doi:10.1017/aju.2024.1

INTRODUCTION TO THE SYMPOSIUM ON DIGITAL EVIDENCE

*Tamar Megiddo** and *Melissa J. Durkee***

The past few decades have seen radical advances in the availability and use of digital evidence in multiple areas of international law. Witnesses snap cellphone photos of unfolding atrocities and post them online, while others share updates in real time through messaging apps. Immigration officers search cell phones. Private citizens launch open-source online investigations. Investigators scrape social media posts. Digital experts verify authenticity with satellite geolocation. These new types of evidence and digitally facilitated methods and patterns of evidence gathering and analysis are revolutionizing the everyday practice of international law, drawing in an ever-wider circle of actors who can contribute to its enforcement and use. Predictably, this evidentiary transformation brings both new possibilities and new risks. This symposium evaluates the state of the art of digital investigation across several areas of international law. It asks what digital evidence is contributing to the international rule of law, and where it poses challenges and should inspire caution or reform.

The prominence of digital evidence is most obvious in the context of international criminal law, which is also where it has received the most academic attention.[1] Over the past years, private keyboard warriors have gathered crucial evidence of international crimes from social media platforms and other online sources. Often it is not officials, but private individuals and civil society organizations that discover this evidence and collaborate with national and international authorities.[2] Indeed, the contributions by non-officials are so significant that the International Criminal Court recently launched a platform aimed at streamlining the submission of evidence by outsiders.[3]

Beyond the realm of international criminal law and the uncovering of mass atrocities, digital evidence has proven consequential for developments in other areas of international law. These impacts have not usually been considered together as products of digital evidence. Viewing these diverse legal moments through the lens of the digital evidence that facilitated them shows the growing significance of digital methods and tools.

For example, as part of its war effort, Ukraine collaborated with private actors like Microsoft, Google, Amazon, and ESET to track, document, and anticipate Russian cyber-attacks.[4] The European Parliament relied in part on

* *Senior Lecturer, Department of International Relations, Hebrew University of Jerusalem, Israel; Research Associate, Three Generations of Human Rights Research Project, Faculty of Law, Hebrew University of Jerusalem, Israel (European Research Council Grant No. 101054745).*

** *Professor of Law, Washington University in St. Louis, United States.*

[1] Lindsay Freeman & Raquel Vazquez Llorente, *Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age*, 19 J. Int'l Crim. Just. 163 (2021); Rebecca J. Hamilton, *Social Media Platforms in International Criminal Investigations*, 52 Case W. Res. J. Int'l L. 213 (2020); Elizabeth White, *Closing Cases with Open-Source: Facilitating the Use of User-Generated Open-Source Evidence in International Criminal Investigations Through the Creation of a Standing Investigative Mechanism*, Leiden J. Int'l L. 1 (2023).

[2] Eliot Higgins, We Are Bellingcat: Global Crime, Online Sleuths, and the Bold Future of News (2021).

[3] ICC Press Release, ICC Prosecutor Karim A.A. Khan KC Announces Launch of Advanced Evidence Submission Platform: OTPLink.

[4] Stéphane Duguin & Paulina Pavlova, *The Role of Cyber in the Russian War Against Ukraine: Its Impact and the Consequences for the Future of Armed Conflict* 7 (European Parliament Working Paper, July 2023).

© The Author(s) 2024. Published by Cambridge University Press for The American Society of International Law. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.1017/aju.2024.1 Published online by Cambridge University Press

documentation by an open-source online evidence-gathering platform to understand Russia's use of cyber warfare in that conflict and its international legal implications.[5] Digital evidence obtained through the Panama Papers leak was key to revealing illegal bribery of foreign officials, activity that contravenes the OECD Convention on Combating Bribery of Foreign Public Officials in International Business.[6] Governments seeking to strengthen immigration controls and to prevent the entry of asylum seekers have relied on digital evidence from personal cell phones and other sources.[7] Digital evidence has exposed the harms of commercial, military-grade spyware and propelled efforts to strengthen controls over the international trade in this technology.[8] Going forward, digital evidence may prove increasingly crucial in land and maritime border disputes, trade disputes, investor-state arbitration, and other areas.

Given its potential to help uncover facts, digital evidence should presumably hold significant promise for international law and the delivery of international justice. Indeed, digital evidence can expose illegal acts, leading to better enforcement of law, and reveal harmful activity that should be subject to regulatory control. Yet, the rise of digital evidence nevertheless evades easy normative categorization. It can be used to enforce law against powerful international criminals and disempowered asylum seekers alike and can be used equally by the aggressor and defender in an illegal use of force.

Increasing reliance on digital evidence can raise a raft of procedural concerns. Evidence gathering by citizens and activists may be difficult to reconcile with traditional criminal procedure rules concerning chain of custody over evidence. Evidence gathering by non-state actors may also raise concerns of bias regarding which situations merit investigation, by whom, and in what manner. What rules should apply to the way digital evidence is collected, authenticated, stored, and used? Civil society and the United Nations have responded to some of these challenges and critiques by developing ethical guidelines, such as the Berkeley Protocol on Digital Open-Source Investigations.[9] As the essays in this symposium demonstrate, those guidelines are a start, but the issues are far from resolved.

Concerns also arise when digital evidence is gathered by formal authorities. For example, is it possible to address bias in availability of evidence when an investigation is conducted in the territory, and with the collaboration, of only one party to a conflict? The conflict in Ukraine is the key contemporary case in point.[10] Do judges and arbitrators across different fora and issue areas possess the necessary expertise to evaluate such evidence? How could international law address new technological developments, such as generative Artificial Intelligence (AI), which increases concerns about the verifiability and authenticity of digital evidence and its potential for manipulation and deceit?

The contributors to this symposium address the rise of digital evidence as a larger, trans-substantive process of emerging importance in international law. The first four essays take up ethical guidelines for citizen investigators and open-source investigations as well as the use of digital evidence in courts and other fora. The fifth and final essay turns to the substantive question of the normative desirability of some digital evidence practices.

[5] *Id.* at 5.

[6] International Consortium of Investigative Journalists, *The Panama Papers: Exposing the Rogue Offshore Finance Industry* (Apr. 3, 2016).

[7] Dennis Broeders, *The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants*, 22 Int'l Sociology 71 (2007).

[8] Siena Anstis, Ron Deibert & Jakub Dalek, *The Ethical and Legal Dilemmas of Digital Accountability Research and the Utility of International Norm-Setting*, 118 AJIL Unbound 40 (2024); UN Human Rights Council, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Surveillance and Human Rights, UN Doc. A/HRC/41/35 (May 28, 2019).

[9] The Berkeley Protocol is an initiative aimed to tackle these concerns, among others. Berkeley Protocol on Digital Open-Source Investigations: A Practical Guide on the Effective Use of Digital Open-Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law (United Nations & University of California, Berkeley eds., 2022).

[10] Tal Mimran and Lior Weinstein, *Digitalize It: Digital Evidence at the ICC*, Lieber Institute West Point (2023).

https://doi.org/10.1017/aju.2024.1 Published online by Cambridge University Press

Siena Anstis, Jakub Dalek, and Ronald J. Deibert of the University of Toronto's Citizen Lab coin the phrase "digital accountability research," which they define as "evidence-based research seeking to track and expose risks to civil society in the digital ecosystem."[11] Their essay lays out the ethical and legal dilemmas that face the digital accountability researcher: which ethical and legal rules should these researchers draw on to guide their work? Should they, for example, expose digital espionage against civil society when doing so would also reveal secret government espionage campaigns against legitimate targets? Or should they publish previously undisclosed zero-day vulnerabilities and thus expose users to targeting by malicious actors who may exploit them? The authors also suggest some answers to this battery of questions. International norm-setting, institution-building, and community-building, the authors conclude, are needed so that researchers can consult with each other on ethical decision-making norms and legal constraints.

Alexa Koenig of the University of California, Berkeley[12] stresses the importance of ethics in open-source investigations. She proposes a three-part approach to responsible decision-making, which involves identifying legal affordances and constraints applicable to investigators, soliciting guidance from professional codes of ethics, and making value judgments, particularly regarding the values of safety, accuracy, and the dignity of research subjects, the public, and the researchers themselves.

Daniel Brantes Ferreira, an independent arbitrator affiliated with the Chartered Institute of Arbitrators, and Elizaveta A. Gromova of South Ural State University,[13] consider the use of digital evidence in interstate dispute resolution. They first survey digital evidence practices in international arbitral proceedings at the Permanent Court of Arbitration and the International Centre for Settlement of Investment Disputes, and then turn to the International Court of Justice. Their essay shows that the broad discretion afforded to justices and arbitrators in admitting and evaluating evidence can lead to variation in practices regarding digital evidence between these different fora. To alleviate concerns associated with digital evidence, and the frequent lack of judicial expertise to evaluate it, the authors develop an innovative proposal: forensic expert committees "empowered to draft guidelines and perform preliminary authenticity checks in open-source and leaked evidence."[14]

Jessica Peake of the University of California Los Angeles takes up the issues of the availability and reliability of user-generated content.[15] As she points out, the availability of digital evidence may be severely hampered by internet shutdowns, either intentionally deployed by governments as a weapon of war, or as a side effect of hostilities. The content moderation policies of social media platforms may also affect the availability of evidence. According to these policies, platforms frequently remove, flag, or de-prioritize sensitive content. This can result in evidence of atrocities being removed or concealed, as this evidence often presents distressing images of violence or harm. The reliability of digital evidence is also under attack from multiple directions, key among them generative AI, which is becoming increasingly sophisticated and being used by various sides to a conflict to manipulate truth. Finally, Peake takes a closer look at the International Criminal Court's rules on the admission of digital evidence, in particular, the technological developments aimed at recording a piece of evidence's chain of custody.

Finally, William Hamilton Byrne and Thomas Gammeltoft-Hansen, both of the University of Copenhagen, consider the increasing use of digital evidence in Refugee Status Determination proceedings.[16] Often the only

[11] Siena Anstis, Ron Deibert & Jakub Dalek, *The Ethical and Legal Dilemmas of Digital Accountability Research and the Utility of International Norm-Setting*, 118 AJIL UNBOUND 40 (2024).

[12] Alexa Koenig, *Ethical Considerations for Open-Source Investigations into International Crimes*, 118 AJIL UNBOUND 45 (2024).

[13] Daniel Brantes Ferreira & Elizaveta A. Gromova, *Digital Evidence in Disputes Involving States*, 118 AJIL UNBOUND 51 (2024).

[14] *Id.*

[15] Jessica Peake, *Challenges of Using Digital Evidence for War Crimes Prosecutions: Availability, Reliability, Admissibility*, 118 AJIL UNBOUND 57 (2024).

[16] William Hamilton Byrne & Thomas Gammeltoft-Hansen, *Digital Evidence in Refugee Status Determination*, 118 AJIL UNBOUND 62 (2024).

https://doi.org/10.1017/aju.2024.1 Published online by Cambridge University Press

"hard" evidence in these proceedings is the applicant's testimony. In recent years, government officials have tried to bolster the evidentiary record through the increasing turn to digital evidence. The authors grapple with the concern that, in the highly unequal relationship between states and asylum seekers, this reliance on digital evidence may risk tilting the balance of power even further toward states. Nevertheless, they point out that digital evidence may also end up supporting an applicant's claims. The authors advocate for uses of digital evidence in refugee status determinations that address arbitrary exercises of power.

As the essays show, digital evidence is disrupting multiple aspects of international legal practice. As is often the case, this change may have constructive as well as harmful consequences. The symposium highlights the value of considering the impact of digital evidence across diverse substantive areas of international law. The highly fragmented and decentralized ways that digital evidence is produced and collected raise common concerns about its availability, reliability, authenticity, and potential bias. Thus, assessing digital evidence as a cross-cutting, rather than issue-bound, phenomenon in international law offers helpful insights about how to confront and respond to these challenges. The essays in this symposium highlight a range of potential responses to these concerns: ethical guidelines and legal frameworks to guide the work of digital researchers, procedural safeguards to ensure the credibility and reliability of digital evidence, and measures to ensure that digital evidence is not used to entrench or exacerbate existing imbalances of power. Of course, these suggestions represent an initial round of insights and call for further inquiry. Taken as a whole, the symposium stands as an invitation to investigate the quotidian practices by diverse actors producing and using digital evidence that shape the larger trajectories of international law.

https://doi.org/10.1017/aju.2024.1 Published online by Cambridge University Press