

American University Washington College of Law

## Digital Commons @ American University Washington College of Law

---

Articles in Law Reviews & Other Academic Journals

Scholarship & Research

---

2018

### User-Generated Evidence

Rebecca Hamilton

American University Washington College of Law, [hamilton@wcl.american.edu](mailto:hamilton@wcl.american.edu)

Follow this and additional works at: [https://digitalcommons.wcl.american.edu/facsch\\_lawrev](https://digitalcommons.wcl.american.edu/facsch_lawrev)



Part of the [Communications Law Commons](#), [Criminal Law Commons](#), [Evidence Commons](#), [International Law Commons](#), [Internet Law Commons](#), and the [Science and Technology Law Commons](#)

---

#### Recommended Citation

Hamilton, Rebecca, "User-Generated Evidence" (2018). *Articles in Law Reviews & Other Academic Journals*. 1285.

[https://digitalcommons.wcl.american.edu/facsch\\_lawrev/1285](https://digitalcommons.wcl.american.edu/facsch_lawrev/1285)

This Article is brought to you for free and open access by the Scholarship & Research at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in Articles in Law Reviews & Other Academic Journals by an authorized administrator of Digital Commons @ American University Washington College of Law. For more information, please contact [kclay@wcl.american.edu](mailto:kclay@wcl.american.edu).

# User-Generated Evidence

REBECCA J. HAMILTON\*

*“Photographs furnish evidence. Something we hear about, but doubt, seems proven when we’re shown a photograph of it. . . . [T]he camera record incriminates.”*

—Susan Sontag<sup>1</sup>

*Around the world, people are increasingly using their smartphones to document atrocities. This Article is the first to address the implications of this important development for international criminal law. While acknowledging the potential benefits such user-generated evidence could have for international criminal investigations, the Article identifies three categories of concern related to its use: (i) user security, (ii) evidentiary bias, and (iii) fair trial rights. Without adequate safeguards, user-generated evidence may address current problems in international criminal justice at the cost of creating new ones and shifting*

---

\* Assistant Professor of Law, American University, Washington College of Law. I served from 2007 to 2009 in the Office of the Prosecutor at the International Criminal Court. The views expressed here are my own and do not necessarily reflect the views of the Court. Thanks for thoughtful editing by the CJTL team. My gratitude for stellar research assistance goes to Deyaa Alrwishdi and James Purce. This Article has benefited from insightful comments from Kal Raustiala, Andrew Woods, Molly Land, Maggie Gardner, Alexa Koenig, Elena Baylis, Janie Chuang, Mark Drumbl, Nancy Combs, Saira Mohamed, Rachel Lopez, Jen Daskal, Meg deGuzman, and from feedback received at the 2017 Mid-Atlantic Junior Faculty Forum at Richmond Law School, the 2017 Women in International Law Workshop at Duke Law School, the 2017 AALS Criminal Law Roundtable in Washington, D.C., the 2017 American Society of International Law Midyear Research Forum in St. Louis, and the 2018 Junior International Law Scholars Association Workshop at Washington College of Law. All errors are my own. Particular thanks to Drs. Syzmanski, Miller, Baschat, and the staff on the Zayed 8W Maternity Ward at Johns Hopkins Hospital for the humor and humanity that got me through the three-month inpatient stay during which this Article was drafted, beating the odds to secure the safe delivery of my twins.

1. SUSAN SONTAG, ON PHOTOGRAPHY 5 (1978).

*existing problems from traditional actors, who have institutional support, to individual users without such protections.*

INTRODUCTION .....	3
I. THE EMERGENCE OF USER-GENERATED EVIDENCE.....	10
A. Problems Facing International Criminal Investigations .....	12
B. User-Generated Evidence as Part of the Solution.....	15
II. MAPPING THE NEW INVESTIGATORY SPACE .....	22
A. Evidence-Focused INGOs .....	23
1. Local Outreach by Evidence-Focused INGOs .....	24
2. Complications Flowing from Local Outreach .....	26
B. Technologists .....	27
C. Users .....	29
D. Private Lawyers .....	32
III. COMPLICATING THE PICTURE.....	34
A. Evidence Collection Stage .....	35
1. Risks to the User.....	35
2. Inequality of Arms.....	39
3. Bias and Distortion .....	41
B. Evidence Evaluation Stage .....	42
1. The Coordination Challenge.....	43
2. Obligations to Defendants .....	44
3. Information Security.....	44
C. Trial Stage and Its Aftermath.....	45
1. Admissibility .....	46
2. Interpretation .....	48
3. Unintended Consequences.....	50
IV. THE WAY FORWARD.....	51
A. Contracts .....	53
1. ICC-INGO Contracts.....	54
2. ICC-User Contracts .....	55
B. Guidelines .....	57
1. ICC Guidelines on the Use of Intermediaries.....	57
2. ICRC Protection Guidelines .....	58

CONCLUSION .....	59
------------------	----

## INTRODUCTION

International criminal investigations are in trouble. Security risks to investigators, limited access to sites of atrocity, and witness intimidation have created evidentiary problems that have derailed high-profile prosecutions of alleged war criminals.<sup>2</sup> In response, there has been a steady rise in the outsourcing of investigations from staff employed by international courts to private actors.<sup>3</sup> This Article homes in on the most recent part of this trend—technologists and criminal justice advocates coming together to encourage individuals to collect what I term “user-generated evidence.”

User-generated evidence is a sub-category of user-generated content. Like other forms of user-generated content, user-generated evidence is recorded on a device such as a smartphone by an ordinary citizen, referred to here as a user.<sup>4</sup> Unlike most types of user-generated content, however, user-generated evidence is recorded with the intent to help achieve legal accountability for wrongdoing.<sup>5</sup> Citizen recordings of police brutality provide an example with which many Americans are increasingly familiar.<sup>6</sup>

One of the consequences of the 2007 launch of Apple’s iPhone, and the subsequent development of lower-cost alternatives, is that millions of people around the world now carry cameras with

---

2. See, e.g., Prosecutor v. Kenyatta, ICC-01/09-02/11, Notice of Withdrawal of the Charges Against Uhuru Muigai Kenyatta, ¶¶ 1–3 (Dec. 5, 2014), [https://www.icc-cpi.int/CourtRecords/CR2014\\_09939.PDF](https://www.icc-cpi.int/CourtRecords/CR2014_09939.PDF) [<https://perma.cc/PP7F-ZKYP>].

3. For the first major law review article on this trend, see Elena Baylis, *Outsourcing Investigations*, 14 UCLA J. INT’L L. & FOREIGN AFF. 121 (2009).

4. Throughout this Article, I refer to the ordinary citizen who records footage for evidentiary purposes as a (smartphone) “user” rather than as a “citizen” so as not to exclude users who do not have citizenship in the places where they are recording or, indeed, are stateless.

5. See Philipp Amann & Mark P. Dillon, *Electronic Evidence Management at the ICC: Legal, Technical, Investigative, and Organizational Considerations*, in INTERNATIONAL CRIMINAL INVESTIGATIONS: LAW AND PRACTICE 231, 234 (Adejoké Babington-Ashaye, Aimée Comrie & Akingbolahan Adeniran eds., 2018) (“Simply put, evidence [as distinguished from other electronic content] is information or intelligence that can be used in court.”).

6. See, e.g., Catherine E. Shoichet & Randi Kaye, *Michael Brown Shooting: Is New Video a ‘Game Changer’?*, CNN (Sept. 12, 2014, 7:49 AM), <https://www.cnn.com/2014/09/11/us/ferguson-michael-brown-shooting-witnesses/index.html> [<https://perma.cc/7GT8-HJC4>].

them virtually 24/7. Much of the footage those cameras record gets uploaded online. Type “Syria atrocities footage” into Google and you will be overwhelmed with a visual library of inhumanity. You will see photographs and shaky footage, recorded on the smartphones of bystanders, showing acts worthy of criminal prosecution.<sup>7</sup>

As further elaborated below, there are now freely available smartphone applications (“apps”) designed to enable individuals to record footage that will satisfy the evidentiary standards of an international criminal courtroom. These user-generated evidence apps automatically (i) embed metadata from satellites, cell phone towers, and surrounding wireless and Bluetooth devices into recordings and (ii) record hash values as a check against subsequent manipulation.<sup>8</sup> The hope is that the footage filmed using these apps will be self-authenticating.

In the best-case scenario, the user-generated evidence will be admissible in international criminal trials without a user ever having to be identified, let alone having to testify.<sup>9</sup> This would offer several advantages that could transform the field of international criminal investigations:

(1) Compared to outside investigators, who typically reach sites of atrocity months after the crimes have been committed, local users can capture evidence immediately, thus preserving evidence that might otherwise be lost or destroyed;

(2) Compared to traditional witnesses, who can be threatened, intimidated, or manipulated, user-generated evidence—if properly secured and verified—records testimony that cannot be changed or recanted;

---

7. See, e.g., Neal Ungerleider, *Syrians Upload Ramadan Massacre Footage onto YouTube with Pen Cameras and Smuggled Tech*, FAST COMPANY (Aug. 1, 2011), <https://www.fastcompany.com/1770731/syrians-upload-ramadan-massacre-footage-youtube-pen-cameras-and-smuggled-tech> [<https://perma.cc/93T8-A2ND>].

8. A hash value is generated by an algorithm “that maps data of an arbitrary length to data of a fixed length.” Amann & Dillon, *supra* note 5, at 237 n.12. This almost always generates a unique value that can then be subsequently used to verify whether a file is identical to its original form. *Id.* at 237.

9. See, e.g., *FAQs: Organisation*, EYEWITNESS [hereinafter eyeWitness Organisation FAQs], <http://www.eyewitnessproject.org> [<https://perma.cc/6XE3-L9W2>] (click “FAQs” link in upper right hand of page, then “Organisation,” and then “Click for more Organisation details”) (“eyeWitness has commissioned extensive research into the admissibility of digital evidence. While this is an evolving issue, a study of cases from international, regional, and national courts shows that evidence must be relevant and reliable. . . . Reliability in relation to photos or videos requires the date/time/location of the recording, assurance that the video has not been altered, and assurance that the footage is the original version. The eyeWitness app ensures all three.”).

(3) Reliance on user-generated evidence would reduce security risks to court investigators, since they would most likely make fewer visits to sites of atrocities; and

(4) User-generated evidence could “democratize” evidence collection by shifting the balance of control from outside professionals to local people.

One way to view the emergence of user-generated evidence is as part of an ongoing process of technological development, stretching back to the late nineteenth century, in which advances in visual documentation make their way into a courtroom setting: from the daguerreotype, to the photograph, to the camcorder, to the cellphone recording.<sup>10</sup> From a courtroom standpoint, this is a plausible way to make sense of the advent of user-generated evidence and suggests that much or all of what we need to know about user-generated evidence can be gleaned from existing principles of evidence.<sup>11</sup> This Article, however, advances a different understanding—at least in relation to international criminal law. By widening the analytic time frame from the moment of trial back into the investigative process, I argue that the emergence of user-generated evidence in international criminal investigations is the most visible sign yet of the fundamental disruption underway within the investigatory ecosystem.

International criminal investigations have always drawn, to some degree, on the work of third-parties, especially so-called first-responder organizations.<sup>12</sup> But the field was traditionally dominated by professional court-appointed investigators. Now, key aspects of investigations are increasingly undertaken by a range of private actors.<sup>13</sup> As a part of this trend—somewhat akin to the emergence of

---

10. See Jennifer L. Mnookin, *The Image of Truth: Photographic Evidence and the Power of Analogy*, 10 YALE J.L. & HUMAN. 1, 8–14 (1998).

11. This perspective will be familiar to those conversant with Judge Easterbrook’s “law of the horse” argument. See Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, U. CHI. LEGAL F. 207, 207–10 (1996).

12. U.C. BERKELEY SCH. OF LAW, HUMAN RIGHTS CTR, FIRST RESPONDERS: AN INTERNATIONAL WORKSHOP ON COLLECTING AND ANALYZING EVIDENCE OF INTERNATIONAL CRIMES 4 (2014) (describing NGOs as “first responder” organizations who “often arrive at crime scenes long before court investigators, who may face diplomatic, legal, or pragmatic obstacles to reaching atrocity sites”).

13. See, e.g., UNITED NATIONS, INDEPENDENT INTERNATIONAL COMMISSION OF INQUIRY ON THE SYRIAN ARAB REPUBLIC (Sept. 17, 2018, 12:29 PM), <http://www.ohchr.org/EN/HRBodies/HRC/IIICISyria/Pages/IndependentInternationalCommission.aspx> [https://perma.cc/Y75X-M3Q8]; Nick Robins-Early, *Inside One Group’s Mission to Bring Assad’s Regime to Justice*, HUFFINGTON POST (Sept. 17, 2018, 12:41 PM), [http://www.huffingtonpost.com/entry/assad-war-crimes-cija\\_us\\_571ed6e6e4b0f309baee63e0](http://www.huffingtonpost.com/entry/assad-war-crimes-cija_us_571ed6e6e4b0f309baee63e0) [https://perma.cc/7TFY-TC6Y] (describing the investigative work of the private non-profit group

Uber or Airbnb with respect to taxis and hotels—user-generated evidence apps are enabling even more novel actors to enter the “market” of international criminal investigations, challenging the taken-for-granted monopoly previously held by court-appointed investigators. This trend raises thorny questions of ethics, safety, and accountability, which are the focus of this Article.

This Article is the first piece of legal scholarship to address the introduction of user-generated evidence into international criminal law.<sup>14</sup> To the extent that others have written on the topic, they have been either practitioners involved in the development of user-generated evidence apps, those looking at digital or open-source evidence more generally, or journalists who cover technology.<sup>15</sup> Unsurprisingly, many of these accounts paint the emergence of user-generated evidence in an overwhelmingly positive light. According to Mark Ellis, Executive Director of the International Bar Association, which has facilitated the development of a user-generated evidence app, “[The] app will be a transformational tool . . . providing a solution to the evidentiary challenges surrounding mobile phone footage.”<sup>16</sup> While I acknowledge all the potential advantages user-

---

the Commission for International Justice and Accountability).

14. A comprehensive literature review reveals only one piece of legal scholarship that touches on the use of user-generated evidence in international litigation. See Lindsay Freeman, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, 41 FORDHAM J. INT’L L. 283 (2018) (describing the emergence of evidence derived from digital technology, such as telecommunications intercepts and financial records of electronic funds transfers). Although this is not the focus of her article, Freeman explains that in *Prosecutor v. Al Mahdi*, a war crimes case at the ICC, the defense agreed to allow user-generated evidence in the form of video footage into the record as part of their client’s guilty plea. *Id.* at 314–20. As there was no trial, the Court did not have to make any determinations regarding the evidence. *Id.* I am working on a project that will extend beyond international criminal law to assess the extent to which other international courts, tribunals, and adjudicatory forums are also starting to rely on user-generated evidence. See Rebecca Hamilton, *New Media Evidence Across International Courts and Tribunals*, in BEYOND FRAGMENTATION: COMPETITION AND COLLABORATION AMONG INTERNATIONAL COURTS AND TRIBUNALS (Chiara Giorgetti & Mark A. Pollack eds.) (forthcoming 2019).

15. See, e.g., Kieran Guilbert, *App Empowers Civilian to Capture Evidence of War Crimes on Smartphones*, REUTERS (June 7, 2015, 7:02 PM), <http://www.reuters.com/article/warcrimes-apps-idUSL5N0YQ19J20150607> [<https://perma.cc/Y96P-HXSP>]; Rory Cellan-Jones, *EyeWitness App Lets Smartphones Report War Crimes*, BBC (June 8, 2015), <http://www.bbc.com/news/technology-33029464> [<https://perma.cc/B96C-4YNV>]; Alexa Koenig et al., *Open Source Fact-Finding in Preliminary Examinations*, in 2 QUALITY CONTROL IN PRELIMINARY EXAMINATION 681 (Morten Bergsmo & Carsten Stahn eds., 2018), <http://www.legal-tools.org/doc/6706c9/pdf/> [<https://perma.cc/X389-C7LL>].

16. Mark Ellis, *quoted in* Owen Bowcott, *Eyewitness to Atrocities: The App Aimed at Bringing War Criminals to Justice*, GUARDIAN (June 7, 2015, 7:01 PM), <https://www>.

generated evidence could bring to international criminal investigations, this Article cautions against any sense of inevitability that this positive potential will be realized.<sup>17</sup>

The admission of user-generated evidence into international criminal litigation has already begun. An August 2017 arrest warrant issued by the International Criminal Court for a Libyan national, Mahmoud Mustafa Busayf al-Werfalli, marked the first time that an international criminal court relied on user-generated footage, posted to social media, to substantiate a criminal allegation—in this case, the war crime of murder.<sup>18</sup> In reviewing video evidence presented by the prosecution, the pre-trial chamber concluded there were “reasonable grounds to believe” that al-Werfalli had committed or ordered the killings recorded in the footage.<sup>19</sup>

Although this Article focuses on international criminal litigation, it is worth noting that other international adjudicatory forums are starting to receive this type of evidence as well. In 2017, Ukraine presented user-generated evidence before the International Court of Justice in its request for provisional measures against Russia.<sup>20</sup> Similarly, the Permanent Court of Arbitration relied on user-generated evidence presented by the Netherlands in determining that Russia had violated its obligations under the U.N. Convention on the Law of the

---

theguardian.com/technology/2015/jun/08/eyewitness-to-atrocities-the-app-aimed-at-bringing-war-criminals-to-justice [https://perma.cc/4M55-RXTZ].

17. See generally EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM (2013) (warning of the pitfalls of expecting technology to unequivocally fix problems).

18. Prosecutor v. Al-Werfalli, ICC-01/11-01/17, Warrant of Arrest, ¶ 3 (Aug. 15, 2017), [https://www.icc-cpi.int/CourtRecords/CR2017\\_05031.PDF](https://www.icc-cpi.int/CourtRecords/CR2017_05031.PDF) [https://perma.cc/D95R-UNFF]. User-generated evidence entered the court record at the ICC one time prior to this, in *Prosecutor v. al-Mahdi*. But in that case, the defense agreed to allow user-generated video footage into the record as part of their client’s guilty plea, which is a significantly different process from an evidentiary perspective than what would transpire in a typical trial. See Prosecutor v. al-Mahdi, ICC-01/12-01/15, Judgment & Sentence, ¶¶ 2, 5 (Sept. 27, 2016), [https://www.icc-cpi.int/CourtRecords/CR2016\\_07244.PDF](https://www.icc-cpi.int/CourtRecords/CR2016_07244.PDF) [https://perma.cc/FC37-UXFJ].

19. “Reasonable grounds to believe” is the evidentiary standard that the Rome Statute requires for the issuance of an arrest warrant. Rome Statute of the International Criminal Court art. 58, *opened for signature* July 17, 1998, 2187 U.N.T.S. 38544 [hereinafter Rome Statute].

20. Terrorism Financing and Racial Discrimination in Ukraine, (Ukr. v. Russ.), Application Instituting Proceedings, ¶ 53, <https://www.icj-cij.org/files/case-related/166/19314.pdf> [https://perma.cc/5RJ5-2AQL]. Ukraine presented photographic and video evidence from eyewitnesses to support its claim that Russia was violating Article 18 of the International Convention for the Suppression of the Financing of Terrorism through the transfer of weaponry that fostered, rather than prevented, terrorist activity. *Id.*



Sea.<sup>21</sup> This phenomenon further reinforces the need to start addressing the implications of this important development in international litigation.

Returning to the international criminal law context, however, al-Werfalli remains at large.<sup>22</sup> Until he is arrested and his trial is convened, it is hard to predict whether the judges will find that the video footage has sufficient evidentiary strength to proceed to trial. But what does seem clear is that there is an urgent need to build our understanding of what this emerging development will mean for the range of actors involved in international criminal justice.

Although the international legal scholarship has been silent on the topic of user-generated evidence, there are other bodies of literature—on domestic policing,<sup>23</sup> on visual bias,<sup>24</sup> and on the use of information and communications technologies for peacebuilding, human rights, and development<sup>25</sup>—that provide material relevant to analyzing the potential impact of user-generated evidence on international criminal investigations. Insights from these materials, when applied to the user-generated evidence context, reveal several risks. Unless these risks are carefully managed, any potential benefits from the production of user-generated evidence will be acquired only at the cost of creating new problems and/or shifting existing problems from professional investigators onto users. In addition, the use of this type of evidence raises challenges for lawyers and potential problems for defendants in cases that rely on user-generated evidence. In sum, decisions made by key legal actors in the very near future will be central to determining the impact of user-generated evidence on

---

21. The Court relied on video footage taken by Greenpeace in its judgment on the merits ordering Russia to pay damages to the Netherlands for violations under articles 56(2), 58(1), 58(2), 87(1)(a), and 92(1) of the U.N. Convention on the Law of the Sea. There was no discussion of the veracity of the videos and there was no submission by Russia, as it did not participate in the proceedings. *Arctic Sunrise (Neth. v. Russ.)*, Case No. 2014-02, Award on the Merits, ¶ 71 (Perm. Ct. Arb. 2015), <https://www.pcacases.com/web/sendAttach/1438> [<https://perma.cc/CPC9-5MG3>]. See generally Hamilton, *supra* note 14 (providing a survey of instances in which international courts and tribunals have had new media evidence, including user-generated evidence, brought before them).

22. *Libyans Deserve Justice, as War Crime Suspects Remain at Large: Prosecutor*, UN NEWS (May 9, 2018), <https://news.un.org/en/story/2018/05/1009262> [<https://perma.cc/ZN6L-R2JQ>].

23. See, e.g., Jocelyn Simonson, *Beyond Body Cameras: Defending a Robust Right to Record the Police*, 104 GEO. L.J. 1559 (2016).

24. See, e.g., Dan M. Kahan et al., *Whose Eyes Are You Going to Believe? Scott v. Harris and the Perils of Cognitive Illiberalism*, 122 HARV. L. REV. 837 (2009).

25. See, e.g., MOLLY LAND ET AL., #ICT4HR: INFORMATION AND COMMUNICATION TECHNOLOGIES FOR HUMAN RIGHTS (2012).

international criminal investigations, and indeed on international criminal justice writ large.

This Article proceeds as follows: After a brief history of the use of visual evidence in court, Part I situates the emergence of user-generated evidence within the context of the underlying challenges facing international criminal investigations, and explains that to view user-generated evidence as simply a new technology-enabled development misses a more fundamental shift that it brings to the investigatory ecosystem. Part II devotes significant space to the necessary task of mapping out, for the first time, the new players that are entering the investigatory sphere thanks to the emergence of user-generated evidence, and identifying the challenges that arise from the interrelationships between them. Part III then walks through the lifecycle of user-generated evidence, from collection and evaluation to a trial and its aftermath. This part, the primary contribution of the Article, further complicates the attractive idea that user-generated evidence can provide a solution to the many problems facing international criminal investigations. It identifies three categories of concern arising from the emergence of user-generated evidence: (i) user security, (ii) evidentiary bias, and (iii) fair trial rights.

With two user-generated evidence apps currently in use, and user-generated evidence already presented in an international arrest warrant, the growth of user-generated evidence seems inevitable.<sup>26</sup> The question, then, is what are the options for addressing the concerns identified? Recognizing that concerns about evidentiary bias and fair trial rights are nothing new, Part IV begins by looking at ways to mitigate security risks to users. Situating the new investigatory ecosystem within the context of the steady move toward the privatization of previously public functions, I explore the possibility of regaining accountability through contract design, and assess the degree to which the ICC's Guidelines on the Use of Intermediaries and the International Committee of the Red Cross's ("ICRC") Guidelines for Protection Actors could be adapted to the user-generated evidence context.

The Article concludes that while the concerns identified are not necessarily fatal to the project of user-generated evidence, they

---

26. See *About eyeWitness: Project Description*, EYEWITNESS [hereinafter *eyeWitness Project Description*], <http://www.eyewitnessproject.org/> [<https://perma.cc/NU5M-6BCC>] (click "About" link in upper right hand of page and then "Project Description"); *CameraV App and the InformaCam System*, GUARDIAN PROJECT, <https://guardianproject.github.io/informacam-guide/en/InformacamGuide.html> [<https://perma.cc/H925-NBU3>]; *Prosecutor v. Al-Werfalli*, ICC-01/11-01/17, Warrant of Arrest, ¶ 3 (Aug. 15, 2017), [https://www.icc-cpi.int/CourtRecords/CR2017\\_05031.PDF](https://www.icc-cpi.int/CourtRecords/CR2017_05031.PDF) [<https://perma.cc/M4QD-JF6V>].

should, at minimum, give pause to those who see user-generated evidence as part of the solution to the problems currently facing international criminal investigations.

## I. THE EMERGENCE OF USER-GENERATED EVIDENCE

The use of visual evidence in criminal investigations and courtroom proceedings is nothing new. As Jennifer Mnookin recounts in *The Image of Truth*, photography was originally the province of experts, but, by the 1880s, technological advances and reductions in cost made photography accessible to ordinary people.<sup>27</sup> In the criminal law context, this meant so-called roving amateurs could now catch people “in the act,” and by the turn of the century, photographs were commonplace in courtrooms across the United States.<sup>28</sup>

When it came to moving images, U.S. courts began routinely permitting the entry of film into evidence as far back as 1935.<sup>29</sup> And long before the emergence of smartphones, video evidence played a high-profile role in the (unsuccessful) effort to prosecute officers of the Los Angeles Police Department for the beating of black motorist Rodney King.<sup>30</sup>

Internationally, the story of film as evidence goes back to the prosecution of Nazi atrocities at Nuremberg. U.S. Supreme Court Justice Robert Jackson, who was U.S. Chief Prosecutor at Nuremberg, turned to the documentary film *Nazi Concentration Camps* to establish “incredible events by credible evidence.”<sup>31</sup> And since then, international and hybrid criminal courts have continued to make use of video footage.<sup>32</sup>

---

27. See generally Mnookin, *supra* note 10.

28. See *id.* at 12–13.

29. See LOUIS-GEORGES SCHWARTZ, *MECHANICAL WITNESS: A HISTORY OF MOTION PICTURE EVIDENCE IN U.S. COURTS* 13–14 (2009).

30. See Forrest Stuart, *Constructing Police Abuse after Rodney King: How Skid Row Residents and the Los Angeles Police Department Contest Video Evidence*, 36 L. & SOC. INQUIRY 327, 331–32 (2011) (describing defense counsel’s ability to recast the footage as justifiable police conduct).

31. Justice Robert Jackson, *quoted in* Lawrence Douglas, *Film as Witness: Screening Nazi Concentration Camps Before the Nuremberg Tribunal*, 105 YALE L.J. 449, 452 (1995).

32. For video footage as evidence at the ICTY, see, e.g., Vladimir Petrović, *A Crack in the Wall of Denial: The Scorpions Video in and out of the Courtroom*, in *NARRATIVES OF JUSTICE IN AND OUT OF THE COURTROOM: FORMER YUGOSLAVIA AND BEYOND* 93–108 (Dubravka Zarkov & Marlies Glasius eds., 2014). For the same at the ICC, see, e.g., *Prosecutor v. Lubanga*, Case No. ICC-01/04-01/06, Transcript of Oral Session, ¶ 11 (Jan. 26,

Still, as recently as five years ago, the idea that an ordinary citizen who witnessed an atrocity could use his or her smartphone to anonymously make a direct evidentiary contribution to an international criminal prosecution was virtually unheard of.<sup>33</sup> For the International Criminal Court (“ICC”) and its predecessor tribunals, like the International Criminal Tribunal for the former Yugoslavia (“ICTY”) and the International Criminal Tribunal for Rwanda (“ICTR”), it had long been assumed that evidence collection requires some in-person contact.<sup>34</sup> With no police force to carry out investigative activities on their behalf, legal teams from these courts have typically sent their own personnel into areas where crimes have allegedly occurred.<sup>35</sup> User-generated evidence disrupts this traditional approach.<sup>36</sup>

The following section sets the stage for understanding the emerging role of user-generated evidence in international criminal investigations and trials. In popular accounts, advances in information and communications technology have driven the possibility of user-generated evidence playing a role in international criminal investigations.<sup>37</sup> While not untrue, this explanation is incomplete.

---

2009), [https://www.icc-cpi.int/Transcripts/CR2009\\_00591.PDF](https://www.icc-cpi.int/Transcripts/CR2009_00591.PDF) [https://perma.cc/TS22-5VMH]. For the same at the various hybrid tribunals for Sierra Leone, Cambodia, and Lebanon, see, e.g., Pedro Pizano, *Court Views 1977 Video Footage of 1<sup>st</sup> January Dam*, CAMBODIA TRIBUNAL MONITOR (May 26, 2015) <http://www.cambodiatribunal.org/2015/05/26/court-views-1977-video-footage-of-1st-january-dam/> [https://perma.cc/44RD-RSK4] (video footage at the Extraordinary Chambers in the Courts of Cambodia); *Shocking Footage at Taylor Trial*, BBC NEWS (Jan. 7, 2008, 5:49 PM), <http://news.bbc.co.uk/2/hi/africa/7174288.stm> [https://perma.cc/B8LA-MLZ2] (video footage at the Special Court for Sierra Leone).

33. Indeed, it was not until 2008 that the ICC even began to consider its capacity to deal with digital evidence of any kind. See U.C. BERKELEY SCH. OF L., HUM. RTS. CTR., DIGITAL FINGERPRINTS: USING ELECTRONIC EVIDENCE TO ADVANCE PROSECUTIONS AT THE INTERNATIONAL CRIMINAL COURT 5 (2014), [https://www.law.berkeley.edu/files/HRC/Digital\\_fingerprints\\_interior\\_cover2.pdf](https://www.law.berkeley.edu/files/HRC/Digital_fingerprints_interior_cover2.pdf) [https://perma.cc/K74L-PVUA].

34. See, e.g., INT’L CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA & U.N. INTERREGIONAL CRIME AND JUSTICE RESEARCH INST., ICTY MANUAL ON DEVELOPED PRACTICES 15–27 (2009), [http://www.icty.org/x/file/About/Reports%20and%20Publications/ICTY\\_Manual\\_on\\_Developed\\_Practices.pdf](http://www.icty.org/x/file/About/Reports%20and%20Publications/ICTY_Manual_on_Developed_Practices.pdf) [https://perma.cc/EN5S-GYP7] (discussing the ICTY’s “information gathering” techniques).

35. See *About: Office of the Prosecutor*, INT’L CRIM. CT., <https://www.icc-cpi.int/about/otp> [https://perma.cc/98TJ-TBSZ].

36. See U.C. BERKELEY SCH. OF LAW, HUMAN RIGHTS CTR., *supra* note 33, at 8 (discussing the decisions the Office of the Prosecutor will have to make as it strengthens its ability to gather and analyze digital evidence, such as whether to train field investigators in digital forensic techniques or hire specialized staff).

37. See e.g., Bowcott, *supra* note 16.

Specifically, it fails to account for non-technology-related factors that have affected international criminal investigations over the past decade. This section describes the problems that have plagued international criminal investigations, and illustrates how the convergence of several factors has led to the current moment, in which user-generated evidence is being proactively advanced as part of the solution to the challenges of evidence collection.

### *A. Problems Facing International Criminal Investigations*

International criminal investigations are never easy. The perpetrators of atrocities and their supporters have a strong interest in hiding or destroying evidence of their crimes.<sup>38</sup> Unlike its predecessor tribunals, the ICC is often faced with the task of investigating while crimes are still ongoing.<sup>39</sup> In this context it has been disappointing, but not surprising, that the ICC's Office of the Prosecutor ("OTP") has struggled to develop a successful approach to its investigative work. As a result, a "lack of quality evidence" has hindered the OTP's ability to secure convictions against alleged perpetrators.<sup>40</sup>

In 2012, the Court acquitted Mathieu Ngudjolo Chui, a warlord from the Democratic Republic of the Congo ("DRC"), whom the OTP had charged with war crimes and crimes against humanity.<sup>41</sup> The judges could not rule out the possibility that crimes had occurred, but concluded that the OTP had not provided sufficient evidence to prove beyond a reasonable doubt that Ngudjolo was responsible.<sup>42</sup>

In a deposition about the challenges faced by the OTP's investigative team working in the DRC on another case, a former lead investigator testified about conditions of immense insecurity on the ground.<sup>43</sup> In addition to the general presence of armed groups, spe-

---

38. See, e.g., *Implicating Humala: Evidence of Atrocities and Cover-Up of Abuses Committed during Peru's Armed Conflict*, HUMAN RIGHTS WATCH (Sept. 7, 2017), <https://www.hrw.org/report/2017/09/07/implicating-humala/evidence-atrocities-and-cover-abuses-committed-during-perus> [https://perma.cc/HF44-RCV8] (describing Former President of Peru Ollanta Humala's direct participation in atrocities and his attempt to cover up incriminating evidence during his electoral campaign for president ).

39. *Situations Under Investigation*, INT'L CRIM. CT., <https://www.icc-cpi.int/pages/situation.aspx> [https://perma.cc/GPH9-WKKS].

40. U.C. BERKELEY SCH. OF LAW, HUMAN RIGHTS CTR., *supra* note 33, at 3.

41. Prosecutor v. Chui, Case No. ICC-01/04-02/12, Judgment, ¶ 7 (Dec. 12, 2012), [https://www.icc-cpi.int/CourtRecords/CR2013\\_02993.PDF](https://www.icc-cpi.int/CourtRecords/CR2013_02993.PDF) [https://perma.cc/Z2T2-XC5T].

42. *Id.* ¶¶ 110, 456, 499, 503, 516.

43. Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Deposition of Witness DRC-

cific threats were made against the ICC investigators, who stood out as foreigners among the local population.<sup>44</sup> Even more problematic were the security threats against anyone thought to be cooperating with the ICC investigators.<sup>45</sup> As a result, potential witnesses were put at risk, and relative to these security concerns, “the work of investigating itself almost became secondary.”<sup>46</sup>

The effort to prosecute those responsible for crimes committed during Kenya’s post-election violence in 2007–2008 epitomizes the way in which evidentiary problems have been hindering the OTP’s ability to secure convictions. In 2014, the OTP announced it would have to abandon its charges against President Uhuru Kenyatta, due to insufficient evidence.<sup>47</sup> Threats and intimidation had led seventeen of the prosecution’s witnesses to change their minds about testifying against the accused.<sup>48</sup>

As problematic as the investigations in the DRC and Kenya have been, they at least involved OTP personnel reaching the crime scenes. By contrast, OTP staff have never investigated in Darfur, Sudan—the site of the first situation that the United Nations Security Council referred to them for investigation.<sup>49</sup> ICC personnel and any-

---

OTP-WWWW-0582, 34–40 (Nov. 16, 2010) [hereinafter *Lubanga* Witness Deposition], [https://www.icc-cpi.int/Transcripts/CR2012\\_00069.pdf](https://www.icc-cpi.int/Transcripts/CR2012_00069.pdf) [<https://perma.cc/M35L-8K25>].

44. *Id.* at 37–38. *But see* Situation in Darfur, Case No. ICC-02/05, Observations of the United Nations High Commissioner for Human Rights invited in Application of Rule 103 of the Rules of Procedure and Evidence, ¶ 75 (Oct. 10, 2006), [https://www.icc-cpi.int/CourtRecords/CR2007\\_02013.PDF](https://www.icc-cpi.int/CourtRecords/CR2007_02013.PDF) [<https://perma.cc/7JPY-Y8HG>] (stating that, in the High Commissioner’s view, the obligation of the Government of Sudan to allow “unfettered access for exhaustive investigations” should have made it possible to send ICC investigators into Darfur).

45. *Lubanga* Witness Deposition, *supra* note 43, at 39.

46. *Id.*

47. Prosecutor v. Kenyatta, Case No. ICC-01/09-02/11, Decision on the Withdrawal of Charges, ¶ 4 (Mar. 13, 2015) [https://www.icc-cpi.int/CourtRecords/CR2015\\_02842](https://www.icc-cpi.int/CourtRecords/CR2015_02842) [<https://perma.cc/7XDW-4LUA>]; *cf.* Prosecutor v. Ruto & Sang, Case No. ICC-09/09-01/11, Decision of Application for Judgments of Acquittal, ¶ 464 (Apr. 5, 2016) [https://www.icc-cpi.int/CourtRecords/CR2016\\_04384.pdf](https://www.icc-cpi.int/CourtRecords/CR2016_04384.pdf) [<https://perma.cc/WX66-XQ2K>]. *See also* Bowcott, *supra* note 16.

48. *See* Prosecutor v. Ruto & Sang, Case No. ICC-09/09-01/11, Statement of the Prosecutor Regarding Trial Chamber’s Decision to Vacate Charges Against Messrs William Samoei Ruto and Joshua Arap Sang Without Prejudice to Their Prosecution in the Future, (Apr. 6, 2016), <https://www.icc-cpi.int/Pages/item.aspx?name=otp-stat-160406> [<http://perma.cc/5WVG-L47A>].

49. *See* Situation in Darfur, Sudan, Case No. ICC-02/05, Prosecutor’s Response to Cassese’s Observation on Issues Concerning the Protection of Victims and the Preservation of Evidence in the Proceedings on Darfur Pending before the ICC, ¶ 16 (Sept. 11, 2016) [https://www.icc-cpi.int/CourtRecords/CR2007\\_02009.pdf](https://www.icc-cpi.int/CourtRecords/CR2007_02009.pdf) [<https://perma.cc/Q5X7-WZBF>].

one suspected of being associated with them have been threatened with death by the Sudanese government.<sup>50</sup>

As the length of time between the commission of a crime and the collection of evidence grows, so does the likelihood of evidence being lost or destroyed. Even in situations where access has not been outright impossible, such as the OTP's investigation in Libya, OTP personnel have been delayed in reaching crimes scenes.<sup>51</sup> And, of course, the universe of atrocities deserving prosecution extends beyond situations over which the ICC has jurisdiction.

The OTP's first effort to overcome the investigatory challenges of security threats to its staff and potential witnesses, witness intimidation, and the problems of access to areas of ongoing conflict involved it turning to so-called "intermediaries" for assistance.<sup>52</sup> These intermediaries were local activists on whom OTP investigators began to rely to reach out to potential witnesses. As locals of the area, the intermediaries attracted less attention than investigative teams from the Hague, thus reducing the security risks to the potential witnesses with whom they came in contact.<sup>53</sup> And because intermediaries were already onsite, their use overcame the access problems faced by OTP personnel.<sup>54</sup>

While the idea of outsourcing some of the OTP's investigative functions to local actors was attractive in theory, it rapidly backfired in practice.<sup>55</sup> On the opening day of the ICC's first-ever trial, a

50. Prosecutor v. Harun & Kushayb, Case No. ICC-02/05-01/07, Public Redacted Version of Prosecution Request for a Finding on the Non-Cooperation of the Government of the Sudan, ¶¶ 33–36 (Apr. 19, 2010), [https://www.icc-cpi.int/CourtRecords/CR2010\\_02788.pdf](https://www.icc-cpi.int/CourtRecords/CR2010_02788.pdf) [<https://perma.cc/B2QJ-XUS4>].

51. See Caroline Buisman, *Delegating Investigations: Lessons to be Learned from the Lubanga Judgment*, NW. J. INT'L HUM. RTS. 30, 53 n.207 (2013) (describing a one-month delay after the collapse of the Gaddafi regime before OTP staff set foot in Libya).

52. *Lubanga* Witness Deposition, *supra* note 43, at 53–54.

53. See OPEN SOC'Y JUST. INITIATIVE, BRIEFING PAPER: WITNESS INTERFERENCE IN CASES BEFORE THE INTERNATIONAL CRIMINAL COURT 2–6 (2016), <https://www.opensocietyfoundations.org/sites/default/files/factsheet-icc-witness-interference-20161116.pdf> [<https://perma.cc/DD5A-UZRR>].

54. See *Lubanga* Witness Deposition, *supra* note 43, at 48 (“[T]here was an advantage, a massive advantage, with them [the intermediaries] compared to us [the OTP staff], and this was that they were really implanted in the population.”).

55. See generally Baylis, *supra* note 3. See also WAR CRIMES RES. OFFICE, INVESTIGATIVE MANAGEMENT, STRATEGIES, AND TECHNIQUES OF THE INTERNATIONAL CRIMINAL COURT'S OFFICE OF THE PROSECUTOR 8–9 (2012), <https://www.wcl.american.edu/impact/initiatives-programs/warcrimes/our-projects/icc-legal-analysis-and-education-project/reports/report-16-investigative-management-strategies-and-techniques-of-the-international-criminal-courts-office-of-the-prosecutor/> [<https://perma.cc/EE2R-3JJJ>].

former child soldier recanted his testimony against accused Congolese warlord Thomas Lubanga. The witness told the court that someone from a local organization—one of the intermediaries used by the OTP—had manipulated him into testifying.<sup>56</sup> Over the course of the trial, several other witnesses told the court that intermediaries had promised them the opportunity to earn money and to study in exchange for false testimony.<sup>57</sup> Although Lubanga was ultimately convicted, it was not on the basis of the testimony of any of the former child soldiers that the OTP put on the stand. Finding that none of the testimony of these witnesses could be relied upon, the court concluded that “the prosecution should not have delegated its investigative responsibilities to the intermediaries . . . notwithstanding the extensive security difficulties it faced.”<sup>58</sup> A 2013 report by the International Bar Association (“IBA”) concluded that the ICC’s reliance on in-court witness testimony “may be unsustainable due to a number of challenges.”<sup>59</sup>

### *B. User-Generated Evidence as Part of the Solution*

As the flaws in traditional approaches to evidence collection were put on display in the Hague, the expansion of information and communications technology (“ICT”) was already well underway. The rapid evolution of modern technology ensured that long-standing financial and non-monetary barriers to the creation of content, including through photography and video recording, by ordinary people were falling away.<sup>60</sup> As people began to carry their smartphones everywhere with them, not only was there no need to buy a camera, there was also no need to plan in advance of taking a photo or video.<sup>61</sup>

---

56. *Witness Recants in Congo War-Crimes Trial*, NBC NEWS (Jan. 28, 2009, 2:47 PM), [http://www.nbcnews.com/id/28891559/ns/world\\_news-africa/t/witness-recants-congo-war-crimes-trial/#.WT8mLU0rL](http://www.nbcnews.com/id/28891559/ns/world_news-africa/t/witness-recants-congo-war-crimes-trial/#.WT8mLU0rL) [<https://perma.cc/G3JM-26P7>].

57. *Prosecutor v. Lubanga*, Case No. ICC-01/04-01/06, Judgment, ¶ 178 (Mar. 14, 2012), [https://www.icc-cpi.int/iccdocs/doc/doc1379838.pdfCourtRecords/CR2012\\_03942.pdf](https://www.icc-cpi.int/iccdocs/doc/doc1379838.pdfCourtRecords/CR2012_03942.pdf) [<https://perma.cc/E3NY-RH6G>].

58. *Id.* ¶ 482.

59. INT’L BAR ASS’N, WITNESSES BEFORE THE INTERNATIONAL CRIMINAL COURT 20 (2013), <https://www.ibanet.org/Document/Default.aspx?DocumentUid=9c4f533d-1927-421b-8c12-d41768ffc11f> [<https://perma.cc/B5JM-AETA>].

60. See Ella McPherson, *Advocacy Organizations’ Evaluation of Social Media Information for INGO Journalism: The Evidence and Engagement Models*, 59 AM. BEHAV. SCI. 124, 128 (2015).

61. This facilitated the move from the premeditated taking of images to what Professor



Crucially, from the perspective of international criminal prosecutions, ICT expansion took place on a global scale. By 2016, eighty-four percent of the population worldwide was covered by a broadband mobile network,<sup>62</sup> and by the end of 2016, there were over 730 million unique SIM connections in Africa.<sup>63</sup>

Human rights researchers became attuned to the impact of the global ICT expansion in the context of the crisis in Syria. International non-governmental organizations (“INGOs”) had difficulty getting their researchers into Syria following the 2011 uprising.<sup>64</sup> Despite the difficulty, they began to see an enormous amount of atrocity footage, captured by ordinary Syrians and uploaded to social media.<sup>65</sup> From an evidentiary perspective, however, the material was largely unusable; there was usually no way of verifying the authenticity of the images that had been uploaded.<sup>66</sup>

The Syria situation is but one example of the more general expansion of user-generated content being uploaded to social media, and a range of actors from fields including journalism and social entrepreneurship have already begun to develop models to utilize that content. Technology entrepreneurs in Kenya drew user-generated content into a platform for mapping the 2007–2008 post-election violence.<sup>67</sup> A U.K. blogger formed Bellingcat, a group dedicated to harnessing user-generated content for investigations<sup>68</sup> into subjects rang-

---

Seth Kreimer describes as “pervasive image capture.” Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Disclosure, and the Right to Record*, 159 U. PA. L. REV. 335, 339–40 (2011). See also Okabe Daisuke, *Camera Phones Changing the Definition of Picture-Eorthy*, JAPAN MEDIA REV. (Aug. 29, 2003), <http://www.dourish.com/classes/ics234cw04/ito3.pdf> [<https://perma.cc/PZ6U-27G8>] (discussing the ubiquity of image capture on cellphones).

62. See INT’L TELECOMM. UNION, ICT FACTS AND FIGURES 2016 (2016), <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf> [<https://perma.cc/VAP2-3J47>].

63. *Over Half a Billion Mobile Subscribers in Africa by 2020*, AFRICA NEWS (July 25, 2017), <http://www.africanews.com/2017/07/25/over-half-a-billion-mobile-subscribers-in-africa-by-2020-hi-tech/> [<https://perma.cc/WX6E-PR4M>].

64. See SYRIA NEEDS ANALYSIS PROJECT, RELIEF ACTORS IN SYRIA 1–12 (Dec. 2013), [https://reliefweb.int/sites/reliefweb.int/files/resources/relief\\_actors\\_in\\_syria.pdf](https://reliefweb.int/sites/reliefweb.int/files/resources/relief_actors_in_syria.pdf) [<https://perma.cc/AC3Q-37PR>].

65. See Maha Abu Shama, *quoted in* Ella McPherson, *Advocacy Organizations’ Evaluation of Social Media Information for NGO Journalism: The Evidence and Engagement Models*, 59 AM. BEHAV. SCI. 124, 125 (2015).

66. See *id.* at 133–34.

67. *About Ushahidi*, USHAHIDI, <https://www.ushahidi.com/about/> [<https://perma.cc/C2LW-2F3C>].

68. *About*, BELLINGCAT, <https://www.bellingcat.com/about/> [<https://perma.cc/6GH2->

ing from Mexican drug cartels<sup>69</sup> to the MH-17 plane crash.<sup>70</sup> The Carter Center relied on crowdsourcing to try to verify instances of violence in Syria.<sup>71</sup> And the Syria Justice and Accountability Center sought to triangulate footage coming in from a range of open sources.<sup>72</sup>

It was during this global ICT expansion, as INGOs started observing the proliferation of user-generated content and began to grapple with how to verify it, that the possibility of user-generated evidence began to arise. Lawyers wondered whether the information needed to authenticate a recording could be embedded within an “app” that would thereby serve as a one-stop technical solution to the verification problem.<sup>73</sup> And in 2011, the first effort to develop an app that would capture user-generated evidence began.<sup>74</sup>

As mentioned in the Introduction, there are presently two apps that have been designed with the specific goal of gathering user-generated evidence for international criminal prosecutions.<sup>75</sup> The *eyeWitness to Atrocities* app was designed by commercial technolo-

---

PTPN].

69. *Geolocating Mexican Sicarios in Chihuahua*, BELLINGCAT (Feb. 25, 2016), <https://www.bellingcat.com/news/americas/2016/02/25/geolocating-mexican-sicarios-in-chihuahua/> [https://perma.cc/DS6T-KV2D].

70. *Russian Colonel General Identified as Key MH17 Figure*, BELLINGCAT (Dec. 8, 2017), <https://www.bellingcat.com/news/uk-and-europe/2017/12/08/russian-colonel-general-delfin/> [https://perma.cc/KR5U-HNWL].

71. CARTER CTR., *Syria Conflict Resolution*, [https://www.cartercenter.org/peace/conflict\\_resolution/syria-conflict-resolution.html](https://www.cartercenter.org/peace/conflict_resolution/syria-conflict-resolution.html) [https://perma.cc/YV7562N3].

72. E-mail from Mohammad Al Abdallah, Exec. Dir., Syria Justice & Accountability Ctr., to Deyaa Alrwishdi, Research Assistant, Am. Univ. Wash. Coll. of Law (June 5, 2017, 10:01 AM EST) (on file with the *Columbia Journal of Transnational Law*).

73. See Mark S. Ellis, *Shifting the Paradigm—Bringing to Justice Those Who Commit Human Rights Atrocities*, 47 CASE W. RES. J. INT’L L. 265, 269–70 (2015) (describing how the question of whether an app could be designed to address verification concerns in the context of a mass of unverifiable user-generated content arose initially in relation to footage out of Sri Lanka that could not be independently verified).

74. Initially, WITNESS and the IBA worked together on app development. At a later point, however, the IBA decided that their goal of “court-level evidence from high-risk environments” was more niche than what WITNESS was trying to develop, and so the two organizations parted ways. See Interview with Wendy Betts, Director of the eyeWitness to Atrocities Program at the Int’l Bar Ass’n (July 6, 2017) (on file with the *Columbia Journal of Transnational Law*).

75. Domestically, the ACLU has designed an app specifically for user-generated evidence collection in cases of police brutality. See *Apps to Record Police Misconduct*, AM. CIVIL LIBERTIES UNION, <https://www.aclu.org/issues/criminal-law-reform/reforming-police-practices/aclu-apps-record-police-conduct> [https://perma.cc/B57HTDER].

gists hired by the IBA, following consultations with lawyers at the ICC and other international and hybrid tribunals.<sup>76</sup> The app, which can be downloaded for free from Google Play, offers users anonymity by connecting verification of uploaded images to the phone itself rather than to any user associated with the phone.<sup>77</sup> Everything a user records while inside the app is automatically tagged and encrypted, with a hash value of the pixel count recorded as a marker against subsequent manipulation.<sup>78</sup>

Vast amounts of metadata, including GPS coordinates, light meter readings, and nearby cell tower signals are recorded to enable the location and time of the footage to be verified.<sup>79</sup> Any new material is automatically encrypted, and once a user has finished filming, they can upload their material through a secure transmission system to the IBA for the purpose of providing evidence to international criminal prosecutions.<sup>80</sup> Evidence sent through to the IBA is stored in a “secure evidence locker” housed in London, where teams of pro bono lawyers, commissioned by the IBA, catalogue the material, hoping to make it useful to a criminal investigation.<sup>81</sup>

The other app that has been developed specifically for user-generated evidence collection in high-risk settings, although not with international criminal prosecutions exclusively in mind, is *CameraV*.<sup>82</sup> *CameraV* is also available at no cost from Google Play and is a joint project of the long-time video advocacy organization WITNESS<sup>83</sup> and a software technology group known as the Guardian Project,<sup>84</sup> with funding from Benetech, a California-based technology

---

76. See Bowcott, *supra* note 16.

77. See Ellis, *supra* note 73, at 270–71 (describing the process involved in verifying footage on an anonymous basis).

78. See *id.* at 273 (describing the process of tagging and pixel count recording).

79. See eyeWitness Project Description, *supra* note 26.

80. *Id.*

81. See Ellis, *supra* note 73, at 276 (explaining that a team of lawyers in London is responsible for reviewing the incoming footage).

82. According to the *CameraV* user manual, the “V” stands for “Verification, Veritas (Truth!) and Vaulted (secured!) [sic].” It also evokes the “V” hand sign for victory and peace. *Trust (But Verify!) What Your Eyes See, CAMERA V APP & THE INFORMA CAM SYSTEM*, <https://guardianproject.github.io/informacam-guide/en/InformacamGuide.html> [https://perma.cc/2D2N-6GCC] (*CameraV* is a project of *InformaCam* platform).

83. *About WITNESS*, WITNESS, <https://witness.org/about/> [https://perma.cc/5TGU-QSZ7] (WITNESS has focused on video advocacy since its founding in 1992).

84. *About the Guardian Project*, GUARDIAN PROJECT, <https://guardianproject.info/> [https://perma.cc/29B3-JZ9T].

company.<sup>85</sup> As the precursor to the *eyeWitness* app, it shares many of the same features, with vast amounts of metadata automatically saved in order to help address concerns about authenticity when the footage reaches a courtroom, be that inside or outside the country that the user is in.<sup>86</sup>

WITNESS is fairly conservative in their description of *CameraV* as a tool that will “help to authenticate what users document.”<sup>87</sup> The IBA is more declarative. As their introductory video to the *eyeWitness* app explains:

As an initiative of the International Bar Association, we know the legal requirements for photos and videos to be admitted as evidence in court. Recognizing the immense risks eyewitnesses take we believe these efforts should never be in vain and potential evidence should always be admissible in a court of law.<sup>88</sup>

The IBA and WITNESS differ somewhat in the degree to which they make assurances about user anonymity as a means of risk reduction, though a technical feature of both *eyeWitness* and *CameraV* is that they offer a built-in anonymity option by creating a unique hash value identifier connected to the phone rather than to the user.<sup>89</sup>

*CameraV* requires an email address from those who upload footage. But without any identifying information about the user recording the footage, there is no check on the veracity of the email address provided.<sup>90</sup> With the *eyeWitness* app, users can opt-in to providing a contact email when they submit footage to the IBA, but it

---

85. *The Benetech Story*, BENETECH, <https://benetech.org/about/> [<https://perma.cc/W829-J3UY>].

86. See Harlo Holmes, *Making Cameras Count*, YOUTUBE (Oct. 24, 2013), <https://www.youtube.com/watch?v=lzjoAdhAKWU> [<https://perma.cc/4SJ2-SZX2>] (describing encryption and metadata features that enable authentication). See also Interview with Sam Gregory, WITNESS Program Director (July 18, 2017) (on file with the *Columbia Journal of Transnational Law*) (explaining that the goal of *CameraV* was to enable users to record evidence that could hopefully withstand authentication requirements in a courtroom, but not making any predetermination about whether that would be an international courtroom like the ICC or a courtroom in the user’s locale).

87. Interview with Gregory, *supra* note 86.

88. Int’l Bar Ass’n, *Eyewitness V2 English Subbed*, VIMEO (June 15, 2017), <https://vimeo.com/221239794> [<https://perma.cc/QM89-W9E6>]. The *CameraV* user manual states that footage recorded on the app is “more likely to be admissible in a court of law.” CAMERA V APP AND THE INFORMACAM SYSTEM, *supra* note 82.

89. See Holmes, *supra* note 86; Ellis, *supra* note 73, at 273.

90. See CAMERA V APP AND THE INFORMACAM SYSTEM, *supra* note 82.

is not required.<sup>91</sup> The *eyeWitness* manual warns users who decide to submit contact information that such information “could be helpful to future investigations, but the user must understand that this information could potentially be turned over to all parties to a legal case.”<sup>92</sup> However, it also assures those choosing to film anonymously that “[w]e do not collect any information about your device that could personally identify you as the user.”<sup>93</sup> In the words of IBA Executive Director Mark Ellis, “We never have to know who you are. . . . We allow that to be a decision that you make and not us.”<sup>94</sup>

In addition to potentially addressing the problems of traditional evidence collection, such as investigator access, evidence destruction, and witness intimidation, user-generated evidence also presents the possibility of mitigating another key critique of international criminal law—namely, that it has a neo-colonialist agenda.<sup>95</sup> As the leaders of African nations have increasingly pointed out, every defendant ever charged by the ICC is African.<sup>96</sup> And, even though African nations were the court’s earliest supporters, the narrative that subsequently gained prominence is that the ICC has an anti-Africa bias and is imposing an imperialist agenda on the least powerful people on the planet.<sup>97</sup> The sight of Western investigators

---

91. See *FAQs: Using the App*, EYEWITNESS [hereinafter *eyeWitness* User FAQs], <http://www.eyewitnessproject.org> [<https://perma.cc/6XE3-L9W2>] (click “FAQs” link in upper right hand of page, then “Using the App,” and then “Click for more details on using the app”).

92. See *id.*

93. See *id.*

94. Ellis, *supra* note 73, at 278. Both *eyeWitness* and *CameraV* were designed before the EU introduced the General Data Protection Regulation (“GDPR”). An analysis of the potential implications of the GDPR for data gathered through these apps would be an interesting consideration for future research.

95. See, e.g., George Monbiot, *Imperialism Didn’t End. These Days It’s Known as International Law*, *GUARDIAN* (Apr. 30, 2012, 3:30 PM), <https://www.theguardian.com/commentisfree/2012/apr/30/imperialism-didnt-end-international-law> [<https://perma.cc/6XNG-89TY>]. But see Douglas Smith, *The International Criminal Court: The Long Arm of Neocolonialism?*, *INT’L AFF. REV.* (Nov. 1, 2009), <http://www.iar-gwu.org/node/87> [<https://perma.cc/WMV7-BR5E>] (arguing that with respect to the ICC, its prosecutorial decisions are driven not by a neo-colonialist agenda, but by the need for political survival). See generally DAVID BOSCO, *ROUGH JUSTICE* (2013).

96. Kenneth Roth, *Africa Attacks the International Criminal Court*, *HUMAN RIGHTS WATCH* (Jan. 4, 2014, 3:22 PM), <https://www.hrw.org/news/2014/01/14/africa-attacks-international-criminal-court> [<https://perma.cc/UPG9=PRZP>].

97. See Rebecca Hamilton, *The ICC, the African Union, and the UN Security Council Narratives and Counter-Narratives*, in *THE ELGAR COMPANION TO THE INTERNATIONAL CRIMINAL COURT* (Margaret deGuzman & Valerie Oosterveld eds.) (forthcoming). Of course, the critique was simply the latest iteration of a long-standing critique of international

flying in from the Hague to gather evidence from people across Africa and then flying straight out again only furthers the perception of international criminal investigations as an “extractive industry.”<sup>98</sup> By contrast, if people in remote and conflict-ridden regions could use their phones to proactively send evidence to the ICC, then a bottom-up narrative of international justice might begin to take hold. Rather than being merely the subjects of an internationally-driven justice agenda, people in conflict-ridden locations could help to direct the focus and scope of international criminal investigations.

The convergence of the expansion of ICT, the beginnings of evidence-specific app design, the increasingly visible problems of traditional evidence collection, and the need to respond to the growing critique of international justice as a top-down imperialist project soon drew the attention of philanthropic organizations interested in strengthening international criminal justice. In October 2013, a major workshop drew together funders to discuss how to “improve the capacity of investigators and prosecutors to gather and analyze digital evidence relevant to serious international crimes.”<sup>99</sup> One of the key recommendations from the workshop was that the OTP partner with technology companies and INGOs with expertise in digital material.<sup>100</sup>

With both technical and financial pieces in place, the IBA and WITNESS began outreach to get people in conflict-affected communities to download *eyeWitness* and *CameraV*, and to use the apps to secure user-generated evidence. Over 5,000 users have downloaded the *eyeWitness* app. And as of July 2017, the IBA had received 1,200 pieces of footage, translating into some seventy hours of potential evidence.<sup>101</sup> Over 10,000 users have downloaded *CameraV*.<sup>102</sup> And

---

law’s imperialist tendencies. See, e.g., U.O. UMOZURIKE, INTERNATIONAL LAW AND COLONIALISM IN AFRICA (1979), cited in James T. Gathii, *Africa*, in OXFORD HANDBOOK OF THE HISTORY OF INTERNATIONAL LAW 407, 420 (Bardo Fassbender and Anne Peters eds., 2013) (“[I]nternational law was used to facilitate or acquiesce in the imposition of [the slave trade and colonialism].”).

98. Dustin N. Sharp, *Human Rights Fact-Finding and the Reproduction of Hierarchies*, in THE TRANSFORMATION OF HUMAN RIGHTS FACT-FINDING 69, 78 (Philip Alston & Sarah Knuckey eds., 2016) (explaining that the term “extractive industry” is used by some critics of human rights fact-finding missions led by INGOs from the Global North).

99. U.C. BERKELEY SCH. OF LA, HUMAN RIGHTS CTR., *supra* note 33, at 1. The workshop was funded by Humanity United, Open Society Justice Initiative, Open Society Foundations, Sigrid Rausing Trust, and the Oak Foundation.

100. *Id.* at 11.

101. See Interview with Betts, *supra* note 74.

102. E-mail from Sam Gregory, Program Director, WITNESS, to author (July 21, 2017 14:41 EDT) (on file with the *Columbia Journal of Transnational Law*). With respect to

still many more users have filmed, and will continue to film, atrocities they witness, even in the absence of an evidence app.

It is not hard to see why the promise of user-generated evidence is attractive. The collection of evidence by local users raises the possibility of displacing Hague-based investigators as the virtually exclusive collectors of evidence for international criminal investigations. This has the potential to be a collective win: the engagement of local users shifts investigations from a top-down to a bottom-up approach, and Hague-based investigators are able to access evidence more quickly and with significantly less security risks to themselves and those they contact. In addition, the involvement of technologists opens up international criminal investigations to a whole new field of expertise, which has the potential to reduce the traditional reliance of courtrooms on eyewitness testimony—and all the problems associated with it.<sup>103</sup> While no one is suggesting that user-generated evidence could serve as a full replacement for evidence gathered in more traditional ways, its appeal as a means of buttressing other evidence is clear. At its best, user-generated evidence promises to provide a form of visual and oral testimony that (i) is secured in real-time, thereby removing the opportunity for evidence to be lost or destroyed;<sup>104</sup> (ii) is not subject to manipulation; and (iii) can be obtained with potentially zero risk to ICC investigators and the witnesses they would otherwise contact.

## II. MAPPING THE NEW INVESTIGATORY SPACE

User-generated evidence necessitates a host of new actors—or existing actors in new roles—to join the investigatory ecosystem. Neither the ICC nor any other international accountability mechanism can do all the work required to put user-generated evidence to use.<sup>105</sup> A share of the work must be outsourced. And, as in any eco-

---

*CameraV*, user footage is not gathered in a centralized location, so there is no data on the extent to which users have recorded on the app. Interview with Gregory, *supra* note 86.

103. See e.g., David A. Sonenshein & Robin Nilon, *Eyewitness Errors and Wrongful Convictions: Let's Give Science a Chance*, 89 OR. L. REV. 263 (2010).

104. See KELLY MATHESON, WITNESS, VIDEO AS EVIDENCE FIELD GUIDE 5 (2016) (“In many situations, citizens and on-the-ground human rights activists and advocates are better positioned to collect evidence of human rights abuse than professional investigators because investigators almost always arrive after-the-fact when evidence has deteriorated or is gone.”).

105. U.C. BERKELEY SCH. OF LAW, HUMAN RIGHTS CTR., *supra* note 33, at 7 (noting that the court does not have the capacity to handle cutting-edge technological developments).

system, the introduction of new actors affects the dynamics in play across the entire investigatory field. Lines of authority and responsibility are “obscure[d] and fragment[ed]” as decision-making is distributed among the new mix of actors in the space.<sup>106</sup>

The emergence of user-generated evidence necessitates the introduction of four groups of actors into the sphere of international criminal investigations. First, there are the evidence-focused INGOs who have pushed for the production of user-generated evidence. In addition to overseeing the development of user-generated evidence apps, they are also responsible for the outreach and training required for the technology to be adopted in conflict-affected regions. Lacking the technical expertise to design the apps themselves, these INGOs have partnered with another set of actors, technologists. The technologists who have been drawn into the investigatory space do not have a background in international criminal justice, but they do have the skills required to translate evidentiary requirements into app design. The next group of new actors is the users who witness atrocities and record what they are seeing. And finally, the fourth group is the private lawyers who take on the roles of cataloguing, coordinating, and potentially curating incoming user-generated evidence.

The following section maps out the roles played by each of the four groups brought into the investigative space by the emergence of user-generated evidence and begins to discuss some of the challenges they face in their interactions, both with each other and with courts that may rely on user-generated evidence.

#### *A. Evidence-Focused INGOs*

The presence of INGOs in the investigatory ecosystem is nothing new. International investigators are unlikely to be the first people to arrive on the scene when atrocities occur. The so-called “first responders” from the international community are instead the human rights, humanitarian, and protection organizations that are already working in the locale or nearby.<sup>107</sup> Material gathered by human rights organizations has been used in international criminal investigations since the start of the contemporary era of international

---

106. See Molly Land & Jay D. Aronson, *The Promise and Peril of Human Rights Technologies*, in NEW TECHNOLOGIES FOR HUMAN RIGHTS LAW AND PRACTICE 1, 11 (Molly Land & Jay D. Aronson eds., 2018). Although Land and Aronson describe the fragmentation of authority in relation to user-generated content more generally, the same concerns apply specifically to user-generated evidence.

107. See U.C. BERKELEY SCH. OF LAW, HUMAN RIGHTS CTR., *supra* note 12, at 4.



criminal trials.<sup>108</sup> What is new here is the recent decision by the IBA and WITNESS to focus on the collection of materials specifically intended, from the pre-collection stage forward, to end up in a courtroom.

### 1. Local Outreach by Evidence-Focused INGOs

The entry of these evidence-focused INGOs into the investigative space began with their involvement in the creation of user-generated evidence apps. But it did not end there. Both WITNESS and the IBA readily understood that fostering the creation of user-generated apps alone would not be enough to bring in useful evidence. People in conflict-affected areas must first be encouraged to download the apps, and then trained on how to use them. It is this outreach to local populations, perhaps even more than the design features of the apps themselves, that will determine whether user-generated evidence is admitted into an international criminal trial.

A key challenge in getting people who have downloaded *eyeWitness* or *CameraV* to record useful content is to educate them on the often counter-intuitive types of evidence needed to build a criminal case.<sup>109</sup> In most atrocity situations, there is little doubt that a crime of some kind has occurred. The investigatory challenge is to

---

108. Human rights reporting by INGOs and international organizations have been relied upon by: the ICTY, *see, e.g.*, Prosecutor v. Tolimir, Case No. IT-05-8/2-T, Judgment, ¶¶ 50–51 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 12, 2012), <http://www.icty.org/x/cases/tolimir/tjug/en/121212.pdf> [<https://perma.cc/48XM-X7WP>] (relying on documentation from Physicians for Human Rights and the International Committee of the Red Cross); ICTR, *see, e.g.*, Prosecutor v. Setako, Case No. ICTR-04-081-T, Judgment and Sentence, ¶ 164 (Int'l Crim. Trib. for Rwanda Feb. 25, 2010), <http://unictr.irmct.org/sites/unictr.org/files/case-documents/ict-04-81/trial-judgements/en/100225.pdf> [<https://perma.cc/4FKW-BCX2>] (entering a report by Committee for the Respect of Human Rights and Democracy in Rwanda into evidence after receiving information on its provenance); ICC, *see, e.g.*, Prosecutor v. Ongwen, ICC-02/04-01/15, Decision on Prosecution's Request to Submit 1006 Items of Evidence, ¶¶ 41–42 (Jan 16, 2017), [http://www.icc-cpi.int/CourtRecords/CR2017\\_01740.pdf](http://www.icc-cpi.int/CourtRecords/CR2017_01740.pdf) [<https://perma.cc/HG3A-KEZP>] (requesting to enter documentation from Amnesty International and Human Rights Watch); and the various hybrid tribunals, *see, e.g.*, Prosecutor v. Fofana, Case No. SCSL-04-14-T, Judgement of the Sentencing of Moinina Fofana and Allieu Kondewa, ¶ 55 (Special Ct. for Sierra Leone Oct. 9, 2007), <http://www.rscsl.org/Documents/Decisions/CDF/796/SCSL-04-14-T-796.pdf> [<https://perma.cc/EV8X-B7UY>] (relying on documentation from the International Committee of the Red Cross). It should be noted, however, that the degree to which courts have accepted third-party evidence has varied based on the stage of the trial proceeding. *See infra* Part III.C.I.

109. *See generally* DAVID CRUMP ET AL., CRIMINAL LAW: CASES, STATUTES, AND LAWYERING STRATEGIES (2d ed. 2010).

gather evidence linking the crime to the person or people responsible (so-called “linkage evidence”).<sup>110</sup> Most people with a smartphone in hand during or after the commission of atrocities will point it in the direction of harmed individuals, dead bodies, or destroyed infrastructure.<sup>111</sup> But this sort of footage does not help investigators establish who is responsible for the suffering captured on film.<sup>112</sup> By contrast, images such as the insignia on soldier uniforms, or communications and transportation equipment, can be invaluable in establishing a chain of responsibility.<sup>113</sup>

To this end, WITNESS produced a 200-page field guide, entitled *Video as Evidence*, which it uses to train groups and individuals who may witness crimes.<sup>114</sup> The field guide uses both text and illustrations to explain basic concepts central to law and evidence, provide pragmatic advice on how to capture useful evidence, and raise some of the safety and ethical challenges involved in filming.<sup>115</sup>

The IBA has also produced training materials, although the focus of these materials is primarily on illustrating how to use the *eyeWitness* app itself.<sup>116</sup> More significantly, the IBA has run an extensive outreach program. In addition to disseminating information about the *eyeWitness* app through traditional media, the IBA has used social media to alert users who are already recording crimes to the

---

110. INT’L BAR ASS’N, EVIDENCE MATTERS IN ICC TRIALS 35–36 (2016) (describing linkage evidence as that which establishes “a relationship between the crimes and the criminal responsibility of an accused” and emphasizing its importance in criminal proceedings). The value of linkage evidence is obviously also high in the domestic context. See Stuart, *supra* note 30, at 338–40 (presenting comparative case study on the impact of video evidence of police criminality taken by a community watchdog group, finding that video containing linkage evidence was more effective than video without such evidence).

111. See, e.g., Nadia Sayej, *War Zone via Smartphone: The Syria Mobile Film Festival*, GUARDIAN (Apr. 8, 2016), <https://www.theguardian.com/film/2016/apr/08/syrian-mobile-film-festival-berlin-films-shot-on-smartphones> [https://perma.cc/7K6N-BSUW].

112. See Jay D. Aronson, *The Utility of User Generated Content in Human Rights Investigations*, in NEW TECHNOLOGIES FOR HUMAN RIGHTS LAW AND PRACTICE 129, 131 (Molly Land & Jay D. Aronson eds., 2018) (explaining how most footage captured by citizens shows evidence that a crime occurred, not evidence of who might be responsible).

113. See Alison Cole, *Pictures of Atrocity: Turning Video Footage into Evidence of War Crimes* EMERGENCY JOURNALISM (Mar. 14, 2014), <http://emergencyjournalism.net/pictures-of-atrocity-turning-video-footage-into-evidence-of-war-crimes/> [https://perma.cc/DKQ4-J9WM]. See also MATHESON, *supra* note 104, at 42.

114. MATHESON, *supra* note 104.

115. *Id.*

116. See, e.g., EYEWITNESS, THE HOW TO INFO-BOOKLET (2017), <http://www.eyewitnessproject.org/wordpress/wp-content/uploads/2017/01/How-To-Info-Booklet-lo-res.pdf> [https://perma.cc/XYK9-9B2T].

availability of the app, and it has also done in-person outreach to local human rights groups in conflict-affected areas in Syria, Kenya, and South Sudan.<sup>117</sup> Overall, then, to make user-generated evidence actually useful to an investigatory team, a significant degree of INGO involvement is required.

## 2. Complications Flowing from Local Outreach

INGO engagement with local populations raises complex questions of accountability. And as has been thoroughly discussed in the literature, INGOs based in the Global North, yet working primarily with populations in the Global South, face a range of stakeholders with potentially conflicting objectives to satisfy.<sup>118</sup>

For an organization whose goal is to secure user-generated evidence, it is not obvious how to balance, for instance, values of empowerment and autonomy for users who want to retain control over what they document and where that footage goes, with the goal of getting footage that will be most useful for criminal proceedings quickly into the hands of an investigative team. Even at this nascent stage, the two main organizations involved in the production of user-generated evidence have taken divergent paths on this issue. Users of the *eyeWitness* app must, per the design of the app, send their footage to the IBA in London before they send it anywhere else for the purposes of sharing or storage.<sup>119</sup> While this reduces the control users have over their footage, the IBA views this as crucial to their ability to vouch for the authenticity of the evidence.<sup>120</sup> The design of *CameraV*, by contrast, offers users unlimited flexibility to decide whether or where to share or store the footage they record. “We don’t want to make assumptions about who is the right entity for grassroots groups to share their evidence with,” explains WITNESS Program Director

---

117. See, e.g., *eyeWitness to Atrocities* (@eyewitnessorg), TWITTER (Mar. 13, 2018, 5:45 AM), <https://twitter.com/eyewitnessorg/status/973495319676837889> [<https://perma.cc/J327-8CXG>].

118. See, e.g., DAVID L. BROWN, CREATING CREDIBILITY: LEGITIMACY AND ACCOUNTABILITY FOR TRANSNATIONAL CIVIL SOCIETY 3–11 (2008); Diana Hortsch, *The Paradox of Partnership: Amnesty International, Responsible Advocacy, and INGO Accountability*, 42 COLUM. HUM. RTS. L. REV. 119, 126–35 (2010) (discussing the International INGO Accountability Charter); Kenneth Anderson, *What INGO Accountability Means—and Does Not Mean*, 103 AM. J. INT’L L. 170, 174 (2009) (summing up the debate with reference to a question posed by David Rieff: “So who elected the NGOs?”).

119. *EyeWitness* User FAQs, *supra* note 91.

120. See Ellis, *supra* note 73, at 273 (explaining how any footage must be sent to the IBA before being shared elsewhere).

Sam Gregory. “In general our bias is toward the autonomy of the user.”<sup>121</sup>

The specific costs and benefits of the involvement of evidence-focused INGOs will become clearer over time. What is not in doubt, though, is that the production of user-generated evidence does not occur through the introduction of an app alone. The engagement of INGOs in outreach to local populations is an essential component of the success (or failure) of getting user-generated evidence into an international courtroom. And this is true regardless of whether or not user-generated evidence is recorded through a specialized app.

### *B. Technologists*

As discussed in Part I, challenges to traditional criminal investigations became increasingly visible around the same time as the global ICT expansion began to facilitate an explosion of user-generated content, leading some to wonder whether user-generated evidence could alleviate the pressure on international investigations.<sup>122</sup> The challenge, however, was how to ensure that footage gathered by smartphone users could be authenticated to satisfy legal standards. To that end, the question arose as to whether there could be a technical solution to the authentication problem through carefully tailored app design. Of course, organizations focused on human rights, justice, and accountability do not—at least at the current moment—have the in-house technical expertise to design apps themselves.

In order to develop a user-generated evidence app, WITNESS partnered with the technology group the Guardian Project, and the IBA hired its own technologists.<sup>123</sup> In neither case did these technologists have any particular background in human rights, justice, or accountability—and there is nothing exceptional about this.<sup>124</sup> Technologists rarely have substantive expertise on the underlying issue

---

121. See Interview with Gregory, *supra* note 86.

122. See Ellis, *supra* note 73, at 269–70 (describing how the question arose, of whether an app could be designed to address verification concerns, in the context of a mass of unverifiable user-generated content).

123. See *Our Apps: CameraV*, GUARDIAN PROJECT, <https://guardianproject.info/apps/camerav/> [<https://perma.cc/8JB4-MVEP>].

124. See, e.g., Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 700 (2017) (explaining that the individual coder of an automated decision-making algorithm is “unlikely to have substantive expertise” about the decision the algorithm is tasked with making).

they design their software to handle.<sup>125</sup>

The control of technologists over design innovations, like user-generated evidence apps, has been a topic of fascination for legal scholars since Lawrence Lessig's groundbreaking work *Code* was published in 1999.<sup>126</sup> It is now commonly acknowledged that "code reflects the values of its writers and owners."<sup>127</sup> And, as Molly Land and others have observed, human rights organizations and technologists each generally bring a distinctly different ethos to their work.<sup>128</sup> While the former are inherently conservative in their calculations of risk, the latter emphasize the value of experimentation and embrace iterative failures in the name of innovation.<sup>129</sup> There is a risk, therefore, that the risk-conservative approach valued by human rights organizations will be lost as their projects are translated into code that they themselves do not understand. Still, human rights organizations can help manage this risk through strong and ongoing communication with the technologists they partner with.

These challenges notwithstanding, both the IBA and WITNESS understood that the development of a technically sophisticated and replicable methodology behind the process of bringing user-generated evidence into courtrooms would be central to the credibility of their claim that what users filmed would be useful in a court of law.<sup>130</sup> In sum, the involvement of technologists is another non-negotiable aspect of bringing user-generated evidence to life.

---

125. *See id.*

126. *See* LAWRENCE LESSIG, *CODE: AND OTHER LAWS OF CYBERSPACE* (1999).

127. Lilian Edwards, *Coding Privacy*, 84 CHL.-KENT. L. REV. 861, 871 (2010).

128. *See* MOLLY LAND ET AL., WORLD BANK, #ICT4HR (INFORMATION AND COMMUNICATION TECHNOLOGIES FOR HUMAN RIGHTS) 31 (2012).

129. *See id.* at 1 (describing the "modus operandi" of the technology field as in tension with that of human rights). *See also* Arvind Narayanan and Shannon Vallor, *Why Software Engineering Courses Should Include Ethics Coverage*, 57 COMM. OF THE ACM 23, 24 (2014) (arguing for ethics to be taught to software engineering students on the grounds that otherwise, when they graduate, "they are likely to adopt the type of thinking that prevails in many parts of the industry – that anything technically feasible is fair game").

130. For a fascinating account of a similar process, albeit in relation to a different technology, see Arthur Daemrich, *The Evidence Does Not Speak for Itself: Expert Witnesses and the Organization of DNA Typing Companies*, 28 SOC. STUD. OF SCI. 741–72 (1998) (detailing how private DNA companies entered the forensic analysis system traditionally run by state actors and describing how it was crucial for these private actors to develop and market the credibility of their methodology for use in a courtroom setting). Underscoring the point, the IBA plans to offer interested courts the code behind the eyeWitness app. *See* Interview with Betts, *supra* note 74.

### C. Users

Smartphone users are the linchpin of user-generated evidence collection. They are a diverse population, ranging from those who have opportunistically filmed an atrocity on a one-time basis, to those who are involved in the systematic collection of atrocity footage.<sup>131</sup> While there are no statistics available, it seems clear from the scale of content uploaded to social media since around 2011 that users involved in evidence collection constitute a sizeable population. And the key question for INGOs involved in marketing user-generated evidence apps or otherwise encouraging local populations to document crimes, as well as for courts relying on user-generated evidence more generally, is the extent to which they are confident that users fully comprehend the risks and benefits involved in evidence collection.

As the U.S. Department of Homeland Security emphasized in its 2011 report on ethical guidelines in ICT research, the kind of comprehension required by informed consent implies that researchers must consider “the complex interconnected relationships between users and the myriad of organizations which provide ICT services.”<sup>132</sup> When it comes to footage, the question of informed consent is typically raised in reference to the relationship between the user and the subject who is being photographed or filmed.<sup>133</sup> While that question is also relevant when it comes to user-generated evidence, the complex issues related to the consent of victims and perpetrators recorded through user-generated evidence apps lies beyond the focus of this Article.<sup>134</sup> Instead, with an eye to the new actors in the investigatory

---

131. See, e.g., *Our Methodology*, VIOLATIONS DOCUMENTATION CENTER IN SYRIA (describing how the organization systematically gathers photo and video of victims in the aftermath of atrocities), <http://vdc-sy.net/our-methodology/> [<https://perma.cc/6Z3N-XPNF>]; *Coletivo PapPapo Reto: Combating Police Violence in Brazil*, WITNESS (Sept. 2017), <https://witness.org/coletivo-papo-reto-combating-police-violence-in-brazil/> [<https://perma.cc/U4EB-EBSH>] (describing the work of a group of activists in Brazil “who use cell phones and social media to counter mainstream narratives, document abuses, and report police violence in the Complexo do Alemão”).

132. U.S. DEP’T OF HOMELAND SEC., *THE MENLO REPORT: ETHICAL PRINCIPLES GUIDING INFORMATION & COMMUNICATION TECHNOLOGY RESEARCH* 10 (2012).

133. See, e.g., Philippe Calain, *Ethics and Images of Suffering Bodies in Humanitarian Medicine*, 98 SOC. SCI. MED. 278 (2013).

134. It is, however, a question worthy of separate scrutiny. Efforts made to address the issue in WITNESS’s *Video as Evidence Field Guide* are commendable but represent only a fraction of what could be said on the topic. The field guide states that “[t]he internationally agreed-upon standard is that informed consent must be secured when taking testimony in writing, via audio recording, or via video recording.” MATHESON, *supra* note 104, at 159. It then notes that in the field “it can be impractical—or even impossible—to follow this recommendation,” before going on to discuss considerations of disclosure, comprehension,

ecosystem, the informed consent question arises with respect to the relationship between the INGOs who have fostered the development of user-generated evidence apps, the users who have downloaded them, and, in time, the courts who will rely on evidence captured by those users.<sup>135</sup>

Best practices vary across diverse fields on what it means to secure meaningful informed consent, but the interconnected principles of voluntariness and comprehension are consistent.<sup>136</sup> Voluntariness incorporates the idea that one party, in this case an INGO, does not promise, nor even raise the prospect of, a benefit that is not assured.<sup>137</sup> This issue of perceived benefits matters because the appeal of what an individual perceives to be a benefit can influence that individual's assessment of whether to undertake the activity in question. An individual may decide it is worth taking a life-threatening

---

voluntariness, and competence. *Id.*

135. Trailblazers in the use of user-generated content within the field of journalism are just beginning to deal with this same question. See *ONA Social Newsgathering Ethics Code*, ONLINE NEWS NAT'L ASS'N, <https://journalists.org/tools/social-newsgathering/> [<https://perma.cc/TY8C-E8VL>] (discussing the need to secure "informed consent for the use of UGC through direct communication with the individual who created it").

136. See, e.g., OXFAM, RESPONSIBLE PROGRAM DATA POLICY 7 (Feb. 17, 2015), <https://oxfamlibrary.openrepository.com/bitstream/handle/10546/575950/ml-oxfam-responsible-program-data-policy-en-270815.pdf> [<https://perma.cc/QU8T-768Q>]; *What is Informed Consent?*, BBC EDITORIAL GUIDELINES, <http://www.bbc.co.uk/editorialguidelines/guidance/consent/what> [<https://perma.cc/D5KX-Z2RH>]. The history of informed consent in the medical context begins with the Nuremberg trials of doctors who conducted unlawful medical experiments during the Holocaust. As part of their verdict, the Nuremberg judges issued what became known as the Nuremberg Code. The Code explains that informed consent must be voluntary and that voluntariness means "without the intervention of any element of force, fraud, deceit, duress, over-reaching, or other ulterior form of constraint or coercion; and [the individual giving consent] should have sufficient knowledge and comprehension of the elements of the subject matter involved as to enable him to make an understanding and enlightened decision." OFFICE OF HISTORY, NAT'L INST. OF HEALTH, THE NUREMBERG CODE, <https://history.nih.gov/research/downloads/nuremberg.pdf> [<https://perma.cc/6KTA-656D>]. The concept of informed consent has also been incorporated into the U.S. criminal justice system, even if not always under that term. See *Brady v. United States*, 397 U.S. 742, 748 (1970) (holding that a defendant's agreement to a plea bargain "must be [a] voluntary . . . knowing, intelligent act[] done with sufficient awareness of the relevant circumstances and likely consequences").

137. This can be tricky even for the most well-intentioned representative. As research with vulnerable populations in humanitarian and journalism contexts has noted, even if INGO workers or journalists state that they cannot provide benefits, it is hard to stop the local population from assuming that there is at least a chance that someone with international connections will be able to provide themselves or their communities with assistance. See, e.g., Eileen Pittaway et al., '*Stop Stealing Our Stories*': *The Ethics of Research with Vulnerable Groups*, 2 J. HUM. RTS. PRAC. 229, 232–34 (2010).

risk to record footage if they believe the footage will be used to help send a perpetrator to jail. They may not make the same decision if they are uncertain about whether a court would consider their footage at all.

EyeWitness Project Director Wendy Betts says that in its outreach and training with users, IBA is careful to explain that until the first piece of this kind of user-generated evidence is introduced in an international criminal trial, no one really knows for sure whether judges will accept it.<sup>138</sup> Even so, given the context of an outside organization introducing a sophisticated piece of technology designed with evidence collection in mind, it seems possible that such caveats are not fully absorbed by would-be users. Even if users are told that what they film may not withstand legal scrutiny, is that what they believe?<sup>139</sup>

The promised benefit to users is that footage they record can be used to further legal accountability. On the flipside of the equation, the risks involved relate to the security of the users, as well as to their family and/or community. The degree to which users who choose anonymity can really be guaranteed that their identity will remain protected throughout an adversarial legal process is arguable.<sup>140</sup> But even the guarantee of anonymity as a purely technical matter is questionable. “We can never know [that a system is fool-proof],” says Dia Kayyali, Senior Program Coordinator for Technology and Advocacy at WITNESS.<sup>141</sup>

In sum, there are unanswered questions affecting the degree to which informed consent can yet be said to be meaningful in the user-generated evidence context. Over time, a fuller understanding of how courts will respond to this kind of evidence, and the degree to

---

138. See *infra* Part III.C.1.

139. In a three-year study of informed consent in the medical transplantation context, there was a significant difference between patient and physician comprehension of the risk of mortality. Even though patients were informed about the risk of mortality, they persistently underestimated the likelihood of this risk applying to them. See Stephanie J. Lee, et al., *Discrepancies Between Patient and Physician Estimates for the Success of Stem Cell Transplantation*, 285 JAMA 1034 (2001). This same issue of heightened patient expectations of a positive outcome, notwithstanding the provision of information about risks in informed consent discussions, has been found in other medical studies. See, e.g., Neal Meropol et al., *Perceptions of Patients and Physicians Regarding Phase I Cancer Clinical Trials: Implications for Physician-Patient Communication*, 21 J. CLINICAL ONCOLOGY 2589 (2003).

140. See *infra* Part III.C.3.

141. Audio tape: Interview by Deyaa Alrwishdi with Dia Kayyali, Senior Program Coordinator for Technology and Advocacy at WITNESS (on file with the *Columbia Journal of Transnational Law*).



which any promises of anonymity can really be upheld, will be crucial.

#### *D. Private Lawyers*

The “cost-free” nature of smartphone recording and the minimal barriers to entry by hitting “record” have resulted in more footage than an international court has resources to sift through in-house. And the IBA and WITNESS have taken different approaches to the question of who should do this curation work. By having no centralized depository for the storage of footage, *CameraV* distributes the workload; WITNESS expects that users will make their own determination of what footage to submit where.<sup>142</sup> By contrast, all footage submitted through the *eyeWitness* app is sent to the IBA in London, necessitating that they take on this work.<sup>143</sup> Thus, depending on design choices made in the creation of the app, the final set of actors who may be brought into the investigative ecosystem by the emergence of user-generated evidence is private lawyers. These are the people who do the necessary work of watching the hours of footage recorded by users to then catalogue the material, connect investigatory teams to that material, and potentially curate which footage could be useful for a criminal case.<sup>144</sup>

The sheer volume of user-generated content worldwide means that the need for cataloguing and curation arises constantly, even outside the evidence-collection context.<sup>145</sup> For example, newsrooms and social media sites have to review incoming material and then make what can be controversial judgment calls about what user-generated footage to make accessible (in the case of newsrooms)<sup>146</sup> or to let

---

142. See interview with Gregory, *supra* note 86.

143. See eyeWitness Organisation FAQs, *supra* note 9 (“When footage is sent to us, a copy is transferred to a specialised database for analysis by the eyeWitness legal team. This team analyse [sic] the footage to determine whether they may show that an atrocity crime was committed.”).

144. See *id.*

145. See Molly Land, *Democratizing Human Rights Fact-Finding*, in THE TRANSFORMATION OF HUMAN RIGHTS FACT-FINDING 399, 402 (Philip Alston & Sarah Knuckey, eds. 2016) (“[N]ew technologies have engendered . . . the collection of a far greater volume of information than ever before possible.”) (emphasis in original).

146. See, e.g., Joe Concha, *Graphic Videos Spark Questions for Facebook, Journalism*, THE HILL (July 10, 2016), <http://thehill.com/homenews/287166-graphic-videos-spark-questions-for-facebook-journalism> [<https://perma.cc/ZL9C-RTQZ>] (discussing CNN’s decision to screen user-generated content of a police officer being executed by a sniper).

remain accessible (in the case of social media sites)<sup>147</sup> to a wide audience. Relative to professionals in these other fields, those involved in international criminal investigations are at an embryonic stage in trying to figure out how to navigate the challenge of having an abundance of user-generated material to sort through.

What seems probable at this point is that, unlike a newsroom where journalists within the same organization catalogue the incoming material and decide which of it to use, in the new investigatory ecosystem, the functions of cataloguing and curation will be split across individuals and organizations.<sup>148</sup> This, then, requires someone—whether a user in a decentralized system or a private lawyer in a centralized system—to take on the role of connecting an investigator to the available material. But access to investigators and their interests is often difficult, and so exactly how best to do this coordination is something that no one working on user-generated evidence collection has yet figured out.<sup>149</sup>

As noted above, WITNESS's approach is to leave the task up to individual users. The IBA, meanwhile, has a full-time senior legal advisor and eleven pro bono attorneys from three law firms who watch and catalogue footage that comes through the *eyeWitness* app. The lawyers' task is to tag the footage for the presence of relevant features, such as license plates and uniform insignia, and to provide an "objective description" of what they watched.<sup>150</sup> As other apps are developed, and as users continue to post their cellphone footage directly on social media sites, this curation task will only become more unwieldy.

---

147. See, e.g., Heidi Glenn, *How Facebook Uses Technology to Block Terrorist-Related Content*, NAT'L PUB. RADIO (June 22, 2017, 4:55 AM), <http://www.npr.org/sections/alltechconsidered/2017/06/22/533855547/how-facebook-uses-technology-to-block-terrorist-related-content> [<https://perma.cc/FDM8-4QKL>] (discussing Facebook's effort to remove terrorist propaganda, while also respecting free speech).

148. See *eyeWitness Organisation FAQs*, *supra* note 9 (explaining that *eyeWitness* may work with local organizations to verify footage, raise awareness, and to ensure that perpetrators are brought to justice).

149. See Interview with Betts, *supra* note 74 (describing coordination as the next major challenge facing the field).

150. See *id.* Objectivity is challenging but important, lest a future investigative team want to use the footage for a purpose that does not match the cataloguer's subjective description.

### III. COMPLICATING THE PICTURE

Part II explained how the advent of user-generated evidence means not only the introduction of a new form of technology into the investigative space, but also a host of new actors and relationships. It mapped out those actors and discussed some of the challenges that their interaction brings. Notwithstanding the significance of some of these challenges, the engagement of new actors is not inconsistent with the possibility that user-generated evidence will serve a transformative function.

The following section, however, delves into more fundamental concerns about the impact of user-generated evidence. Moving sequentially through each stage in the lifecycle of user-generated evidence, from collection and evaluation to a criminal trial and its aftermath, this section identifies several recurring concerns that can be grouped into three broad categories: (i) user security, (ii) evidentiary bias, and (iii) fair trial rights.

The burden of the first of these concerns falls on the shoulders of the user who may have taken life-threatening risks to document atrocities in the belief they could help achieve legal accountability, only to find that the footage never reaches a court investigator or that, even after reaching a court, it ultimately serves a different purpose than the user intended. Even if the user's expectations are met in terms of how their footage is used, risks to the user's security follow users from the moment of filming through to the aftermath of an eventual trial. In traditional international investigations, the court takes on protection obligations to those who have supported the court's work. Yet in the new investigations ecosystem described in Part II, there is no one accountable if—or when—a user's safety is in jeopardy.

The second set of concerns, related to evidentiary bias, poses a challenge for more traditional legal actors. Judges, as well as prosecution and defense lawyers, need to be attuned to the risks that arise not only through the biases that affect our perception of visual evidence in general, but also through the selective nature of real-time evidence collection, especially when those doing the documentation may have a personal stake in what they are recording.

These actors must also be vigilant when it comes to the final category of concern: fair trial rights. To date, the collection of user-generated evidence in the international criminal realm has been a project directed toward strengthening the hand of prosecutors.<sup>151</sup> In this

---

151. See U.C. BERKELEY SCH. OF LAW, HUMAN RIGHTS CTR., *supra* note 33, at 3

regard, not only is a lack of parity unfair to defendants, it also undermines the legitimacy of international criminal justice more generally.

If not addressed, these concerns could undermine any transformative role that user-generated evidence might play. Indeed, the emergence of user-generated evidence may end up addressing some of the problems with the current investigatory system at the cost of creating new problems, entrenching old ones, and/or simply shifting existing problems from traditional actors, who have institutional support, to individual users who have no such institutional protections.

### *A. Evidence Collection Stage*

The collection of user-generated evidence begins with users in a conflict-affected area documenting evidence of atrocities. This stage in the lifecycle of user-generated evidence brings several risks: security threats to users, the potential that evidence gathered by these users will reflect intra-conflict partisan bias, and the possibility that the material they gather will feed into an evidentiary record that skews systematically in favor of the prosecution, thereby exacerbating existing concerns about the inequality of arms in international criminal law.

#### *1. Risks to the User*

Collecting incriminating evidence is an inherently risky task under many circumstances. Those risks are heightened significantly when it comes to user-generated evidence because the evidence collection often happens in real time.<sup>152</sup> As a result, the perpetrator(s) and their allies are likely to be on the scene or in the vicinity, and thus can retaliate against the user.

The advent of user-generated evidence is too new for there to

---

(“Improving the collection and analysis of digital information can enhance the Office of the Prosecutor’s ability to secure quality evidence that results in convictions, as well as diversify evidence coming into the courtroom.”).

152. See, e.g., *FAQs: User Safety*, EYEWITNESS [hereinafter eyeWitness User Safety FAQs], <http://www.eyewitnessproject.org/#> [<https://perma.cc/XXZ8-WHZB>] (Click “FAQs” link in upper right hand of page, then “User safety,” and then “Click for more details on user safety”) (“There are always risks involved with documenting human rights abuses. There is not only danger from the user’s proximity to a volatile situation, but also the risk of arrest or other repercussions from authorities who do not want information about their actions to be publicised. No technology can completely eliminate those risks.”).

be a robust literature on the risks of retaliation that users may face. But the likelihood of retaliation can be gleaned from other sources. Domestically, for example, there was an initial optimism running through the scholarship and commentary on domestic policing, about the possibility of cellphone recordings shifting the existing (im)balance of power between police and citizens. “When there are no cameras, the advantage goes to the shooter. . . . Where there are cameras, however, the playing field is leveled.”<sup>153</sup> Yet the citizens who filmed the high-profile police shootings of Alton Sterling, Philando Castile, Freddie Gray, and Eric Garner were all subsequently arrested.<sup>154</sup>

Even in lower-profile cases, citizens who have recorded police conduct that they believed was questionable or unlawful have been subject to a range of retaliatory actions. In states with strict wiretapping statutes, police have arrested users and charged them with violations of wiretapping provisions.<sup>155</sup> Courts have generally found that such statutes do not extend to police officers performing official duties in public; however, this has not stopped police from using wiretapping statutes as the basis for making an arrest, even if the charges are ultimately dismissed.<sup>156</sup> Moreover, in states without such wiretapping provisions, police have used broader charges, such

---

153. Charles Cooke, *quoted in* David Uberti, *How Smartphone Video Changes Coverage of Police Abuse*, COLUM. JOURNALISM REV. (Apr. 9, 2015), [https://www.cjr.org/analysis/smartphone\\_video\\_changes\\_coverage.php](https://www.cjr.org/analysis/smartphone_video_changes_coverage.php) [<https://perma.cc/US8P-E8G9>]. See also Simonson, *supra* note 23, at 1564 (“When civilians film the police, local residents become the ones ensuring police accountability, resulting in a palpable power shift. Local residents remain in control of the footage and the information.”).

154. See PEN AM., *More Than 40,000 Americans Call on Justice Department to Investigate Retaliation Against Those Who Document Alleged Police Misconduct* (Oct. 26, 2016), <https://pen.org/press-release/more-than-40000-americans-call-on-justice-department-to-investigate-retaliation-against-those-who-document-alleged-police-misconduct> [<https://perma.cc/B6DP-DSTV>]. The majority of these arrests did not result in any formal charges against the detained cameraperson. See Jamiles Lartey, *Film Makers Demand Inquiry into ‘Targeting’ of People Who Record Police*, GUARDIAN (Aug. 12, 2016, 3:55 BST), <https://www.theguardian.com/film/2016/aug/10/filmmakers-citizen-journalists-justice-department-investigation> [<https://perma.cc/5YBP-AV5T>].

155. See, e.g., Dustin F. Robinson, *Bad Footage: Surveillance Laws, Police Misconduct, and the Internet*, 100 GEO. L.J. 1399, 1400–13 (2012) (describing cases involving prosecutions under wiretapping statutes for the filming of police misconduct). See also Michael Potere, Comment, *Who Will Watch the Watchmen? Citizens Recording Police Misconduct*, 106 NW. U.L. REV. 273 (2012).

156. See Radley Balko, *Despite Court Rulings, People Are Still Getting Arrested for Recording On-Duty Cops*, WASH. POST (May 13, 2014), [https://www.washingtonpost.com/news/the-watch/wp/2014/05/13/despite-court-rulings-people-are-still-getting-arrested-for-recording-on-duty-cops/?utm\\_term=.c9afed401422](https://www.washingtonpost.com/news/the-watch/wp/2014/05/13/despite-court-rulings-people-are-still-getting-arrested-for-recording-on-duty-cops/?utm_term=.c9afed401422) [<https://perma.cc/AA86-TGD4>].

as disorderly conduct, to arrest users for filming.<sup>157</sup> And beyond the risk of arrest and prosecution, users have reported feeling so unsafe as to have given up on filming police misconduct altogether.<sup>158</sup>

Internationally, the risks are clear from the forms of retaliation faced by those seeking to document atrocities in Syria. As of October 2018, the Committee to Protect Journalists had confirmed the killings of 123 Syrian journalists.<sup>159</sup> Further indications of the risks involved come from retaliation faced by local Syrians who have been working for the Syrian Commission on Justice and Accountability, a Brussels-based non-profit group that is trying to smuggle documentation out of Syria with an eye to eventual criminal prosecutions. Several of their local investigators have been injured and at least one is presumed dead.<sup>160</sup>

Finally, the security threats faced by past and current ICC witnesses may also provide some indication of the risks involved for users. Many users are, in a literal sense, witnesses; they often witnessed the commission of the atrocities they seek to document. While the Court does not publish statistics on the number of its witnesses that face security threats, it is possible to get a sense of the scale of the problem when considering that in the Court's first case, the OTP, over a ten-week period, referred thirty-two witnesses into the Court's protection program.<sup>161</sup> That program was established to

157. See, e.g., Kreimer, *supra* note 61, at 361; N. Stewart Hanley, *A Dangerous Trend: Arresting Citizens for Recording Law Enforcement*, 34 AM. J. TRIAL ADVOC. 645, at 647–50 (2010). See also Emma Whitford, *Man Who Filmed Eric Garner's Murder Begins 4 Year Prison Sentence Today*, GOTHAMIST (Oct. 30, 2016), [http://gothamist.com/2016/10/03/eric\\_garner\\_ramsey\\_orta.php](http://gothamist.com/2016/10/03/eric_garner_ramsey_orta.php) [<https://perma.cc/B2K5-7SL6>].

158. See *Interview with a Representative of a Cop-Watching Organization*, in Jocelyn Simonson, *Copwatching*, 104 CAL. L. REV. 393, 429 n.203 (2016).

159. *123 Journalists Killed in Syria/Motive Confirmed*, COMM. TO PROTECT JOURNALISTS, <https://cpj.org/killed/mideast/syria/> [<https://perma.cc/46BC-68Q8>]. See also, Rayan Mohammad, *Syrian journalists Who Sacrificed Everything to Cover the Revolution*, NEW ARAB (Mar. 15, 2017) (Karim Traboulsi trans.), <https://www.alaraby.co.uk/english/indepth/2017/3/15/syrian-journalists-who-sacrificed-everything-to-cover-the-revolution> [<https://perma.cc/CDC7-8SKC>] (providing a narrative account of five Syrian journalists targeted for their documentation activities).

160. See *At Great Risk, Group Gathers Evidence of War Crimes in Syria*, NAT'L PUB. RADIO (Jan. 26, 2014), <http://www.npr.org/2014/01/26/266504389/at-great-risk-group-gathers-evidence-of-war-crimes-in-syria> [<https://perma.cc/HMQ8-89H5>].

161. HUMAN RIGHTS WATCH, *COURTING HISTORY: THE LANDMARK INTERNATIONAL CRIMINAL COURT'S FIRST YEARS TRANSFORMATION OF HUMAN RIGHTS* 161–62 (July 2008) [https://www.hrw.org/sites/default/files/reports/icc0708\\_1.pdf](https://www.hrw.org/sites/default/files/reports/icc0708_1.pdf) [<https://perma.cc/UWH7-TKQN>] (relying on court documents to determine that twenty-four witnesses were referred to the Court's protection program in September 2007, followed by about eight in mid-December of that year).

protect those who are at risk of “harm and/or death.”<sup>162</sup>

The INGOs and technologists involved in the design of user-generated evidence apps are aware of the risk of retaliation.<sup>163</sup> As a result, both *eyeWitness* and *CameraV* have been designed with inbuilt safety features to enable users to quickly delete material and, in the case of *eyeWitness*, to make it appear to the lay viewer as though the app is not even on the phone at all.<sup>164</sup>

As IBA Executive Director Mark Ellis readily acknowledges, however, these design features are not infallible: “If you are using this in a country that is pretty good at figuring out how to deal with these, will they be able to take the device and say ‘all right . . . I’m going to find out what’s in there?’ I think it would be disingenuous to say no. . . . [But we wanted to create] a first line of defense. . . . I think that’s the best we can do.”<sup>165</sup>

Still, it is at least questionable that users on the ground factor in these risks when they have an app in hand that contains these security features. To the extent that true informed consent is actually achieved, any security threat to the user is plausibly the responsibility of that fully informed user. But what about those for whom the informed consent process is deficient?<sup>166</sup>

Under the traditional approach to evidence collection at the ICC, the Court itself takes on protection responsibilities for “witnesses, victims who appear before the Court, and others who are at risk on account of testimony given by such witnesses.”<sup>167</sup> Users who record crime as it unfolds are witnesses to that crime, and to the extent they go on to testify about what they filmed, they fall squarely under a traditional understanding of who a witness is. For those users who film linkage evidence after the fact, and who never appear in the Hague, their role is arguably more akin to that of an intermediary—someone who connects the Court with a witness. And, for now at least, the Court only offers protection services to intermediaries on

---

162. INT’L CRIM. CT., REGULATIONS OF THE REGISTRY, Reg. 96(1) (2006).

163. See, e.g., Ellis, *supra* note 73, at 274 (2015) (“We learned early on in this process that one hundred percent security will never be met; can’t do it.”); MATHESON, *supra* note 104, at 7, 18, 29, 39, 57, 76, 89, 102, 111, 137, 166 (noting at the top of every section that “[f]ilming for human rights can be dangerous. It can put you, the people you are filming and the communities you are filming in at risk. Carefully assess the risks before you press ‘record.’”).

164. EyeWitness User Safety FAQs, *supra* note 152.

165. Ellis, *supra* note 73, at 279.

166. See *supra* Part II.C.

167. Rome Statute, *supra* note 19, art. 43(6).

a case-by-case basis.<sup>168</sup> Still, it is fair to conclude that if users were part of the traditional investigatory space, rather than the new one described in Part II, the Court would be responsible for the protection of many of them.

In practice, this would mean that users would have access to a twenty-four/seven emergency line—the Initial Response System—through which the Court would evacuate them if necessary.<sup>169</sup> And it would mean they could be assessed for a range of other protective measures, including permanent relocation.<sup>170</sup> To be sure, the Court’s protection system is far from perfect. As Human Rights Watch concluded when the OTP’s Kenya cases fell apart, “The court appears to have been unprepared to deal adequately with witness protection needs.”<sup>171</sup> Nonetheless, access to a protection system that needs improvement is a far cry from the complete absence of options currently available to users working in the new investigatory ecosystem.

## 2. Inequality of Arms

Drawing on human rights law, international criminal tribunals have recognized the equality of arms as a fundamental principle of a defendant’s right to a fair trial.<sup>172</sup> Equality of arms requires that the defendant can present his case to the court “under conditions that do not place him at a disadvantage vis-à-vis his opponent.”<sup>173</sup> Yet, the emergence of user-generated evidence risks creating exactly this sort of disadvantage to defendants relative to the prosecution.

User-generated evidence is more likely to be gathered, in the international context at least, by users seeking to document incriminatory, rather than exculpatory, evidence—in other words, material

---

168. See *infra* Part IV.B.1.

169. INT’L CRIMINAL COURT, SUMMARY REPORT ON THE ROUND TABLE ON THE PROTECTION OF VICTIMS AND WITNESSES BEFORE THE INTERNATIONAL CRIMINAL COURT 1–2 (2009), [https://www.icc-cpi.int/NR/rdonlyres/19869519-923D-4F67-A61F-35F78E424C68/280579/Report\\_ENG08767415-4F1D-46BA-B4085B447B3AFC8D/0/ProtectionseminarSUMMARY.pdf](https://www.icc-cpi.int/NR/rdonlyres/19869519-923D-4F67-A61F-35F78E424C68/280579/Report_ENG08767415-4F1D-46BA-B4085B447B3AFC8D/0/ProtectionseminarSUMMARY.pdf) [<https://perma.cc/4EVW-7397>].

170. *Id.*

171. ICC: Kenya Deputy President’s Case Ends, HUMAN RIGHTS WATCH (Apr. 5, 2016, 3:02 PM), <https://www.hrw.org/news/2016/04/05/icc-kenya-deputy-presidents-case-ends> [<https://perma.cc/6HTK-974V>].

172. See, e.g., Prosecutor v. Tadić, Case No. IT-94-I-A, Judgment, ¶ 44 (Int’l Crim. Trib. for the Former Yugoslavia July 15, 1999), <http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf> [<https://perma.cc/T33P-JHCV>]; see also Rome Statute, *supra* note 19, art. 67.

173. Bulut v. Austria, 24 Eur H.R. Rep. 84, ¶ 47 (1996).



that will serve the prosecution. The primary reason for this is that there are no organized groups of citizens in atrocity situations who are mobilized by the goal of ensuring the rights of those accused of war crimes.<sup>174</sup> And this disparity is compounded by the fact that, for reasons discussed earlier, the promotion of user-generated evidence apps has been motivated by a desire to strengthen the investigative work of international prosecutors against the backdrop of high-profile prosecution failures at the ICC.<sup>175</sup> As such, while both the IBA and WITNESS have made efforts to reach out to defense counsel, the design and marketing of user-generated apps invariably flow from consultation with more prosecutors than defense lawyers.<sup>176</sup> While courts have shunned the idea that equality of arms requires equality of resources,<sup>177</sup> the collection of user-generated evidence may nonetheless exacerbate already significant problems regarding equality of arms between prosecution and defense in international criminal trials.<sup>178</sup>

---

174. By contrast, there is a growing awareness in the domestic context of the risk of wrongful conviction, especially in altercations between black citizens and police, and the need to ensure that exonerating evidence is preserved.

175. See *supra* Part I.A.

176. See Interview with Betts, *supra* note 74 (explaining that while the IBA sees the material gathered through its app as potentially just as useful for exonerating purposes, the defense counsel they have met with have indicated ambivalence). Notwithstanding Betts's view of the potential to document exonerating evidence, the *eyeWitness* materials make no reference to exonerating evidence, and their advisory board includes several well-respected international prosecutors but no one who has worked for a defense team. See *About eyeWitness—Our People*, EYEWITNESS, <http://www.eyewitnessproject.org/> [https://perma.cc/V9Q7-3LUD] (click "About" link in upper right hand corner and then "Our people"). WITNESS's Video as Evidence field guide does make an effort at balance when it lists as a core principle the goal of seeking the truth. To that end, it notes, "If you capture evidence that suggests someone's innocence, don't fear it. The end goal is to hold accountable those actually responsible for crimes and to ensure the innocent are not wrongly accused." MATHESON, *supra* note 104, at 48. But here again, the initial collaboration between the IBA and WITNESS meant that part of the consultations that fed into the *CameraV* concept were also skewed in favor of a prosecution perspective.

177. See, e.g., Prosecutor v. Kayishema, Case No. ICTR-95-1-A, Judgment, ¶¶ 63–70, (June 1, 2001).

178. See, e.g., Charles Jalloh & Amy DiBella, *Equality of Arms in International Criminal Law: Continuing Challenges*, in THE ASHGATE RESEARCH COMPANION TO INTERNATIONAL CRIMINAL LAW-CRITICAL PERSPECTIVES, at 251 (William Schabas et al. eds., 2013). This concern is applicable to third-parties involved in the investigatory sphere more generally, not just users doing documentation on a user-generated evidence app. Baylis, *supra* note 3, at 144 ("[M]any of the involved third parties are committed to promoting particular ideals and are not constrained by ethical obligations of fairness to particular defendants.").

### 3. Bias and Distortion

It is difficult for the designers of an app to control who will download it. And once an app is onsite, users have discretion as to what to capture. Moreover, user-generated evidence of any form can be gathered by a rebel fighter intent on documenting atrocities committed by his or her enemy as readily as it can be gathered by a civilian intent on faithfully documenting atrocities committed by any party to a conflict. This reality has the potential to skew the investigative process.

To take a simplified example, imagine a conflict where rebel group A commits, on average, twenty percent of the atrocities and rebel group B commits the remaining eighty percent. In this scenario, if rebel group B documents violations committed by rebel group A, then the incoming footage from the conflict will capture many crimes committed by rebel group A, but none by rebel group B, thus generating a distorted picture of what is actually happening on the ground.

Moreover, to the extent that user-generated evidence displaces other material gathered by third-parties, such as that typically gathered by first responder INGOs, there may be some distortion in the ultimate trial record. Material recorded with an eye to individual criminal prosecutions is likely to be systematically different from material recorded for broader analysis or advocacy purposes.<sup>179</sup> As discussed earlier, the assessment of what is valuable in a given scene is tightly circumscribed when the goal is evidence collection for a criminal prosecution, in a way that it is not otherwise.<sup>180</sup> First-responder organizations generally gather material to establish the broader context in which atrocities are occurring.<sup>181</sup> And as trained

---

179. For a fuller discussion on the way individual criminal prosecutions risk obscuring the full picture of criminality, see Rebecca Hamilton, *State-Enabled Crimes*, 41 YALE J. INT'L L. 302 (2016).

180. See *supra*, notes 84–85 and accompanying text. Professor Lawrence Douglas has raised this concern in relation to the use of documentary footage in the Nuremberg trials, noting how the framing and narration of the footage focused on what was needed to support the legal case in relation to the commission of crimes against the peace, at the expense of focusing on genocide, which was not central to the legal case. See Douglas, *supra* note 31, at 480. See also Noel Whitty, *Soldier Photography of Detainee Abuse in Iraq: Digital Technology, Human Rights and the Death of Baha Mousa*, 10 HUM. RTS. L. REV. 689, 689–90 (2010) (observing how certain images of atrocity have served to limit our understanding of atrocities).

181. See Diane F. Orentlicher, *Bearing Witness: The Art and Science of Human Rights Fact-Finding*, 3 HARV. HUM. RTS. J. 83, 99–101 (1990) (explaining how the very conscious effort by human rights organizations to “contextualize” the atrocities they report on serves to

professionals, they are attuned to questions of representativeness in a way that most users are not.<sup>182</sup> For those who believe that a core purpose of international criminal trials is to provide an accurate historical record of a conflict, a shift from relying on materials from first-responder organizations to user-generated evidence may undermine that goal.<sup>183</sup>

One obvious way to guard against these sorts of distortions is to ensure that user-generated evidence is not the only form of evidence flowing into an investigative process. Its optimal role is to bolster other forms of evidence gathered by professionals who are attuned to questions of impartiality and representativeness. Yet even assuming user-generated evidence only serves this supplementary function, there is a risk that those assessing the various types of incoming evidence will give user-generated evidence an outsized weight. As Susan Sontag recognized some four decades ago, people routinely find visual evidence more compelling than evidence presented in textual form.<sup>184</sup>

### *B. Evidence Evaluation Stage*

Once user-generated evidence has been gathered, the next step is to evaluate its legal relevance. As discussed in Part II, the sheer volume of material created by users means that courts do not themselves have the resources to take on the entirety of this evalua-

---

“anticipate and address” potential charges of bias that would discredit their reporting).

182. Jay D. Aronson, *Mobile Phones, Social Media and Big Data in Human Rights Fact-Finding: Possibilities, Challenges, and Limitations*, in *THE TRANSFORMATION OF HUMAN RIGHTS FACT-FINDING* 443, 445 (Philip Alston & Sarah Knuckey eds.) (2016) (discussing how representativeness is an ongoing concern within the human rights community).

183. For the debate about whether the creation of an accurate historical record should be a core goal of international criminal justice, see e.g., HANNAH ARENDT, *EICHMANN IN JERUSALEM: A REPORT ON THE BANALITY OF EVIL* 253 (Penguin Books 2006) (1963) (arguing that any effort to use a trial to create a historical record “can only detract from the law’s main business: to weigh the charges against the accused, to render judgment, and to mete out due punishment”); cf. RUTI TEITEL, *TRANSITIONAL JUSTICE* 73 (2000) (“[T]he criminal trial enables the establishment of a historical record at the highest legal standard of certainty.”).

184. SONTAG, *supra* note 1, at 5. Sontag’s work is part of a significant body of literature concerned with the power of the visual image, in areas spanning foreign affairs, see, e.g., David Domke et al., *The Primes of our Times? An Examination of the ‘Power’ of Visual Images*, 3 *JOURNALISM* 131 (2002), and trial advocacy, see, e.g., Open Forum, *A Videotape is Worth a Thousand Words: The Use of Demonstrative Evidence in the Defense of an Automobile Products Liability Case*, 50 *INS. COUNSEL J.* 94 (1983).

tive work. External actors must do some filtering; this raises the question of how to coordinate the transfer of material from those external actors into the hands of investigators. Moreover, this curation work raises its own challenges, and the outsourcing of a typically public function into private hands again raises concerns regarding the fair trial rights of defendants and the security of users.

### 1. The Coordination Challenge

At present, those eager to see user-generated evidence make its way into international courtrooms are still grappling with how to get such footage into the hands of an investigative team. “We don’t know what information we have that may or may not be relevant to an investigation,” explains IBA Director Wendy Betts.<sup>185</sup> It is not only a problem of not knowing what situations are under investigation but, within a given investigation, what lines of inquiry are being pursued. And this coordination problem is not limited to the IBA. “There’s a number of groups also doing verification of information,” says Betts, “and investigators don’t have the resources to go door-to-door of every organization to ask what material they have.”<sup>186</sup> Nor are they able to reach out to every user directly. Thus, there is a risk that valuable evidence may be recorded yet never make it into a criminal investigation.

Unless or until this is resolved, it must be asked: what kind of harm occurs when a user takes risks to film evidence on the assumption that it will inform a criminal investigation, when in fact the footage never reaches anyone with authority to launch an investigation? The harm is not a strictly legal one; there is no contract guaranteeing that footage filmed by a user will make it into an investigation. The organizations doing outreach urge users not to put themselves in harm’s way. And concerns about informed consent notwithstanding, the decision to take risks to secure footage is ultimately in the hands of the user. But there is still something disquieting about a scenario in which users take risks, perhaps even losing their lives, in the belief that they are securing footage that will contribute to legal accountability for what they have witnessed, only for that footage never to reach an investigator’s desk.

---

185. Interview with Betts, *supra* note 74.

186. *Id.*

## 2. Obligations to Defendants

Whether user-generated evidence is recorded directly, or through *CameraV*, *eyeWitness*, or other apps designed in the future, the task of curating which footage will be used in a criminal case would ideally remain in the hands of court investigators. For it to be otherwise would mean, in the case of an app designed with a central depository like *eyeWitness*, that private lawyers would be using their discretion to help determine which crimes might or might not be investigated and which individuals might or might not be prosecuted—in other words, the kind of function usually reserved to a prosecutor.<sup>187</sup>

In addition, when material comes into a prosecutor's office, there is an obligation to review it, not only for incriminating evidence, but also for exculpatory material that the prosecution must disclose to the defense.<sup>188</sup> To the extent that private lawyers are not bound by these obligations, outsourcing the curation of this material to them could harm the rights of the accused.

## 3. Information Security

Security is a serious concern at the evidence collection stage, but it does not end there. Even if footage is encrypted and sent to a secure location (the IBA's "secure evidence locker" in the case of the *eyeWitness* app, or a site of the user's choosing in the case of *CameraV*), the information is not necessarily safe, for two reasons.<sup>189</sup> First, there is always a risk that these secure sites will be hacked. In relation to evidence recorded on the *eyeWitness* app, the IBA promises that "[o]ur partnerships with Lexis Nexis, DLA Piper, and international law firms make sure that all footage is secure from hack-

---

187. It should be noted that there is nothing stopping a user of either of the user-generated evidence apps currently in existence from sending their footage directly to the ICC. One of the ICC's statutory provisions ensures that the court receives communications from members of the public who have information about alleged crimes. Rome Statute, *supra* note 19, art. 15. And in such a scenario, court staff review the incoming material themselves. But the court has not done any broad public outreach about this option, and it is unlikely that non-professionals would, on their own, manage to navigate their way to the court's website, find information about this option, and send sensitive information to the generic "information desk" email provided. See *Get Involved*, ICC-CPI, <https://www.icc-cpi.int/get-involved/Pages/ngos.aspx> [<https://perma.cc/4SAR-RJ7X>].

188. In relation to the ICC, this obligation flows from Art. 67(2) of the Rome Statute. Domestically, the obligation flows from the U.S. Constitution, as first articulated in *Brady v. Maryland*, 373 U.S. 83, 87–88 (1963).

189. See, e.g., *eyeWitness* User Safety FAQs, *supra* note 152.

ing.”<sup>190</sup> Yet with all the best protocols in place, recent experience suggests that highly motivated hackers are able to breach sophisticated information security systems.<sup>191</sup> Second, it is difficult to say how any of the secure sites to which users transmit their footage would handle a government subpoena for footage or the metadata associated with it.<sup>192</sup>

Uncertainties over information security relate, once again, to questions about obligations toward users who transmit footage from a user-generated evidence app on the assumption that the footage will be secure. If a secure server is hacked, or a government does request footage, who—if anyone—is responsible to the users who relied on assurances that the footage they submitted would be secure?

### *C. Trial Stage and Its Aftermath*

As should be clear, a significant portion of the user-generated evidence story unfolds in the period before this evidence is ever considered for admission in a courtroom. Nonetheless, the trial and its aftermath do raise another set of salient concerns in the context of user-generated evidence. First, there is the threshold question of whether courts will even agree to admit this kind of evidence at trial, and whether they can or should do so without compromising the anonymity of users who wish to remain anonymous. Second, there is the issue of how judges will interpret and weigh user-generated evidence that they do admit, and what role cognitive and visual bias may play in that process. Finally, it is important to recognize that the security risks to users extend beyond the end of the trial itself.

---

190. INT’L BAR ASS’N, *supra* note 110.

191. See, e.g., Tracey Lien, *Yahoo Hacked: Personal Data Stolen from at Least 500 Million Accounts*, L.A. TIMES (Sept. 22, 2016, 3:00 PM), <http://www.latimes.com/business/technology/la-fi-tn-yahoo-hacked-20160922-snap-story.html> [<https://perma.cc/SRB9-5QWL>].

192. Wendy Betts, Director of the eyeWitness to Atrocities Program, says her team assumes it is only a matter of time before they receive a subpoena requesting footage that they are storing. With their server located in London, their response will vary based on the bilateral agreement that the U.K. has with the requesting government. Betts says that based on their research of these agreements, they are at least confident that they will be protected from any “fishing expeditions.” She adds, “if we have a specific piece of information that is useful for a legitimate investigation, we are not opposed to that information going forward.” Interview with Betts, *supra* note 74.

## 1. Admissibility

The promise of user-generated evidence rests on the assumption that courts will actually be willing to admit it. At least until the al-Werfalli trial commences, however, there is no certainty around that assumption. Still, there is some cause for optimism given the high degree of judicial discretion built into the ICC's evidentiary standards.

Article 69(4) of the Rome Statute requires that judges consider "the probative value of the evidence and any prejudice that such evidence may cause."<sup>193</sup> And Rule 63(2) of the ICC's Rules of Procedure and Evidence gives judges the authority to "assess freely all evidence submitted in order to determine its relevance or admissibility."<sup>194</sup> The broad parameters around the admission of evidence at the ICC will be striking to most readers accustomed to the U.S. domestic practice system. But this has long been the norm within international criminal justice, on the basis that international courts do not have a jury. Dating back to the views of Justice Jackson during the Nuremberg Trials, more relaxed standards of evidence have been justified on the assumption that judges, as opposed to laypeople, are less influenced by exposure to non-credible or prejudicial arguments.<sup>195</sup>

Those who have led the development of user-generated evidence apps hope that judges will use their discretion to treat video as evidence. "There's a valid legal argument to make that the app itself *is* the witness," says eyeWitness to Atrocities Program Director

---

193. Rome Statute, *supra* note 19, art. 69(4).

194. Rules of Procedure and Evidence of the International Criminal Court, Assembly of States Parties, 1st Sess., Rule 63(2), ICC-ASP/1/3 (2002) [hereinafter ICC Rules of Procedure], <https://www.icc-cpi.int/iccdocs/pids/legal-texts/rulesprocedureevidenceeng.pdf> [<https://perma.cc/FF6N-RR75>].

195. See Douglas, *supra* note 31, at 467 (referencing comments made by Justice Jackson and explaining judges, as opposed to juries, could "weigh the relevance of hearsay testimony and would be less susceptible to being swayed by tendentious or prejudicial arguments"). See also Ellen Wessel et al., *Credibility of the Emotional Witness: A Study of Ratings by Court Judges*, 30 L. HUM. BEHAV. 221 (2006) (for evidence to support confidence in the relative expertise of judges); *Scott v. Harris*, 550 U.S. 372, 378 n.5 (2006). In *Scott*, eight justices signed onto an opinion that highlighted the overwhelming power of visual evidence; the justices chastised the lower court for deciding that (non-visual) testimony provided by Harris created enough of a dispute about the facts to deny Officer Scott's motion for summary judgment when, in the view of the justices, the dashboard camera recording supported Scott's version of events. In the majority opinion, which has since been critiqued for its visual literalism, Justice Scalia wrote that the lower court "should have viewed the facts in the light depicted by the videotape." *Id.* at 381. For a compelling critique of the Court's decision in *Scott*, see Kahan et al., *supra* note 24.

Wendy Betts.<sup>196</sup>

With respect to situations in which a user is willing to be identified, the IBA's confidence in the admissibility of user-generated evidence seems well-founded. ICC judges have routinely admitted evidence gathered by third-parties, such as INGOs, when that third-party is known to the court and the evidence they present can be shown to have a reliable methodology behind it.<sup>197</sup> The judges have, however, noted that such reports may only be admitted "for the limited purpose that the information contained therein may serve to corroborate other pieces of evidence."<sup>198</sup> Still, if the goal of user-generated evidence is to supplement, rather than supplant, other forms of evidence, then this corroborating role is all that is needed.

With respect to users who have chosen to be anonymous, however, the clues to be gleaned from the court's decisions to date suggest that the admission of user-generated evidence is much less certain. For example, the *Gbagbo* case suggests a bleak outlook for user-generated evidence captured by an anonymous user. The judges in that case found it "highly problematic" when they did not know the source of the information presented by the prosecution and concluded that without such information it was "impossible to determine what probative value to attribute to the information."<sup>199</sup> This skepticism is consistent with the view of judges at the ICTY who also "expressed particular concern about admission of reports based on anonymous testimony."<sup>200</sup>

Another possibility is that the judges simply demand that the identity of an anonymous user be disclosed to the defense before admitting user-generated evidence captured by that individual. If the technology works as promised, then the prosecution would not themselves know the identity of a user who chose to be anonymous.<sup>201</sup> This would obviously mean they would be unable to comply with the

---

196. Interview with Betts, *supra* note 74.

197. See, e.g., Prosecutor v. Gombo, Case No. ICC-01/05-01/08, Decision on the Admission into Evidence of Items Deferred in the Chamber's "Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute," ¶ 21 (June 27, 2013), [https://www.icc-cpi.int/CourtRecords/CR2013\\_04725.pdf](https://www.icc-cpi.int/CourtRecords/CR2013_04725.pdf) [<https://perma.cc/494G-HVRP>] (admitting reports by Amnesty International and Fédération Internationale des Droits de l'Homme into evidence).

198. *Id.* ¶ 22.

199. Prosecutor v. Gbagbo, Case No. ICC-02/11-01/11, Decision Adjourning the Hearing on the Confirmation of Charges, ¶ 29 (June 3, 2013), [https://www.icc-cpi.int/CourtRecords/CR2015\\_04878.pdf](https://www.icc-cpi.int/CourtRecords/CR2015_04878.pdf) [<https://perma.cc/57ZY-BAY6>].

200. Baylis, *supra* note 3, at 129.

201. See *supra* note 192 and accompanying text.



court's order, presumably leading the Court to deem the piece of user-generated evidence inadmissible. If, on the other hand, the prosecution has been able to find out the identity of the user, then they will be faced with the dilemma of choosing between honoring the user's desire of anonymity and using the evidence.

Lest the above scenario sound extreme, it is worth recalling that the ICC trial chamber in *Lubanga* ordered the prosecution to disclose the identity of one of its intermediaries to the defense.<sup>202</sup> Given the security concerns that the prosecution raised in relation to its intermediaries, the trial chamber was initially comfortable with the anonymity of intermediaries being maintained. But once credible allegations arose that a particular intermediary may have coerced witnesses into giving false testimony, the court concluded that the defense had the right to know the identity of that intermediary.<sup>203</sup> And when the prosecution refused, the court went so far as to stay the proceedings.<sup>204</sup> There is a clear analogy to be drawn between an intermediary and a user to the extent that both take on the role of gathering evidence on behalf of the prosecution. Given this, it seems at least plausible that the court would refuse to admit evidence procured by someone whose identity is hidden from the defense if the defense raised credible allegations about the veracity of the evidence provided.

## 2. Interpretation

Certain visual biases systematically influence what we see.

---

202. Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Redacted Decision on Intermediaries, ¶ 37 (May 31, 2010), [https://www.icc-cpi.int/CourtRecords/CR2010\\_03672.pdf](https://www.icc-cpi.int/CourtRecords/CR2010_03672.pdf) [<https://perma.cc/QV9K-5EVT>] (ordering the prosecution to disclose the identity of one of its intermediaries to the defense).

203. *Id.* ¶¶ 135–50 (explaining the reasons for ordering the disclosure of an intermediary's identity).

204. Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Redacted Decision on the Prosecution's Urgent Request for Variation of the Time Limit to Disclose the Identity of Intermediary 143, ¶ 20 (July 8, 2013), [https://www.icc-cpi.int/CourtRecords/CR2010\\_04749.pdf](https://www.icc-cpi.int/CourtRecords/CR2010_04749.pdf) [<https://perma.cc/GLJ7-ZUM6>] (ordering a stay of proceedings after the prosecution refused to disclose the identity of an intermediary). This decision was ultimately overturned by the Appeals Chamber on the grounds that sanctions should have first been implemented before resorting to a stay. See Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Judgment Decision on the Prosecutor's Appeal of the Prosecutor Against the Decision of Trial Chamber I of 8 July 2010, ¶ 33 (Oct. 8, 2010), [http://www.worldcourts.com/icc/eng/decisions/2010.10.08\\_Prosecutor\\_v\\_Lubanga1.pdf](http://www.worldcourts.com/icc/eng/decisions/2010.10.08_Prosecutor_v_Lubanga1.pdf) [<https://perma.cc/SM26-WZ7R>] (reversing the Trial Chamber's decision to stay proceedings upon finding that sanctions should have been implemented first, before resorting to a stay of proceedings).

When it comes to watching video footage, the phenomenon of illusory causation leads us to attribute an unwarranted degree of causal influence to the object or person we happen to be looking at.<sup>205</sup> Over two decades of research by cognitive scientists demonstrates the real-world applicability of this phenomenon. For example, when asked to watch a video of a suspect's confession where the camera is facing the suspect, viewers were consistently more likely to perceive the suspect's confession as voluntary and judge the suspect to be guilty than when presented with the exact same testimony in textual form or when the camera was facing the interviewing officer.<sup>206</sup>

Judges are not immune to these biases. A 2007 study presented experienced judges with a videotaped confession filmed from different perspectives.<sup>207</sup> The study found that judges were just as susceptible to the phenomenon of illusory causation as laypeople.<sup>208</sup> The judges were significantly more likely to conclude that the suspect's confession was voluntary when the camera was facing the suspect than when they watched the identical confession with the camera in a neutral position or facing the interviewing officer.<sup>209</sup>

In addition to interpreting what they see, international judges are also responsible for determining how much weight to give to what they have watched.<sup>210</sup> Here, the question of the user's identity may again be central. Presented with the same segment of footage, judges may assign differing levels of evidentiary weight based on characteristics related to the user who filmed the footage. An in-depth study of European judges who were tasked with determining what weight to assign different forms of electronic evidence found that "the person in charge of gathering electronic evidence is the fac-

---

205. See G. Daniel Lassiter, *Illusory Causation in the Courtroom*, 11 CURRENT DIRECTIONS IN PSYCHOL. SCI. 204, 204 (2002) (citing to research done by Koffka in 1935, showing that when sitting in a darkened room, people consistently attributed the growing gap between two pinpoints of light to be caused by the light they were watching, regardless of which of the lights was actually moving, KURT KOFFKA, PRINCIPLES OF GESTALT PSYCHOLOGY (1935)).

206. G. Daniel Lassiter et al., *Videotaped Interrogations and Confessions: A Simple Change in Camera Perspective Alters Verdicts in Simulated Trials*, 87 J. APPLIED PSYCHOL. 867, 868 (2002). See also Michael D. Storms, *Videotape and the Attribution Process: Reversing Actors' and Observers' Points of View*, 27 J. PERSONALITY & SOC. PSYCHOL. 165 (1973); Jennifer J. Ratcliff et al., *Camera Perspective Bias in Videotaped Confessions: Experimental Evidence of Its Perceptual Basis*, 12 J. EXPERIMENTAL PSYCHOL. 197 (2006).

207. G. Daniel Lassiter et al., *Evaluating Videotaped Confessions: Expertise Provides No Defense Against the Camera-Perspective Effect*, 18 PSYCHOL. SCI. 224, 224–25 (2007).

208. See *id.* at 225.

209. See *id.* at 224.

210. See ICC Rules of Procedure, *supra* note 194, Rule 63(2).

tor that influences most the evidential value attributed to it.”<sup>211</sup> This is consistent with the jurisprudence that has come out of the ICC to date, where the judges have looked to the credibility of the source as they assess evidence gathered by third-parties.<sup>212</sup> And it illustrates again just how difficult it may be for the Court to accept user-generated evidence taken by a user who wishes to remain anonymous. Indeed, even for users who are willing to be identified, it may often be hard for many of them to achieve the same kind of credibility, in the eyes of the court, as long-standing INGOs with a well-documented methodology and a track record of providing impartial information.

### 3. Unintended Consequences

Once footage is admitted into evidence, there is no guarantee that it will be interpreted in the way that the user intended. Notwithstanding intuitions that video footage will speak for itself, cognitive science clearly shows that interpretation is in the eye of the beholder.<sup>213</sup>

In addition to the impact of visual bias, video footage is also mediated by the legal construction placed on it by the parties. To take just the most high-profile example of this, when the prosecution in the Rodney King case introduced video footage of police officers beating King they did not imagine that the footage would be used by the defense to help exonerate the officers.<sup>214</sup> As Professor Lawrence Douglas concluded in his analysis of the use of video footage at Nuremberg, “in a trial, even evidence that claims to speak for itself of atrocity ultimately must be spoken for. The legal meaning of such evidence must be secured even as what it shows cannot be denied.”<sup>215</sup>

Once user-generated evidence comes into court, there is nothing to say that it will not be used to the advantage of the defense. And while this is entirely appropriate from a legal standpoint, the question again is if this is what the user understood to be a possibility

---

211. CYBEX, THE ADMISSIBILITY OF ELECTRONIC IN COURT: FIGHTING AGAINST HIGH-TECH CRIME 39 (2006), [https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd\\_meeting\\_docs/contributions/libro\\_aeec\\_en.pdf](https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf) [<https://perma.cc/J5CX-EAC8>].

212. See *supra* notes 177–179 and accompanying text.

213. See, e.g., Kahan et al., *supra* note 24.

214. See Stuart, *supra* note 30, at 327 (“[B]aton blows and punches were re-narrated [by the defense] and transformed into warranted officer conduct.”).

215. Douglas, *supra* note 31, at 481.

when they took risks to record the footage. Of course, users have every right to take enormous risks to record. But the choice to do so should be one that is informed by an accurate understanding of the ends the footage may serve.

While filming, a user risks onsite retaliation. But threats to the user's security do not end once their footage makes it to trial. Even for users who uploaded their footage on the basis of being able to maintain their anonymity, there is always the possibility that a motivated defense team will be able to uncover their identity. A defendant who appears in the footage may be able to identify the person who was filming, or bystanders to the scene may have noticed someone holding out their phone. Indeed, with respect to the above-mentioned intermediary whose identity the prosecution initially refused to disclose to the defense during the Lubanga trial, the defense discovered the intermediary's identity regardless, well in advance of the prosecution ultimately deciding to disclose that information.<sup>216</sup>

These security risks do not necessarily end at the conclusion of the trial. Even if a defendant is convicted, that defendant's allies may be motivated to try to find the person who gathered evidence that helped secure a conviction. And as with more traditional forms of evidence, users who have agreed to be identified as the source of user-generated evidence may face retaliation against themselves, their family, or their community in the aftermath of a trial, regardless of whether the defendant is found guilty.<sup>217</sup>

#### IV. THE WAY FORWARD

Individuals are gathering user-generated evidence in conflict-affected areas around the world. And there are reasons to be optimistic about this new reality. User-generated evidence may democratize the investigatory space and help preserve evidence that would otherwise be lost or destroyed. But given the risks identified above, there are also reasons to be worried.

Part III identified recurring concerns that can be usefully grouped into three broad categories: (i) user security, (ii) evidentiary bias, and (iii) fair trial rights. The way that lawyers and judges respond to each of these categories will be crucial to determining the

---

216. See Buisman, *supra* note 51, at 59.

217. See, e.g., PHIL CLARK & NICOLA PALMER, TESTIFYING TO GENOCIDE: VICTIM AND WITNESS PROTECTION IN RWANDA 24–29 (2012), <http://www.redress.org/wp-content/uploads/2018/01/oct-12-Testifying-to-Genocide-Rwanda.pdf> [<https://perma.cc/L9EG-DAMD>] (describing threats in retaliation against those who testified in local Gacaca trials).

impact that user-generated evidence will have on international criminal justice. But in the remaining part of the Article I address, as a prescriptive matter, only the first of these categories—user security. This is because it is the one concern that is unique to the introduction of user-generated evidence and, as a result, no attention has yet been given to how to remedy it. By contrast, concerns about evidentiary bias and fair trial rights, while equally important in determining the impact of user-generated evidence, have been extensively covered in the existing literature, thus providing a wealth of suggestions that could usefully be transposed to the user-generated evidence context.<sup>218</sup>

Security risks to users—and potentially their families and communities—are inherent in the role of evidence collection and are present to some degree no matter how many precautions a user takes. But these risks can, and should, be mitigated. Users calibrate their risk-taking to their expectations about what purpose their footage will serve. The greater their expectations, the more risks they are likely to be willing to take.

The following section makes an initial effort to survey what options are available to reduce security risks to the user, to minimize the likelihood that the user will overestimate the chance that their footage will be used to achieve legal accountability, and, crucially, to increase clarity about who is responsible if these efforts fail. I look first to the role of contracts and then to the role of guidelines. In the interests of providing a concrete example, I present the survey in relation to user-generated evidence that ends up at the ICC. However, both contracts and guidelines could be adopted in situations where user-generated evidence is submitted to other courts.

The use of contracts holds promise, but it is at best a partial solution as it will not always be feasible to form a contract with a given user. When the formation of a contract is not an option, I consider what role guidelines can play as a safety net. While they lack the legally binding force of a contract, written guidelines can provide

---

218. See, e.g., Adam Benforado, *Frames of Injustice: The Bias We Overlook*, 85 IND. L.J. 1333, 1359 (describing “numerous potentially promising approaches” to minimize the impact of camera perspective bias and illusory causation, including urging courts not to use video evidence in a conclusory manner, and only allowing footage that is filmed from an equal-focus (alleged perpetrator and alleged victim) perspective); Charles C. Jalloh & Amy DiBella, *Equality of Arms in International Criminal Law: Continuing Challenges*, in THE ASHGATE RESEARCH COMPANION TO INTERNATIONAL CRIMINAL LAW—CRITICAL PERSPECTIVES 251, 279–82 (Yvonne McDermott & William Schabas eds., 2013) (arguing that the existing inequality of arms could be alleviated by courts pushing States to allow defense investigator access); *id.* at 283–86 (arguing that equality of arms concerns require stronger enforcement of the prosecution’s disclosure obligations).

a level of clarity currently lacking in the new investigative ecosystem. In terms of specifics, I consider two existing sets of guidelines: the ICC Guidelines on the Use of Intermediaries and the ICRC Guidelines on Protection Actors. But looking to these guidelines represents only the very beginning of what a fuller exploration should involve; guidelines from other areas—including user-generated content in journalism,<sup>219</sup> crisis mapping,<sup>220</sup> and other ICT efforts—may also contain directives that could be applied to the context of user-generated evidence. And, encouragingly, an effort to develop guidelines on open-source evidence more generally is already underway.<sup>221</sup>

### A. Contracts

In considering the role of contracts, I draw on Professor Laura Dickinson's insight that contracts can be a way of getting private actors to follow norms that apply to public actors,<sup>222</sup> thus playing a so-called "publicization" function.<sup>223</sup> Of relevance here is Dickinson's acknowledgment that not only private for-profit organizations, but also nonprofit INGOs, have increasingly been used to take on public functions in the international arena.<sup>224</sup>

Dickinson's argument in favor of the use of contracts is that they can encourage private actors to take on the values of a public organization through contract provisions, including self-evaluation, training, and monitoring.<sup>225</sup> The creation of a contract in no way

219. See, e.g., *ONA Social Newsgathering Ethics Code*, ONLINE NEWS NAT'L ASS'N, <https://toolkit.journalists.org/social-newsgathering/> [https://perma.cc/HT4K-9SY4].

220. See, e.g., *Ethics in the Use of ICT in Development Projects: An Interview with Jennifer Chan*, <https://bestict4d.wordpress.com/tag/ethics/> [https://perma.cc/6ZXD-HFPJ].

221. U.C. BERKELEY SCH. OF LAW, HUMAN RIGHTS CTR, THE NEW FORENSICS: USING OPEN SOURCE INFORMATION TO INVESTIGATE GRAVE CRIMES 13 (2017), [http://www.law.berkeley.edu/wp-content/uploads/2018/02/Bellagio\\_report\\_2018\\_9.pdf](http://www.law.berkeley.edu/wp-content/uploads/2018/02/Bellagio_report_2018_9.pdf) [https://perma.cc/FRW8-UZJD] (recommending the production of guidelines "to support the improved quality of open source investigations for legal accountability").

222. See Laura A. Dickinson, *Government for Hire: Privatizing Foreign Affairs and the Problem of Accountability Under International Law*, 47 WM. & MARY L. REV. 135, 199 (2005).

223. See Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285, 1285 (2003) (stating that, as first defined by Freeman, the term "publicization" refers to the idea that it is possible to get private actors to take on public norms).

224. See Dickinson, *supra* note 222, at 154–56 (discussing government outsourcing of foreign aid to NGOs).

225. Laura A. Dickinson, *Public Law Values in a Privatized World*, 31 YALE J. INT'L L. 383, 403–23 (2006) (describing how contracts would require private actors to live up to

guarantees this outcome,<sup>226</sup> and Dickinson herself identifies the risk that “the added costs of compliance and oversight may . . . swallow the purported benefits of privatization in the first place.”<sup>227</sup> Nonetheless, the current situation for users could be improved upon as a result of two different types of contracts. The first is a contract between the ICC and the INGO responsible for outreach about user-generated evidence collection, such as the IBA or WITNESS; the second type of contract is between the ICC and the user.

### 1. ICC-INGO Contracts

This first type of contract would be a way for the Court to help ensure that users are not taking risks on the basis of false expectations about whether and how their footage will be used by the Court. While the two organizations behind the user-generated evidence apps that are currently on the market are trying to reduce the risk of unmet expectations in their outreach programs, the situation for users going forward cannot be left to the good faith of these organizations. There is nothing to prevent other organizations entering this market in the future, and—in the absence of a contract or similar mechanism—no guarantee that such organizations will follow the practices that the IBA and WITNESS have been trying to develop.

A contract between an arm of the ICC<sup>228</sup> and an INGO, or other private actor doing outreach to users, could draw on the existing model contract and associated code of conduct that the Court already uses with some of its intermediaries. Indeed, the analogy between these INGOs and intermediaries seems appropriate since the function of both is to connect Court officials to evidence.

Any contract would need to address the two major concerns previously identified: user security and the realistic management of user expectations. In terms of security, the OTP should, at a minimum, require that INGO interactions with users operate under the principle of harm minimization, and that all INGOs receive training

---

public law values through requirements such as self-evaluation, training, and monitoring).

226. See, e.g., Martha Minow, *Public and Private Partnerships: Accounting for the New Religion*, 116 HARV. L. REV. 1229, 1270 (2003) (describing failures of contract oversight by entities ranging from the U.S. Department of Defense to the University of California Los Angeles).

227. Dickinson, *supra* note 222, at 207.

228. For reasons discussed above, this is, at the present time, most likely to be the OTP. See *supra* Part III.A.2. But there is no inherent reason why defense counsel or, in the ICC’s case, counsel for victims could not contract with an INGO doing outreach to gather user-generated evidence.

on the Court's Guidelines on Good Practices on Risk Prevention.<sup>229</sup>

In terms of expectations management, the OTP could usefully draw from the language in its existing Code of Conduct for Intermediaries to specify that an INGO doing outreach on user-generated evidence "shall not make commitments to . . . (potential) witnesses . . . that he/she/it is not in a position to fulfil."<sup>230</sup> This would mean INGOs could not promise anonymity to users unless or until the first case involving user-generated evidence establishes that the Court will accept the idea of users staying anonymous. The contract could also require INGOs to be explicit with users about the fact that material they record may not ever be used by the ICC and, if used, will be available to both defense and prosecution.

Compliance with these and other provisions could be secured by requiring the INGOs to submit regular self-evaluations to the Court, as well as sending Court staff to monitor the INGO's outreach work where possible. Such approaches are not foolproof, but a provision stating that the OTP will not rely on user-generated evidence secured on the contractor's app if any provision of the contract is violated would serve as a strong incentive for INGOs to comply.

## 2. ICC-User Contracts

Consideration of a second type of contract—between the Court and the user—necessarily comes with a degree of uncertainty because it depends on how the ICC judges decide to characterize user-generated evidence. If they accept the argument that a user-generated evidence app *is* a witness, then the user who recorded the footage is best analogized to an intermediary—someone who has helped the Court gain access to a witness. If, on the other hand, the judges require the authenticating testimony of a user to admit the video into evidence, then that user is best analogized to a witness.

If the Court views a user as a witness, then the user can be

---

229. See e.g., INT'L CRIM. CT., CODE OF CONDUCT FOR INTERMEDIARIES § 5.2 (2014) [hereinafter ICC Intermediaries Code], <https://www.icc-cpi.int/iccdocs/It/CCI-Eng.pdf> [<https://perma.cc/8TGP-DXT4>] ("An Intermediary shall ensure that in any dealings with a person with whom the Intermediary has contact in the course of his/her/its Functions, the potential for harm to the contacted person is minimised."); *id.* § 5.3 (requiring the intermediary to operate in a "manner that limits the risks to any person with whom the Intermediary has contact in the course of his/her/its Functions, especially when those risks arise in connection with the Intermediary's Functions" and, in doing so, "observe the *Guidelines on Good Practices on Risk Prevention*").

230. *Id.* § 6.3.



brought within the Court's existing witness protection scheme.<sup>231</sup> While, as noted above, this scheme has significant flaws, bringing a user under its rubric would at least mean that an individual is no worse off from a security perspective on account of having recorded user-generated evidence than they would have been if they had testified to the Court directly about what they had witnessed.

The great hope of those involved in developing user-generated evidence apps, however, is that judges will accept the app itself as the witness. After all, the purpose of building so much metadata into the app design is to enable the evidence recorded on the app to be self-authenticating. If this is the path that the judges take, then a user is better analogized to an intermediary and would therefore not automatically fall within the Court's witness protection scheme. This, then, is the scenario in which an ICC-user contract could be beneficial.

As explained above, there is precedent for the establishment of a contract between the ICC and an intermediary. And once someone is formally acknowledged by the Court as an intermediary in this way, then the Court has a degree of responsibility for that intermediary's security. The Court's responsibility is a subsidiary one. Per the model contract between the ICC and an intermediary, the primary responsibility for the intermediary's security lies with the intermediary itself.<sup>232</sup> But under the Court's Guidelines on the Use of Intermediaries, if "the performance of the functions of an intermediary creates security risks to the intermediary, the Court must take measures to manage those risks," up to and including the use of protective measures.<sup>233</sup> Beyond the issue of security, a contract between the ICC and a user that follows the model contract would also reinforce the stipulations in a contract between the ICC and an INGO regarding the requirements that intermediaries inform the user about the risk of their identity being exposed,<sup>234</sup> and that they make no repre-

---

231. See *supra* note 137 and accompanying text.

232. See INT'L CRIM. CT., MODEL CONTRACT FOR INTERMEDIARIES, Art. 8 (2014) [hereinafter Model Contract for Intermediaries], <https://www.icc-cpi.int/iccdocs/It/MCI-Eng.pdf> [<https://perma.cc/97NE-H6HY>] (specifying that the intermediary must take actions to safeguard his or her own security and immediately notify the court of any security threat).

233. INT'L CRIM. CT., GUIDELINES GOVERNING THE RELATIONS BETWEEN THE COURT AND INTERMEDIARIES 17 (2014) [hereinafter ICC Intermediaries Guidelines], <https://www.icc-cpi.int/iccdocs/It/GCRI-Eng.pdf> [<https://perma.cc/TY83-B9FM>].

234. Model Contract for Intermediaries, Art. 10 ("The intermediary acknowledges and agrees that the Court (*or* the Counsel) may disclose his/her/its identity when and if requested to do so by the relevant judicial authority in charge of the respective judicial procedure.").

sentations to the user that cannot be fulfilled.<sup>235</sup> Unfortunately, however, the Court does not generally contract with “self-appointed” or “one-off” intermediaries,<sup>236</sup> which is likely to be an accurate characterization of most users.

### *B. Guidelines*

The formation of contractual relationships between some of the actors in the new investigatory ecosystem mapped out in Part II may be a “first best” option, but, as with “self-appointed” intermediaries mentioned above, it will not be possible in all cases. Thus, written guidelines, while not legally binding, could serve as a backstop and provide clarity about which actors are responsible for reducing risks to users (as well as what users are themselves responsible for).

#### 1. ICC Guidelines on the Use of Intermediaries

The ICC Guidelines on the Use of Intermediaries were responsive to the Court’s concern about the OTP’s (mis)use of intermediaries in the *Lubanga* case.<sup>237</sup> Under the definition provided in the guidelines, intermediaries include those who “assist a party or participant to conduct investigations by identifying evidentiary leads and/or witnesses and facilitating contact with potential witnesses.”<sup>238</sup> Thus, if the Court determines that a user-generated evidence app is self-authenticating, then users can plausibly be described as intermediaries.

Not all intermediaries automatically fall within the Guidelines; those who have entered into a contractual relationship with an organ of the Court do, but for those operating outside a contractual relationship, “a determination [of their coverage under the Guidelines] shall be made on a case-by-case basis.”<sup>239</sup> This would leave most users in a position of uncertainty. A preferable approach would be for the Court to make a formal determination, ideally in advance of the al-Wefalli trial, that any user whose footage is used at any stage of the legal process falls within the Guidelines.

---

235. ICC Intermediaries Code, *supra* note 229, § 6.3.

236. *Id.* § 194.

237. See *supra* Part I. The current guidelines were “revisited after the 14 March 2012 *Lubanga* judgment to ensure they addressed the concerns raised by Trial Chamber I.” ICC Intermediaries Guidelines, *supra* note 233, at 4.

238. *Id.* at 6.

239. *Id.*

Making a categorical determination in relation to users whose footage the Court relies on would be a marked improvement in the security situation for users. The Guidelines stress the responsibility of the intermediary—in this case, a user—to take precautions for their own safety (alongside a concurrent responsibility for the Court to avoid putting the user’s safety at risk). But when these measures nonetheless fail to protect the user, then the Guidelines stipulate that “appropriate protective measures *shall* be implemented [by the Court].”<sup>240</sup>

## 2. ICRC Protection Guidelines

The ICRC Protection Guidelines were revised in 2013 to account for advances in ICT.<sup>241</sup> While the Guidelines are targeted toward human rights and humanitarian protection actors, they seek also to be “a source of inspiration to all those who seek to have a positive impact on protection.”<sup>242</sup> Specifically, they state that the Guidelines “will also be of interest to people who do not necessarily see themselves as protection actors, such as people working in social media, or people setting up crisis mapping independently from traditional humanitarian and human rights organizations.”<sup>243</sup> In the next revision of the Guidelines, INGOs who do outreach on user-generated evidence could, and should, be incorporated into this list.

The Guidelines address the handling of sensitive information, and highlight several risks that are particularly germane to the collection of user-generated evidence. These include: “The risk of raising false expectations that there will be a rapid response or in fact any response at all . . . [and] the inability of people who have had little or no . . . experience with modern information technology to give real

---

240. *Id.* at 14 (emphasis added).

241. INT’L COMM. OF THE RED CROSS, PROFESSIONAL STANDARDS FOR PROTECTION WORK 4 (2013), <http://www.shop.icrc.org/professional-standards-for-protection-work-carried-out-by-humanitarian-and-human-rights-actors-in-armed-conflict-and-other-situations-of-violence-2540> [https://perma.cc/WYE8-L78L]. (“In light of the rapidly proliferating initiatives to make new uses of information technology for protection purposes, such as satellite imagery, crisis mapping and publicizing abuses and violations through social media, the advisory group agreed to review the scope and language of the standards on managing sensitive information. The revised standards reflect the experiences and good practices of humanitarian and human rights organizations as well as of information and communication technology actors.”).

242. *Id.* at 5.

243. *Id.* at 81.

informed consent.”<sup>244</sup>

The Guidelines seek to mitigate these risks. One directive states that “[i]nformation that is not necessary for the purpose identified prior to, or at the time of collection, should simply not be collected, in order to avoid unnecessary risks . . . or false expectations on the part of those providing the information.”<sup>245</sup> Adherence to this in the user-generated evidence context would require INGOs doing outreach on user-generated evidence to be very clear about the kind of footage that a criminal investigation is likely to find useful. It would ensure that the sort of training guidance presenting in WITNESS’s Video as Evidence manual, emphasizing the importance of linkage evidence in investigations, becomes the standard for other organizations seeking to enter this space in the future.

Another directive of relevance is that “[p]rotection actors must integrate the notion of informed consent when calling upon the general public, or members of a community, to spontaneously send them information.”<sup>246</sup> Compliance with this provision would ensure that INGOs think through how to explain the potential risks and benefits involved in recording on their apps before doing outreach.

Of course, INGOs are not legally required to follow these, or any other, guidelines. But Courts seeking to use user-generated evidence in their investigations and proceedings could establish a norm of getting INGOs to do so by stipulating that they will only accept user-generated evidence gathered through organizations that adhere to these guidelines. The hope is that the better-informed users are about the costs and benefits of gathering evidence, the better decisions they will make about their own security.

## CONCLUSION

Across the globe, people are using their smartphones to gather evidence, and there is no indication that they will stop doing so anytime soon. This Article identified the emergence of user-generated evidence, mapped the new actors, roles, and inter-relationships that this kind of evidence brings to the investigatory ecosystem, and distilled three categories of concern arising from this development: user security, evidentiary bias, and fair trial rights. The question going forward is not whether users should gather evidence, but rather, what

---

244. *Id.* at 82.

245. *Id.* at 88.

246. *Id.* at 95.

can be done to mitigate the problems that arise when they do?

One of the perceived advantages of bringing user-generated evidence into international criminal investigations is that of risk reduction. To the degree that user-generated evidence can stand in place of evidence collected by traditional methods, court investigators will have to make fewer trips to conflict-ridden locations, thereby reducing risks to themselves and those they interact with. But in reality, the turn to user-generated evidence may more accurately be described as risk-shifting, rather than risk-reduction. User-generated evidence certainly enables international lawyers to obtain hard-to-access evidence at no risk to themselves. But if the risk associated with evidence collection does not disappear so much as get transferred—from professionals backed by an international court to individual users with no such institutional safety net—then the turn toward user-generated evidence is harder to justify. As has so often been the case with new technology, user-generated evidence apps may serve to merely replicate, rather than transform, existing power hierarchies.<sup>247</sup>

The INGOs currently doing outreach about user-generated evidence are working diligently to try to do the right thing by users. However, simply hoping not only that these organizations will continue to do so but also that organizations entering this space in the future will act in the same way is not a plan for mitigating the very serious risks identified in this article.

Many of the concerns that user-generated evidence raises are not novel; bias, fair trial rights, and security of witnesses, if not users, have long been part of the landscape of international criminal investigations. But user-generated evidence is entering this landscape at a time when, relying on traditional evidentiary approaches, the ICC is struggling to put on a successful trial. This heightens the risk that the more pernicious aspects of user-generated evidence will be overlooked in the service of boosting courtroom activity. It is not too far-fetched to imagine case-selection being driven, to a greater or lesser extent, by the availability of user-generated evidence—raising the specter of justice being ultimately led away from those places and events that are inherently less susceptible to capture on a smartphone.

Those involved in the project of international criminal justice may only fully appreciate the significance of this current moment—immediately before user-generated evidence enters an international courtroom for the first time—in hindsight. Regardless, it is incumbent upon those who support the project of international criminal jus-

---

247. See Sharp, *supra* note 98, at 69–87.

tice to begin addressing the concerns raised in this Article as a matter of priority. The decisions we make in the very near future will determine whether user-generated evidence has a positive impact, or if it merely promises to address some current problems with international criminal investigations, only at the expense of shifting security concerns from investigators to users, creating new forms of evidentiary bias, and entrenching the existing inequality of arms in international criminal law.