CENSORSHIP THROUGH FORENSICS: VIDEO ANALYSIS IN POST-WAR CRISIS
Co-authors: Rebecca Wexler and Carey R. Murphey

I ABSTRACT

Amateur video shot on mobile devices worldwide is helping to hold authorities to account for war crimes, human rights violations, and other abuses of power. What happens when the authenticity of that video is in doubt? The possibility of justice depends on forensic investigators who sometimes shroud their tools and methods in secrecy, inhibiting reproducibility of their results and disabling scrutiny of their authenticity claims.

This chapter examines a forensics dispute over the authenticity of a leaked video depicting alleged war crimes in Sri Lanka, and argues that obstacles to reproducibility in forensic investigations of video evidence constitute preemptive censorship by suppressing potential critique. In this instance, secret, closed or proprietary tools restrict opportunities to contest video authenticity claims. In other words, they preclude counter-speech. Only with open tools and methods can publics contest the meaning of the video-speech.

More broadly, this case study suggests that the technological mediation of knowledge in the production of authoritative objective truth is a fertile arena for “new school” speech regulation. As digital information products become increasingly uncontrollable, effective censorship may nonetheless be possible by disrupting the tools and methods of analysis that produce meaning from widely available information. The cultural honorific of objectivity that surrounds science and technology makes that sphere a likely site for the manipulation of consensus-based public truths, and hence encourages obstruction of access to knowledge in the most profound manner. Citizen engagement in, and response to, this form of censorship will depend on publics’ ability to scrutinize expert claims. Widespread open access to tools for producing information, like video editing equipment, and decentralized participation in the creation of information products, like videos, may enable resistance.

To counter this form of preemptive censorship through forensics, we advocate transparent and reproducible investigative methods and technologies for forensic video evidence. In a dispute of any consequence, parties deserve the opportunity to question the methods behind expert testimony against them. In a public dispute touching post-war stability, as does the video authentication struggle examined in this chapter, the risk of censorship through meaning-manipulation becomes greater, and the need for open methods more urgent. Forensic methods of reducing video data to measurements, application of these measurements to a given case, and steps leading to conclusive opinions, should all be open to scrutiny.

II ARGUMENT

This chapter posits secret, closed, or proprietary forensic video tools and methods as material and procedural forms of censorship. Unruly digital information and accompanying cultures of transparency have increased reliance on material objects to perform the role of censor. Closed forensic video tools and methods produce censorship through two separate yet
related processes: first, they preclude counter-speech; and second, they annul the meaning of video in plain sight.

Closed video forensic tools and methods impose procedural and material obstructions to the reproducibility of investigative methods. These obstructions hamper or extinguish any possibility of external review and critique. Lack of external review in turn precludes contestation of authenticity claims. In other words, procedural and technological barriers to the reproducibility of experiments censor investigators on either side from engaging in counter-speech.

The power to censor also manifests in part through rendering incomprehensible that which is in plain sight. The idea here is to censor meaning, rather than to block the flow of information. As we move towards greater information transparency, this function to render meaningless information that has become uncontrollable may prove an increasingly significant mechanism for censorship.

To explore these ideas, this chapter analyzes video evidence of war crimes in Sri Lanka as a form of speech. We argue that closed, proprietary investigative tools and methods in video forensics inhibit external reproducibility and review, preclude counter-speech, and thus obstruct the process of making meaning out of video-speech. Forensic tools and methods that inhibit scrutiny and review act as prior restraints on counter-speech, and render incomprehensible that which is in plain sight.

We examined the forensic video analysis (FVA) reports on each side of a dispute over the authenticity of a video depicting war crimes in Sri Lanka. We found obstacles to the reproducibility of methods and results in investigations on both sides of the dispute, conducted by the U.N. and the Government of Sri Lanka (GoSL). These obstacles result from procedural actions on the part of investigators, and as well from material limits imposed by some of the proprietary software used in the investigations. These procedural and technological barriers produce censorship because they preclude counter-speech. This case study shows that process-oriented and substance-oriented censorship are inextricably intertwined. To preclude counter-speech to particular authenticity claims is in itself tantamount to substantive censorship.

Video evidence increasingly directs public opinion. Digital video resists censorship in certain respects because it largely defies containment. In the case at hand, the Sri Lankan video has been widely duplicated and broadly accessed. Yet, the standards to authenticate it are concealed. This concealment renders publics unable to know whether or not determinations of authenticity are incompetent. Here, obstructions to the reproducibility of FVA methods produce censorship because they annul communication of the meaning of a video in plain sight. The FVA dispute over the Sri Lankan video is a high stakes example of censorship in a regime of hyper-visibility.

To resist this “censorship through forensics,” communities engaged in disputes over video evidence should demand transparent, replicable forensic tools and methods that are open to scrutiny by all. We suggest development of FVA tools that use open methods, incorporating the opportunity for investigators to observe and analyze all levels of functionality. Finally, in the
specific case of the Sri Lankan video -- and notwithstanding the recent Reddit Boston Marathon bombing fiasco -- we further advocate crowd-sourced investigations into the videos’ authenticity. Open investigative methods, and crowd-sourced analysis of results, would facilitate a minimum level of peer-review that could help to unmask subtle defects, provide courts with newly efficient economies of scale, and further democratic legitimacy by reducing preemptive censorship of critique, and facilitating public debate. We suggest that the development of such a model of best practices would strengthen FVA standards more broadly, and enhance the ability of this emergent discipline to facilitate consensus.

II SCENARIO

On Tuesday, May 19, 2009, Sri Lanka celebrated the end of thirty years of civil war. Lieutenant General Sarath Fonseka, commander of the Sri Lankan army, announced, “We have liberated the whole country from terrorism.”6 The government of Sri Lanka (GoSL) had defeated the Liberation Tigers of Tamil Eelam (LTTE), an insurgent group designated a terrorist organization by the United States (U.S.) and thirty-one other countries.7 Sri Lanka’s High Commissioner in London proclaimed the defeat the first victory against terrorism in the modern age.8 Sri Lanka began to navigate a complex post-war scenario.

Yet, the celebratory narrative soon fractured. On August 25, 2009, Channel 4 News in the United Kingdom (U.K.) broadcast a video depicting men in Sri Lankan military uniforms shooting naked, bound prisoners in the head. Channel 4 acquired the video, approximately one minute long, from Journalists for Democracy in Sri Lanka (JDS), which in turn obtained it on condition of the total anonymity of its source.9 The video provoked pained public outcries, and became a focal point for frustration, mistrust, and controversy surrounding post-war self-making and national re-formation.

The unknown provenance of the video complicated efforts to authenticate it.10 Authenticity here refers to the veracity of the scene depicted in an image, rather than the integrity of the image itself.11 Without an unbroken chain of custody from an original and identifiable producer, speculation flourished about the circumstances of the video’s creation. Some believed that a Sri Lankan military soldier recorded the video on a cell phone while witnessing a war crime.12 Others suggested that the video might be a fictional scene produced with actors by a commercial film crew intent on discrediting the GoSL.13

Forensic analysts sought to resolve these speculations by examining the video file for traces of image manipulation. Digitally altered portions of a frame, or a match between the video file and the type of light sensor only present in large commercial cameras, would discredit the video as a cell phone recording of an historical incident. Absence of such manipulation, or a match between the video file and the type of light sensor only present in cell phone cameras, would support the opposite assumption of authenticity. Forensic investigators working on request of the United Nations (U.N.) found evidence of authenticity strong enough to warrant investigation into possible war crimes.14 Yet forensic investigators working on request of the GoSL found evidence that the video is either inauthentic or unverifiable.15 As a result, the GoSL declined to investigate the incidents depicted.16

On December 2, 2010, Channel 4 released a second, longer video of approximately five minutes in length, which appears to contain the contents of the first. U.N. investigators again found evidence of authenticity, while GoSL investigators again found evidence of fakery and declined to investigate the incidents depicted.\textsuperscript{17} Subsequent leaks of additional photographs and videos portraying similar scenes from other incidents did not alter the GoSL’s stand.\textsuperscript{18}

Meanwhile, controversy surrounding the initial videos continues.\textsuperscript{19} Accountability for possible war crimes, on the one hand, meets on the other hand a possible double standard as to which nations face such allegations in the first place. At stake is the GoSL’s ability to obtain foreign aid, in addition to its legitimacy in the eyes of its own population. The opportunity to construct a stable peace hangs in the balance.

\textit{Reproducibility and the Credible Authority of FVA Investigations:}

Scientific authority depends on reproducibility, or the plausibility of replicating an experiment. Experimental findings gain credibility when a different investigator, similarly equipped and following the same procedures, produces the same results.\textsuperscript{20} This ideal that scientific experiments should be replicable in principle underlies consensus-based construction of facts.\textsuperscript{21}

To be sure, public science policy today must balance principles of reproducibility against competing interests in restricting scientific transparency. On one hand, as historian Sheila Jasanoff has written, democracy mandates that the polity have some means with which to evaluate “knowledge claims that justify actions taken on its behalf.”\textsuperscript{22} On the other hand, peer and market competition, on which much scientific knowledge production depends, mandate a minimal level of secrecy around investigative methods and procedures.\textsuperscript{23} This chapter seeks to show that at this moment, in the specific and newly developing field of FVA, interests in reproducibility should outweigh interests in its proprietary restrictions.

Current FVA methods are inadequate. Strategies draw primarily on forensic techniques developed for digital stills. Still image digital forensics seeks to identify irreversible footprints of digital processing steps within an image, and then to reverse engineer these steps to reconstruct the circumstances of first-generation production of that image. Researchers thereby may attempt to determine the mechanical source of a still image, including the camera model and vendor, whether an image has been manipulated via cut-and-paste operations, and the processing history of an image.\textsuperscript{24}

Yet, leading researchers in the field caution that, “the peculiarities of video signals” thwart easy application of still image forensic techniques to FVA.\textsuperscript{25} Digital manipulation of a video may apply both to single frames, which appear twenty-four to thirty times per second, and to the temporal alignment of frames within a sequence. Video data is thus of a different order of magnitude from stills. Further, the high compression ratio of most video formats can erase footprints left by signal modification, making it difficult or impossible to reconstruct a video’s processing history.\textsuperscript{26} In short, FVA is an emergent discipline with unresolved issues.\textsuperscript{27}
At the same time, because digital video itself is both infinitely reproducible and broadly accessible, it throws an unprecedented burden on the authority claims of forensic analysis. Whereas with comparatively limited physical evidence like DNA or fingerprints, a small group of forensic investigators may be procedurally incompetent yet nonetheless have purchase on the best expertise, the same does not extend to video. For example, the Channel 4 videos are easy to view on television, and to circulate or download from the Internet. Decision-makers throughout publics and governments can access their own copies. As a result, they may be more likely to incorporate their own analysis into a determination of authenticity, rather than accept the conclusions of a forensic report on expert authority alone.

What is more, several competing paradigms exist beyond FVA for the authentication of video evidence. News organizations may triangulate verification from multiple sources prior to publication. Genre expectations can influence an individual’s trust in the veracity of an image. And individuals’ personal experience with the tools of video production, such as cell phone cameras and home editing software, contributes a broad base of technological literacy against which decision-makers may measure authenticity claims.

Reproducibility of investigative procedures is crucial to generate consensus in this environment of decentralized access and knowledge, competing authentication paradigms, and existing limitations within the FVA discipline. Rigorous commitment to the production of transparent investigative procedures, and technologies open to scrutiny, will both strengthen current FVA standards and also facilitate public trust in the future credible authority of FVA investigations.

Obstacles to reproducibility in the Channel 4 video FVA reports:

The forensics dispute between the GoSL and the U.N. began with an obfuscation of investigatory methods. On September 9th, 2009, GoSL forensic analysts sent the U.N. their conclusion that the video is a fake, but omitted documentation of the investigations that had produced this finding. The U.N. then repeatedly requested the full texts of their analyses, but GoSL investigators did not provide them until 2011, two years later. Unfortunately, procedural obfuscations and barriers to reproducibility only grew from here.

For instance, incomplete documentation regarding evidence preservation cast doubt on whether or not all of the investigators actually analyzed identical copies of the videos. Researchers may employ a cryptographic hash to verify their copy of a digital file. The hash algorithmically generates a number to uniquely identify the content of a digital file. Anyone who runs this algorithm and produces the same numeric identifier can determine that they have an unaltered copy of the file. Yet, none of the U.N. and GoSL FVA reports includes a hash.

At least one investigator attributed omission of the hash to the anonymity of the original videographer. True, a hash under these circumstances would not have established preservation of evidence from the first-generation source. Still, the unknown nature of the source does not excuse the omission. Rather, the opposite is true. Multiple second-generation sources for the videos under investigation mean a hash would have been particularly useful. A hash would have clarified whether or not all the FVA investigators were analyzing the same video files, which is a
prerequisite to reproducibility. Absent this foundational piece of information, none of the parties can challenge or accept the conclusions of the others. Skepticism as to whether all parties analyzed the same piece of evidence renders any consensus about its authenticity meaningless.

In fact, there are strong reasons to doubt that all the investigators did actually examine unaltered copies of the videos. In the first round of reports on the initial, shorter video, U.N. and GoSL investigators each described analyzing videos of different lengths, names, and formats, while GoSL investigator Chathura De Silva reported difficulty obtaining a copy of the video at all. De Silva eventually analyzed, “an available streaming media source on the Internet, which had been trans-coded several times and lacked most of the forensic features." Had a cryptographic hash been used, investigators would have known if they were analyzing fragments or the whole of the same piece of evidence or not, regardless of their source.

A second round of investigations ameliorated some of this confusion. This round followed release of an extended version of the video, approximately five minutes in length, which appears to contain the contents of the first. Christof Heyns, U.N. Special Rapporteur on Extrajudicial Executions, reports that he distributed this video to both U.N. investigator Jeff Spivack and to the GoSL. However, despite the promising start of a shared source, discrepancies abound. Spivack identifies the video file as, “SL1.3GP,” and sources it to Heyns. U.N. investigator Grant Fredericks identifies it by the same name, but sources it to Mr. Orest Nowasad from the U.N. Office of the High Commissioner for Human Rights, rather than to Heyns, and adds that it is five minutes twenty-five seconds. Two pages later, Fredericks changes his length approximation to five minutes twenty-four seconds. He also establishes that he will re-examine the initial, shorter video, which he first identified as one minute seventeen seconds but now claims is one minute fourteen and a half seconds. De Silva’s report matches Fredericks’s first declared length of five minutes twenty-five seconds, but identifies the file under investigation as, “SL1 Channel 4.3GP.” Finally, Evangelos Yfantis, a third GoSL investigator, describes analyzing two videos obtained from the GoSL, one in 3GP format and a second “downloaded from an internet broadcast site.”

Once again, use of a cryptographic hash would have neutralized these discrepancies by establishing continuity of the evidence across sites, time, and researchers. Instead, omission of the hash serves as a procedural obfuscation that allows inconsistencies to multiply in number and consequence. Altogether, the variances erode trust both in the competence of the investigations and in the meaning of their reports.

Spivack and Fredericks further contradict each other on the number of frames in each video. Both initially identify the second, extended video as containing 2411 frames. Yet, Fredericks later identifies the last image as, “Image 2410." Spivack indexes the shorter video as, “frame 1 – 542." Fredericks, on the other hand, calculates five groups of 100 frames, plus an additional group of 41 “images.” If images and frames are equivalent, which he does not clarify, this would mean that Fredericks calculates the shorter video to contain only 541 frames. Perhaps Fredericks began his index at zero, while Spivack began his at one. While this would be a relatively simple explanation, the reader must still hypothesize a solution to the discrepancies. Although for a difference of one frame it may be tempting to discard this as a trivial mistake, any concrete discrepancies provide grounds for doubt and dispute of the whole.

Doubt about whether the GoSL and U.N. analysts actually examined the same video files preempts meaningful consensus. Further, these discrepancies degrade the credibility of the forensic investigations as a whole. Weak forensic credibility leaves publics more likely to ignore or confuse any and all results, and to turn to alternative sources of authority such as their own personal experience.

Proprietary claims to investigative methods and tools also obstruct reproducibility of the Channel 4 forensic analyses. For instance, De Silva introduces his report by declaring, “The experimental procedures used in this analysis include techniques that have been developed … at the University… These techniques or their results may not be deployed … without appropriate permission.” The implicit suggestion is that some investigators may obtain permission, but not all. Those denied would also be denied the opportunity to scrutinize the full methodology and data behind De Silva’s findings.

Subtler yet also problematic, Spivack deploys proprietary Cognitech VideoInvestigator software in his investigation in a manner that inhibits external review, whether or not permission is given to analyze his broader experimental techniques. In so doing, Spivack produces three significant obstacles to reproducibility: black-boxing technical functions, risking procedural artifacts that could obscure rather than clarify the evidence, and presenting a mediated manipulation of evidence instead of the evidence itself. As a result, the authority of his report is based in part on preclusion of counter-scrutiny rather than the accountability of scientific peer review.

First, Spivack offers no explanation of how Cognitech software actually operates. He writes of one investigative action, “Cognitech VideoInvestigator software was used … apparent velocity estimation was calculated and the resulting data applied to a mosaic reconstruction utility to create a single panoramic still image from the video segment.” In other words, Cognitech proprietary software pieced together a series of video frames into one composite still image, called a mosaic reconstruction. Yet none of the data produced during the intermediary step of “apparent velocity estimation” is included, nor is there any reference to a functional definition of the mosaic method applied. Absence of such documentation black-boxes technical functions and inhibits external review of the stated interpretation.

Second, vaguely defined manipulation of the original image in this manner risks imposing artifacts and distortions on the video. These artifacts may obscure rather than enlighten the video’s forensic truth-value. To his credit, Spivack warns of this risk, writing, “As a normal consequence of [the] procedures … visual artifacts from the image boundaries are visible, as are variations in histogram values that present as differences in lighting and contrast in different regions of the images [Figure 1].” (De Silva, using a different mosaic reconstruction function with similar risk of artifacts, gives no such warning.) Had Spivack clarified the method, or even referenced a specific definition of the method, and shown a sample of the component images, a reviewer might be able to observe the effects and reason about them. Leaving an explicit trail of each step of the manipulation, documented for review, could also reduce the peril of mistaking procedural artifacts for relevant evidence. Absence of such transparency once again prohibits external scrutiny of the investigative procedure.

Third, performing the mosaic manipulation offered no clear benefits to Spivack’s analysis, raising questions as to why it was done in the first place. Spivack explains that his goal for the procedure was, “to produce a still image of the individual previously described … as wearing a ‘clean white shirt.’” Following production of the composite still, he concludes, “the white shirt has visible red stains.” Spivack offers no further data, reasoning or opinions about this mosaic manipulation apart from reproducing the resulting image [Figure 1].

In other words, the sole finding he generates is that red stains are visible on the white shirt in the image. Yet, it was not necessary to perform the proprietary velocity estimation and mosaic manipulation to reach that conclusion. Fredericks reproduces in his report a single frame of video, unaltered, in which the red stains are also readily visible [Figure 2]. In short, the findings presented – red stain visible – are disconnected from the means that supposedly achieved them – Cognitech mosaic manipulation. Proprietary software manipulations performed with neither clear benefit nor functional transparency mask the original evidence. Readers are able to reason about Spivack’s mediated manipulation of the evidence, but not about the evidence itself.

Figure 1
“Frame 804 – 816 Apparent Velocity Estimation Calculated Mosaic Reconstruction” (Spivack). The black rectangles along the top of the image are examples of image boundary artifacts.
An additional concern is raised when Spivack appropriately discloses that he is a beta tester and technical representative for Cognitech, Inc., the company that produces and sells the software he uses to perform these mosaic reconstructions. Professional conflict of interest poses a risk of bias toward applying this tool without clear benefit, and obscuring rather than illuminating the evidence. Commercial interest may conflict with disclosure of methods and algorithms. In the worst-case scenario, then, Spivack’s application of Cognitech mosaic manipulations promotes marketing rather than furthering the analytic conclusions of the investigation. Moreover, there is a continuing question of conflict of interest in the emergent field of FVA more broadly, if forensic software developers accumulate uncontested authority.

The report of GoSL investigator Evangelos Yfantis provides still clearer evidence of the urgency of conflict of interest protections for FVA software developers, and the exigency of transparency in investigative methods and technologies. Yfantis wrote his own forensic software for the purposes of the Channel 4 investigation. He then deployed it with far less transparency of function and purpose than Spivack did with Cognitech mosaic reconstructions.
For example, Yfantis developed a test to compare images of blood in the Channel 4 videos with representations of blood in a reference pool of images of known violent crime scenes. First, he obtained the set of reference images from The Metropolitan Police Department in the U.S. Then, he employed “self-developed in house computer software,” to extract the red, green, and blue planes from a digital image. Next, he measured the histogram of the red video plane, a graph of the frequency of red brightness values. The histogram shows peaks that identify the pixel brightness values that occur most often in the plane. Finally, he used “mathematical computations” to contrast the red histogram values of blood scenes in the two leaked videos with red histogram values of blood scenes in a series of reference crime scene photo and video images. Finding a significant difference, Yfantis deduces that blood depicted in the Channel 4 videos “is not real blood.” In other words, the difference in red histogram values between the leaked videos and his reference images leads him to conclude that the Channel 4 videos depict living persons wearing fake blood.

The investigative methods and technologies that Yfantis created and deployed lack even the most basic transparency necessary for external evaluation or experimental replication. Yfantis provides no information about the selection mechanism either for the pool of reference images, or for the individual frames of video analyzed. He provides no reporting of error measurement for his self-developed software. The report fails to state the controls of the experimental measurement, and the observed measurement error under those controls. In other words, readers have no way of knowing whether the measurement does in fact discriminate between real and blood substitute, or whether the software just reports measurement noise. Without this information, there is little to no opportunity for third parties to evaluate the accuracy of his techniques.

Unfortunately, the Channel 4 FVA dispute has failed to promote agreement among parties, and instead become yet another obstacle to reconciliation in post-war Sri Lanka. This chapter suggests that lack of disclosed methods, and analytic gaps between evidence and conclusions, in the FVA reports may have contributed to this outcome. That the problem of concealed methods appears in both the U.N. and GoSL FVA reports demonstrates a systematic weakness in the investigatory paradigm. Presentation of an experimental finding without explaining the mechanism by which it was achieved forces the audience into blind trust. Concealing investigative methods, and restricting access to investigative technologies, prevents others from challenging the accuracy of the results. It precludes reproducibility, and thus preemptively censors critique.

VI CONCLUSIONS

The opposing Channel 4 FVA reports, along with their varied public reception, raise fundamental questions both about the emerging field of video forensics, and about the technological mediation of knowledge in the production of authoritative objective truth. This case study illuminates the need for widespread access to tools for producing information, like video editing equipment, and highlights the urgency of decentralized participation in the creation of information products, like videos, in order to promote critical media and technological literacy. The value of such literacy extends beyond the value of any individual knowledge-
embedded good produced.\textsuperscript{67} Without such literacy, widely dispersed, the cultural honorific of objectivity that surrounds science and technology becomes vulnerable to the manipulation of consensus-based truths in public spheres, and hence obstruction of access to knowledge in the most profound manner. Such manipulation degrades not only the knowledge of specific content, but also the power of knowledge-producing methodologies, such as the scientific method, that when protected and applied at their best can help to cut through social and political bias.

By examining obstructions to reproducibility in the Channel 4 FVA reports, this chapter also raises a further question for review: What are the resources granted lay viewers to make judgments in this situation? This question is particularly urgent because no court of law has yet asserted control over the Sri Lanka war crimes allegations. As a result, these allegations are a trial primarily in the court of public opinion. In other words, public and governmental decision-makers, not judges or juries, comprise the target audience for the FVA reports. The judgments of these lay reviewers have consequence for post-war stability and foreign aid.

One possible answer, as law professor Dan Kahan has argued, is that lay and expert decision-makers alike arrive at judgments based on a wide variety of inputs, including political and identity alignments.\textsuperscript{68} Indeed, politics, identity, and lived experience in the Sri Lankan civil war, may wield particular influence in how viewers interpret the Channel 4 video. Author Rebecca Wexler recently returned from working in Sri Lanka as a Fulbright Senior Research Scholar investigating the dynamic between the country’s diverse media groups and post-war national re-formation. In a series of personal interviews conducted with Sri Lankan nationals, she found some individuals of both Sinhala and Tamil ethnic backgrounds who believe the videos are authentic, and others who believe that they are fake. One interview with M.V. Kanamaylnathan, editor of the newspaper \textit{Uthayan}, offered clarification. When asked about the authenticity of the Channel 4 videos, he answered, that the people who believe the video are the people who have witnessed similar atrocities “with their own eyes.”\textsuperscript{69} Kanamaylnathan told Wexler that he lives inside his newspaper compound in constant fear of assault. He said he has not left its premises in years. Kanamaylnathan’s observations support Kahan’s proposal that factors other than methodological rigor and transparency wield substantial influence over the reception of scientific information.

Yet, recognition that multiple factors, including lived experience, may play a role in lay viewers’ reception of the Channel 4 forensic reports does not justify restricting lay access to scientific methods and results. Rather, it makes such access all the more urgent. While eyewitness experience is an important and probably ineradicable factor, consensus should benefit from better tools than personal experience alone.

We advocate removing limits to reproducibility in the Channel 4 FVA investigations for three reasons: the infinitely replicable nature of the video evidence, the crucial role that peer-review plays in the public authority of science, and the volatile nature of this particular dispute. For the same three reasons, we further advocate crowd-sourced investigations into the authenticity of the video evidence. Greater access to knowledge of FVA investigative methods, and greater literacy in the tools of video production and editing, could advance the ability of lay members of the Sri Lankan public and the international community to act as a quality check on

FVA investigations. Hopefully, open participation in the process of authentication will enable future consensus-based production of public truths in Sri Lanka and around the world.

1 Rebecca Wexler is a documentary filmmaker, co-founder of the Visual Law Project and Fellow of the Information Society Project at Yale Law School, who recently returned from work as a Fulbright Senior Research Scholar in Sri Lanka. Carey R. Murphey is a frequent contributor to open source software, and currently a forensic scientist at White Oak Labs Inc. in Houston, Texas. The authors thank Kiel Brennan-Marquez, Robert Crusz, Dan Kahan, Eli Omen, Lisa Larrimore Ouellette, and Nagla Rizk for providing generous feedback on earlier drafts.


3 There is growing recognition of the need for more rigorous standards for inclusion of scientific and technological information in litigation. See Jackson v. Pollion, No. 12-2682, at 8 (7th Cir., Oct. 28, 2013) (“The legal profession must get over its fear and loathing of science.”).

4 Forensic experts, forensic tool vendors, and courts should all participate in increasing transparency. Experts should disclose a reproducible basis for each opinion, which cannot occur without transparent methods. Vendors should provide, at a minimum, a sound scientific basis for the interpretation of results conveyed to courts. Finally, courts should have the ability to compel disclosure of investigative methods.


10 It remains difficult to seek to establish veracity of a video using blind methods that do not depend on prior knowledge of the video’s source. Investigators may seek to conclusively determine whether compression artifacts, such as spatial frequencies skewed by quantization, are consistent or inconsistent with expected values. E.g. I-Chuan Chang et al., *A DCT Quantization-Based Image Authentication System for Digital Forensics*, PROCEEDINGS OF THE FIRST INTERNATIONAL WORKSHOP ON SYSTEMATIC APPROACHES TO DIGITAL FORENSIC ENGINEERING (SADFE’05, 2005), and Babak Mahdian & Stanislav Saic, *Blind Authentication Using Periodic Properties of Interpretation*, 3:3 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (Sept. 2008).


16 See U.S. DEPARTMENT OF STATE, supra note 11, at 16 (“The State Department is not aware of any action by the GSL …establishing an independent investigation into the Channel 4 videos.”).


See Lasanda Kurukulasuriya, Channel 4 unravelled, lies unpacked, The Sunday Times (Aug. 7, 2011) (reporting on a video produced by the GoSL in response to Channel 4, arguing that allegations of war crimes and media evidence in support were manufactured in the West), available at http://www.sundaytimes.lk/110807/Columns/Lasandak.html, and SRI LANKA MEDIA WATCH, APPALLING JOURNALISM, Nov. 2011 at 23-24 (reporting that the videos may have been filmed with a video camera rather than a mobile phone, and suggesting that they may depict LTTE cadres performing executions while wearing Sri Lankan military uniforms and speaking in Tamil), available at http://www.engagesrilanka.com/mediawatch.html.

See generally The Editorial Board, Holding Sri Lanka to Account, THE INTERNATIONAL N.Y. TIMES, Feb. 4, 2014. See also PERMANENT PEOPLE’S TRIBUNAL & THE INTERNATIONAL HUMAN RIGHTS ASSOCIATION - BREMEN, PEOPLES’ TRIBUNAL ON SRI LANKA, Dec. 2013 (considering both video and photographic forensic evidence, often together with eye witness accounts of torture or rape. These accounts put the forensic analysis in a broader perspective of similar events in series, which the report concludes to be state sponsored patterns of directed violence.).


In an early precursor to crowd sourcing during the seventeenth century, European scientists began to report rich circumstantial details to encourage readers to envision and explicate experimental scenes that they did not directly observe. See Steven Shapin, Pump and Circumstance: Robert Boyle’s Literary Technology, 14:4 SOCIAL STUDIES OF SCIENCE 481, 483 (Nov. 1984) (“Boyle proposed that matters of fact be generated by a multiplication of the witnessing experience.”). Historians Steven Shapin and Simon Schaffer have termed this process, “virtual witnessing.” STEVEN SHAPIN & SIMON SCHAFFER, LEVIATHAN AND THE AIR-PUMP: HOBBS, BOYLE, AND THE EXPERIMENTAL LIFE 60 (1985). Within that model, “the constitution of matters of fact,” they point out, “involved the multiplication of witnesses.” Id. at 20.


Id. at 22.


For instance, Derek Bousé argues that most wildlife films operate according to formal dramatic conventions, rather than scientific criteria, because the neutral objectivity that is the goal of scientific observation would never survive the ratings-driven television market. Yet, Bousé also points out that filmmakers conceal this fact in order to achieve documentary appeal. Derek Bousé, False Intimacy: Close-Ups and Viewer Involvement in Wildlife Films, 18:2 VISUAL STUDIES 123-32 (2003).


Both the U.N. and GoSL reports do make an initial assessment of the metadata annotations held in an 'outer' container of the video file format, completely separate from the ‘inner’ containers holding the video and audio streams. While this might appear to be a test of integrity, it is not. The reports acknowledge that the outer container metadata is easily manipulated without a trace, and thus invalid for the purpose of any conclusive interpretation of video data properties, and not a substitute for the hash function. See Appendix to ALSTON, Addendum, supra note 27, at 9 (“It is theoretically possible to alter or delete metadata in a multimedia file, so the metadata contained in the file submitted for analysis cannot be considered absolutely conclusive with respect to accuracy or containing all possible file attributes.”).

Jeff Spivack, telephone communication with author Rebecca Wexler, Jan. 2013.

In the first round of reports on the initial, shorter video, U.N. investigator Grant Fredericks analyzed a one minute seventeen second file named “massacrevideo.3gp,” sourced to a London Times reporter. HEYNS, Addendum, supra note 14, at 451. Yet Journalists for Democracy in Sri Lanka (JDS), the earliest known source in the chain of custody, provided the authors with a one minute seventeen second video named “VideoDJ.3GP.” JDS assured the author that this file is “exactly the same original file received from Sri Lanka,” and maintains that the original video was in 3GP format. Bashana Abeywardane, JDS convener, email communication with author Rebecca Wexler, Feb. 22, 2013. “VideoDJ.3GP” is also the name of the file that U.N. investigator Jeff Spivack examined, sourced to JDS via the U.N. Appendix to ALSTON, Addendum, supra note 27, at 2. Yet, GoSL investigator Siri Hewawitharana analyzed an AVI and QuickTime formatted video of slightly over one minute two seconds. Id. at 268. GoSL investigator Chathura DeSilva analyzed a video of one minute twenty-five seconds. Annexes to LLRC Report, supra note 9, at 157.

Annexes to LLRC Report, supra note 9, at 157.

Id., Addendum, supra note 14, at 425.

Id., at 430.

Id., at 451.

Id., at 453.

Id., at 453.

Annexes to LLRC Report, supra note 9, at 159-160.
Spivack writes, “Frame by frame analysis of the 2411 video frames for content was conducted using Cognitech Video Investigator and Elecard StreamEye.” HEYNS, Addendum, supra note 14, at 434. Fredericks concurs that the extended video contains 2411 frames. Id., at 453.

Annexes to LLRC REPORT, supra note 9, at 158.

Crime lab forensics may prefer commercial forensic tools because they provide third party support for the credibility of methods. Yet preference for such tools also creates an incentive for investigators to fit their investigation of the data to the tool, rather than the reverse. Open-source forensic tools could help to resolve this issue by allowing investigators to customize tools to the specific problem they are investigating.

Annexes to LLRC REPORT, supra note 9, at 174.

Heyns, Addendum, supra note 14, at 438.

Id., at 439.

Id., at 438.

Id., at 460.

Id., at 439.

Id., at 460.

Annexes to LLRC REPORT, supra note 9, at 300.

Appendix to ALSTON, Addendum, supra note 27, at 1.

Spivack appropriately obtained peer-review of his methodology and conclusions prior to publication, yet there are no references to any publication of the methods or algorithms applied. Further, one of the two reviewers was also an employee of Cognitech, Inc., and therefore may also have exhibited a conflict of interest. HEYNS, Addendum, supra note 14, at 443.

Annexes to LLRC REPORT, supra note 9, at 219.

Id., at 219.

For an excellent overview of theories of access to knowledge and knowledge-embedded goods, see ACCESS TO KNOWLEDGE IN THE AGE OF INTELLECTUAL PROPERTY (Gaëlle Krikorian & Amy Kapczynski eds., 2010).

Dan M. Kahan et al., The Polarizing Impact of Science Literacy and Numeracy on Perceived Climate Change Risks, 2 NATURE CLIMATE CHANGE 732-735 (2012) (suggesting that scientific information is more likely to persuade listeners when framed according to their political and identity self-interests).

M.V. Kanamaylnathan, interview communication with author Rebecca Wexler, September 2012. Audio recording on file with the author.