Finding the Signal in the Noise

International Criminal Evidence and Procedure in the Digital Age

Lindsay Freeman* and Raquel Vazquez Llorente**

Abstract

The constituent documents of the International Criminal Court (ICC) were formulated in the 1990s, at a time when the internet was still relatively new to most of society. In the four years between the signing of the Rome Statute in 1998 and its entry into force in 2002, there was a surge in technological development. The replacement of dial-up connections by home broadband and wireless internet, the commercial launch of 3G, and the introduction of camera phones all took place during that period, followed only a few years later by the founding of Google, YouTube and Facebook. This trend has only continued. Advanced technologies have changed the way in which societies create information and share it, generating an ever-growing volume of data. The availability and accessibility to new sources of information open up opportunities for international criminal investigators, but the task of using them effectively is not without its challenges. Recent cases before the ICC indicate that digital evidence will play an increasingly central role in investigations and prosecutions. In national jurisdictions, digital evidence is now introduced in the majority of criminal cases, and there have been significant reforms in

* Law and Policy Director, Technology and Human Rights Program, Human Rights Center, UC Berkeley School of Law, USA; Member of the Pacific Council on International Policy and ABA's International Criminal Justice Standards Advisory Group; Member of the Technology Advisory Board of the ICC. [lfreeman@berkeley.edu]

** FIDH's Permanent Representative to the ICC; Member of the Technology Advisory Board of the ICC. At the time of writing, she was Senior Legal Advisor, eyeWitness to Atrocities – International Bar Association, and Research Visitor at the Bonavero Institute of Human Rights, Faculty of Law, University of Oxford (2019–2020). [rvazquezllorente@fidh.org]

The views in this article are those of the authors and do not reflect the views of the International Criminal Court or any other organization. The authors would like to thank Alexa Koenig, Alex Whiting, Megan Hirst, Wendy Betts and Yvonne McDermott for their comments, and Jacobo Dopico Gomez-Aller, Viviane Dittrich and Alexander Heinze for reviewing an earlier draft.

Journal of International Criminal Justice **19** (2021), 163–188 doi:10.1093/jicj/mqab023
Advance Access publication 17 May 2021

domestic statutes on evidentiary and procedural rules from admissibility to e-discovery. However, such reforms have not yet materialized at the ICC. This article assesses whether the Rome Statute and Rules of Procedure and Evidence, and their current interpretation, remain effective and appropriate in the face of technological change. The authors examine the emerging challenges related to the use and handling of digital evidence, as well as the unique nature of the internet and other dissemination channels. By drawing attention to the main issues with the existing rules and practices, and raising unresolved questions, the authors highlight the importance of reassessing rules based on obsolete assumptions and expectations as we move towards the future.

1. Introduction

Images of uniformed troops heroically freeing Jewish prisoners from Nazi concentration camps flickered on screen.[1] The mood in the courtroom shifted. They had heard the stories and read the orders, they knew the scale of the crimes and had even seen photographs, but the impact of live footage of the war's final days had an undeniable impact on the judges. Opening in 1945, the Nuremberg trials serve as one of the earliest examples of video as evidence in legal proceedings.[2] This innovative choice to show a film in a courtroom marked a profound shift in the proffering of evidence in criminal prosecutions. The video, introduced by Prosecutor Thomas Dodd rather than a witness, spoke for itself, and required no expert for authentication.[3]

Two years after the landmark trials at Nuremberg came the invention of transistors — the underpinning of digital technology and the beginning of what would later be designated 'the Digital Revolution'.[4] The continuous and exponential evolution of transistors over many decades has brought us

1 United States Army, 'Nazi Concentration Camps', 1945, available online at https://archive.org/details/nazi_concentration_camps_mp4 (visited 18 February 2021). In particular, the film 'Nazi Concentration Camps' in which Allied troops liberated the camps was presented as evidence in the courtroom with great impact on 29 November 1945. Evidentiary files can be consulted at Harvard Law School Library, 'Nuremberg Trials Project', available online at http://nuremberg.law.harvard.edu/ (visited 18 February 2021).

2 The authors' research uncovered records of only a few prior examples. In 1929, *Feather River Co v. United States*, a moving picture of a burnt forest was admitted as evidence of a fire that was caused carelessly and negligently, spreading upon public lands, US Court of Appeals for the Ninth Circuit, *United States v. Feather River Lumber Co.*, Judgement, 4 February 1929; A.R. Michaelis, 'Cinematographic Evidence in Law', 8 *The Quarterly of Film Radio and Television* (1953), at 186–193. Around the same time in the UK, a surveillance video captured in 16 mm by the police was used as evidence in the trial of 39 defendants accused of illegal street betting. K. McGahan, '1930s Hidden-camera Footage is First Film used as Evidence in UK Courts', BFI, 4 August 2015, available online at https://www.bfi.org.uk/news-opinion/news-bfi/features/1930s-hidden-camera-footage-first-film-used-evidence-uk-courts (visited 18 February 2021).

3 United States Holocaust Memorial Museum (USHMM), 'Film at the Nuremberg Trial', available online at https://www.ushmm.org/learn/timeline-of-events/1942-1945/film-at-the-nuremberg-trial (visited 18 February 2021).

4 Science and Technology Facility Council, 'A Brief History of the Digital Revolution', available online at https://stfc.ukri.org/files/digital-revolution-infographic/ (visited 18 February 2021).

into the Digital or Information Age,[5] where data has become one of the world's most valuable resources.[6] With globalized internet connectivity and growing smartphone usage, international criminal investigators are faced with an ever-growing volume of digital data that can be potentially probative. This abundance of digital information was likely not foreseen by the founders of the International Criminal Court (ICC or 'the Court'). How could they have anticipated that within a decade of the signing of the Rome Statute, half the world would carry devices in their pockets millions of times more powerful than the NASA computers that launched Apollo 11?[7] Today, most film and photography, as well as audio and written communications, are digital, bringing challenges that other types of evidentiary material such as physical documents or analogue film do not present.[8] Digital video cannot speak for itself — often it requires additional information to establish its authenticity and integrity, or expert testimony to be introduced and understood in court.

Digital material can be faked, forged, or altered — intentionally or unintentionally — in a number of different ways, sometimes remotely and often in a manner that is difficult to detect without specialized software or forensic expertise. Moreover, with recent improvements to artificial intelligence derived from the use of adversarial neural networks and big data sets, it is predicted that even forensic software will soon have difficulty detecting digital fakes.[9] In 2016, Oxford Dictionaries selected 'post-truth' as the word of the year,[10] and in 2018, ICC Judges noted that 'it has become ever more difficult to distinguish facts from "fake news"'.[11] Disinformation now spreads faster and with greater reach and influence than ever before.[12] In this context, this article asks: what does this new age of connectivity and digitalization mean for the ICC?

5 'The modern age is regarded as a time in which information has become a commodity that is quickly and widely disseminated and easily available especially through the use of computer technology.' Dictionary by Merriam-Webster.

6 'The world's most valuable resource is no longer oil, but data', *The Economist*, 6 May 2017, available online at https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (visited 18 February 2021).

7 T. Puiu, 'Your Smartphone is Millions of Times more Powerful than the Apollo 11 Guidance Computers', *ZME Science*, 11 February 2020, available online at https://www.zmescience.com/science/news-science/smartphone-power-compared-to-apollo-432/ (visited 18 February 2021).

8 N. Mezey, 'The Image Cannot Speak for Itself: Film, Summary Judgment, and Visual Literacy', 48 *Valparaiso University Law Review*, (2013), available online at https://scholar.valpo.edu/cgi/viewcontent.cgi?article=2316&context=vulr (visited 18 February 2021).

9 H. Farid, 'Digital Forensics in a Post-truth Age', 289 *Forensic Science International* (2018) 268–269, available online, https://farid.berkeley.edu/downloads/publications/fsi18.pdf (visited 18 February 2021); Al Engler, 'Fighting Deepfakes when Detection Fails', (Brookings Institute), 14 November 2019, available online at https://www.brookings.edu/research/fighting-deep fakes-when-detection-fails/ (visited 18 February 2021).

10 Oxford Languages, 'Word of the Year', available online at https://languages.oup.com/word-of-the-year/2016/ (visited 18 February 2021).

11 Separate opinion of Judge Christine Van den Wyngaert and Judge Howard Morrison, *Bemba Gombo* (ICC-01/05-01/08-3636-Anx2), Appeals Chamber, Judgment, 8 June 2018, § 5.

12 J. Anderson and L. Rainie, 'The Future of Truth and Misinformation Online', *Pew Research*, 19 October 2017, available online at https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/ (visited 18 February 2021); C. Wardle, 'Information

Digital evidence will inevitably play an increasingly central role in ICC trials. The growing use of digital technologies in armed conflicts, by civilians and combatants alike, is producing potentially relevant data at an exponentially rapid rate.[13] The ever-increasing volume of digital data creates challenges for ICC investigators, who need to identify, collect and preserve relevant evidence hidden in a sea of information that is vulnerable to alteration or destruction. This volume and vulnerability of digital information also creates challenges for the judges, who must assess admissibility and weight of digital evidence. Focusing on the procedures and practices at the Court, this article assesses whether the Rome Statute ('Statute') and Rules of Procedure and Evidence ('RPE' or 'Rules') maintain their appropriateness and effectiveness in the face of technological change. Section 2 gives an overview of the unique attributes of digital information and the online environment through which that information is disseminated and consumed, raising unresolved questions for the Court. In Section 3, we analyse how the role of the Prosecutor will be impacted by new sources of information, in particular how the creation and storage of digital information will affect the Prosecutor's investigative duties and powers. We also consider whether the Chambers are sufficiently prepared to evaluate the authenticity, relevance and probative value of digital evidence.[14] To conclude, we provide recommendations for reforming the practices and procedures of the Court.

2. New and Emerging Challenges in Digital Evidence

Digital evidence has been used in criminal proceedings for roughly 30 years now,[15] however, we have only recently started to grapple with the more complex legal and technical considerations at play. For example, the exploitation of user-generated content found on social media platforms,[16] leaked

Disorder, Part 1: The Essential Glossary', (First Draft: Medium), 9 July 2018, available online at https://medium.com/1st-draft/information-disorder-part-1-the-essential-glossary-19953c544fe3 (visited 18 February 2021); H. Romerstein, 'Disinformation as a KGB Weapon in Cold War', 1 *Journal of Intelligence History* (2011) 54–67, available online at https://www.tandfonline.com/doi/abs/10.1080/16161262.2001.10555046 (visited 18 February 2021).

13 L. Freeman, 'Law in Conflict: The Technological Transformation of War and its Consequences for the International Criminal Court', 51 *New York University Journal of International Law & Politics* (2019) 807–869.

14 R. Braga da Silva, 'New Technologies, Old Practices: The Authentication of Digital Evidence in the International Criminal Court', in this Special Issue of the *Journal*.

15 D. W. Hagy, 'Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors US Department of Justice' (Office of Justice Programs), 2007, at xi, available online at https://www.ncjrs.gov/pdffiles1/nij/211314.pdf (visited 18 February 2021).

16 R. J. Hamilton, 'User-Generated Evidence', 57 *Columbia Journal of Transnational Law* (2018) 1–61, available online at https://digitalcommons.wcl.american.edu/facsch_lawrev/1285 (visited 18 February 2021).

documents obtained from whistleblowing websites,[17] and data generated by Internet of Things devices[18] as evidence in legal proceedings is still in its infancy. There is undoubtedly a growing recognition of the need for lawyers, investigators and judges to better understand technology and the basics of digital forensics.[19]

This part describes the unique characteristics of digital evidence that distinguish it from the traditional forms of evidence (i.e. physical, testimonial and documentary).[20] It also explores the distinct features and complexities of the internet's information ecosystem, including the introduction of new voices, information sources and means and methods of communicating. The internet's architecture and governance have evolved over the past decades into an environment that fosters disinformation (false information deliberately created or disseminated to cause harm) and misinformation (false information spread without the intended purpose to cause harm);[21] bots that automate the dissemination of information;[22] and push algorithms and micro-targeting.[23] Social networks, in particular, have given rise to a host of idiosyncratic cultural trends like the use of coded language, memes and emojis. While understanding the digital format is important for assessing the authenticity of digital evidence, understanding the online information environment, the essential context which data inhabit, is necessary for evaluating the relevance of such evidence to an investigation.

17 A. Sevasti, 'The other WikiLeaks: 8 Whistleblowing Sites you Probably don't know about' (Memeburn), 14 June 2011, available online at https://memeburn.com/2011/06/8-whistleblowing-sites-you-probably-didn't-know-about/ (visited 18 February 2021).

18 The Internet of Things is a global infrastructure that enables advanced services and the transfer of data over a network without requiring human-to-human or human-to-computer interaction. International Telecommunication Union, 'Overview of the Internet of Things', Recommendation ITU-T Y.2060, at 1, available online at http://handle.itu.int/11.1002/1000/11559 (visited 18 February 2021).

19 D. Jackson, 'Can Lawyers be Luddites? Adjusting to the Modification of the ABA Model Rules of Professional Conduct Regarding Technology', 84 *The Oklahoma Bar Journal*, (2013) 2637–2642; D. Jackson, 'Lawyers Can't Be Luddites Anymore: Do Law Librarians Have a Role in Helping Lawyers Adjust to the New Ethics Rules Involving Technology', 105 *Law Library Journal* (2013) 394–404; N.P. Miller and D. Witte, 'Helping Law Firm Luddites Cross the Digital Divide—Arguments for Mastering Law Practice Technology', 12 *Science and Technology Law Review* (2008-2009) 113–123.

20 G. Boas, 'Creating Laws of Evidence for International Criminal Law: The ICTY and the Principle of Flexibility', 12 *Criminal Law Forum* (2001) 41–90.

21 Wardle, *supra* note 14.

22 Homeland Security, 'Social Media Bots Overview', Office of Cyber Infrastructure Analysis, May 2018, available online at https://www.cisa.gov/sites/default/files/publications/19_0717_cisa_social-media-bots-overview.pdf (visited 18 February 2021).

23 B. Bodó, N. Helberger, and C. H. de Vreese, 'Political Micro-targeting: a Manchurian Candidate or just a Dark Horse?' 6 *Internet Policy Review* (2017) 1–13.

A. The Unique Attributes of Digital Information

Traditional categories of evidence are physical, documentary and testimonial, with the more recent additions of scientific or expert evidence and digital, electronic or electronically stored evidence. In the public domain, the labels 'electronic', 'electronically-stored' and 'digital' are often used as synonyms to describe information or evidence.[24] Since the majority of modern computing devices are both electronic and digital, this interchangeability is sometimes appropriate. However, these terms have distinct meanings. The term 'electronic' does not necessarily encompass digital information found on the internet, server networks or the cloud.[25] Electronic devices can be digital or analogue.[26] In analogue technology — such as audio cassettes, transistor radios and VCRs — data is translated into electronic pulses of varying amplitude.[27] Digital technology, on the other hand, translates data into binary format.[28] Computers, laptops, smartphones and most modern electronic technologies are digital, and so is the information they generate and store. Digital information can be created or saved on an electronic device, a network or a system of interconnected networks like the internet.[29] For example, it may be stored across several servers and accessed by any device that connects to the internet, rather than being held on a single electronic device.

Digital evidence is any potentially relevant and probative information stored in digital format that a party to a court case may use at trial. It may include emails, text messages, websites, files on a hard drive, satellite imagery, drone footage, machine logs, financial transactions and government records. Digital evidence comprises both initially produced digital information[30] and digitized

24 For the purposes of this article, we use 'information' and 'data' interchangeably, whereas we reserve 'evidence' for referring to information that is used to establish facts in a legal investigation or proceeding. See *Black's Law Dictionary*. This article uses the label digital, rather than electronic or electronically stored, because the authors see it as the more current and appropriate term encompassing newer types of information, such as web content or data created digitally and stored in the cloud.

25 Software and services that run on the internet, instead of locally on a computer. Microsoft Azure, 'What is Cloud Computing?', available online at https://azure.microsoft.com/en-gb/overview/what-is-cloud-computing/#cloud-computing-models (visited 18 February 2021).

26 L. Null and J. Lobur, *The Essentials of Computer Organization and Architecture* (Jones & Bartlett Publishers, 2006), at 121.

27 Diffen, 'Analog vs Digital', available online at https://www.diffen.com/difference/Analog_vs_Digital (visited 18 February 2021).

28 A binary format is a format in which file information is stored in the form of ones and zeros, or in some other binary (two-state) sequence. Techopedia, 'Binary Format', available online at https://www.techopedia.com/definition/938/binary-format (visited 18 February 2021).

29 D. Lomer, '15 Types of Evidence and how to use them', *i-Sight*, 6 April 2016, available online at https://i-sight.com/resources/15-types-of-evidence-and-how-to-use-them-in-investigation/ (visited 18 February 2021).

30 'Born Digital Information' refers to data that was created using a computer and exists only in digital format. Born digital information may be machine-generated (e.g. internet search history or metadata of a word document) or user-generated (e.g. a Facebook post or content of a word document).

information from prior sources.[31] It may be user-generated (e.g. an email) or machine-generated (e.g. browser search history), and come from either closed (e.g. a text message) or open sources (e.g. Twitter posts).[32] The digital format has unique attributes. With analogue information, like a videotape or a physical document, there is a clear distinction between an original versus a copy of the information. Such a distinction does not translate equally to digital information, for which there may be multiple copies indistinguishable from the first created version. Digital information can also exist in multiple locations at the same time. For example, an email may live on the computers and/or email accounts of both the sender and the receiver, as well as on the email provider's network, and potentially any backup servers or systems. If investigators want to collect an email message as evidence, they can obtain it from any one of these locations or sources. [33] Thus, the author or creator of the material may be different from the source providing the information to the investigator or the custodian from which it is obtained — possibly resulting in variances in the format and in the accompanying information or metadata.[34] The array of collection methods and sources may call for different requirements for authentication at trial, such as through an expert witness, lay witness or with corroborating evidence.

In practice, it is the volume and vulnerability of digital information that creates significant hurdles for international criminal investigators. Even a simple burglary case may result in terabytes of data from CCTV footage, mobile phones and GPS devices. That volume is magnified in international cases that have significantly wider geographic and temporal scopes. On average, 188 million emails and 18.1 million text messages were sent every 60 seconds in 2019.[35] Over 500 hours of video were uploaded to YouTube per minute as of 2018.[36] If Facebook were a country, the number of monthly active users — 2.7 billion — would surpass by more than 600 million the total population of

31 Digitized information refers to data in physical material that is converted into a format which is computer-readable (e.g. scanning a physical document to create a PDF).

32 Open source is publicly available information that can be obtained by request, purchase, or observation. R.A. Best Jr. and A. Cumming, 'Open Source Intelligence (OSINT) Issues for Congress', *CRS Report for Congress*, 5 December 2007, available online at https://fas.org/sgp/crs/intel/RL34270.pdf (visited 18 February 2021).

33 A source is a person, place or thing from which digital data comes or can be obtained.

34 Metadata is data that provides information about other data. It can help provide context to investigators and answer questions like when, where or who.

35 L. Lewis, '2019: This is what happens in an Internet Minute', *All Access*, 5 March 2019, available online at https://www.allaccess.com/merge/archive/29580/2019-this-is-what-happens-in-an-internet-minute (visited 18 February 2021); see also Hootsuite, 'Social Media Trends Reports for 2019', available online at https://hootsuite.com/en-gb/resources/social-media-trends-report-2019 (visited 18 February 2021).

36 Interview with Ben McOwen Wilson, YouTube EMEA's regional director, in Anmar Frangoul, 'With over 1 Billion Users, here's how YouTube is Keeping Pace with Change', *CNBC*, 14 March 2018, available online at https://www.cnbc.com/2018/03/14/with-over-1-billion-users-heres-how-youtube-is-keeping-pace-with-change.html (visited 18 February 2021).

the five permanent members of the United Nations Security Council.[37] As a result of this volume of data, there is more information available to provide leads and investigate crimes than ever before.[38] In 2013, Edward Snowden leaked over 1.7 million digital documents from the US National Security Agency to journalists Glenn Greenwald and Laura Poitras.[39] In 2017, German reporters published 'The Paradise Papers', a string of stories based on 13.4 million confidential digital documents relating to offshore investments.[40] It is not unreasonable to imagine that the ICC could face a similar data dump in the future (if it has not already).

The volume of data, while beneficial in many regards, places a tremendous strain on investigative and prosecutorial bodies that do not have the tools, resources or capacity to intake and analyze that amount of information. While the ability to keyword search through bulk digital documents alleviates some of the burden, for digitized documents, optical character recognition is not yet well developed in some languages.[41] Emails, text messages, images, videos and other types of digital files can be searched by metadata, assuming it has not been stripped, but machine-learning and computer vision-based technologies still struggle to consistently identify requested content.[42] The Independent International Investigative Mechanism on Syria makes a telling case in point. A finite group of United Nations investigators, lawyers and analysts have been tasked with collecting and preserving information relevant to alleged international crimes committed in the context of the Syrian civil war, which has been ongoing since 2011. YouTube alone offers more hours of video of the Syrian conflict uploaded by users than there have been hours in the conflict itself,[43] making it an impossible task to view all the potential video evidence. Without the capacity to conduct an

37 Facebook, 'Facebook Reports Third Quarter 2020 Results', 29 October 2020, available online at https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Third-Quarter-2020-Results/default.aspx (visited 18 February 2021).

38 The Software Alliance and BSA, 'More Data is Available to Law Enforcement Than Ever Before', available online at https://www.bsa.org/files/policy-filings/BSA_Encrypt_AvailabilityData-web.pdf (visited 18 February 2021).

39 M.B. Kelley, 'NSA: Snowden Stole 1.7 Million Classified Documents And Still Has Access To Most of Them', *Business Insider*, 13 December 2013, available online at https://www.businessinsider.com/how-many-docs-did-snowden-take-2013-12 (visited 18 February 2021).

40 E. Zerofsky, 'How a German Newspaper Became the Go To Place for Leaks like the Paradise Papers', *The New Yorker*, 11 November 2017, available online at https://www.newyorker.com/news/news-desk/how-a-german-newspaper-became-the-go-to-place-for-leaks-like-the-paradise-papers (visited 18 February 2021).

41 Optical character recognition converts images of typed, handwritten or printed text into digital text.

42 This problem is more salient for image analysis of content that may depict violations of international criminal law. For an in-depth overview of computer vision and machine learning for human rights video analysis, J.D. Aronson, 'Computer Vision and Machine Learning for Human Rights Video Analysis: Case Studies, Possibilities, Concerns, and Limitations', 43 *Law and Social Inquiry* (2018) 1188–1209.

43 A secondary source citing an interview with Justin Kosslyn, product manager for Jigsaw, 'You have more hours of footage of the Syrian civil war on YouTube then there actually are hours of the war in real life.', in A. Rosen, 'Erasing History: YouTube's Deletion Of Syria War Videos Concerns Human Rights Groups', Fast Company, 3 July 2018, available online at https://www.

itemized review, investigators are forced to make hard decisions about what videos to collect, store and use as evidence.

Another unique attribute of digital information is the ease with which it can be altered, destroyed or lost if proactive steps are not taken to preserve it. Social media content can be taken down by the uploader or the platform.[44] A digital file can be converted from one format to another, transferred from one device to another, or processed in a number of different ways, all of which create opportunities for alteration or spoliation.[45] Inadvertently or not, any kind of processing can modify the integrity of digital evidence. Machine learning is incrementing the sophistication levels of image changing software like Photoshop, which is decreasing the time, money and technical skills required to create synthetic media or deepfakes.[46] This susceptibility to manipulation means that it is more necessary than ever before to collect and preserve digital material in a forensic manner, maintain and document a clear chain of custody, ensure secure storage of originals offline, and engage technical experts in the handling of digital evidence at all stages.

B. Understanding the Digital Information Ecosystem

The internet has created a novel and complex environment for creating, sharing and receiving information. It has fundamentally changed the way in which individuals communicate with one another. The Court's Statute and Rules were formulated at a time when the internet was still in its nascent phase, filled with static webpages that users could read, but not alter. A revolution came in the early 2000s with the introduction of interactive or 'writable' webpages on which internet users could comment and contribute to the content.[47] Search engines have organized the world's information and brought it to our fingertips, but that information varies greatly in quality and accuracy.

---

fastcompany.com/40540411/erasing-history-youtubes-deletion-of-syria-war-videos-concerns-human-rights-groups (visited 18 February 2021).

44 H. Al Khatib and D. Kayyali, 'YouTube is Erasing History', *The New York Times*, 23 October 2019, available online at https://www.nytimes.com/2019/10/23/opinion/syria-youtube-content-moderation.html (visited 18 February 2021); A. Asher-Schapiro, 'YouTube and Facebook are Removing Evidence of Atrocities, Jeopardizing Cases against War Criminals', *The Intercept*, 2 November 2017, available online in https://theintercept.com/2017/11/02/war-crimes-youtube-facebook-syria-rohingya/ (visited 18 February 2021).

45 J.G. Browning, 'Burn after Reading: Preservation and Spoliation of Evidence in the Age of Facebook', 16 *Science and Technology* (2013) 273–308; R. Durrant, 'VII. Spoliation of Discoverable Electronic Evidence', *Loyola of Los Angeles Law Review* (2005) 1803–1834.

46 For instance, FakeApp allows users to swap faces in videos, and uses TensorFlow, a free open source machine-learning software by Google. Hany Farid, of University of California, Berkeley, specializes in detecting the signs of digital manipulation and has spoken and published extensively on the topic. For a full list of academic papers and public interventions, see his website, available online at https://farid.berkeley.edu/ (visited 18 February 2021).

47 These two periods are often referred to as Web 1.0 and Web 2.0. G. Cormode and B. Krishnamurthy, 'Key Differences Between Web 1.0 and Web 2.0', *First Monday*, 2008 available online at https://firstmonday.org/article/view/2125/1972 (visited 18 February 2021).

This ecosystem adds additional complexities to our understanding of digital evidence and how it should be assessed in the courtroom.

First, the expanding use of digital technologies has given rise to new content creators. The propagation of smartphones has enabled the spread of information from the battlefield to the living room, introducing novel sources of potential evidence. With growing connectivity and the advancement of information and communication technologies, ordinary citizens in conflict zones are empowered to document what is happening on the ground and share that information on the internet.[48] This content is often referred to as 'user-generated content',[49] and it is generally disseminated via social media platforms. Information captured with smartphones may also be closed source, though, and distributed only through private messaging applications. Obtaining access to this data may require cooperation from national authorities or service providers.

In addition to introducing new sources into the information ecosystem, the internet has changed the means and methods by which members of the public receive information. The internet is not neutral, nor is it consistent. There are a number of factors that impact online search results — not every person views the same results to the same queries. For example, running an identical Google search will produce different results depending on the IP address of the device used. A large percentage of websites turn a profit through targeted advertising, which capitalizes on data collected about their users. Algorithms use this information to offer specific types of content or advertisements to users on the basis of their behaviour and other factors, affecting the information each user is shown.[50] For instance, the right side of the YouTube page recommends the next video to watch, prioritizing similar videos to the one being played as well as others previously viewed. Since algorithms are built by humans, they are often embedded with their biases. Consequently, investigators using online sources must be aware not only of their own personal biases, but also of how the internet architecture prejudices what they see.[51]

Finally, the internet and mobile applications have changed the very nature of information and communications themselves. Text messages and tweets, which are limited in characters, incorporate shorthand — some of which is very specific to certain groups of people. Just as there are experts to explain the meaning of graffiti, symbols and insignia in gang-related criminal cases, there is an increasing need for experts who can interpret online communications within a cultural context. In national jurisdictions, emojis[52]

48 D. Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century* (Basic Books, 2017).

49 Hamilton, *supra* note 18, at 1.

50 S.C. Woolley and P.N. Howard, "Automation, Algorithms, and Politics', 10 *International Journal of Communication* (2016) 4882–4890.

51 Y. McDermott, A. Koenig and D. Murray, 'Open Source Information's Blind Spots: Human and Machine Bias in International Criminal Investigations', in this Special Issue of the *Journal.*

52 An emoji is 'any of various small images, symbols, or icons used in text fields in electronic communication (as in text messages, e-mail and social media) to express the emotional attitude

and memes[53] have already showed up in the courtroom.[54] In international criminal cases, recorded public speeches, radio broadcasts and propaganda are frequently introduced as evidence. While speech in and of itself is not criminalized (with the narrow exception of incitement to commit genocide), hate speech, fear speech and incitement have been important components in establishing the criminal intent of perpetrators.[55] On the internet, speech can be targeted, amplified or spread in different ways,[56] through humans or bots.[57] Understanding why and how certain content goes viral, who it reaches, and how it impacts those who see it are all foundational components in the process of analysing online speech and its relevance to an investigation.

3. International Criminal Evidence and Procedure

The ICC Statute and Rules derive from the statutory instruments of the ad hoc international criminal tribunals for the former Yugoslavia and Rwanda, which preceded the ICC, as well as domestic procedures and statutes from different legal traditions — all fused together to create a unique framework.[58] This article does not discuss the merits of this mixed legal basis. Rather, it focuses only on whether the current system can effectively deal with the challenges that accompany new types of digital evidence. This part looks at how the Court's current framework will fare when faced with evidentiary issues requiring technological sophistication. While the Statute, Rules and other key texts do not explicitly address digital evidence, there are several provisions that apply to its collection, preservation, disclosure, submission and/or and evaluation.

---

of the writer, convey information succinctly, communicate a message playfully without using words, etc.' Dictionary by Merriam-Webster.

53 'A meme is an image, video, piece of text, etc., typically humorous in nature, that is copied and spread rapidly by Internet users, often with slight variations.' *Oxford Dictionary*.

54 S. Harrison, 'How Emojis Have Invaded the Courtroom', *Slate*, 26 November 2019 available online at https://slate.com/technology/2019/11/emoji-court-cases-crime-free-speech-contract-law.html (visited 18 February 2021).

55 P. Dojcinovic (ed.), *Propaganda, War Crimes Trials and International Law: From Speakers' Corner to War Crimes* (Taylor and Francis, 2012).

56 Former Director of the Anti-Defamation League, Brittan Heller provides a prime example of this complexity in the evolution of a cartoon frog used as a mascot for slackers, co-opted by white supremacists and categorized as hate speech, and then transformed once again to serve as a symbol for democracy in Hong Kong. Only in one of these cases did the frog serve as hate speech. B. Heller, 'Is This Frog a Hate Symbol or Not?', *The New York Times*, 24 December 2019, available online at https://www.nytimes.com/2019/12/24/opinion/pepe-frog-hate-speech.html (visited 18 February 2021).

57 A bot is a software application that is programmed to run certain tasks. P. Martineau, 'What is a Bot?', *Wired*, 16 November 2018, available online at https://www.wired.com/story/the-know-it-alls-what-is-a-bot/ (visited 18 February 2021).

58 K. Ambos, *Treatise on International Criminal Law: Volume III: International Criminal Procedure* (Oxford University Press, 2016), at 2–7.

A. The Prosecutor's Duties, Powers and Obligations

The Statute contains provisions that address the duties, powers and obligations of the Prosecutor with respect to investigations, each focusing on different parts of the process. Here we examine the duty to investigate incriminating and exonerating circumstances equally, the power to collect or preserve at-risk evidence, and the obligation to disclose relevant information to the defence — and the tensions that arise between all these competing factors vis-à-vis the unique attributes of digital evidence.

1. Duty to Investigate Incriminating and Exonerating Circumstances Equally

Article 54(1)(a) Rome Statute requires that the prosecutor 'extend the investigation to cover all facts and evidence relevant to an assessment of whether there is criminal responsibility under this Statute, and, in doing so, investigate incriminating and exonerating circumstances equally.'[59] This principle of objectivity was included in the Statute to bridge the role of the prosecutor and the investigating judge between different legal traditions,[60] and it raises issues concerning the scope of the obligation and consequences of a breach.[61] Technology has created vastly more information available than ever before, but most of it is not relevant to criminal investigations. While *prima facie* irrelevant material, such as cat videos, can be easily discarded, there remains a large volume of information for which its relevance is not immediately apparent. In addition, what is relevant might change during the course of an investigation as the case hypothesis evolves.

If the Article 54(1)(a) duty is interpreted too broadly, the volume of digital data will make this duty impracticable. Take for example the Syrian Archive, a collective of human rights activists curating visual documentation of human rights violations in Syria, which has collected over 3.5 million items of digital content through manual and automated processes.[62] If the ICC had jurisdiction over the Syrian conflict, would the prosecutor be obligated to gather and review each item of this collection? The amount of documentation of modern armed conflicts means that the defence will always be able to argue that the prosecution did not do enough, especially if the defence identifies relevant information that the prosecutor missed. Conversely, if the prosecutor discloses the entire universe of information, the defence will argue that the prosecutor

59 Article 54(1)(a) ICCSt.

60 M. Bergsmo and P. Kruger, 'Article 54: Duties and Powers of the Prosecutor with Respect to Investigations', in O. Triffterer (ed.), *Commentary of the Rome Statute of the International Criminal Court* (2nd edn., Beck/Hart, 2008), at 1078. The principle has also been incorporated in Art. 49(b) and (c) of the Code of Conduct for the Office of the Prosecutor, 5 September 2013.

61 Several proceedings have dealt with the obligation of Art. 54(1)(a) ICCSt. For instance, Transcripts, *Katanga and Ngudjolo Chui* (ICC-01/04-01/07-T-81), Trial Chamber II, 25 November 2009, §§ 28–36. Decision on the confirmation of charges, *Mbarushimana* (ICC-01/04-01/10-465-Red), Pre-Trial Chamber II, 16 December 2011, § 51.

62 Syrian Archive website, available online at https://syrianarchive.org/en (visited 18 February 2021).

dumped too much information on them with insufficient screening to work out what is actually relevant.

While online evidence gathering is less costly than collecting physical evidence and interviewing witnesses across countries, internet-based investigations can be deceptively resource intensive and costly when factoring in data processing and storage. With an overwhelming and constantly changing amount of digital data on the web, there is no obvious end point to an online investigation. Based on the Trial Chamber's interpretation of Article 54(1)(a) in the *Lubanga*,[63] *Kenyatta* and *Ruto and Sang* cases,[64] the duty extends to investigating the credibility of all witnesses insofar as it 'may affect the credibility of prosecution evidence'. An increasing number of ICC witnesses will have an online presence, raising the question of whether this duty requires the prosecutor to look to the internet to assess the credibility of every witness, and if so, how much internet-based research is enough. An overly broad interpretation or lack of clear guidance on how Article 54(1)(a) applies to online investigations and digital evidence collection will quickly overwhelm investigators.

2. The Power to Collect or Preserve Evidence

In criminal investigations, the golden hour refers to the period immediately after an offence has been committed, when material is readily available in relatively high volumes to investigators.[65] Proactive action during this period maximizes the chances of securing evidence that will be admissible in court, and minimizes the chances of such evidence being lost or contaminated.[66] In national criminal cases, law enforcement are generally able to access the crime scene, collect evidence and interview witnesses soon after the crime occurs. In contrast, ICC investigators are rarely, if ever, able to start their inquiries during this period, because they are not officially mandated to investigate until a number of factors are assessed and met, which may take years.[67] As a result, international criminal investigations are reliant on the preservation decisions of first responders, who rarely have the knowledge to identify what will be relevant nor the tools and expertise to preserve potential evidence in a forensic manner.

63 Judgment, *Lubanga* (ICC-01/04-01/06-2842), Trial Chamber I, 5 April 2012, §§ 178—182.

64 Defence Application for a Permanent Stay of the Proceedings due to Abuse of Process, *Kenyatta*, (ICC-01/09-02/11-822-Red), Trial Chamber V(b), 10 October 2013, § 92. For a similar reasoning, see Joint Defence Application for Further Prosecution Investigation Concerning [REDACTED] of Certain Prosecution Witnesses, *Ruto and Sang* (ICC-01/09-01/11), Trial Chamber V(A), 12 January 2015, §§ 33 and 34.

65 College of Policing, 'Investigation', available online at https://www.app.college.police.uk/app-content/investigations/investigation-process/#golden-hour (visited 18 February 2021).

66 *Ibid.*

67 A. Pues, 'Towards the "Golden Hour"? A Critical Exploration of the Length of Preliminary Examination's', 15 *Journal of International Criminal Justice* (2017) 435–453.

The investigation duty set forth in Article 54(1)(a) does not just apply to searching for relevant information, but also to collecting it. The prosecutor's investigative powers are described in Article 54(3), in particular, the power to '[t]ake necessary measures, or request that necessary measures be taken, to ensure ... the preservation of evidence'.[68] This investigative authority to preserve evidence is reinforced by Article 56, which provides for unique investigative opportunities. Pursuant to Article 56, the prosecutor shall inform the Pre-Trial Chamber if a unique opportunity arises to examine, collect or test evidence, which may not be available subsequently for the purposes of a trial.[69] Hence, the Pre-Trial Chamber can approve necessary measures to be taken to ensure the evidence is handled and preserved for a future trial.

When it comes to digital evidence, the window for the golden hour may be short, while the procedures for file identification and forensic extraction can take significant time. Therefore, the vulnerability of digital information may force investigators to capture content in bulk before reviewing it for relevance. It may also push them to preserve such information in a manner that is fast but not forensic. In the case of the former, bulk collection can cause serious problems for the prosecutor, who is obliged to review all information in her possession or custody for disclosure purposes. Bulk collections, which can easily contain a volume of data beyond what an investigation team can feasibly review over the course of years will, at best, cause bottlenecks throughout the investigation, pre-trial, and trial process. At worst, it will cause the prosecutor to breach disclosure obligations and, in turn, violate the rights of the accused. In the latter case, investigators may end up preserving digital evidence that cannot be authenticated, and therefore might not be admissible at trial.

The question then becomes how to make decisions around what digital information to preserve, and how to preserve it. Information on the internet will always be at risk of removal by the person who posted it or by the platform itself, which raises additional questions of how to assess relevance at an adequate speed. With social media platforms like Facebook using artificial intelligence and automated processes to enhance the effectiveness of online content moderation, potentially relevant information might be removed before investigators discover it, particularly if the content violates the platform's terms of service or national laws.[70] The preservation of closed source digital evidence

68 Art. 54(3)(f) ICCSt.

69 Art. 56(1)(a) ICCSt. Examples of the wide range of measures that the Pre-Trial Chamber may take are listed in Art. 56 (1)(b) ICCSt.

70 The removal of content by social media companies has been widely documented in the context of the Syrian war. For other examples, see B. Warner, 'Tech Companies Are Deleting Evidence of War Crimes', *The Atlantic*, 8 May 2019, available online at https://www.theatlantic.com/ideas/archive/2019/05/facebook-algorithms-are-making-it-harder/588931/ (visited 18 February 2021); M. Rajagopalan, 'The Histories of Today's Wars are Being Written On Facebook and YouTube. But What Happens When They Get Taken Down?', *BuzzFeed*, 22 December 2018, available online at https://www.buzzfeednews.com/article/meghara/facebook-youtube-icc-war-crimes (visited 18 February 2021); M. Ingram, 'YouTube Takedowns are making it Hard to Document War Crimes', *Columbia Journalism Review*, 24 October 2019, available online at https://www.cjr.org/the_media_today/youtube-takedowns-war-crimes.php (visited 18 February 2021); K. O'Flaherty,

can also be time-sensitive. Call data records have already proven to be highly relevant evidence in international criminal cases,[71] but telecommunication providers retain user data containing call and cell site information for a finite period, and tend to routinely and permanently delete transactional records in order to comply with data protection laws and keep storage costs low.[72] In situations of mass human rights violations and core international crimes, the arc of justice is long and difficult to predict. Thus, anything that is preserved for future investigations and prosecutions usually needs to be stored for many years to come, acknowledging that much of the stored material might never become relevant for legal purposes. If Chambers interpret the Statute too narrowly and overly restrict the prosecutor's activities during preliminary examination, relevant and probative digital evidence will unquestionably be lost.

3. The Obligation to Disclose Relevant Information

Finally, as noted above, questions on whether and what to collect will inevitably impact disclosure. Several provisions address the prosecutor's obligations to the defence, including the obligation to disclose information relevant to the proceedings. Article 61(3)(b) recognizes the right of the accused to be informed of the evidence on which the prosecutor intends to rely for the confirmation of charges, who is also required to disclose evidence in his or her 'possession or control which he or she believes shows or tends to show the innocence of the accused, or to mitigate the guilt of the accused, or which may affect the credibility of prosecution evidence.'[73] Chambers have clarified that this disclosure duty applies to all information under the prosecutor's possession or control, including exculpatory evidence.[74] There are only a few restrictions, such as when the information has been obtained by the prosecutor on the condition of confidentiality and solely for the purpose of generating new evidence,[75] or when the disclosure may endanger the security of the witnesses.[76] Similarly,

'YouTube keeps Deleting Evidence of Syrian Chemical Weapon Attacks', *Wired*, 26 June 2018, available online at https://www.wired.co.uk/article/chemical-weapons-in-syria-youtube-algorithm-delete-video (visited 18 February 2021).

71 Judgment, *Bemba et al.* (ICC-01/05-01/13), Appeals Chamber, 8 March 2018. See also, Decision on the admission of call sequence tables related to the movements of Mr Rafik Hariri and related events, and four witness statements, Special Tribunal for Lebanon, *Ayyash et al.* (STL-11-01/T/TC), Trial Chamber, 31 October 2016.

72 Usually 6–18 months, depending on the cell provider. P. Siewert, 'Cellular Provider Record Retention Periods', in *Forensic Focus*, 18 April 2017, available online at https://articles.forensicfocus.com/2017/04/18/cellular-provider-record-retention-periods/ (visited 18 February 2021).

73 Art. 67(2) ICCSt.

74 Decision on the consequences of non-disclosure of exculpatory materials covered by Art. 54(3)(e) agreements and the application to stay the prosecution of the accused, together with certain other issues raised at the Status Conference on 10 June 2008, *Lubanga* (ICC-01/04-01/06-1401), Trial Chamber I, 13 June 2008, § 59.

75 Art. 54(2) ICCSt.

76 Art. 68(5) ICCSt.

Rules 81 and 82 restrict disclosure when it may endanger further investigations or conflict with other evidentiary obligations of the prosecutor. These exceptions often mean that the prosecutor must carefully review all information before it is disclosed to assess whether it needs to be redacted, and to ensure the security of witnesses while simultaneously ensuring the rights of the accused.

While access to a vast repository of information may be beneficial for investigators, if too much is collected, it will become impossible for lawyers to comply with disclosure obligations that require itemized review.[77] Overly burdensome disclosure obligations, along with the fear of breaching those obligations, will hamper the investigative process and risk losing relevant digital material. Lawyers in domestic legal systems have embraced new e-discovery techniques and technologies, such as metadata searches or technology-assisted review, which uses machine learning to identify responsive items for disclosure.[78] Nevertheless, certain types of digital evidence cannot be easily addressed with these search tools, such as videos and images, audio files or documents in languages for which processing software is not yet available. In addition, much of the software used to assist e-disclosure at the national level appears too expensive for the ICC, and it has not been prioritized despite the advantages it may bring to all parties. Therefore, until those in charge of the budget recognize that the long-term efficiency gains of these technologies outweigh their upfront cost, investigators will continue to err on the side of caution and avoid over-collection. This approach may prevent burdensome bottlenecks at the time of disclosure, but as discussed above, it also risks the loss of important digital evidence.

B. The Chambers' Approach to Evaluating Evidence

Early ICC investigations focused on protracted internal armed conflicts, which involved small government militaries and non-state militias using old communications technologies such as two-way radios. The events under investigation occurred in the early 2000s and, as a result, had minimal digital evidence. There were a few exceptions, such as the ten video clips submitted as evidence to prove the use of child soldiers by Lubanga's troops in the ICC's first trial, *Prosecutor v. Lubanga*.[79] Investigators relied heavily on witnesses testifying years after traumatic incidents occurred and on reports that contained

77 Disclosure obligations should be read in conjunction with Rules of Procedure and Evidence of the International Criminal Court ('RPE'), 9 September 2002, Rule 76 ICC RPE (pre-trial disclosure of prosecution witnesses), and Rule 77 ICC RPE (inspection of material).

78 Exterro, 'Chapter 7B: Predictive Coding (Technology Assisted Review) and Artificial Intelligence', available online at https://www.exterro.com/basics-of-e-discovery/predictive-coding/ (visited 18 February 2021).

79 WITNESS, 'The Role of Video in the Criminal Justice Process', available online at https://vae.witness.org/portfolio_page/role-of-video-in-the-criminal-justice-process/ (visited 18 February 2021). For other instances where digital evidence was used as evidence at the ICC, see L. Freeman, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies

anonymous or secondary hearsay from NGOs and United Nations agencies with better and more proximate access to the situation. The Judges found this evidence to be weak without further corroboration.[80]

There is now an increasing recognition of the importance of forensic science and digital evidence. In *Katanga and Ngudjolo*, the prosecutor introduced satellite images, drone and ground images taken by ICC investigators during a site visit.[81] In *Bemba et al.*, call data records were introduced to prove that the accused 'remained in frequent, lengthy and unsanctioned contact to coach witnesses'.[82] In 2017, an arrest warrant for Libyan commander Al Werfalli for murder as a war crime was based primarily on seven videos found on Facebook and other websites.[83] The prosecutor has started to assess the viability of financial investigations that can lead to the tracing, freezing, seizing or recovery of assets of the accused.[84] Such investigations will necessarily carry with them other types of digital evidence, such as electronic financial transactions. In addition, as digital information warfare assumes a prominent role in modern armed conflicts — where platforms like Facebook and Twitter have become weapons of war[85] — social media will acquire increased importance in presenting a narrative of how conflicts unfold and evolve.

The volume of digital information, combined with the ephemeral nature of digital material, make the set of rules governing the evaluation of evidence a cornerstone of the success of any effort to achieve international justice. The freedom and flexibility that have been built into these provisions, and the practices that have emerged from Chambers, should be examined in light of the unique attributes of digital evidence. Starting with the Nuremberg Charter, the statutory foundations of international criminal tribunals have taken a minimalist approach to evidentiary rules, with much discretion left to the Judges.[86] The ICC is no exception.[87] Article 64(9)(a) of the Statute provides

on International Criminal Investigations and Trials', 41 *Fordham International Law Journal* (2018) 283–336.

80 Judgement pursuant to Article 74, *Katanga* (ICC-01/04-01/07-3436-tENG), Trial Chamber II, 7 March 2014, §§ 83–93.

81 Transcript, *Katanga and Ngudjolo Chui* (ICC-01/04-01/07-T-90-ENG ET WT), 26 January 2010, §§ 24–25.

82 Public Redacted Version of 'Prosecution's Closing Brief', *Bemba Gombo et al.* (ICC-01/05-01/13-1905-Red), 10 June 2016, § 21.

83 Warrant of Arrest, *Al-Werfalli* (ICC-01/11-01/17-2), 15 August 2017.

84 International Criminal Court, 'Financial Investigations and Recovery of Assets', November 2017 available online at https://www.icc-cpi.int/iccdocs/other/Freezing_Assets_Eng_Web.pdf (visited 18 February 2021).

85 P.W. Singer and E.T. Brooking, *LikeWar: The Weaponization of Social Media* (Houghton Mifflin Harcourt Publishing Company, 2018).

86 D.K. Piragoff and P. Clarke, 'Article 69', in O. Triffterer and K. Ambos (eds), *The Rome Statute of the ICC: A Commentary* (3rd edn., Oxford University Press, 2016) 1716.

87 In the negotiations for the ICC, the conduct of the proceedings and drafting of the Rules were highly contentious. See P. Lewis, 'Trial Procedure', in R.S. Lee (ed.), *The International Criminal Court: Elements of Crimes and Rules of Procedure and Evidence* (Transnational Publishers, 2001); see also S.A. Fernández de Gurmendi, 'The Process of Negotiations', in R.S. Lee (ed.), *The*

for the general power of the Trial Chamber to '[r]ule on the admissibility or relevance of evidence', the Rules authorizing the Judges 'to assess freely all evidence submitted'.[88]

Under the Statute, the parties submit evidence relevant to the case,[89] and the Trial Chamber will take into account 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.[90] Evidence is relevant if it makes the existence of a fact at issue more or less probable.[91] Whether or not this is the case depends on the purpose for which the evidence is adduced. The probative value of a piece of evidence is its ability to establish a given fact, and it may take into account considerations of reliability, authenticity and importance of the piece in question.[92] In providing further guidance, the Rules indicate that evidence ruled irrelevant or inadmissible shall not be considered by the Chamber,[93] and that any issues in this regard must be raised at the time of submission — unless it was unknown, in which instance it should be raised immediately after it has surfaced.[94] The main instruction for excluding evidence is Article 69(7), when it has been obtained in violation of the Statute or internationally recognized human rights, *if* the violation casts substantial doubt on the reliability of the evidence or the admission of the evidence would be antithetical to and would seriously damage the integrity of the proceedings.

The free assessment of evidence bestowed on the Judges should be read in conjunction with the flexibility given to the Chambers to conduct their own proceedings. The Trial Chamber is responsible for ensuring that trial proceedings before the Court are fair and expeditious, conducted with full respect for the rights of the accused and due regard for the protection of victims and witnesses.[95] Article 64(3)(a) allows each newly composed Trial Chamber to independently adopt the procedures it believes are necessary to facilitate the proceedings.[96] This provision gives judges discretion in deciding when and how they rule on admissibility of evidence, not requiring consistency across cases. As a result, the procedural approaches for the evaluation of evidence taken by different Chambers vary greatly in practice. This raises two distinct, but

International Criminal Court: The Making of the Rome Statute, Issues, Negotiations, Results (Kluwer Law International, 1999) 217, 224–226; Piragoff and Clarke, *supra* note 86, at 1717.

88 Rule 63(2) ICC RPE.

89 Art. 69(3) ICCSt, (ICC-A/CONF.183/9).

90 *Ibid.*

91 Decision on the Prosecutor's Bar Table Motions, *Prosecutor v. Katanga and Ngudjolo Chui*, (ICC-01/04-01/07-2635), 17 December 2010, § 16.

92 Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute of 6 September 2012, *Prosecutor v. Bemba Gombo*, (ICC-01/05-01/08-2299-Red), 8 October 2012, § 8; *Décision relative aux requêtes du Procureur aux fins d'admission de pièces qu'il entend verser directement aux débats, Le Procureur c. Katanga et Ngudjolo Chui*, (ICC-01/04-01/07-2635-tFRA), 17 Décembre 2010, §§ 21 and 34.

93 Rule 64(3) ICC RPE.

94 Rule 64(1) ICC RPE.

95 Art. 64(2) ICCSt.

96 Art. 64(8)(b) ICCSt. See also Arts 64(9) and 69(4) ICCSt.

inherently connected, issues. The first is the timing of evidentiary decisions. In particular, at what stage of the proceedings (i.e., during trial or in the final judgment) decisions on admissibility should be rendered. The second concerns the way in which judges evaluate evidence and articulate their reasoning — specifically, whether the Judges must rule on the admissibility for each item of evidence.

The timing of evidentiary decisions can follow two varying approaches.[97] The 'admission model', by which each piece of evidence is assessed at the moment it is submitted by the party, was the practice followed by the Judges in *Lubanga*,[98] and *Katanga and Ngudjolo*.[99] The alternative is the 'production or submission model', when the Chamber delays the admissibility assessment to the end of the trial. Until then, the evidence is considered just submitted or produced before a Chamber. Such was the model followed by the Trial Chambers in *Gbagbo and Blé Goudé*,[100] the Appeals Chamber Majority Decision in *Bemba et al.* (supporting the practice of the Trial Chamber),[101] and the Trial Chamber in *Ongwen*.[102] As already advanced, there is a second connected issue, which is how the Judges reason their decision. Academics have analysed the jurisprudence of the Court and previous tribunals at length, identifying the emergence of two different approaches to the evaluation of evidence that follow two schools of thought.[103] These are the 'atomistic or deconstruction' approach, versus a 'holistic or intuitive holistic' assessment.[104]

97 F. Guariglia, '"Admission" v. "Submission" of Evidence at the International Criminal Court: Lost in Translation?' 16 *Journal of International Criminal Justice* (2018) 315–339.

98 Decision on the admissibility of four documents, *Lubanga*, (ICC-01/04-01/06-1399), Trial Chamber I, 13 June 2008, § 27.

99 Decision on the Prosecutor's Bar Table Motions, *Katanga and Ngudjolo Chui* (ICC-01/04-01/07-2635), Trial Chamber II, 17 December 2010.

100 Decision on the submission and admission of evidence, *Gbagbo and Blé Goudé* (ICC-02/11-01/15), Trial Chamber I, 29 January 2016, § 12.

101 *Bemba et al.* case, *supra* note 82, at §§ 599 and 601.

102 Initial Directions on the Conduct of the Proceedings, *Ongwen* (ICC-02/04-01/15-497), Trial Chamber IX, 13 July 2016, § 24.

103 For a seminal work on the different approaches to the evaluation of evidence across legal traditions, see M.R. Damaška, 'Atomistic and holistic evaluation of evidence: a comparative view', in D.S. Clark (ed.) *Comparataive and Private International Law: Essays in Honor of John Henry Merryman* (Duncker & Humblot, 1990), at 91–104. For other analysis of domestic jurisprudence: M. Schweizer, 'Comparing Holistic and Atomistic Evaluation of Evidence', 13 *Law, Probability and Risk* (2014) at 65–89; M.S. Pardo, 'Juridical Proof, Evidence, and Pragmatic Meaning: Toward Evidentiary Holism', 95 *Northwestern University Law Review* (2000) 399–442; J.L. Mnookin, 'Atomism, Holism, and the Judicial Assessment of Evidence', 60 *UCLA Law Review* (2013) 1524–1585.

104 See for instance, Y. McDermott, 'Strengthening the Evaluation of Evidence in International Criminal Trials', 17 *International Criminal Law Review* (2017) 682–702. See also, Y. McDermott, 'The International Criminal Court's Chambers Practice Manual: Towards a Return to Judicial Law Making in International Criminal Procedure?' 15 *Journal of International Criminal Justice* (2017) 873–904; Y. McDermott, 'Inferential Reasoning and Proof in International Criminal Trials: The Potentials of Wigmorean Analysis', 13 *Journal of International Criminal Justice* (2015), 507–533, and M. Klamberg, 'Epistemological Controversies and Evaluation of Evidence in International Criminal Trials', in K.J. Heller

In ICC practice, the first approach favours an examination of each piece of evidence in the context of the full record before supporting a conclusion.[105] This reasoning methodology was taken by Judge van den Wyngaert in the judgment for *Katanga* (criticized by her colleagues),[106] and the Appeals Chamber in *Ngudjolo* (also raising a dissenting opinion).[107] In contrast, the holistic method evaluates the evidence as a whole.[108] This was the practice followed largely by the Appeals Chamber in *Lubanga* (upholding the evidentiary analysis of the Trial Chamber),[109] the Appeals Chamber Majority decision in *Bemba et al.* (supporting the practice of the Trial Chamber),[110] the Trial Chamber in *Ntaganda*[111] and the Trial Chamber in *Gbagbo and Blé Goudé.*[112]

The founding documents of the ICC gave ample flexibility to the Judges to conduct proceedings in the manner they best see fit.[113] The practice that has emerged begs the question of how the volume and vulnerability of digital information will stand the evidentiary test of relevance and admissibility. While the submission model seems to be anchored on the idea that it is preferable to assess evidence as a whole,[114] it is worth noting that these approaches or models are not incompatible.[115] Evidentiary rulings during the trial (i.e. admission model) do not preclude a holistic assessment of the

et al. (eds), *The Oxford Handbook of International Criminal Law* (Oxford University Press, 2020) chapter 19.

105 McDermott, *supra* note 104.

106 Judgment pursuant to Article 74 of the Statute, Concurring opinion of Judges Fatoumata Diarra and Bruno Cotte, *Katanga* (ICC-01/04–01/07), Trial Chamber II, 7 March 2014, § 4.

107 Judgment on the Prosecutor's Appeal against the Decision of Trial Chamber II entitled 'Judgment Pursuant to Article 74 of the Statute', Joint Dissenting Opinion of Judge Ekaterina Trendafilova and Judge Cuno Tarfusser, *Ngudjolo Chui* (ICC-01/04-02/12-271-AnxA), Appeals Chamber, 7 April 2015, §§ 44–51.

108 McDermott, *supra* note 104, at 688.

109 Judgment on the appeal of Mr Thomas Lubanga Dyilo against his conviction, *Lubanga* (ICC-01/04–01/06A5), Appeals Chamber, 1 December 2014, §§ 22.

110 Judges van den Wyngaert and Morrison point out that in some cases, the Chambers have taken a somewhat mixed approach, generally appraising the body of evidence as a whole, but also making a few itemized decisions on specific pieces of evidence. *Bemba et al.* case, *supra* note 82, at §§ 600 and 601.

111 Judgment, with public Annexes A, B and C, *Ntaganda* (ICC-01/04-02/06), Trial Chamber VI, 8 July 2019, § 45.

112 Reasons for oral decision of 15 January 2019 on the Requête de la Défense de Laurent Gbagbo afin qu'un jugement d'acquittement portant sur toutes les charges soit prononcé en faveur de Laurent Gbagbo et que sa mise en liberté immédiate soit ordonnée, Public Redacted Version of Reasons of Judge Geoffrey Henderson, *Gbagbo and Blé Goudé* (ICC-02/11-01/15-1263-AnxB-Red), Trial Chamber I, 16 July 2019, §§ 31, 255, 1056, 1121, 1667 and 1864.

113 Piragoff and Clarke, *supra* note 86, at 1715. See also, C. Kress, 'The Procedural Law of the International Criminal Court: Anatomy of a Unique Compromise', 1 *Journal of International Criminal Justice* (2003) 603–617, at 603, 605, 606.

114 For example, Decision concerning the Prosecutor's submission of documentary evidence on 13 June, 14 July, 7 September and 19 September 2016, *Gbagbo and Blé Goudé* (ICC-02/11-01/15-773), Trial Chamber I, 9 December 2013, § 33. Also, Guariglia, *supra* note 97; citing *Bemba et al.* case, ft. 22.

115 Guariglia, *supra* note 97, citing *Bemba et al.* case, at 322.

evidence and the full record.[116] In the Court's first case alone, the Trial Chamber heard 67 witnesses and received 1,373 items of documentary evidence from the Parties.[117] As ICC investigations get closer to crimes committed in contexts where digital information is more readily available, judges may struggle with troves of evidence the relevance and reliability of which may be difficult to establish without the aid of experts who would need to be called during the proceedings. Hence, digital evidence may increasingly require the Trial Chambers to make early deliberations on admissibility to allow the parties to introduce arguments at the time, improving the judges' understanding of that evidence.

In addition, the highly personal and often intrusive nature of many types of digital evidence will raise important issues around privacy. The Appeals Chamber has concluded that the right to privacy is an actionable right under Article 69(7),[118] and the jurisprudence supports early admissibility decisions to avoid continued interference throughout the duration of the trial.[119] With data protection laws evolving rapidly, such challenges to admissibility based on violating an individual's right to privacy will inevitably increase in the Information Age. The assessment of the probative value and prejudicial effect of evidence will also become increasingly complex and critical in the Information Age, particularly with machine-generated data and digital information derived from secondary sources. Certain types of digital evidence, such as cell site data,[120] cannot be evaluated as if they were an exact science,[121] but can serve as highly probative circumstantial evidence. When the interpretation of data requires the use of software to translate the data points into information that can be understood by humans, judges will need at least some minimal specialized training and expertise before drawing inferences from the data.[122] They will also have to learn to strike a balance between

116 Judgment, Separate Opinion of Judge Henderson, *Bemba et al.* (ICC-01/05-01/13-2275-Anx), Appeals Chamber, 8 March 2018.

117 *Lubanga* case, *supra* note 63, at 14, § 11.

118 Decision on Requests to Exclude Western Union Documents and other Evidence Pursuant to Article 69(7), *Bemba et al.* (ICC-01/05-01/13-1854), Trial Chamber VII, 29 April 2016; Decision on Requests to Exclude Dutch Intercepts and Call Data Records, *Bemba et al.* (ICC-01/05-01/13-1855), 29 April 2016; *Lubanga*, *supra* note 64, at §§ 81–86.

119 For other scenarios, where early admissibility decisions could be necessary and examples of jurisprudence supporting a preliminary exam under Rule 68 (admission of prior recorded testimony), Rule 71 (evidence of the prior sexual conduct of the victim or witness) and Rule 72 (in camera procedures when dealing with consent to an alleged crime of sexual violence) of the ICC RPE; Guariglia, *supra* note 97.

120 Cell site analysis uses call data records to identify the potential location of a phone.

121 Denmark had to review 10,700 court cases to assess whether errors in the interpretation of cell phone location data led to incorrect convictions. M.S. Sorensen, 'Flaws in Cellphone Evidence Prompt Review of 10,000 Verdicts in Denmark', *The New York Times*, 20 August 2019, available online at https://www.nytimes.com/2019/08/20/world/europe/denmark-cell phone-data-courts.html (visited 18 February 2021).

122 For instance, location data points, which are a string of numbers and codes, need first to be translated into geolocation coordinates by a software. These coordinates can then be plotted on a map, from which a human can draw an inference.

being overly permissive — and give too much weight to digital evidence that may appear quasi-scientific when it is not — and being overly restrictive for fear of misinterpreting the data.

4. Preparing the Court for the Future

This article has brought to light some of the most important dilemmas with which the ICC will have to wrestle in keeping up with technological change. Our analysis shows that deep reflection and action are unquestionably needed. However, this does not necessarily require amending the Statute or the Rules, which can be a difficult feat. Rather, many of the coming challenges could be addressed by updating the interpretations of existing rules and adopting new practices and technologies. This part identifies the areas we believe require action or at least merit further discussion.

A. Create Guidelines for Online Investigations in Compliance with Article 54 (1)(a)

The prosecutor's duty to establish the truth is uncontroversial, but the interpretation of Article 54(1)(a) is still developing. In a 'post-truth world', establishing facts is a much more complex affair. The magnitude of potential evidence for mass atrocities in the Information Age, paired with the limited budget and resources upon which the ICC operates, requires a delicate balancing act between the prosecutor's duty to investigate all circumstances and the efficiency of the proceedings. Investigators will have to make difficult decisions about what to review and collect. When online investigators are faced with millions of potentially relevant tweets and TikTok videos related to a single incident, they will need clear guidance on their duty and direction from lawyers on what is relevant given the case hypothesis. Thus, a narrow and reasonable interpretation of Article 54(1)(a) by the judges, acknowledging the challenges of the online information environment, in combination with more pre-planning on the part of the prosecutor to better guide investigators could go a long way in addressing these issues.

B. Allow for Early Digital Preservation during Preliminary Examinations and Investigations

The fleeting nature of probative digital evidence raises the question of what kind of interventions are appropriate, or even possible, under the current Statute. While the prosecutor's powers are limited before an investigation is open, the borderless nature of the internet and spread of digital communications may require a relaxing of these limitations during preliminary examinations. Valuable digital information available during the buildup or the early stages of a conflict might be lost if the prosecutor cannot intervene and

preserve it in a forensically sound manner until an investigation is opened. For example, the prosecutor should be able to use the cooperation framework to make requests to telecommunications and internet service providers to preserve user data beyond their usual retention periods. While state cooperation is voluntary during the preliminary examination stage, state parties should see this as part of their duty to support the Court. In addition, the prosecutor should utilize automated tools for bulk collection and analysis of internet data, and even considering playing a role in securing digital devices and data in high risk environments as early on as possible.

During the investigation phase, the use of Article 56 could be creatively applied to preserve digital information in countries where the prosecutor is not allowed to enter the physical territory. As of January 2020, the prosecutor has only used Article 56 to preserve the testimony of witnesses that are likely to become unavailable,[123] but there is no reason why this provision should be limited to testimonial evidence. Digital evidence may be stored in multiple locations, and its collection may not require physical access to the territory of a state. This is a crucial development for ICC investigators, who rely on the cooperation of state authorities to be able to access and seize evidence. Lack of international assistance has hampered investigations in the past, but with data being stored across borders and traveling through servers hosted in many different countries, the prosecutor should think creatively about how state parties can facilitate the preservation of digital evidence in transit or in servers that can be accessed in territories within the Court's jurisdiction. While the prosecutor may still need judicial cooperation to avoid breaking cybersecurity and privacy laws, digital evidence opens up a range of remote investigative practices that may not require the assistance of unwilling states. It is out of the scope of this article to delve into the options that could be used to access, examine or preserve digital evidence — some of which would undoubtedly be controversial. Our suggestion is that the use of Article 56 for these purposes is poised for legal and investigative creativity, and this area requires further attention.

C. Issue Early Admissibility Decisions to Avoid Cluttering the Evidentiary Record

Regardless of Chambers adopting an atomistic or holistic approach to judicial decision-making, neither of these two options preclude the Judges from issuing evidentiary rulings during pre-trial or trial. With the ICC moving closer to investigations where digital information may be more readily available, new sources of evidence will enter the courtroom, generating larger case files. Some digital evidence may also require the aid of experts for establishing its relevance and reliability, allowing the parties to introduce arguments that can help improve the Judges understanding of the evidence presented. If evidence is manifestly irrelevant or unreliable, judges may have to exercise their

123 P. Bradfield, 'Preserving Vulnerable Evidence at the International Criminal Court – the Article 56 Milestone in *Ongwen*', 19 *International Criminal Law Review* (2019) 373–411.

discretion under Article 69(4) and exclude it in order to avoid cluttering the evidentiary record.[124] If left unchecked, increased accessibility to information can risk translating into an approach of 'paper over cracks' — with deficiencies of certain pieces of evidence being 'sanitized' by submitting more evidence.[125] This cumulative effect may generate inefficiencies in the proceedings, in turn jeopardizing the rights of the accused and undermining the fairness of the trial.

D. Provide Clear and Logical Reasoning on How Evidence is Relied on by Judges

Jurisprudence not only helps shape future cases, but can also set the standards by which evidence is collected and justice is served. Explaining which items of evidence supported the prosecution's theory of the case — or in the contrary, acted in favour of the accused — not only meets the more immediate and obvious goal of determining the role of the defendant in the alleged acts. Such reasoning can also clarify the Judges' expectations for all parties, and help defence counsel prepare better their counter-arguments — in turn upholding the rights of the defendant. In pointing out the deficiencies in the evidence, Chambers can provide the parties with valuable guidelines that can help them determine the quality of their information prior submission to the prosecutor or the Court. With first responders now using smartphones to capture photos and videos that can be probative of crimes, and civil society collecting potentially relevant information from the internet, the ICC will have to deal with a large number of actors gathering information following varying standards. Transparency and clarity can then have self-regulatory effects in the long term, eventually establishing a benchmark for evidence gathering. This would not only ease the burden of the Office of the Prosecutor (OTP) in having to verify and authenticate an ever-increasing number of disparate sources of information, but would also contribute to the overall development of international criminal investigations.

E. Educate All Parties, from First Responders to the Judges

The ability of the Judges to clearly explain their admissibility rulings will increasingly depend on their capacity to interrogate technology systems, enhance their familiarity with digital evidence, and increase their understanding of new sources of information. The role of expert witnesses will be crucial, and the Registry will play an important part in making sure their roster of experts can help the Judges comprehend the intricacies of highly technical evidence. However, a reliance on experts will be insufficient. Defence, prosecution, victims' representatives and judges should be open to specialized training that

124 In a similar vein, for an assessment of evidence limited to relevance, see M. Klamberg, *Evidence in International Criminal Trials: Confronting Legal Gaps and the Reconstruction of Disputed Events* (Martinus Nijhoff, 2013), at 357, 513; also, Guariglia, *supra* note 97.

125 McDermott, *supra* note 104, at 688.

gives them the foundation they need to investigate or adjudicate crimes that will progressively involve a significant amount of technology. This training can be of different degrees of complexity and depth depending on the Party, but it should also include first responders and civil society groups — which play an active role in collecting and preserving information available online. Building the technological knowledge of all parties involved across the life cycle of evidence, from capture to assessment, will improve investigative and judicial practice. Additionally, members of the Assembly of States Parties must also understand the importance of investing in training and infrastructure that will be increasingly critical for the operations of the Court. There have been notable attempts at translating complex science and technical jargon into understandable guidelines or tools.[126] However, these initiatives will be of little value if there is not a concerted effort to prepare all parties for the courtrooms of the future.

F. Invest in IT Infrastructure and Regular Updates to the E-court Protocol

In order to keep pace with technological change, the e-Court Protocol should be reviewed and updated regularly by a committee with representatives of all organs of the Court and other stakeholders. The ICC can look for solutions to this dilemma in domestic jurisdictions where those dealing with complex civil litigation have faced similar challenges. In recent years, the United States, Canada and the United Kingdom have developed new e-discovery guidelines, which can serve as a reference point for reforms to the Rules and e-Court Protocol.[127] The challenges raised by digital evidence cannot be solved through legal and policy changes only; they will also require the adoption of new technologies that can be used to improve the collection, preservation,

126 S. Dubberley, A. Koenig and D. Murray (eds), *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability* (Oxford University Press, 2020); the Human Rights Center at UC Berkeley School of Law developed the *Berkeley Protocol on Digital Open Source Investigations* with the UN Human Rights Office. Organizations like EyeWitness to Atrocities have done research on how to maintain authenticity and chain of custody of transmitted and preserved digital images and videos. See also: The Public International Law & Policy Group (PILPG), 'Chapter 3, Collection of Information', in *Handbook on Civil Society Documentation of Serious Human Rights Violations* (2016), available online at https://www.vu.nl/nl/Images/PILPG_Handbook_on_Civil_Society_Documentation_of_Serious_Human_Rights_Violations_Sept_2016_tcm289-785328.pdf (visited 18 February 2021); Global Rights Compliance (GRC), *Basic Investigative Standards ('BIS') for First Responders to International Crimes*, (2017), available online at https://www.globalrightscompliance.com/en/news/grc-publishes-basic-investigative-standards-for-first-responders-to-international-crimes (visited 18 February 2021).

127 For instance, UK Crown Prosecution Service, 'Disclosure Manual', 26 February 2018, available online at https://www.cps.gov.uk/legal-guidance/disclosure-manual (visited 18 February 2021); UK Crown Prosecution Service, 'National Disclosure Improvement Plan', January 2018; and US Department of Justice, 'Recommendations for Electronically Stored (ESI) Discovery Production', February 2012. See also S. Broderick et al., 'Criminal E-Discovery: A Pocket Guides for Judges', Federal Judicial Center, 2015.

review, and analysis of digital information.[128] Technology changes faster than the law, in contrast to procurement processes within international organizations like the ICC, which are slow and bureaucratic. Thus, the IT infrastructure, including hardware and software, used for the processing, storage and management of digital evidence must be robust, up to date, and available to all parties who need it, including defence and the legal representatives of the victims. Cultivating relationships with academia and the private sector to keep abreast of the latest developments on technologies such as machine learning and artificial intelligence, and exploring how they can be applied to the work of the Court is essential. This will require a sustainable financial commitment from the assembly of states parties, which approves the budget.

5. Conclusion

Almost 20 years since the entry into force of the Rome Statute, it is worth examining how the operational environment of the ICC has changed. This article addressed how the Rules of Procedure and Evidence will fare when faced with the challenges posed by newer types of digital evidence. The digitalization of information and communications, while presenting new and exciting investigative opportunities, has made it increasingly difficult to find the signal (reliable, direct evidence) in the noise (indirect evidence, hearsay, misinformation and disinformation). Further, with digital evidence becoming more available but also being vulnerable to loss and alteration, the duties of the prosecutor will be impacted — in particular, the obligations connected to the collection, acquisition and disclosure of information. Judges must also be vigilant in their interpretation of the rules of evidence and procedure to avoid undermining the efficiency and fairness of proceedings. In studying the relevant provisions of the Statute and the Rules vis-à-vis the unique attributes of digital evidence, we hope to shine a light on the most important issues that the Court will face in the near future, and some of their long-term effects if left unchecked. Lastly, while not intending to be prescriptive nor exhaustive, this article has offered some suggestions to help the Court prepare for the challenges ahead.

128 M. Dillon and D. Beresford, 'Electronic Courts and the Challenges in Managing Evidence: A View from Inside the International Criminal Court', 6 *International Journal for Court Administration* (2014) 29–36.