Using the Leiden Guidelines to address key issues in digitally derived evidence

Irving, E.; Heinsch, R.W.; Rewald, S.

Using the Leiden Guidelines to Address Key Issues in Digitally Derived Evidence

opiniojuris.org/2022/08/23/using-the-leiden-guidelines-to-address-key-issues-in-digitally-derived-evidence/

August 23, 2022

*[**Dr. Emma Irving**, M.A., LL.M., is a consultant in the fields of international criminal law, human rights, and technology and was formerly the senior researcher in the Leiden IHL Clinic's Digitally Derived Evidence Project. **Dr. Robert Heinsch**, LL.M. is an Associate Professor of Public International Law at the Grotius Centre for International Legal Studies of Leiden University, and is the Director of its Kalshoven-Gieskes Forum on International Humanitarian Law as well as the founder of the Leiden IHL Clinic. **Sabrina Rewald**, J.D., LL.M., is a researcher at the Kalshoven-Gieskes Forum on International Humanitarian Law and a supervisor of the Leiden IHL Clinic's Digitally Derived Evidence Project.]*

Introduction

The invasion of Ukraine has focused the world's attention like never before on the importance of Digitally Derived Evidence ("DDE") for accountability in conflict zones. Efforts to document the Ukrainian conflict through digital means have been in high gear since the beginning – e.g., three days after the invasion began, an interactive map was launched to plot conflict related events as they happened. Civilians on the ground are submitting videos and photos of war activity and crimes using digital tools that have been set up or repurposed by Ukrainian authorities. The importance of the digital material being carried by everyday Ukrainians on their smartphones was also recognised by foreign

governments. The UK posted signs at entry points asking Ukrainian arrivals to share photos, videos, and other information they might have relevant to war crimes and crimes against humanity with police. This potential evidence is being handled by UK police who in turn are supporting the ICC Ukraine investigation.

The situation regarding digital material in Ukraine is far from unique; all modern-day conflicts leave a digital footprint. The Syrian conflict is said to be the most heavily documented in history, which has enabled countries such as the Netherlands and Sweden to convict individuals of war crimes using DDE. Other conflict areas with a significant digital footprint include Myanmar, Cameroon, Iraq, Libya – the list goes on.

The global developments have shown one thing clearly: there is a lack of guidance and clarity when it comes to using DDE in the courtroom. Due to the fast evolution of digital technology and the (often, by design) slow evolution of courts and tribunals, the treatment of DDE within and between national and international accountability fora suffers from an absence of uniformity at best, and a lack of any useful guidance at worst.

The Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals ("The Leiden Guidelines") were created to address this legal lacuna by examining the various ways in which DDE has been treated in international criminal law. The Guidelines identify overarching standards of treatment, derived from the jurisprudence of international criminal courts and tribunals ("ICCTs"), that practitioners should consider when collecting and tendering DDE.

The increase in the importance of DDE in international accountability processes does not come without its challenges. Four such challenges, and how they are addressed by the Leiden Guidelines, are highlighted below.

Inherent Problems Related to DDE Before ICCTs That are Addressed by the Leiden Guidelines:

1. Need for Expertise to Translate Tech Evidence, Impacting Time and Resources

DDE is often highly technical in nature, and can require certain expertise to understand fully. Take Call Data Records (CDRs) as an example: in their raw form, CDRs are strings of numbers that mean nothing to the untrained eye. When properly analysed, CDRs can be converted into Call Sequence Tables (CSTs), which allow for individual mobile phones to be traced. In *Ayyash et al* at the Special Tribunal for Lebanon, CSTs were important evidence identifying the defendants as being involved in the assassination of Prime Minister Hariri.

In acknowledgement of the complexity of using CDRs as evidence, Leiden Guideline E1, for example, stipulates that relevant data should be extracted from CDRs and presented to the court as CSTs. Furthermore, Leiden Guideline E4 indicates that the reliability of the CSTs depends on the authenticity of the underlying CDRs, which must be proven through an expert witness.

Satellite and aerial images seem, by contrast, simpler to understand; they provide a birds-eye view of significant sites in a conflict, allowing, for example, for the identification of mass graves or the massing of troops. However, the technical processes that go into retrieving, verifying, and storing satellite images are not straightforward.

For this reason, Leiden Guideline C6 states that satellite and aerial images should be considered authentic and reliable if they are corroborated by an expert or witness. This includes information about whether such images can be altered, how they are dated, and how they were used in an investigation.

2. Voluminous Nature of the Evidence, Impacting Time

When working with DDE, investigators and lawyers can be faced with an enormous amount of data. The sheer volume of digital information produced as a result of modern-day conflicts is difficult to fathom: hundreds of thousands of hours of videos, millions of photos, countless mobile phone calls. Added to this is the complication that a large amount of DDE exists in duplicate form because of the many actors engaged in collecting this information, including national and international bodies, NGOs, private individuals, and so on. From among these terabytes of data investigators must find relevant, probative evidence to present in accountability proceedings. This is no small task.

In relation to CDRs and satellite and aerial images, the Leiden Guidelines provide some assistance when it comes to how voluminous DDE should be presented in court: For CDRs, the commentary of Leiden Guideline E1 elaborates on how the makeup of CSTs can translate unwieldy CDRs into a more accessible format, and Leiden Guideline C1 states that voluminous satellite and aerial imagery material can be entered into evidence via expert summary reports. For the latter, this approach can be taken when the evidence goes to proof of a matter other than the acts and conduct of an accused as charged in the indictment.

The Guidelines do not currently offer direction beyond how some types of voluminous DDE should be presented in court. In particular, they do not discuss how investigators should approach the large amount of data they must grapple with on a daily basis. This is due to the lack of case law on this point, but is a matter that should be closely monitored as the courts become more comfortable and confident in the role of DDE in accountability proceedings.

3. Difficulties Establishing the Probative Value of Open Source Information

Videos, photographs and audio recordings posted online by individuals or journalists on the ground can help to establish crucial details and build a picture of a conflict that might otherwise be inaccessible. Yet, another dilemma when it comes to DDE concerns establishing the probative value of such open source material. Assessing probative value is a fact-specific inquiry that involves analysing various indicia of reliability and authenticity, and DDE that is open source may lack crucial information as to how and by whom the evidence was made.

ICCT deliberations on open source social media DDE have yet to be substantial enough to warrant curated guidelines. Nevertheless, the Leiden Guidelines derived from discussions on the probative value of open source audio and video media broadcasts serve as a helpful starting point. In this context, Leiden Guideline A6 states that the reliability of an open source media broadcast from a well-known media source is bolstered by its public availability on the media outlet's official website. Other indicia of reliability for open source broadcasts include the date of the DDE's emission, images or voices of the interviewees, and media source logos on video broadcasts (particularly if they are continually displayed and uninterrupted). Given the fact that any online DDE can also be removed from the internet, the Guideline's commentary states that the provision of a verifiable date and location as to where the DDE had previously been found online can in itself serve as indicia of reliability.

4. Challenges Ensuring the Chain of Custody

In a world of increasingly indistinguishable deepfakes, providing a clear chain of custody of DDE is key to establishing its prima facie authenticity and, thereby, probative value. The ICC e-Court protocol offers guidance as to how the OTP should manage digital evidence and maintain its chain of custody once in the OTP's hands. Such an intra-institutional chain of custody guidance is necessary; indeed, investigators may need to verify the evidentiary implications of any changes they make to DDE they receive. For example, if DDE is in some way distorted upon receipt, any steps taken by investigators to correct the distortion may run the risk of inadvertently undermining the DDE's probative value.

And yet, before reaching a prosecutor's hands, the handling of DDE from creation to collection is often the most critical, and difficult, part of a chain of custody to establish with certainty. As an illustration, Leiden Guideline D3 outlines how a prima facie basis to admit intercepted communication evidence exists where the person who originally intercepted the communication testifies to its chain of custody. Where witness testimony is unavailable to make such an attestation, the Guideline's commentary outlines how the authenticity of intercept evidence, for example, can be bolstered: An *overwhelming* weight of corroborating evidence, such as forensic reports of the intercept or another officer's identical intercept of the same conversation, can serve to ameliorate the DDE's theoretical possibility of tampering.

5. Even Less Information to Come?

Over the past decade, ICC Judges have been making far less focused deliberations on admissibility. This is due to a shift to a submission standard, permitting evidence to be submitted and leaving admissibility to be determined at the close of proceedings per the procedural discretion provided under Rule 63(2) of the ICC Rules of Procedure and Evidence. What this means for DDE before the ICC in particular is that the nuances of admissibility criteria of novel or less-discussed forms of DDE may not be assessed and known until Judgement. It also means that key discussions by chambers on the treatment of DDE that would have otherwise been found in decisions on the admission of evidence

will diminish, as the Judgement, in the end, may still fail to elaborate, substantially or at all, on the relevance, probative value, and/or prejudicial effect of specific forms of DDE. For example, the ICC Trial Chamber in *Al Hassan* sidestepped discussion of the probative value of sixty-three open source exhibits by permitting their submission and postponing until Judgement any discussion as to their admissibility.

Outlook for the Future of (Digital) Investigations of International Crimes

With the 20th anniversary of the ICC on 1 July 2022, and after almost three decades of modern international criminal law jurisprudence since the establishment of the ICTY on 25 May 1993, we have reached a turning point with regard to how investigations of international crimes are being conducted. Recent case law at the ICC, STL and in national jurisdictions as well as the developments in the context of the Ukraine conflict, but also in Myanmar, Iraq and Libya, have shown that more and more reliance is put on digitally derived evidence. It seems inevitable that within the next decade the traditional reliance of international prosecutors on witness statements will be heavily complemented by the use of digital evidence. With the widespread use and availability of video and photo capacities on mobile phones even in conflict zones, the unreliability of witness statements can be improved by the use of DDE. The possibilities for national and international investigators to build cases against war criminals will increase dramatically, since digital evidence is often easier to access than witness statements. However, this positive development can only lead to higher accountability of war criminals if investigators, prosecutors, and judges are also aware that digital evidence is not the same as physical evidence and that there are inherent dangers in relying on this kind of evidence due to the possibilities of manipulation. This is exactly where the Leiden Guidelines on Digitally Derived Evidence come in and offer an important first step in establishing objective and legally sound standards for using DDE in international criminal proceedings.