could be prohibitively costly for a defense team. See Stinson, *supra* note 142.

146. See generally Wexler, *supra* note 113.

147. See generally Dieneke De Vos, *Another first at the ICC: Convictions for offences against the administration of justice*, INTLAWGRRLS BLOG (Oct. 20, 2016), <https://ilg2.org/2016/10/20/another-first-at-the-icc-convictions-for-offences-against-the-administration-of-justice/> [https://perma.cc/5NS3-3NLU] (archived Jan. 22, 2018).

148. See generally *First ICC Witness Tampering Trial: All you Need to Know*, COALITION FOR THE INTERNATIONAL CRIMINAL COURT, <http://www.coalitionfortheicc.org/news/20150926/first-icc-witness-tampering-trial-all-you-need-know> [https://perma.cc/A9ZW-Z3T2] (archived Jan. 22, 2018). Four members associated with Bemba's Defence - Aimé Kilolo Musamba (Kilolo), Jean-Jacques Mangenda Kabongo (Mangenda), Fidèle Babala Wandu (Babala) and Narcisse Arido (Arido) – were charged with offences of corruptly

informant as a source of information, the first ICC case to use financial transactions as evidence, and the first case addressing important legal issues regarding attorney-client privilege and the right to privacy. Due to the nature of the charges, it was also a shorter investigation and trial than the majority of cases that preceded it. Before providing the case background, however, it is important to understand this case's relationship to another case, *Prosecutor v. Jean Pierre Bemba Gombo* ("Bemba" or "Main Case"), since the two are inherently linked.

1. Brief overview of the Main Case

During 2002-2003, an armed conflict took place in the Central African Republic between the Central African governmental authorities, supported by the MLC, and an organized armed group of rebels led by General Bozize.¹⁴⁹ Jean-Pierre Bemba Gombo, a Congolese citizen, was the MLC President and Commander-in-Chief of the ALC, the organization's figurehead, and source of its funding, goals and aims. During the conflict, MLC soldiers directed widespread attacks against the civilian population under Bemba's command.¹⁵⁰ In May 2007, the Office of the Prosecutor, at the request of the Government of the Central African Republic (CAR), launched an investigation concerning the crimes alleged to have been committed in CAR.¹⁵¹ A little over a year later, the Pre-Trial Chamber issued an arrest warrant for Bemba who was residing in Belgium where he was arrested. Bemba was subsequently transferred to The Hague and charged with war crimes and crimes against humanity

influencing witnesses, presenting false evidence and giving false testimony when under an obligation to tell the truth, within the meaning of Article 70(1)(a) to (c) of the Rome Statute. See *Case Information Sheet, The Prosecutor v. Jean-Pierre Bemba et al.*, INTERNATIONAL CRIMINAL COURT (March 2017), <https://www.icc-cpi.int/car/Bemba-et-al/Documents/Bemba-et-alEng.pdf> [<https://perma.cc/SGA8-3NXE>] (archived Jan. 22, 2018).

149. ICC press release, *ICC Trial Chamber III declares Jean-Pierre Bemba Gombo guilty of war crimes and crimes against humanity* (Mar. 21, 2016), <https://www.icc-cpi.int/Pages/item.aspx?name=pr1200> [<https://perma.cc/66KK-UBVU>] (archived Jan. 17, 2018).

150. *Prosecutor v. Bemba*, Judgment pursuant to Article 74 of the Statute, ICC-01/05-01/08-3343 (Mar. 21, 2016), ¶ 1, https://www.icc-cpi.int/CourtRecords/CR2016_02238.PDF [<https://perma.cc/C34U-HLS4>] (archived Jan. 17, 2018).

151. *Case Information Sheet, The Prosecutor v. Jean-Pierre Bemba Gombo*, INTERNATIONAL CRIMINAL COURT (Jan. 5, 2018), <https://www.icc-cpi.int/iccdocs/PIDS/publications/BembaEng.pdf> [<https://perma.cc/D2RV-CXQ2>] (archived Jan. 17, 2018).

under the principle of command responsibility.¹⁵² The Pre-Trial Chamber also issued a decision to request the identification, tracing, freezing and seizure of the property and assets of Bemba by national authorities.¹⁵³ Charges against Bemba were confirmed in June 2009 and the trial opened on November 22, 2010. While the trial was ongoing, the Office of the Prosecutor received an anonymous email providing information concerning an alleged witness bribery scheme orchestrated by Bemba and his defense council to influence the testimony of witnesses against Bemba.¹⁵⁴ This email tip is where the second case, *Prosecutor v. Bemba et al* (“*Bemba et al*” or “Article 70 Case”) begins.¹⁵⁵

2. Case Background

The anonymous tip launched a new investigation into the interference with witnesses in the Main Case, which proceeded while the first trial was still in progress.¹⁵⁶ Due to the nature of the second case, there is no public decision regarding the opening of an official Article 70 investigation, but it is known that the investigation began while the Prosecution was still presenting its case-in-chief. There were essentially three main prongs to this investigation – surveillance of email and telephone communications, “following the money,” and getting cooperation from the scheme’s insiders – which resulted in a high amount of non-testimonial evidence.¹⁵⁷ In many ways this investigation was more akin to a national public corruption case than a traditional international criminal justice case. Finding that there was truth to the allegation, and after collecting evidence with the help of national law enforcement partners, the Prosecution submitted an application in November 2013 for an arrest warrant against Bemba, his lawyer Kilolo, and three others for their involvement in the crime

152. *Id.*

153. *Id.*

154. *Id.*

155. Article 70 of the Rome Statute proscribes the crime of offenses against the administration of justice, which is why this case is often referred to as the Article 70 case, Bemba Article 70, or CAR Article 70. *See* Rome Statute of the International Criminal Court art. 70, July 17, 1998, 2187 U.N.T.S. 90.

156. *See* Prosecutor v. Bemba et al., Case No. ICC-01/05-01/13, Second Decision on the “Defence request for disclosure” submitted by the Defence for Jean-Pierre Bemba on 20 February 2014 and relating filings, ICC-01/05-01/13-298 (Mar. 27, 2014), <http://www.legal-tools.org/doc/c43642/pdf/> [<https://perma.cc/P3RA-4R9Z>] (archived Jan. 17, 2018) (discussing whether anonymous informant must be disclosed).

157. *Bemba*, Judgment, ¶ 209.

of witness interference.¹⁵⁸ It is significant that these allegations were pursued and made it to trial, since there had been issues in almost all previous cases with witness interference, including cases from the Democratic Republic of Congo, Kenya, and Cote d'Ivoire. The closing statements in the Main Case were given on November 12, 2014.¹⁵⁹ The verdict was still outstanding when the second trial for the Article 70 case opened on September 29, 2015. In *Bemba et al*, the Prosecution introduced a high number of items of non-oral evidence, including evidence documenting money transfers through Western Union provided by the Austrian authorities, and evidence of telephone communications provided by Dutch authorities and the ICC Detention Centre.¹⁶⁰ The Defense challenged the admissibility of the Western Union Documents, the provenance of recorded and intercepted telephone calls, text messages (SMS), and emails on a number of grounds including improper procedure in their collection and violation of the Accused's right to privacy.¹⁶¹ The Chamber admitted the evidence, but provided valuable reasoning explaining the importance of the right to privacy when considering the admission of these sorts of materials.¹⁶²

3. Digital Financial Evidence

Financial investigations are not new, but are growing in importance for all sorts of criminal investigations in national and international jurisdictions, particularly those involving corruption. A wire transfer is a method of moving electronic funds from one person or entity to another, a service that began with the establishment of the first Western Union in 1872. The first online banking services started in New York in the 1980s, but were not offered to the public through

158. *Case Information Sheet, The Prosecutor v. Jean-Pierre Bemba Gombo, Aimé Kilolo Musamba, Jean-Jacques Mangenda Kabongo, Fidèle Babala Wandu and Narcisse Arido*, INTERNATIONAL CRIMINAL COURT (March 2017), <https://www.icc-cpi.int/car/Bemba-et-al/Documents/Bemba-et-alEng.pdf> [<https://perma.cc/YQG4-GSZF>] (archived Jan. 17, 2018).

159. *Id.*

160. *See generally Bemba*, Judgment.

161. *Id.*

162. *Bemba*, Decision on Exclusion of Western Union Documents, ¶¶ 46-61. This reasoning will likely inform future decision on digital evidence, since, as Sean Goodison explains, digital information is more personal and sensitive, and will raise more privacy implications. *See* SEAN E. GOODISON, ET AL., PRIORITY CRIM. JUST. INITIATIVE, DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM: IDENTIFYING TECHNOLOGY AND OTHER NEEDS TO MORE EFFECTIVELY ACQUIRE AND UTILIZE DIGITAL EVIDENCE 3 (2015).

mobile devices until 1999.¹⁶³ Technology facilitating the transfer and exchange of money is one that, while always evolving, has undergone substantial development since the invention of smart phones after 2010.¹⁶⁴ Rather than giving cash bribes, the Accused in this case used Western Union to transfer funds, which created a record and, in turn, irrefutable evidence of the transactions.

To prove the money transfers between the accused and the witnesses the Prosecution presented financial records (“Western Union Documents”) provided by the Austrian authorities. These records listed money transfers effected through Western Union that indicate the sender’s name, the amount, the date and time of the transfer, the sender’s telephone number, as well as the name and telephone number of the recipient and the date and time on which the money was collected. The Defense never challenged the reliability and accuracy of the information contained in these records, but objected to their admissibility under Article 69(7) of the Statute on the grounds that they were obtained in breach of national laws and the internationally recognized human right to privacy of the accused.¹⁶⁵ The defense teams filed a joint request to declare the Western Union Documents inadmissible, submitting that due to the specific circumstances in which the Western Union Documents were collected, their admission into evidence would be antithetical to and would seriously damage the integrity of the proceedings in the sense of Article 69(7)(b) of the Statute.¹⁶⁶ The Chamber decided to rule on the application for exclusion of this particular evidence during trial as an exception to the decision to defer its assessment of the admissibility of evidence until deliberating its judgment.¹⁶⁷ The Chamber rejected these objections, yet declared that the right to privacy is an internationally recognized human right.¹⁶⁸ The Chamber

163. See Ruth Sarreal, *History of Online Banking: How Internet Banking Became Mainstream*, GO BANKING RATES (Oct. 7, 2016), <https://www.gobankingrates.com/banking/history-online-banking/> [<https://perma.cc/7ARZ-QHC8>] (archived Dec. 29, 2017).

164. See *id.*

165. *Bemba*, Judgment, ¶ 211.

166. *Bemba*, Decision to Exclude Western Union Documents, ¶ 14.

167. Prosecutor v. Bemba, Case Nos. ICC-01/05-01/13-1013-Red, ICC- 01/05-01/13-1113-Red, ICC-01/05-01/13-1170-Conf, Decision on Prosecution Requests for Admission of Documentary Evidence, ¶¶ 9, 13 (Sept. 24 2015) [hereinafter *Bemba*, Decision on Prosecution Requests], <https://www.icc-cpi.int/Pages/record.aspx?docNo=ICC-01/05-01/13-1285> [<https://perma.cc/VF8H-MC2C>] (archived Dec. 29, 2017).

168. See Universal Declaration of Human Rights, art. 12, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948); Convention for the Protection of Human Rights and Fundamental

explained that the right to privacy includes financial information such as data kept by banks and, by extension, by financial service companies such as Western Union, and affirmed that the right to privacy is one that may not be interfered with except “in accordance with the law.”¹⁶⁹ Thus, procedural safeguards are necessary before investigators can seize such materials. Based on the facts of this case, the Chamber concluded that the measures taken by the authorities were in fact governed by the Statute and the Rules since proper procedural safeguards were in place.¹⁷⁰ The Chamber formally submitted the financial records emanating from Western Union during trial¹⁷¹ and heard testimony from a Western Union representative who served as the Prosecution’s point of contact.¹⁷² The Chamber relied on the Western Union Documents primarily to corroborate other evidence concerning payments, in particular witness testimonies.¹⁷³

Freedoms art. 8, Sept 3, 1953, 213 U.N.T.S. 262; International Covenant on Civil and Political Rights, art 17, Dec. 16, 1966, S. Treaty Doc. No. 95-20, 6 I.L.M. 368 (1967), 999 U.N.T.S. 171; American Convention on Human Rights, art. 11, Nov. 21, 1969, 1144 U.N.T.S. 143; League of Arab States, Arab Charter of Human Rights, art. 21, May 22, 2004; *Bemba*, Decision to Exclude Western Union Documents.

169. See Convention for the Protection of Human Rights and Fundamental Freedoms *supra* note 168, at art. 8(2); *M.N. and others v. San Marino*, 28005/12 Eur. Ct. H.R. at ¶ 51-53 (2015). Interference with this right is subject to other requirements, such as the interference being “necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country,” but there is no argument in the present case that any privacy rights have been violated in these respects.

170. Prosecutor v. Bemba, Case No. ICC-01/05-01/13, Decision on Kilolo Defence Motion for Inadmissibility of Material, ¶¶ 16-21 (Sept. 16, 2015), <https://www.icc-cpi.int/pages/record.aspx?uri=2060859> [<https://perma.cc/6VL7-6JH7>] (archived Dec. 29, 2017).

171. See generally *Bemba*, Decision on Prosecution Requests, at ¶¶ 9-17 (explaining that the Chamber will consider the relevance, probative value and potential prejudice of submitted items in its judgments pursuant to Article 74(2) and will recognize items as “formally submitted” and discussed within the meaning of Article 74(2) of the Statute).

172. Prosecutor v. Bemba, Case Nos. ICC-01/05-01/13-T-33-ENG, ICC-01/05-01/13-T-34-Conf-ENG, ICC-01/05-01/13-T-35-Conf-ENG, Transcripts of hearings on 2, 3 and 4 November 2015 (Nov. 2-4, 2015), <https://www.icc-cpi.int/Pages/record.aspx?docNo=ICC-01/05-01/13-T-33-ENG> [<https://perma.cc/ASY2-ZZX6>] (archived Dec. 29, 2017), <https://www.icc-cpi.int/Pages/record.aspx?docNo=ICC-01/05-01/13-T-34-Red-ENG> [<https://perma.cc/T22A-UETH>] (archived Dec. 29, 2017), <https://www.icc-cpi.int/Pages/record.aspx?docNo=ICC-01/05-01/13-T-35-Red-ENG> [<https://perma.cc/UM4H-2DX8>] (archived Dec. 29, 2017).

173. *Bemba*, Judgment, ¶ 210.

4. Telecommunications and Intercept Evidence

The telephone communications evidence presented in *Bemba et al* included both call data records with metadata regarding the telephone use, as well as intercepts with the content of the communications between parties introduced as digital audio-recordings. As in *Ayyash et al*, the Prosecution presented a series of ‘call sequence tables’ indicating the date, numbers involved and the source from which the information was collected in order to prove communications among the accused or between the accused and witnesses.¹⁷⁴ The attribution of the telephone numbers to the individuals concerned was demonstrated by indicating the number and the name. The contacts between particular individuals were set out in chronological order.

One difference from the use of telecommunications evidence in *Ayyash et al* is that this case focused on the numbers and frequency of contacts, and did not use any geolocation data. The call data records were introduced through bar table motion, and no employee of the communications service provider was required to testify.¹⁷⁵ What this example indicates, perhaps, is that the defense may be more willing to accept metadata about numbers and frequency of calls from CSPs, but will want to challenge the technology used to geolocate users based on signals to cell tower sites since there is more room for interpretation in the way this is done by experts.

An analyst from the Office of the Prosecutor, who was responsible for preparing the call sequence tables, testified in court. In addition to the tables, the Prosecution presented call data records (‘CDRs’) of national, private telecommunication companies.¹⁷⁶ The Prosecution also introduced expert testimony on the CDR.¹⁷⁷ Where national authorities intercepted communications, audio recordings, together with corresponding call logs, were submitted.

Finally, the Prosecution presented call logs and audio recordings emanating from incoming and outgoing communications from the ICC Detention Centre between Bemba and others.¹⁷⁸ One issue that

174. *Id.* at ¶ 213.

175. *See generally* Prosecutor v. Bemba et al., Prosecution’s First Request for the Admission of Evidence from the Bar Table, Case No. ICC-01/05-01/13-1013-Red (June 16, 2015).

176. *Id.* at ¶ 214.

177. *Id.* at ¶ 221.

178. *Id.* at ¶ 215.

came up with the recordings from the detention center was that the two sides of the call were separated. Therefore, an analyst had to edit together a cohesive conversation in order for it to make sense. The Defense challenged this, but the Chamber was not persuaded by their argument that the recording was unreliable. The Chamber was able to apply common sense and logic to understand the conversation came together and were conscious of any shortcomings.

The Defense objected to the use of these communications and corresponding logs on grounds that the Prosecution had failed to sufficiently establish their authenticity and chain of custody and that the Prosecution did not call a witness to authenticate recordings or intercepted communications.¹⁷⁹ The Chamber did not buy this argument because there was an “array of mutually reinforcing information confirming the accuracy of the intercepted communications and their corresponding logs.”¹⁸⁰ The Chamber further noted that some communications and logs had inherent indicia of authenticity such as corporate watermarks of the telecommunications provider.¹⁸¹ It is significant to note that the Chamber did its own analysis rather than taking the Prosecution’s word. According to its judgment in the case, the Trial Chamber did its own verification in order to confirm the Prosecutor’s findings. “When determining the relevant details of the telephone communications, such as the speakers, relevant numbers and the date of the call, the Chamber has conducted its own independent assessment of the evidence.”¹⁸² Seeing the judges making an effort to engage with the evidence is a positive sign. Similar to the *Al Mahdi* case, the digital evidence enabled the judges to take a more active role in examining and engaging with the evidence.

5. Digital Communications Evidence

During the investigation, the prosecutor’s office confiscated Bemba’s laptop and cellular phone in the Detention Center and extracted emails and other digital documents. The Prosecution introduced into evidence an email from one of the accused, Arido, to one of the witnesses in which he cautioned the witness about using social media, stating that they should communicate outside

179. *Id.* at ¶ 217.

180. *Id.* at ¶ 218.

181. *Id.* at ¶ 219.

182. *Id.* at ¶ 216.

“facebook”.¹⁸³ The Defense argued that the Prosecution had not provided sufficient information concerning the provenance or attribution of the emails it wished to admit, and therefore should be excluded. Further, the Defense argued that the contents of these emails revealed no impropriety, stating that it was “highly concerning that the Prosecution sought to infer wrongful conduct from a caution to witnesses to avoid using Facebook, when such a caution is required by ICC best practices for witness protection.”¹⁸⁴

Despite cautions not to use Facebook, the investigators found evidence on Facebook in the form of four photographs that were used to link individuals and corroborate other evidence. The four photographs were allegedly extracted from the Facebook pages of a defense witness and a prosecution witness. The defense argued that the photos were not *prima facie* authentic or reliable “because the Prosecution provided no material supporting the attribution of the Facebook pages.” Since the creation of a Facebook account does not require valid and verifiable identification, the defense argued that it was not possible to ascertain that a Facebook account under a certain name is attributable to that person.¹⁸⁵ The prosecution argued that they are *prima facie* reliable and authentic. In its final judgment, the Trial Chamber did not address these photographs from Facebook, giving no clear ruling either way. This is likely because the facts that photos were submitted to prove was proved through other evidence, such as witness testimony admitting that a relationship between the individuals pictured existed. The Chamber did not need to address the admissibility of these photos, since they were not relevant to its decision, thus kicking the can down the line to future Chambers to decide on the admissibility of social media photos, perhaps in a case where they play a more significant role in directly proving the elements of the crimes. While this case did not provide jurisprudence on the admissibility of social media photo or answer questions on how investigators and lawyers should view this sort of information

183. *Id.* at ¶ 675.

184. Prosecutor v. Bemba, Case No. ICC-01/05-01/13-1245, Public Redacted Version of Defense Response to Prosecution’s Third Request for the Admission of Evidence from the Bar Table, ¶. 44 (Oct. 9, 2015) [hereinafter *Bemba*, Defense Response to Third Request for Admission of Evidence], <https://www.icc-cpi.int/pages/record.aspx?uri=2085491> [https://perma.cc/CKK9-J4HS] (archived Dec. 29, 2017).

185. *Bemba*, Defense Response to Third Request for Admission of Evidence, ¶¶ 83-84; This is not entirely true, since Facebook requests identification and takes steps to eliminate anonymous or fake users from its website.

(i.e., as lead information only, for corroboration, or as direct evidence), it is likely that those answers will come very soon. As discussed in the next Part, the international criminal cases on the horizon involve significantly more of these newer types of evidence.

IV. THE FUTURE OF EVIDENCE IN WAR CRIMES PROSECUTIONS

The cases in Part III suggest that digital technologies are profoundly changing international criminal investigations and prosecutions in two distinct ways: (1) the data and digital information produced by the use of digital devices has created a new and fruitful body of potential evidence; and (2) new technologies are changing the landscape of evidence presentation. In looking towards future cases, it is clear that digital evidence will be increasingly relied upon, which means prosecutors, investigators, defense attorneys, and judges all need to be prepared.

As of this writing, there are three trials underway at the ICC – *Prosecutor v. Laurent Gbagbo and Charles Blé Goudé*, *Prosecutor v. Bosco Ntaganda*, and *Prosecutor v. Dominic Ongwen*.¹⁸⁶ These cases all deal with crimes committed before 2012, and thus at a time when digital communication, especially over social media, was less prevalent than it is today, and when investigators had less access to remote sensing technologies. There are currently no other accused persons in custody in The Hague, and so there is no trial on deck. However, the ICC website lists that there are open investigations in ten countries and preliminary examinations in ten other countries.¹⁸⁷ When considering the potential for digital evidence in some of the preliminary examinations, there are a few notable situations, such as conflicts in Ukraine, Iraq, and Afghanistan. The wars in both Iraq and Afghanistan are marked, in particular, by the expansive use of drone technologies for both surveillance and weaponry.¹⁸⁸ In the past, covert

186. *The Prosecutor v. Laurent Gbagbo and Charles Blé Goudé*, Case No. ICC-02/11-01/15; *The Prosecutor v. Bosco Ntaganda*, Case No. ICC-01/04-02/06; *The Prosecutor v. Dominic Ongwen*, Case No. ICC-01/04-01/15.

187. See *Situations under investigation*, INT'L CRIM. CT., <https://www.icc-cpi.int/pages/situations.aspx> [<https://perma.cc/Q2MA-97QD>] (last visited Dec. 29, 2017); *Preliminary examinations*, INT'L CRIM. CT., <https://www.icc-cpi.int/pages/preliminary-examinations.aspx> [<https://perma.cc/4S4R-BS28>] (last visited Dec. 29, 2017).

188. See Josh Smith, *Exclusive: Afghan drone war - data show unmanned flights dominate air campaign*, REUTERS (Apr. 20, 2016), <https://www.reuters.com/article/us-afghanistan-drones-exclusive/exclusive-afghan-drone-war-data-show-unmanned-flights->

surveillance would have to be conducted by a person on the ground, forced to keep a low profile due to the risk of detection and security concerns. This placed a high burden and responsibility on the surveilling individual to make decisions based on the apparently available information. If actions were taken, that person's testimony would serve as the primary evidence. With the use of drones, which can surveil targets from above with little risk of detection, multiple investigators or officers in the military can watch the same feed and conduct surveillance without increasing the risk of detection.¹⁸⁹ Drones can go where humans cannot, and high-resolution telephoto lenses on drones can magnify the images, giving investigators a closer look.¹⁹⁰ When drones are used in this manner, they are not simply providing a live feed, but also creating a digital record of the footage that can be reviewed later or even used as evidence in court. In modern conflict zones, military are equipped with a variety of digital devices providing information about their movements on the ground. In addition, civilians in and around conflict zones have cell phones. Between the satellites monitoring of a situation from space, drones observing the situation from above, and persons recording the situation on the ground, there is enough imagery and footage to portray modern conflict situations from all angles and at all times. If judges need to assess whether certain actions taken by investigators or officers in the military were reasonable based on the information available to them, they can review the drone or cell phone footage rather than relying on testimony.

Another conflict situation for which there is likely to be significant evidence and leads provided for in the digital or cyber space is Ukraine, a conflict in which Russian is potentially implicated.¹⁹¹ While there is not much information on the ICC's preliminary examination, which focuses on the alleged crimes committed in the context of the "Maidan" protests since November

dominate-air-campaign-idUSKCN0XH2UZ [https://perma.cc/NKP9-PQD5] (archived Jan. 17, 2018); Drones Operating in Syria and Iraq, CENTER FOR THE STUDY OF THE DRONE AT BARD COLLEGE (Dec. 13, 2016), <http://dronecenter.bard.edu/drones-operating-in-syria-and-iraq/> [https://perma.cc/RZ8L-7VRK] (archived Jan. 17, 2018).

189. *A guide to military drones*, DW, <http://www.dw.com/en/a-guide-to-military-drones/a-39441185> [https://perma.cc/JP3X-4LUB] (last visited Jan. 17, 2018).

190. *Id.*

191. See, e.g., CHAPTER 4 in DAVID PATRIKARAKOS, WAR IN 140 CHARACTERS: HOW SOCIAL MEDIA IS RESHAPING CONFLICT IN THE TWENTY-FIRST CENTURY, DISCUSSION ON THE USE OF FACEBOOK AS A DIGITAL PLATFORM TO MOBILIZE THE EUROMAIDAN PROTESTERS (2017).

21, 2013 and other events in Ukraine since February 2014,¹⁹² there is another investigation related to Ukraine, which may provide some insights into what can be expected for the ICC's investigation. On July 27, 2014, Malaysia Airlines flight MH17 from Amsterdam to Kuala Lumpur crashed in eastern Ukraine.¹⁹³ 196 Dutch nationals were among the 298 passengers and crewmembers.¹⁹⁴ In response, a Joint Investigative Team (JIT) was created to look into the incident and identify those responsible.¹⁹⁵ While this case has not yet gone to trial, much of the evidence and findings of the investigation have been published, attributing responsibility to Russia. In the presentation of their findings, they refer to significant quantities and types of digital evidence use in the investigation including Facebook profiles, chat room conversation, cell phone photos, street view images, cell phone videos uploaded to the internet and other open source information, telecom data and telephone wiretaps, and a geographic information system to capture, store, manipulate, analyze, manage, and present relevant geospatial data. The presentation, which can be found online, is slick and compelling, showing how they linked all the information, much of which was publicly available together.¹⁹⁶ The MH17 investigation, while not a case involving Rome Statute crimes, is a perfect example of what lawyers and judges can expect to see in the courtroom in the near future.

On August 15, 2017, the ICC released a new public arrest warrant in the Situation in Libya against Mahmoud Mustafa Busayf Al-Werfalli based in large part on videos of executions found on social media websites.¹⁹⁷ International criminal justice has seen the first “documentary trial” at Nuremberg, the “media case” at the ICTR, and the “cell phone case” at the STL. With this new arrest warrant,

192. ICC Report on Preliminary Examination (Nov. 14, 2016), ¶ 146, https://www.icc-cpi.int/iccdocs/otp/161114-otp-rep-PE_ENG.pdf [<https://perma.cc/ARN5-HHTJ>] (archived Jan. 17, 2018).

193. *MH17: The Open Source Investigation Three Years Later*, BELLINGCAT REPORT at 1, <https://www.bellingcat.com/wp-content/uploads/2017/07/mh17-3rd-anniversary-report.pdf> [<https://perma.cc/K53C-5CD3>] (last visited Jan. 17, 2018).

194. *Id.*

195. *MH17 Crash*, OPENBAAR MINISTERIE, <https://www.om.nl/onderwerpen/mh17-crash/> [<https://perma.cc/YG75-HPGV>] (last visited Jan. 17, 2018).

196. See Joint Investigation Team, *JIT presents first results of criminal investigations of MH17 crash*, YOUTUBE (Sept. 28, 2016), https://www.youtube.com/watch?v=2BtBEV_rAd0.

197. Prosecutor v. Al-Werfalli, Case No. ICC-01-11-01/17-2, Public Warrant of Arrest (Aug. 15, 2017), https://www.icc-cpi.int/CourtRecords/CR2017_05031.PDF [<https://perma.cc/XX5Y-DWXX>] (archived Dec. 29, 2017).

there is now the first “social media case”. In fact, initial blog posts and commentaries on the Al-Werfalli arrest warrant are already dubbing it as such.¹⁹⁸ Talking about technology and digital evidence in war crimes prosecutions is no longer a forecast or a hypothetical. It is here.

In addition to the docket at the ICC, there are current conflicts beyond the ICC’s reach that may nevertheless end up litigated in an international tribunal. The most prominent of these is Syria. The conflict in Syria has been referred to as the “crisis of our generation,” and the international justice community has kept a watchful eye on it for years. The ICC does not have jurisdiction over this conflict.¹⁹⁹ However, that has not stopped international investigators and lawyers from outside the ICC from taking action. A number of organizations such as the Syrian Archive and the Commission for International Justice and Accountability (“CIJA”) have engaged in evidence collection, even though there is not yet a forum to receive that evidence for prosecution.²⁰⁰ CIJA has used willing activists to smuggle over 50,000 photos and documents out of Syria. The Syrian Archive has been collecting and preserving social media videos and other online content documenting the conflict. The mass flow of information is a defining characteristic of the war in Syrian. Citizen journalism has exploded in the Middle East as a way to counter oppressive regimes and, as a result, there is a vast amount of relevant open source content available. How to channel the mass information available into a court of law in order to get accountability is a problem that needs solving. In December 2016, the United Nations Security Council passed a resolution to establish a new International,

198. See Alex Whiting, *The ICC’s New Libya Case: Extraterritorial Evidence for an Extraterritorial Court*, JUST SECURITY (Aug. 23, 2017), <https://www.justsecurity.org/44383/iccs-libya-case-extraterritorial-evidence-extraterritorial-court/> [<https://perma.cc/3963-2JGB>] (archived Jan. 17, 2018); Emma Irving, *And So It Begins . . . Social Media Evidence In An ICC Arrest Warrant*, OPINIO JURIS, <http://opiniojuris.org/2017/08/17/and-so-it-begins-social-media-evidence-in-an-icc-arrest-warrant/> [<https://perma.cc/QUZ9-9YP3>] (last visited Jan. 17, 2018).

199. At least not without a referral from the United Nations Security Council, which is a non-starter because of the Russian veto.

200. Ben Taub, *The Assad Files*, THE NEW YORKER (Apr. 18, 2016), <https://www.newyorker.com/magazine/2016/04/18/bashar-al-assads-war-crimes-exposed> [<https://perma.cc/9B9K-BDMS>] (archived Jan. 17, 2018). CIJA does not have a website, as they keep a low profile, but you’ll find mention of the operations here: Mark Kersten, *What Counts as Evidence of Syria’s War Crimes?*, JUSTICE IN CONFLICT (Oct. 29, 2014), <https://justiceinconflict.org/2014/10/29/what-counts-as-evidence-of-syrias-war-crimes/> [<https://perma.cc/WP9U-GRBD>] (archived Jan. 22, 2018).

Impartial and Independent Mechanism (“IIIM”) to collect and analyze evidence of mass atrocities and human rights violations in Syria. While the Mechanism will not have the power to prosecute cases, its creation brings the international community a step closer to justice. The conflict in Syria is the most documented conflict in history, with more hours of video footage of the conflict than the conflict itself.²⁰¹ The Libya and Syria cases demonstrate that *Ayyash et al*, *Al Mahdi*, and *Bemba et al* are not anomalies or temporary deviations, but rather the first in a growing trend.

A. Considerations for international criminal law practitioners

The amount of available data will grow exponentially with increased connectivity and integration of portable electronics.²⁰² This is a blessing but also a curse because the sheer quantity has the potential to overload investigative resources and create an unmanageable digital evidence backlog.²⁰³ With constant changes in technology, international investigators and prosecutors must continually adapt their policies and practices to address novel legal issues involving digital evidence. International criminal investigators, lawyers, and judges must be constantly learning to stay up to date with new technologies and devices, as well as developments in how existing technologies are being used and adapted.²⁰⁴

The near universal adoption and technical improvements of cell phones, coupled with the faster change and development of technology itself have at the same time increased uncertainty. The positive aspect for international criminal lawyers is that they are accustomed to uncertainty, since the international criminal legal field has always presented, in many ways, an uncertain terrain. The ICC can both learn from and contribute to the understanding and use of digital evidence in national jurisdictions. New types of digital evidence and technologically produced and stored data are valuable to court proceedings, but may require modified standards for admissibility in order to protect the fairness of proceedings and the interests of justice. Difficult issues will almost certainly have to be confronted, especially those concerning rights of privacy. *Bemba et*

201. Koenig, *supra* note 133.

202. *See generally* GOODISON, ET AL., *supra* note 162.

203. *Id.*

204. *Id.*

al. was just the first such case. Privacy concerns are far greater and more salient with digital evidence than with analog evidence.²⁰⁵ Ensuring that parties and judges fully understand how digital evidence is authenticated and verified may require laborious testimony from experts. Digital tools for presentation of evidence, while effective, will need a closer and more critical look into their potential for bias and issues of equality.

Major developments in the information technology landscape over the past two decades have made the collection and analysis of digital evidence an increasingly important tool for solving crimes and preparing court cases. The ability of lawyers and judges to embrace these new types of evidence and understand these new technologies may ultimately determine whether international criminal justice is here to stay.

Digital evidence exploitation is a skill all investigators should have and all criminal lawyers should understand. While it is undeniable that these new types of evidence are useful and will inevitably make their way into the courtroom, their introduction should be deliberate, educated, and cautious. Thus, there are three issues of which to stay particularly vigilant: the fairness of proceedings, the equality of arms, and the balancing of resources. Open source investigations are cheap but the evidentiary value of this material is still considered low, while other investigative methods such as forensic missions might lead to probative evidence, but at a prohibitively high cost. It will be essential for the fairness of proceedings for the Prosecution to involve the defense earlier in the process and analysis of raw data.

Past articles that have been written on digital evidence in national or international jurisdictions share similar recommendations about creating standards and providing additional training. While these are constructive recommendations, they fail to address the rapid rate of change in digital technology. The speed of growth and change is itself accelerating, and lawyers and investigators need to be more agile than ever to stay current. By the time standard operating procedures are created for handling digital evidence in its present state and relevant actors are trained on existing technologies, there will already be a new backlog of issues and challenges to address. Instead of being reactionary, lawyers and investigators need to get

205. GOODISON, ET AL., *supra* note 162.

ahead of the curve and will have to look towards the future and think about how they themselves can innovate and utilize new technologies.

V. CONCLUSION

In examining the Prosecution's evidence in the three case examples above, one thing is clear: witness testimony is no longer the only critical body of proof. In *Ayyash et al*, the defendants were identified through their use of cellular phones in the planning and preparation of the attack on Beirut. In *Al Mahdi*, the defendant was identified through video footage for which he willingly posed and which he himself posted to social media as propaganda and promotion of Ansar Dine's attack on cultural heritage sites in Timbuktu. In *Bemba et al*, the defendants were identified through their use of cellular phones and emails to communicate and the wire transfers made to supply the funds to carry out their crimes. In all three cases it was the technological tools that the accused themselves used to facilitate their criminal activities that allowed investigators to identify them and created the evidence used by prosecutors to prove their culpability beyond reasonable doubt. Investigators and prosecutors do not get to determine what evidence is available for them to collect and use – the criminals do. As long as criminals are operating in the modern world and relying on technology to facilitate their criminal conduct, evidence of their crimes will inevitably be, to some extent, digitally recorded.

The arena in which technology, international human rights, and criminal prosecution intersect is new and growing. The first international cases dealing with digital evidence have come to trial in the last few years, which marks the beginning of what will soon be the norm for international criminal cases. This topic can no longer be thought of as an area of specialization for which one knowledgeable individual is brought into court because he or she possesses the requisite area of expertise. Just as the investigators, prosecutors, defense attorneys and judges at Nuremberg, the ad hoc tribunals, the hybrid tribunals and the ICC had to become experts in how to collect, preserve, and present documents, physical evidence, and forensic expert reports for past cases, all practitioners in the international criminal justice field should be enhancing their technical understanding of new digital technologies and should be cultivating a deeper social understanding of how social media and other digital communications are being used in conflict zones.

