DRAFT prepared for Nov. 6-7 Pound/Hastings Symposium. Final version to appear in HASTINGS LAW JOURNAL Vol. 73, Issue 5

BAD FORENSICS:
A CRITIQUE OF DIGITAL OPEN SOURCE METHODS

Alexa Koenig and Lindsay Freeman[1]

I. INTRODUCTION

On the morning of January 6, 2021, the day Congress was set to affirm Joe Biden's victory in the U.S. presidential election, a large crowd of Trump supporters gathered on the Capitol lawn. At noon, then-President Trump spoke to his supporters. Claiming—despite all evidence to the contrary—that he and not Biden had won the election, he told his followers to "show strength" and to "walk with [him] down to the Capitol." Many turned to march. By 1:00 pm, the crowd had overwhelmed the building's security and breached its barricades. Angry rioters armed with camera phones and, in some cases, weapons swarmed the building while thousands more clashed with officers outside, forcing legislators and staff into hiding. It was several hours before the sergeant-at-arms was able to declare the building secure.[2] By then, the damage was done—the building trashed, five people dead or dying, and democracy degraded.

The Department of Justice responded by launching what has been described as the largest investigation in U.S. history, both in terms of number of defendants and the volume of digital evidence. Their work was supplemented by an army of online citizen investigators who provided copious tips and related analysis to the FBI and other law enforcement to support the identification of perpetrators. As of October 2021, close to 700 people had been charged for

---

[1] Lecturer-in-Residence and Executive Director, Human Rights Center, UC Berkeley School of Law and Technology Law and Policy Program Director, Human Rights Center, UC Berkeley School of Law, respectively. The authors thank Anthony Ghaly for his research and drafting support, and Kelly Matheson and Annie O'Reilly for their feedback. Any errors are, of course, the authors' own.

[2] Timeline of Events by the New York Times; Timeline of Events by USA Today

their alleged role in the riots.[3] Given insurrectionists' widespread use of smartphones and social media to share photos, videos, and other information online as events unfolded, such content has proven especially critical to finding, identifying, and charging perpetrators.

Digital open source information pulled from social media and other online spaces is playing an increasingly important role in establishing the who, what, why, where, when and how of world events.[4] Given the growing use of digital information and communication technologies, the value of publicly available information on the internet and the burgeoning area of practice known as "digital open source investigations" is rapidly growing.[5] Such investigations—which rely heavily on user-generated content such as videos and photos posted to social media and on commercial satellite imagery[5]—differ both qualitatively and quantitatively from more traditional, analog forms of open source content, such as news clippings or radio broadcasts.

While digital open source investigation techniques and the complementary work of third party online investigators can offer tremendous value to law enforcement, the introduction of any new scientific or technical investigative methods and evidence into legal proceedings also comes with significant risks.[6] In seeking accountability for the events of January 6, investigators have faced a "glut of social media evidence," a phenomenon that has both helped and hindered

[3] *See, e.g.*, Madison Hall, Skye Gould, Rebecca Harrington, Jacob Shamsian, Azmi Haroun, Taylor Ardrey, and Erin Snodgrass, "684 people have been charged in the insurrection so far. This searchable table shows them all," Insider, 19 October 2021, at https://www.insider.com/all-the-us-capitol-pro-trump-riot-arrests-charges-names-2021-1 (last visited 27 October 2021).

[4] Open source information is defined as information that is publicly accessible on the internet and that any person can collect through observation, request or purchase. Berkeley Protocol on Digital Open Source Investigations (2020).

[5] See generally, special issue in the Journal of International Criminal Justice, volume 19 (2021); Berkeley Protocol on Digital Open Source Investigations, UN OHCHR (2020).

[5] Rebecca Hamilton, *User-Generated Evidence*, 57 COLUMBIA JOURNAL OF TRANSNATIONAL LAW (2018).

[6] The risk of wrongfully convicting an innocent person while the real perpetrator goes free.

their ability to parse fiction from fact.[6] The events of that day have also underscored the difficulties and limitations endemic to the field of forensic image and video comparison—a practice that includes matching visual clues in separate pieces of visual evidence, such as videos, photos, satellite imagery or drone footage—raising the possibility that the wrong people will be identified as perpetrators via the data posted online.[7]

In this article, we explore the potential risk of harm caused by the reliance on digital open source information as evidence in criminal litigation. Compelling videos and over-confident analysis may mask the many ways in which digital imagery can mislead its viewers—obscuring facts, rather than illuminating them. For example, the story of Sunil Tripathi, who was falsely accused by online "digital detectives" of being one of the Boston Marathon bombers in April 2013 is an important cautionary tale about facial misidentification. [8] Sunil had gone missing earlier that year and his family had posted photos and videos of him to the internet, asking if anyone had information with regards to his whereabouts. An internet mob jumped on the images, claiming he looked like one of the two perpetrators seen in footage released by law enforcement. These vigilantes took to Reddit and other online forums to post hateful messages and spread accusations that turned out to be false. They insisted that they had the right man. They did not.[9]

The misidentification led to serious consequences for Sunil's family, which received numerous death threats while searching for their missing son. Unfortunately, Sunil's story is not

[6] "Mistaken Identity: FBI probe into Jan 6 rioters sees challenges," Al Jazeera, 6 May 2021, available at https://www.aljazeera.com/news/2021/5/6/mistaken-identity-fbi-probe-into-jan-6-rioters-sees-challenges (last visited 26 October 2021).
[7] *Id*.
[8] Adam K. Raymond, *7 Times Internet Detectives Got the Wrong Guy*, N.Y. Mag.: Intelligencer (Jun. 14, 2020), https://nymag.com/intelligencer/2020/06/seven-times-internet-detectives-got-the-wrong-guy.html.
[9] David Kushner, *What Anonymous Got Wrong in Ferguson*, New Yorker (Sept. 5 2014), https://www.newyorker.com/tech/annals-of-technology/anonymous-got-wrong-ferguson.

unique. There are numerous examples of amateur cyber sleuths who publish accusations online without the training, expertise, or ethical guidance necessary to prevent damaging false claims.[10] Inaccurate accusations by internet users who piece together clues from online information are becoming an increasingly frequent occurrence, with numerous news stories and true crime documentaries emerging on the topic.[11] Most of these portrayals are overwhelmingly positive, with one of the most recent lauding the impressive power of the "people's panopticon."[12]

Social media, as a relatively new and information-rich environment, undoubtedly offers exciting opportunities for criminal investigators and prosecutors, and there is an important role for well-intentioned civilians to play in supporting law enforcement efforts.[13] However, it's important not to let this enthusiasm blind practitioners to the realities and limitations of technology. While several scholars have now written about the advantages of relying on digital open source information from a prosecution perspective (including us),[14] few have addressed

[10] Raymond, *supra* note 9.
[11] Netflix, Hotel Cecil; *Don't F**k with Cats: Hunting an Internet Killer* (Netflix broadcast Dec. 19, 2019).
[12] *The Promise of Open-Source Intelligence*, Economist (Aug. 7, 2021), https://www.economist.com/leaders/2021/08/07/the-promise-of-open-source-intelligence.
[13] *See, e.g.*, Press Release, *Justice Initiative Joins Syrian Groups in Filing First Criminal Complaint on Behalf of Sarin Attack Victims*, Open Soc'y Just. Initiative (Oct. 6, 2021), https://www.justiceinitiative.org/newsroom/justice-initiative-joins-syrian-groups-in-filing-first-criminal-complaint-on-behalf-of-sarin-attack-victims; Human Rights Center UC Berkeley School of Law, *Chemical Weapons Attack in Eastern Ghouta, Syria: A Visual Summary of an Open Source Investigation*, (Oct. 7, 2020), https://storymaps.arcgis.com/stories/56c19f1dbcbb4054b524cacc5f6a9fa5; *The MH17 Trial Part I: New Material from the Four Defendants*, Bellingcat (Apr. 20, 2020), https://www.bellingcat.com/news/uk-and-europe/2020/04/20/the-mh17-trial-part-1-new-materials-from-the-four-defendants/; *ICC Digital Platform: Timbuktu, Mali*, Situ Rsch. (2020), https://situ.nyc/research/projects/icc-digital-platform-timbuktu-mali.
[14] See, e.g., Emma Irving, *And So It Begins… Social Media Evidence in an ICC Arrest Warrant*, OpinioJuris Blog (Aug. 17, 2017), http://opiniojuris.org/2017/08/17/and-so-it-begins-social-media-evidence-in-an-icc-arrest-warrant/; Alexa Koenig and Lindsay Freeman, *Strengthening Atrocity Cases with Digital Open Source Investigations*, Lieber Inst. W. Point (Apr. 1, 2021); Lindsay Freeman, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, 41 Fordham Int'l L.J. 283 (2018); Alexa Koenig et al., *Open Source Fact-Finding in Preliminary Examinations*, *in* 2 Quality Control in Preliminary Examinations 681 (Morten Bergsmo & Carsten Stahn eds., 2018); Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation and Accountability (Sam Dubberley, Alexa Koenig & Daragh Murray eds., 2020) (multiple sources).

the vulnerabilities and dangers of these methods from a defense perspective.[15] Potential shortcomings should be acknowledged for a number of reasons, not only because it is important for attorneys and investigators to be prepared for them as digital open source investigations increase in popularity, but also to ensure that the integration of these materials into legal processes does not harm due process or impede the truth.

Although digital open source investigative methods are relatively new, misidentification stories like Sunil's that hinge on social media content and low quality visual comparison bear an eerie resemblance to earlier wrongful conviction cases that were based on later-invalidated forensic science. In the United States, a reliance on "bad forensics" has been the basis for roughly half of all prosecutions that have resulted in DNA-based exonerations. Many now debunked or discredited "forensic" techniques were introduced quickly and optimistically into courtrooms and used to secure convictions in criminal cases before they were ever meaningfully tested. Years later, when DNA exonerations began to reveal a common theme of poor-quality forensics leading to problematic prosecutions, significant grant money was given to scientists to test forensic practices. The results were shocking.[16]

This article begins with a brief summary of noteworthy instances of problematic forensics used to convict and/or impugn the innocent. These cases offer important lessons about the need to proceed with care when introducing new forms of technical, scientific, or other expert evidence into criminal cases. With the steep increase in the use of internet-derived evidence in criminal cases, lawyers and judges should pay close attention to these cautionary tales—

---

[15] See Yvonne McDermott et al., *Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations*, 2021 J. Int'l Crim. Just. 1-21, for initial critiques.

[16] "In May 2015, a $30 million grant by NIST was given to a team of statisticians and legal professionals tasked with analyzing matches to determine the likelihood of, for instance, a hair sample to that of another individual or bite mark to that of another person's teeth." https://www.tnduiattorney.com/blog/2016/03/ballistics-testimony-a-practice-contributing-to-wrongful-convictions.shtml

especially the damage caused by judges who allow unverified and/or untested forensic methods into their courtrooms. We take a critical perspective to exploring these digital investigation methods with the goal of strengthening the quality and professionalism of the results. Adopting the skeptic's perspective, this article breaks down the phases of a digital open source investigation to highlight its vulnerabilities. Our critical perspective is not meant to hinder the growing use of digital open source information, but rather to ensure that such information is introduced into courtrooms responsibly and effectively. Lowering the bar, only to introduce mistaken findings in criminal cases and produce bad verdicts, can do significant damage to the long-term credibility of these techniques and the legitimacy of our legal system.

II. A BRIEF HISTORY OF "BAD FORENSICS"

In 1991, Cameron Todd Willingham was accused of setting a fire that killed his three young daughters in his family's home in Corsicana, Texas.[17] Local Deputy Fire Marshal Manuel Vasquez served as an expert in the trial, providing his interpretation of "burn patterns" that had been found in the Willinghams' home.[18] For decades, discolored burn patterns had meant one thing: arson. The theory, as taught to fire investigators, was that such burn patterns indicated that an accelerant had been used, suggesting that the fire was intentional rather than accidental. It was a well-accepted assumption that pour patterns were the result of sustained burning in the locations where the accelerant had been poured. Based in large part on Vasquez' testimony, Willingham was convicted, sentenced to death, and executed.[19]

[17] *See, e.g.*, Arson Review Committee, Report on the Peer Review of the Expert Testimony in the Cases of State of Texas v. Cameron Todd Willingham and State of Texas v. Ernest Ray Willis 1-45 (2016), https://www.innocenceproject.org/wp-content/uploads/2016/04/file.pdf.
[18] *Id.*
[19] *Id.*

However, since Willingham's execution, "Each and every one of the indicators relied upon [in his case] have since been scientifically proven to be invalid."[20] When the pour pattern theory was finally tested in a laboratory setting, researchers discovered that pour patterns were not caused by accelerants. Rather, such patterns were the result of uneven ventilation, which causes fire to burn more intensely in certain spots.[21] This research threw the entire field of forensic fire investigation into question, along with the convictions that relied on such expert testimony. Willingham's case is a particularly tragic example of what can happen when a case's outcome hinges on a forensic technique that has not yet been scientifically validated. If defense attorneys had known how to challenge the scientific basis of the arson experts' conclusions or judges had been stricter gatekeepers, Willingham may never have been executed.

Stories like Willingham's are not unique, nor are they limited to arson investigations. The comparative sciences—such as fiber, footprint, and fingerprint comparison—have all resulted in equally tragic outcomes.[22] As just one example, in 2005, the FBI stopped utilizing an unreliable forensic test used to determine the source of bullets and was forced to review more than 2,500 cases that had relied on that test.[23] In 2009, the National Research Council (NRC) issued a landmark report that condemned the lack of research underlying many areas of forensic science.[24] Arson investigation mentioned, as was bite mark comparison, hair comparison, latent

[20] *Tragedy in Texas*, Innocence Project (Jan. 10, 2011), https://innocenceproject.org/tragedy-in-texas/.
[21] See *Understanding the Impact of Ventilation on Burn Patterns Can Aid Arson Investigations*, Nat'l Inst. Just. (Aug. 24, 2020), https://nij.ojp.gov/topics/articles/understanding-impact-ventilation-burn-patterns-can-aid-arson-investigations, for an overview of the relationship between ventilation and burn patterns.
[22] Innocence Project (Jan. 10, 2011), https://innocenceproject.org/all-cases/.
[23] *See* Press Release, *FBI Laboratory Announces Discontinuation of Bullet Lead Examinations*, FBI Nat'l Press Office (Sept. 1, 2005), https://archives.fbi.gov/archives/news/pressrel/press-releases/fbi-laboratory-announces-discontinuation-of-bullet-lead-examinations; *See also Three Freed, and FBI Continues to Review Ballistic Cases*, Innocence Project (Jan. 19, 2010), https://www.innocenceproject.org/three-freed-and-fbi-continues-to-review-ballistic-cases/.
[24] National Research Council, *supra* note 17.

fingerprint analysis, and comparative bullet lead analysis have all been invalidated,[25] resulting in hundreds of convictions being overturned. And in 2016, scientists from Canisius College and University at Buffalo School of Dental Medicine published the results of a landmark study that tested the hypothesis that bite marks are unique to individuals and can provide a basis for perpetrator identification. "Using a variety of dental impressions, they examined more than 1,000 human dentitions and studied hundreds of bite marks in cadaver skin. With the help of computer analysis and applied statistics, the team then worked to match its database of bite marks to the correct dental impressions."[26] They found that contrary to assumptions, a single bite mark is not distinct enough to be linked to a particular individual and can actually point to many different people.[27] According to the Innocence Project, at least 25 individuals convicted on bite-mark evidence have since been exonerated based on DNA testing.[28] It took several decades and hundreds of convictions for a troubling truth to emerge: several fields of forensic "science" were not scientific at all.[29]

These cases force us to ask: why did this happen and how can we prevent it in the future? In several cases, experts over-confidently stated that a conclusion was certain—for example, two fibers presented as a match—when the human eye is too fallible and the analysis too subjective to be able to make that kind of claim with the necessary reliability. As noted by Aviva Orenstein in her research into the use of "junk science" as evidence, "Experts in bitemark

---

[25] *Id.*; *see also* National Research Council, *Forensic Analysis: Weighing Bullet Lead Evidence*, The National Academies Press (2004), https://doi.org/10.17226/10924; *Unvalidated Forensic Science*, New England Innocence Project, https://www.newenglandinnocence.org/unvalidated-forensic-science.
[26] *Bite-Mark Analysis Can Lead to False Convictions, Landmark Research Shows,* ScienceDaily (Jan. 8, 2016), https://www.sciencedaily.com/releases/2016/01/160108134949.htm.
[27] *Id.*
[28] Daniele Selby, *Why Bite Mark Evidence Should Never Be Used in Criminal Trials*, Innocence Project (Apr. 26, 2020), https://innocenceproject.org/what-is-bite-mark-evidence-forensic-science/.
[29] *See* Richard A. Leo & K. Alexa Koenig, *Police Interrogation and Coercion in Domestic American History: Lessons for the War on Terror, in* Confronting Torture: Essays on the Ethics, Legality, History and Psychology of Torture Today 146 (Martha C. Nussbaum & Scott A. Anderson eds., 2018).

and microscope hair analysis often offered overblown conclusions and failed to provide proper foundations…. For instance, experts conducting microscopic hair analysis overstated the probative value of finding two hair samples microscopically indistinguishable in identifying a perpetrator. They regularly testified that in their experience it was very rare for them not to be able to tell hairs apart, a meaningless anecdotal boast."[30] Social science research has repeatedly established that humans have a high degree of confidence in their ability to visually compare images; unfortunately, however, this confidence does not consistently correlate with accuracy.[31] As a result, methodological flaws have led to a concerning pattern of wrongful convictions. In the United States, the misapplication of forensic science is the second most common contributor to wrongful convictions and has played a pivotal role in nearly half of all DNA exoneration cases.[32] The use of untested forensic disciplines[33] or forensic methods that cannot be

[30] Aviva A. Orenstein, *Debunked, Discredited, but Still Defended: Why Prosecutors Resist Challenges to Bad Science and Some Suggestions for Crafting Remedies for Wrongful Conviction Based on Changed Science*, 48 Seton Hall L. Rev. 1139, 1142 (2018). *See* Maneka Sinha, *Radically Reimagining Forensic Evidence*, 73 Ala. L. Rev. (forthcoming 2022)[need Sinha's permission to cite], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891788, for further information on how prosecutors have resisted revisions to forensic science—and calls to dismantle the forensic science system given its relatively powerful role in the United States' very racialized criminal justice system,

[31] *Watching Others Makes People Overconfident in Their Own Abilities*, Ass'n for Psych. Sci. (Mar. 8, 2018), https://www.psychologicalscience.org/news/releases/watching-others-makes-people-overconfident-in-their-own-abilities.html; Don A. Moore & Paul J. Healy, *The Trouble with Overconfidence* 1-75 (Tepper Sch. of Bus. Working Paper No 341, 2007), https://www.researchgate.net/publication/5305238_The_Trouble_With_Overconfidence.

[32] *Overturning Wrongful Convictions Involving Misapplied Forensics*, Innocence Project, https://www.innocenceproject.org/causes/misapplication-forensic-science/ (last visited Aug. 21, 2021).

[33] The Innocence Project and others have conducted studies that demonstrated that some forensic methods used in criminal investigations cannot consistently produce accurate results. For example, bite mark comparison—identifying a suspect based on comparing teeth to a bite mark made on skin—is unreliable and inaccurate. Microscopic hair comparison is not based on sound science.

scientifically validated,[34] along with misleading or exaggerated expert testimony, have been identified as the primary factors in such wrongful conviction cases.[35]

The maturation of digital open source investigations shares several noteworthy parallels with the introduction of various forensic sciences into legal processes in the mid- to late-twentieth century. The similarities are especially strong with various visual comparison methods, analytical processes that rely on a comparison between two or more pieces of visual information—such as videos with satellite imagery (to confirm the likely coordinates where the video was shot, for example), or a photo of a known person with a video of an unknown perpetrator (as in the case of Sunil). Such methods are especially error prone, vulnerable to human biases, and misrepresentation by experts.[36] Because scientific and digital evidence can be relatively complex and highly technical, experts are often needed for the judge or jury to understand the evidence and to ensure its admission in court, creating sometimes problematic over-dependencies on those experts' opinions.

While the harms caused by wrongful convictions cannot be undone, the legal world can learn important lessons from its history of allowing new forensic methods and outcomes into the courtroom before proper vetting. When any new investigative technique emerges, the world should be wary. Appropriately wary. Dismissing a new technique out of hand comes with its

[34] Some forensic disciplines are capable of consistently producing accurate results but are not yet sufficiently researched to establish validity. Accuracy of a method should be established using large, well-designed studies. Without these studies, an analysis cannot be interpreted. For example, shoe print analysis as a basis of identifying the unique source of a print has not been sufficiently validated.

[35] Forensic testimony given by experts at trial can overstate or exaggerate the significance of similarities between evidence from a crime scene and evidence from a suspect. It can also oversimplify the data—a frequent occurrence, sometimes the result of pressure from the judge. Examples include testimony that suggests a collection of features is unique or overstates how rare or unusual it would be to see these features, implying that it is quite likely that the suspect is the source of the evidence, and testimony that doesn't convey all possible conclusions, as can arise with masking in serology testing.

[36] Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, Strengthening Forensic Science in the United States: A Path Forward (2009), https://www.ojp.gov/pdffiles1/nij/grants/228091.pdf.

own set of problems, of course. However, there is an equivalent danger of relying on new categories of evidence before they have been thoroughly tested, including digital investigative methods that are increasingly making their way into courtrooms.

III. OPENINGS FOR CHALLENGING DIGITAL OPEN SOURCE EVIDENCE

In this next section, we discuss the components of a digital open source investigation that are most vulnerable to cross-examination—six lines of inquiry that attorneys can use to probe the quality of such investigations, and for which both proffering attorneys and expert witnesses should be prepared. These include challenges to 1) the investigator's qualifications and experience, 2) the investigative process, 3) the evidence itself, 4) the analytical conclusions, 5) the witnesses' testimony about the evidence and analysis, and 6) the in-court presentation of the evidence.

A. Challenging the Investigator

Due to the relative newness of social media and smartphones, many of the lay and professional individuals conducting open source investigations were not formally trained for the job. Instead, digital open source investigators are often self-taught, drawing on skills from a number of different fields of practice and educational resources.[37] Of course, the fact that there is not yet a well-established field of practitioners does not preclude their participation in justice

[37] A number of digital open source investigation "toolkits" and trainings support the learning of new tools and methods; see, *e.g*, Justin Nirdine, *OSINT Framework*, https://osintframework.com/ (last visited Aug. 21, 2021); *OSINT Techniques*, https://www.osinttechniques.com/osint-tools.html (last vistied Aug. 21, 2021); *OSINT.Link*, https://osint.link/?__cf_chl_jschl_tk__=pmd_zYiy28FklWuQb6uaf8lM6iDHwxZzDCfOeCRx1TR1v9w-1629768034-0-gqNtZGzNAdCjcnBszQh9 (last visited Aug. 21, 2021). See *Trainings and Workshops*, U.C. BERKELEY HUM. RTS. CTR, https://humanrights.berkeley.edu/resources/trainings-and-workshops (last visited Aug. 21, 2021), for examples of training courses; *Open Source Investigations for Human Rights*, AMNESTY INT'L, https://advocacyassembly.org/en/partners/amnesty/ (last visited Aug. 21, 2021); *Training*, BELLINGCAT, https://www.bellingcat.com/tag/training/ (last visited Aug. 21, 2021); Michael Bazzell, *Online OSINT Video Training*, INTELTECHNIQUES, https://inteltechniques.com/training.html (last visited Aug. 21, 2021).

processes. However, the absence of standard procedures grounded in proper testing and objectively verifiable successes makes them particularly vulnerable to challenge, providing the defense with multiple lines to attack their credibility on voir dire.

Many open source investigators do not have the academic credentials or certifications that are typical for expert witnesses who attest to the validity of scientific evidence in court. Defense attorneys may argue that without formal scientific training the investigator or analyst may not adhere to the same standards or take the same precautions against bias as those who have that training. Defense attorneys may also argue that such lay investigators do not understand the methodological value of safeguards such as peer review, working with multiple hypotheses, and clear documentation of the investigative process.

Professional criminal investigators, whether national or international, have usually received formal training as analysts, police officers, or researchers. The typical corollary to formal training would be years of experience, ideally under the supervision of a more experienced investigator. Today, in many large organizations, open source investigations are led by relatively young or junior members of a team because of their facility with digital technologies. However, even in this newer information environment, basic principles of research and analysis apply—and thus having a deep understanding of the building blocks of quality research is critical.

Open source investigators are often generalists: people who understand how and where individuals communicate online, and have a sense of the broad array of tools and platforms that can assist in finding and evaluating that information. They are jacks of all trades, and masters of none. While they draw on a vast repository of online data and software, experimenting with tactics affiliated with well-established disciplines, including digital forensics, data science,

geospatial analysis, forensic image and video comparison, and forensic image and video interpretation, they have not established themselves as experts in any of these fields. While the ability to self-educate is an important one, such breadth of expertise—while invaluable—should complement and not supplant the depth of understanding that comes with expertise in established fields of practice.

Disciplinary canons exist for a reason: to ensure quality work, minimize blind spots and ideally protect the legitimacy of an area of practice. In the open source investigation context, the *Berkeley Protocol on Digital Open Source Investigations* offers professional, methodological, and ethical principles that speak to the necessary ability of the investigator to credibly perform various open source investigation tasks, and to assess when an expert in a subfield of digital investigations should be called in to either supplant or supplement a generalist's process and analysis. The principles require indicia of accountability, competency, accuracy, objectivity, legality, humility, independence, transparency and security awareness, among others.[38]

Other critical considerations include whether the investigator has pre-existing biases that may prejudice the investigation, and if so, the kinds of pre-existing biases; whether the investigator may have been biased or prejudiced by the information environment he/she inhabits; and whether the investigator is susceptible to external influence that may call into question the quality of their conclusions, either because of funding sources, reputational concerns, or otherwise.

In the next section, we move from challenges to the investigator to challenges to their process.

[38] Berkeley Protocol, *supra* note 10.

B. Challenging the Investigation Process

After examining the investigator's qualifications and competencies, lawyers should assess the quality of the investigation itself—in particular, the process by which the investigator identified, collected, and preserved online information. Such an examination should evaluate the thoroughness and objectivity of online inquiries to ensure that the investigator has not intentionally or inadvertently cherry-picked source information, the criteria that was used to determine what to collect, and the forensic soundness of the tool used to capture and preserve the information.

One of the biggest opportunities *and* challenges for online investigators is the sheer scale of information flooding the Internet. As of late 2018, approximately 6000 tweets were being sent out every second; more than 400 hours of stories were being uploaded to Instagram each day; and 500 hours of videos uploaded to YouTube each minute. This volume makes it impossible for human investigators to thoroughly review all potentially relevant information online. The vast and dynamic nature of the internet and the significant volume of information it holds make digital investigations vulnerable to multiple challenges regarding the investigator's decision-making process, especially their determination of what is and is not relevant and what they choose to collect. This becomes especially critical in cases where relevant information has been removed from the internet between the time of the event and the start of a formal legal investigation, for example due to social media content moderation or the perpetrator or other uploader regretting their post. In such cases, the data collected by a lay investigator may be the only version available by the time the case gets to trial.[39]

[39] Most courts require or prefer that social media evidence come from the company that hosted the content, not third parties such as citizen investigators.

The average person may not be familiar with the many biases that influence online investigations, but professionals and lay investigators who document information from the internet should be aware of such biases and should take proactive measures to counter them.[40] Three categories of bias are especially important to consider. The first is *access bias*, which relates to who has access to digital tools and who does not, and thus whose perspectives and experiences are and are not represented online. The second is *algorithmic bias*, which refers to a search engine's programming and how it determines which search results should be shown to its users. Search results from Google, Yahoo, Bing, Yandex, Baidu and DuckDuckGo differ between users, and between each other. Their search algorithms use several data points—including, but not limited to, the user's location, device, browser and prior search history—to prioritize and customize which websites are displayed. Therefore, digital investigators must take proactive measures to maximize the neutrality of their search results. The specific keywords and languages they use along with the Boolean operators deployed to connect sources and keywords, can also radically influence results.[41] The third consists of the investigator's *cognitive biases*, which may influence not only how and where the investigator searches for information, but how they interpret results, what they choose to collect and preserve, and what they disregard.[42]

---

[40] See, e.g., Richards J. Heuer JR., Psychology of Intelligence Analysis (Central Intelligence Agency 1999), for an overview of biases especially relevant to digital open source investigations; *See* Yvonne McDermott et al., *Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations*, 2021 J. Int'l Crim. Just. 1-21.

[41] *See* Yvonne McDermott, Alexa Koenig and Daragh Murray, "Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations," 19 J. Int'l Crim. L 85 (2021).

[42] *See, e.g.,* Alexa Koenig and Ulic Egan, "Power and Privilege: Investigating Sexual Violence with Digital Open Source Information," 19 J. Int'l Crim. J. 55 (2021); Alexa Koenig and Ulic Egan, "Hiding in Plain Site: Using Online Open-Source Information to Investigate Sexual Violence and Gender-Based Crimes," in Alexandra Moore and James Dawes, eds., Technologies of Human Rights Representation (forthcoming 2022) (both describing how cognitive biases can interview with the effective investigation of international crimes).

Another issue is documentation: one of the biggest differences between amateur and professional investigators is how they document their investigation—or fail to do so. Accepted standards require that all technical processes, such as the extraction and processing of images, must be documented in detailed contemporaneous notes.[43] These notes should include details of any hardware or software used to process, and the parameters applied. Such notes may be disclosed in court. Investigators without legal or other formal training may be unaware of documentation expectations, which can have significant downstream effects. As one example, poor documentation notably led to the exclusion of Facebook evidence in *Regina v. Hamdan*[44]—a Canadian terrorism case that relied on the defendant's posts, which were excluded because the various agencies involved in the investigation did not document their collection, collected information in different ways, and failed to use forensic software that would have automatically created a record of the process.[45]

In examining the investigation process, lawyers should scrutinize whether the investigator can provide clear, thorough and, to the extent possible, contemporaneous documentation of the online inquiry and collection processes; whether those processes can be audited; and whether the investigator can account for any documentation gaps or procedural violations.

In the next section, we move from issues with the process, to issues with the evidence.

---

[43] Simon A. Cole, Who Will Regulate American Forensic Science, Seton Hall Law Review, Vol. 48, 563 (Apr. 28, 2018); See also, Forensic Image Comparison and Interpretation Evidence: Guidance for Prosecutors and Investigators 2 (National Crime Agency, CPS, Metropolitan Police and Forensic Science Regulator 2016), (U.K.), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/912880/Image_Comparison_and_Interpretation_Guidance_Issue_2.pdf.

[44] *Regina v. Othman Ayed Hamdan*, 2017 CanLII 1770 (Can. B.C. S.C.R.).

[45] *Id.*

C. Challenging the Evidence

After examining the investigation process, the opposing party should look for vulnerabilities in the evidence—the digital information on which the analyst or expert bases their conclusions. As with other types of evidence, lawyers must authenticate digital files—establish that an item is what the proffering party says it is—in order to have it admitted at trial. The malleability and ephemerality of digital material, however, make such evidence especially vulnerable to authenticity challenges.[46] Proving the authenticity of online evidence is further complicated by anonymous and pseudonymous sources, lack of provenance, and widespread mis- and disinformation. The internet is replete with inauthentic sources—bots and botnets, cyborgs, imitator accounts, sock puppets, and pseudonyms—complicating the ability to determine who created and who posted the item.[47] Authentication does not have a high bar, but generally requires establishing an item's author/creator, provenance, chain of custody, and integrity.

Author/creator and provenance can be assessed together in digital open source investigations, as the term "source" is often used broadly to encompass both the author/creator and the provenance of online content, including the platform on which it was found and the user who uploaded it to that platform. If the content's origins are unknown, then reverse image searches and websites like the Wayback Machine that offer a historical timeline and record of online data may be used to help the analyst establish the content's provenance and author.[48] Investigators should start by establishing whether the content can be attributed to a particular

[46] For an overview of various authentication techniques for digital evidence, see Jonathan W. Hak, "Image Alteration (Forgery) Detection: An Overview of Passive Techniques," Blog Series, 26 Oct. 2021, at https://www.jonathanhak.com/2021/10/26/image-alteration-forgery-detection-an-overview-of-passive-techniques/

[47] Carlotta Dotto and Seb Cubbon, How to Spot a Bot (or Not): The main indicators of online automation, co-ordination and inauthentic activity, First Draft News (Nov. 28, 2019) at https://firstdraftnews.org/articles/how-to-spot-a-bot-or-not-the-main-indicators-of-online-automation-co-ordination-and-inauthentic-activity/.

[48] Internet Archive, Wayback Machine, https://archive.org/web/ (last visited Aug. 21, 2021).

person or organization, and whether it is primary (first-hand knowledge) or secondary (including second-hand information or commentary about primary content).

The investigator will also have to address the information's chain of custody. There are two chains of custody to consider when dealing with digital open source evidence—first, the chain that stretches from when an item is created to its collection by the investigator. The second refers to custody, possession, or control of the item from the time of its collection to its presentation in court. Establishing that the digital item has not been altered once in the investigator's possession is important for confirming its authenticity. This includes detailing how the digital item has been preserved and stored, including whether the item was hashed and reliably timestamped at the point of collection. Opposing lawyers will want to ask several questions to determine whether the digital evidence has been properly preserved. For example, was the evidence collected in a forensically-sound manner or using an approved tool for forensic collection? Lawyers will also want to assess whether the collection was complete. In other words, was enough accompanying information captured in conjunction with the digital item to understand the context that surrounded it?

The integrity of digital information may be difficult to establish but is especially challenging (and especially important) if investigators are unable to establish the author or provenance, or critical links in the chain of custody. The internet is rife with intentionally inauthentic information—including visual or audio disinformation that was misleadingly presented, edited, distorted, or computer-generated.[49] The internet is also saturated with information that is unintentionally inauthentic—misinformation that includes everything from

[49] *Deepfakes, Shallowfakes and Speech Synthesis: Tackling Audiovisual Manipulation*, EUR. SCIENCE-MEDIA HUB (Dec. 4, 2019), https://sciencemediahub.eu/2019/12/04/deepfakes-shallowfakes-and-speech-synthesis-tackling-audiovisual-manipulation/.

distorted imagery to misguided reporting. The increased accessibility and rapidly falling costs of sophisticated photo and video-editing software has lowered the bar for amateurs to enter the digital manipulation game, and is aided by the fact that humans are notoriously bad at detecting image manipulations.[50]

In addition to authenticity, the proffering party will need to establish the information's reliability. Reliability is considered at different stages in different jurisdictions, sometimes as part of the admissibility assessment and sometimes as part of the weight assessment. In the absence of the traditional indicia of reliability—such as a witness who can testify to the origins and accuracy of evidence—investigators must be creative about collecting enough contextual and corroborating information for a judge or jury to be comfortable relying on it. In the open source investigation context, reliability can be established through a three-pronged verification process that includes source analysis, content analysis and technical analysis.[51] According to the Scientific Working Group on Digital Evidence (SWGDE), image authentication involves an examination of visual information within an image (the content) and non-visual information about the image itself (technical aspects like the structure of pixels and any metadata).[52] When it comes to information found on the internet rather than provided by a witness directly, authentication also involves an examination of the source of the image.[53] Source analysis differs from the attribution analysis mentioned above. Attribution analysis is the process of identifying

[50] Sophie J. Nightingale et al., *Can People Detect Errors in Shadows and Reflections?*, 81 Attention, Perception & Psychophysics 2917 (2019). Seven experiments tested people's ability to use shadows to determine whether an image has been manipulated. Overall, detection rates were poor.
[51] Berkeley Protocol, *supra* note 10.
[52] Scientific Working Group on Digital Evidence, SWGDE Best Practices for Image Authentication 1-14 (2018), https://drive.google.com/file/d/1Z0DsJMa6aDZlFJ9kRfOL8cow5VjhVT0t/view.
[53] Scientific Working Group on Digital Evidence, SWGDE Best Practices for Image Authentication 1-14 (2018), https://drive.google.com/file/d/1Z0DsJMa6aDZlFJ9kRfOL8cow5VjhVT0t/view.

the original source, if possible, whereas source analysis occurs once the source is identified and needs to be evaluated. Thus, source analysis means examining the *credibility* of the source.

Content analysis refers to an analysis of the information contained within the "four corners" of the digital item, whether it be an image, video, audio file, document, spreadsheet, social media post, or something else. In the U.S., the most important factor for the court is usually whether the item is a "fair and accurate portrayal" of a fact at issue in the case. Using a video pulled from social media as an example, analysis may include a review of the built or natural environment depicted in the video to determine if what is seen is consistent with the purported place and time; scrutiny of human features to determine if known perpetrators, victims or witnesses are depicted; evidence of staging; the photographic conditions, such as the quality of lighting; and more.[54]

Technical analysis includes an examination of any metadata or Exif (Exchangeable Image File) data that may be attached to the item. In order for forensic video analysts to interrogate imagery, they collect data on "image size, pixels, type of compression, frame rate, aspect ratio, GOP structure, file format, etc."[55] Relevant metadata may include the make, model, serial number, and settings of the device used to capture the image; the date and time of creation, as well as image resolution and size; any GPS coordinates or elevation data; information about frame rate, lens or flash; and thumbnails.[56] Lay open source investigators often use free online tools like InVid or FotoForensics to review and extract the metadata. However, this differs from the tools and methods used by certified forensic analysts.

---

[54] *Id.*
[55] *Interpreting Video Images: Can You "Say What You See"?,* Jonathan W. Hak, Q.C. Blog (May 12, 2020), https://www.jonathanhak.com/2020/05/12/interpreting-video-images-can-you-say-what-you-see/.
[56] SWGDE Best Practices, *supra* note 44, 1-14.

One especially concerning consideration for digital videos is compression—a process that reduces and removes redundant information so that the digital video file can more easily be streamed over the internet or transferred across a network.[57] Most digital videos that are emailed or uploaded online are subject to something called "lossy compression," which means the loss of original information. When there is a loss of data during compression, a computer later "fills in" the areas that were lost when compressed. This results in "artifacting"—a noticeable distortion in the video's quality. Such distortion can be a problem for lay investigators, who may not be aware of the ways in which such distortion can be spotted and how it can affect an analysis.

One form of distortion affects perception of movement due to variability in frame rates. The frame rate of a video is the number of frames in one second of video. There are standards for real time frame rate, which can vary.[58] When a video is played at that standard rate or higher, the human eye perceives motion accurately. However, if the frame rate falls below the standard because of compression, the human brain misinterprets the motion captured in the video. Thus, analysts cannot rely on the motion or movement in a video that has a frame rate below the standard.

Such human misperception can have disastrous consequences.[59] One example is a case from Florida in which a woman who worked as a nanny was accused of abusing an infant in her care and charged with eight counts of child abuse.[60] Key evidence was footage captured by a

---

[57] *Digital Video and Compression*, RGB Spectrum, https://www.rgb.com/digital-video-and-compression#:~:text=Video%20compression%20is%20a%20process,transmission%2C%20recording%2C%20or%20storage (last visited Aug. 21, 2020).
[58] The real time frame rate for analog video is 30 frames per second under the North American standard and 25 frames per second under the European standard.
[59] *Florida v. Muro*, So. F.2d (Fla. Dist. Ct. App. 2005), https://caselaw.findlaw.com/fl-district-court-of-appeal/1429591.html.
[60] *Id.*

"nanny cam," a home surveillance system used to monitor and document caregivers' behavior, often without their knowledge. At 30 frames per second, the video captured by the system is consistent with what the "human eye is capable of seeing, so the image appears fluid."[61] However, this rate is achieved when only one of the four cameras in the system is operating at a given time; with each additional camera the resolution drops, all the way down to 7.5 frames per second if all four cameras are operating—a rate far below what the human eye expects, and one that produces a "choppy" image.[62]

On the day the parents reviewed the nanny cam recording, their relatively choppy video appeared to show the nanny shaking the baby. The parents took the baby to the emergency room and called the police. Although the baby had no visible injuries, the nanny was arrested for child abuse after a detective viewed the footage. Because the father allowed the nanny cam to keep running (police forgot to tell him to turn it off to preserve evidence) the original video was overwritten and all that was left of 14 days' worth of recordings—which would have provided helpful context and data—was a two hour long copy preserved by a law enforcement technician. The nanny spent two years in jail, refusing to take a plea deal, before the case was ultimately thrown out. While the parents continued to believe that the video was clear evidence of abuse, "prosecutors acknowledged that the video evidence was worthless" due to compression and framerate, which "could make [even] gentle motions appear violent."[63]

In addition to compression and framerate, video and image analysis can be tainted by a distortion in the aspect ratio, namely the relationship of width to height and the number of lines

---

[61] *Id.*
[62] *Id.*
[63] *Nanny Cleared of Violently Shaking Baby*, ABC NEWS (Mar. 21, 2006), https://abcnews.go.com/GMA/LegalCenter/story?id=1749672.

of information in the video.[64] Reliable comparison analysis cannot be done on a video with an incorrect aspect ratio, therefore aspect ratio must be corrected before analysis. Similarly, reliable comparison analysis cannot be done on a video or image that is too low quality. A video or image's quality—or resolution—might also interfere with analysis. Low resolution results in blurring. Resolution degrades with every copy, and most online videos and images are copies that further degrade when uploaded to social media platforms and again when downloaded by the investigator. Unlike aspect ratio, poor image quality cannot be corrected. Thus, while image comparison can provide compelling evidence in the courtroom, the strength of the comparison depends in part on the quality of the imagery. Insufficient quality imagery results in unreliable findings.[65]

Ultimately, digital open source investigators must properly verify the digital information on which they rely. False, forged, manipulated, degraded and other problematic data can lead to erroneous findings. A significant volume of digital information, even when seemingly corroborative, cannot compensate for these underlying weaknesses. Once the digital evidence itself has been subjected to scrutiny, attorneys should look to the methods used to interpret, analyze and draw conclusions about the raw information.

---

[64] Hany Farid, Fake Photos, The MIT Press Essential Knowledge Series (Sept. 10, 2019).

[65] Federal Bureau of Investigation, Best Practices for Forensic Image Analysis, Scientific Working Group on Imaging Technology (Mar. 14, 2005); National Institute of Justice, Webinar on Image Quality and Clarity: The Key to Forensic Digital Image Processing, Aug. 3, 2021; See also FORENSIC IMAGE COMPARISON AND INTERPRETATION EVIDENCE: GUIDANCE FOR PROSECUTORS AND INVESTIGATORS 2 (National Crime Agency, CPS, Metropolitan Police and Forensic Science Regulator 2016), (U.K.), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/912880/Image_Comparison_and_Interpretation_Guidance_Issue_2.pdf; Jonathan W. Hak, Evaluation of the Forensic Science Regulator's recommendations regarding image comparison evidence, Forensic Science International: Synergy, Vol. 1., 294-297 (2019).

D. Challenging the Analytical Findings

In addition to challenging the imagery on which a conclusion was reached, lawyers can also critique the method of analysis, particular if it does not comply with a set standard in the relevant jurisdiction. Investigators and analysts should verify digital information before analyzing and reaching conclusions based on the information. Open source investigators' lack of validated analytical methods creates vulnerabilities, which opposing parties can attack on cross examination. At the same time, open source investigations' perceived newness may blind lawyers to the similarities between open source investigation methods and well-established analytical methods. For example, an untrained open source investigator might compare two images to corroborate or disprove the location depicted in one of the images, failing to realize that there is an established discipline of forensic image comparison that has its own best practices. Similarly, open source investigators might try to confirm the location of a particular incident by comparing a video or photograph of the event to publicly available satellite imagery, while ignorant of the potential distortions, edits and other pitfalls of which geospatial analysts are well aware.[66]

The scientific process, including the deployment of protocols, is a means of combating bias when examining and drawing conclusions from data. With video comparison forensics, professional video analysts employ a methodology known as ACE-VR, an acronym for Analyze Compare Evaluate Verify and Report. The process includes peer review.

One of the most common open source investigation techniques is geolocation, which involves matching built and natural objects in videos and photographs to satellite imagery in order to determine the physical location where the images were shot. The process of identifying

[66] Stephanie Croft (forthcoming).

visual clues in a video or photograph and matching those clues to known imagery is frequently used in professional investigations. While many claim this practice is new, it is not. What these investigators are doing falls within a well-defined subset of forensics: forensic image comparison, as discussed above. Forensic image comparison is defined as "an assessment of the correspondence between features in questioned items depicted in images and either questioned or known objects or images for the purpose of rendering an expert opinion regarding identification or elimination (as opposed to a demonstrative exhibit)."[67] Given this overlap, the analytical technique used by open source investigators should be considered and judged based on the standards that have already been established and vetted.

Some important considerations in forensic image comparison include "class and individual characteristics, image conditions, and the availability of statistical models."[68] When it comes to the ACE-VR method, according to SWGDE best practices, "In order to accurately interpret the content of an image…it is imperative that the examiner recognize the conditions and limitations that occurred during image capture, processing or editing."[69] These conditions and limitations may include resolution, optical or sensor defects, lighting conditions, motion and/or focal blur.[70]

Even when following established practice, however, scholars have pointed out that the interpretative or subjective dimension of comparisons have long lacked experimental support. For example, humans have struggled to correctly match fingerprints, despite courts having

[67] Scientific Working Group on Digital Evidence, SWGDE Technical Overview for Forensic Image Comparison 1-11 (2019), https://drive.google.com/file/d/11Pa7DOJmSJ00AieJcjNEGu7BJkCnvQkF/view.
[68] Scientific Working Group on Digital Evidence, SWGDE Technical Overview for Forensic Image Comparison 1-11 (2019), https://drive.google.com/file/d/11Pa7DOJmSJ00AieJcjNEGu7BJkCnvQkF/view.
[69] *Id.*
[70] *Id.*

accepted fingerprint analysis for more than a hundred years.[71] Acceptance is ultimately based on the examiner's training and experience, fidelity to the ACE-VR method, and an assumption about the uniqueness of fingerprints—an assumption that has increasingly been questioned.[72]

The assumption of "uniqueness" and its potential fallibility has tainted a variety of comparison methodologies, where the assessment of uniqueness has not undergone proper scientific testing. For example, investigators may rely on the skyline of a mountain range to geolocate a video without knowing how unique that skyline is to a particular mountain range.

In a comparison analysis report, the analyst must describe their process and provide a subjective opinion as to whether their analysis supports a finding that two or more items (such as people, cars, weapons or mountain ranges) are the same. Historically, one of the biggest issues in the comparison sciences has not been how the process was conducted, but the foundation upon which the conclusions were drawn.

For example, when it comes to fingerprint evidence, the analyst is often presented with an unknown print, usually a partial print, recovered from a crime scene. That print may be of poor quality or otherwise lacking critical detail. Before any sort of conclusion can be drawn, the examiner must first decide if the print provides sufficient information to be interpreted.[73] It is only after this determination that the print can be compared to a known print and assessed as to whether it's a "match." These are ultimately subjective processes. Bite mark analysis has obvious similarities to fingerprint comparisons as both rely on pattern matching. Both are often treated as legitimate forensic processes, even though the theory that individuals have unique

---

[71] Gary Edmond et al., *A Guide to Interpreting Forensic Testimony: Scientific Approaches to Fingerprint Evidence*, 13 *Law, Probability and Risk* 1, 2 (2013).
[72] *Id.*; *see also, e.g.*, S.A. Cole, *Who Speaks for Science? A Response to the National Academy of Sciences Report on Forensic Science*, 9 Law, Probability & Risk 25–46 (2010); *See* J.J. Koehler, *Fingerprint Error Rates and Proficiency Tests: What They Are and Why They Matter*, 59 Hastings L. J.,1077 (2008); J.J. Koehler, *Proficiency Tests to Estimate Error Rates in the Forensic Sciences*, 0 *Law, Probability and Risk,* 1–10 (2012).
[73] Edmond et al., *supra* note 60.

dentition has never been scientifically validated. Thus, best practices suggest distinguishing between technical processes and subjective interpretation.[74] Ultimately, expert witnesses should be cautious not overstate the soundness of their conclusions— and defense attorneys should be on the lookout for when this happens.

Once conclusions have been interrogated, attorneys can look to the quality of the witnesses' testimony.

E. Challenging the Testimony

A researcher reviewed the trial transcripts of 137 cases where people were convicted but later exonerated based on DNA testing. The researcher found that in 82 of these cases (nearly 60 percent) the prosecution's forensic analyst had provided invalid testimony in court—meaning their testimony either misstated empirical data or included conclusions that were unsupported by that data.[75]

When it comes to open source investigations, beyond the soundness of an expert witness' testimony, there is the threshold issue of whether a digital open source investigator should be considered a lay witness or an expert witness. Lay witnesses can only testify as to what they did or observed, while an expert witness may also share opinions and conclusions. For certain types of evidence, lawyers have different options for how to introduce such evidence at trial.

For example, graphology, otherwise known as hand-writing analysis, is an example of a comparative method that can be testified to by a lay witness or an expert. Such evidence can be

---

[74] Forensic Image Comparison and Interpretation Evidence: Guidance for Prosecutors and Investigators 2 (National Crime Agency, CPS, Metropolitan Police and Forensic Science Regulator 2016), (U.K.), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/912880/Image_Comparison_and_Interpretation_Guidance_Issue_2.pdf.

[75] Garrett, Brandon L., & Peter J. Neufeld, *Invalid Forensic Science Testimony And Wrongful Convictions*, 95 Virginia Law Rev., 1 (2009), https://www.virginialawreview.org/wp-content/uploads/2020/12/1-2.pdf.

introduced in three ways: either 1) a person who is familiar with the handwriting in question can testify to its validity; 2) a graphology expert can compare an unknown sample to a known sample; or 3) the two samples may be presented to the fact-finder (either judge or jury) to make their own determination about whether the two are likely from the same person. Similarly, comparisons made as part of a digital open source investigation can likely be introduced by an expert, a lay witness, or presented without analysis to the fact-finder to make their own determination. In many cases involving open source investigations, the best approach might be to simply share the collected photos, videos or satellite imagery with the fact-finders, and allow the fact-finders to make up their minds about whether two locations, objects, or people match.

In most jurisdictions, case law or statutory rules establish who can be considered an "expert" in legal proceedings and thus provide opinions related to the evidence. In the United States, the standards were established by the *Frye* (1923) and *Daubert* (1993) cases, and codified in Federal Rule of Evidence 702. Per that rule:

> A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
>
> **(a)** the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
>
> **(b)** the testimony is based on sufficient facts or data;
>
> **(c)** the testimony is the product of reliable principles and methods; and
>
> **(d)** the expert has reliably applied the principles and methods to the facts of the case.

U.S. case law establishes that the burden is on the proffering party to establish the admissibility of expert testimony to a preponderance of the evidence, while judges are responsible for excluding unreliable and unhelpful expert testimony. With regards to the practices they might talk about, *Daubert* lays out a nonexclusive, non-dispositive checklist that courts can use when

assessing reliability that includes whether the theory or technique has been tested or subjected to peer review and publication, and whether it has attracted "widespread acceptance within the relevant scientific community."[76]

Since digital open source investigators are often generalists, however, rather than masters of any particular forensic practice, a third issue concerns the potential scope of their expertise. Even if the investigator qualifies as an expert and can therefore provide opinions, it remains unclear as to what they can opine *on*. In war crimes cases, for example, a single video might contain images of aircraft, munitions, destroyed buildings, and dead bodies. Expertise in aircraft may be necessary to reliably determine the type of aircraft, while military experts might be needed to identify the munitions, whereas a medical forensic expert may be required to suggest the likely cause of death, and an architect needed to explain the likely cause of a building's collapse. Rarely will one person qualify in all of the areas of expertise about which many open source investigators might draw conclusions—for example, basing weapons identifications on information pulled from a video game or aircraft identification based on photos from Wikipedia.

As established above, in U.S. Federal Rule 702, expert testimony can be provided by someone "who is qualified as an expert by knowledge, skill, experience, training, or education."[77] Other jurisdictions have similar requirements. While a witness' expert status is often determined via training and education, lay digital investigators may nonetheless qualify as there are not yet many formal programs that provide training in open source investigation methods. The Federal Rules also provide that an individual may testify if his or her "scientific,

[76] Christine Funk, *Daubert v. Frye: A National Look at Expert Evidentiary Standards*, Expert Inst. (Aug. 9, 2021), https://www.expertinstitute.com/resources/insights/daubert-versus-frye-a-national-look-at-expert-evidentiary-standards/
[77] Fed. R. Evid. 702.

technical or other specialized knowledge will help the trier of fact to understand the evidence," the "testimony is based on sufficient facts or data," "the testimony is the product of reliable principles and methods" and "the expert has reliably applied the principles and methods to the facts of the case."[78] Interpretation of all of these prongs is relatively unsettled as applied to digital open source investigators and their methods. This leaves openings for attack—attacks that should be anticipated by the person testifying and others involved in the case's progression.

F. Challenging The Presentation

Finally, how digital open source evidence is presented in court, for example, via data visualizations that are packaged as demonstrative evidence, may raise serious concerns.[79] Demonstrative evidence—visual information that is aggregated, packaged and designed to aid the fact-finder(s) in understanding the geographic layout or other features of a crime or related event—is not evidence per se, but a visual aid designed to assist the judge or jury in their assessment of the actual evidence.[80] Such demonstrative evidence has historically consisted of charts and graphs. In the open source investigation context, they are often compilations of many types of data, ranging from videos to photographs to satellite imagery, and may include 3D reconstructions of crime scenes, including built and natural layouts.

---

[78] *Id*.

[79] *See* Sarah Zarmsky, "Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law," 19 J. Int'l Crim. L. 213 (2021) (discussing the strengths and weaknesses of introducing demonstrative evidence in international courtrooms); see also SITU Research, https://situ.nyc/research (last visited Aug. 21, 2021), as one example of such visualizations; See e.g., Forensic Architecture, https://forensic-architecture.org/ (last visited Aug. 21, 2021), as a second example of such visualizations; See also Alexa Koenig, *Open Source Evidence and Human Rights Cases: A Modern Social History*, *in* Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation and Accountability (Sam Dubberley, Alexa Koenig & Daragh Murray eds., 2020), for a brief history of the use of such visualizations in international criminal trials.

[80] *See, e.g.*, Working Draft: Practitioner Guidelines on the Use of Digitally Derived Evidence in International Accountability Mechanisms (Leiden University 2021): 43-49.

Since this "aid to visually link evidence" to the underlying facts of a case is merely supposed to assist a court's understanding of the evidence, it is not supposed to be treated as evidence itself.[81] However, there's a risk that such visual aids may be overly compelling and convincing, resulting in prejudice about how the facts of the case come together that even professional judges cannot undo—or of which they may be unaware.[82] This can be particularly damaging if, for example, a reconstruction or other compilation is based on faulty underlying information, or poorly interpreted or constructed.

While the underlying data—the individual videos and photographs that are evidence—must be introduced separately, the compilation may present and yet simultaneously obscure the underlying data. Not all data is equally reliable, so the individual data that comprise the whole might mislead, as might the compilation. Ultimately, the judge and jury may be unable to interrogate each part of a potentially persuasive or even prejudicial whole.

In addition, these reconstructions can be expensive, ultimately exacerbating equality of arms considerations between prosecution and defense. Finally, the demonstrative evidence may be constructed in such a way that it not only represents underlying facts but tells a story: it might fill in gaps or unknowns to make a narrative of events flow better, or establish a platform that enables the viewer to fill in gaps in their head that may take on a sense of being the "truth."

IV. CONCLUSION

At its core, the introduction of highly technical, scientific, or other expert evidence into legal cases raises several overarching concerns, including the difficulty of distinguishing experts

[81] Working Draft: Practitioner Guidelines on the Use of Digitally Derived Evidence in International Accountability Mechanisms (Leiden University 2021): 43.
[82] Waltraud Baier et al., *Introducing 3D Printed Models as Demonstrative Evidence at Criminal Trials*, 63 J. For. Sci., 1298 (2017); Rachael M. Carew et al., *A Preliminary Investigation into the Accuracy of 3D Modeling and 3D Printing in Forensic Anthropology Evidence Reconstruction,* 64 J. For. Sci., 342 (2018).

from convincing frauds; confusion caused by disagreements between experts; a lack of judicial training in the underlying methods and their vulnerabilities; and an exacerbation of equality of arms issues, especially when prosecutors are better resourced than the defense.[83] Under-scrutinized and unchallenged forensic science has led to serious miscarriages of justice in the past, and it is the responsibility of the current and next generations of legal professionals to ensure that the same mistakes do not unfold with digital open source evidence. While many of the digital methodologies that feed into criminal investigations can be promising additions to investigative toolkits, enthusiasm for these techniques should be tempered with healthy skepticism—and knowledge of the most helpful questions to ask about any open source investigative process.

This task is not easy, nor straightforward. The complexity of the online information environment—riddled with botnets, sock puppets, trolls, deepfakes and fake news, and operating at an almost unfathomable speed and scale—is simultaneously overwhelming and yet invaluable for identifying information that can contribute to justice and accountability. Our goal with this article has been to break down the very real vulnerabilities in digital open source investigations and encourage careful analysis of each component in order to make the risks more manageable.

Given the issues detailed above, we recommend that lay/third party investigators preserve content according to emerging forensic standards and take the extra investigative steps needed to properly document their investigative process. We also recommend the creation of clearer

[83] In addition to the resource differentials, junk science has often been found to benefit the prosecution more than the defense. *See generally* Aviva A. Orenstein, *Debunked, Discredited, but Still Defended: Why Prosecutors Resist Challenges to Bad Science and Some Suggestions for Crafting Remedies for Wrongful Conviction Based on Changed Science*, 48 SETON HALL L.REV., 1139 (2018), https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3712&context=facpub.

legal criteria for assessing the credibility of third party digital open source investigators. Without clear standards, we are likely to see a repeat of past judicial responses to scientific evidence—where judges were either overly impressed by the slick newness of the methods and thus failed to adequately evaluate the quality of the underlying data and methodologies, or were so unsure of how to evaluate the information that they failed to give it the weight it was due.

Witnesses should refrain from giving opinions on matters to which they do not have the proper expertise, while lawyers and judges need to be equipped to adequately ascertain the reliability and validity of digital open source information and the quality of its analysis. In the meantime, digital open source information should be triangulated with physical, testimonial, or other documentary evidence whenever possible, and not be allowed to stand on its own.

Ultimately, the January 6 siege on the United States Capitol is an excellent example of the power of citizen investigators to find and verify videos and images posted to social media and other websites to support official investigators like the FBI. The individuals who took to the internet to identify the rioters provided helpful eyes and ears in response to a potentially overwhelming volume of online content for law enforcement to sift through and analyze.[84] If conducted carefully and professionally, such lay investigations can offer tremendous value for fact-finding processes, including criminal proceedings.[85]

---

[84] Ryan J. Reily, *'Sedition Hunters': Meet The Online Sleuths Aiding The FBI's Capitol Manhunt*, HUFFPOST U.S. (Jun. 30, 2021), https://www.huffingtonpost.co.uk/entry/sedition-hunters-fbi-capitol-attack-manhunt-online-sleuths_n_60479dd7c5b653040034f749?ncid=other_twitter_cooo9wqtham&utm_campaign=share_twitter.

[85] *See generally* OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS & HUMAN RIGHTS CENTER AT BERKELEY LAW, BERKELEY PROTOCOL ON DIGITAL OPEN SOURCE INVESTIGATIONS 12-13 (2020), https://www.ohchr.org/Documents/Publications/OHCHR_BerkeleyProtocol.pdf.