A Counter-Forensic Audit Trail: Disassembling the Case of *The H8ful (CM)8*

Matthew Fuller & Nikita Mazurov

It's always good to start with a scandal, and all the better if it is one that consists of celebrity outrage, appropriation of goods, and some slippery file-transfers. In the middle of such a scandal is where this article ends up, but it is also one that aims to trace some of the conjunctures that form it and by which it plays out. In order to do so we draw on resources in recent research that uses forensics as both a set of techniques, and as a complex of approaches and attunements in novel ways. We argue that this conjuncture allows for an understanding of the posthumanities as inviting a deepened relation between the enquiries into meaning and of power characteristic of the humanities, and the imaginary and composition of the technical, a form of culture often reduced to being the implementation of scientific knowledge. Technology however has numerous complexes and possibilities of its own. This multiple quality is of special interest at a time when digital technologies are recognised for their articulation and amplification of cultural and social forces.

The particular "object lesson" presented here is the leak of a "screener" file of the 2015 film *The Hateful Eight* by Quentin Tarantino. A watermarked copy of the film intended for pre-distribution circulation to film-award judges was leaked prior to the film's general release and became a highly popular download. The case, and a subsequent tranche of files leaked from Sony, create the opportunity to map a micropolitics of leaks, and of the forensic and counter-forensic moves being made within and around such files. The volume and variety of the

information available on this case make it an opportune point of investigation. This article develops an approach that, by working through technical details and the structures and techniques of control they point towards and entail.

One of the consequences of such an approach is what, to some, may seem like an over-attentiveness to such detail. An argument often made in areas such as Software Studies, proposes the close reading of technical objects as one necessary means of understanding digital culture. The attentiveness is an attempt to recognise how what may commonly pass below the threshold of critical interpretation may be consequential. The past few years' sequence of revelations from figures such as Edward Snowden, and around Facebook and other systems, only confirm this. We therefore beg the readers' indulgence --and attentiveness -- during some of the passages in this text that may read with a certain dryness as we examine various technical and legal documents, and the video files themselves. We want to suggest here that such approaches may contribute to a wider way in which the Posthumanities address and work through the technical as a key site of contemporary culture. Such attentiveness to small-scale material differences also characterises work in contemporary versions of forensics, to which we now turn.

Forensics and Counter-Forensics

Cultural materialism is being contributed to by what Eyal Weizman (2014) suggests is an increasing attention to forensics, a way in which the history and handling of an artefact or event can be approached through assaying it as a set of material and medial traces, and in which the differences between matter and media become moot, as matter more broadly becomes seen - through the forensic imagination - as a storage and inscription device for events such as chemical

leaks, missile impacts, the residue of human bodies. Weizman proposes a post-architectural practice that firstly sees buildings and settlements as sites of inscription. Such projects aim to open up the question of what constitutes the forensic, returning it to the notion of the forum through gathering publics around bodies of evidence. In this rendering, forensics involves the establishment of documents that operate as forums and intervene into decision-making systems such as those of the law.

In order to make such an opening however, it needs to operate at other determining scales. A collection of photographs may be analysed according to what they depict, but also as form of measuring device that can be calibrated via an analysis of the microscopic effects of media. For instance, using the scale of a pixel at a certain resolution, at a certain distance from the source of light, to provide an unit of measurement. Such measurement can then be triangulated to the size of a certain object, for instance the dust-cloud following an explosion. (Schuppli, forthcoming). Here, there is a concurrence with an earlier proposal from literary theorist Matthew Kirschenbaum that the "forensic imagination" is activated whenever "process collapses into product" (2008: 253) and where "storage, inscription and instrumentation" (2008: 254) afford capacities for the elicitation of a certain kind of trace. Such traces have a particular double quality. We can call them - following the Dutch word - "spoor", a term that is appropriate in the sense of meaning both waste or superfluous material, and (train) tracks.

Spoors' efficacy in forensics is because of the additional meaning or information that they provide that is more than that for which they are designed. As tracks, they are both traces in the sense familiar from deconstruction and the work of interpretation, but they are also tracks – technical entities that keep things running along fixed, programmable, lines. The spoors traced

in classical forensics call upon objects as witnesses. Bones become recording devices for the presence of poisons or bullets, but may also be notable for their placement or displacement. Things act as witnesses by being acted on, and acted in. Such "material witnessing", as Susan Schuppli calls it, elaborates a subtle relation to what has accreted as the past by working through how substances act as condensed spoors of social, ecological and chemical events and processes. Forensics is thus concerned with the movements between the patterns of presence or absence of certain deformations and the capacities for arranging detectability of such patterns and deformations. Tracking the logics of their interactions provide a means for ascertaining the event that they endow with being and as part of which they manifest. Counter-forensics, we will suggest below, is concerned both with this, and with the means of interfering with the question of detectability. It moves between the two aspects of the spoor, as trace and as track, figuring out how for different subject positions, for different systems, the one might act as the other in a concatenation of interpretation and formation.

Does forensics in this mode deal in proofs or in evidence as forms of spoor? By making the question of producing the forum and of testing the nature of the forum at its core it does not abjure, but rather tends to lay to one side, the question of proof. In working to develop and elicit evidence it recognises that any forensic interpretation and significance is part of a wider set, that of epistemic systems, such as law, media, human rights, various forms of politics, by means of which, and by virtue of the procedures proper to them, it may in turn gain the status of proof. The question of what constitutes a proof is in turn subject to a range of variable and mobile regimes, which include law, but also automated systems that monitor, filter and inspect the circulation of data. The doubled nature of the spoor, that it is both track and trace characterise

much of computational media systems. Forensics and counter-forensics in such systems concern us here.

The question of the capacity to arrange detectability is fundamental to the forensic domain. In such a context, the evidential function of technologies explicitly designed to bear witness is of particular significance. In this article we show that the proliferation of forensics includes the development of forms of technology that pre-structure objects in order to make them more susceptible to tracing. The challenge for the design of systems and the interfaces between complexes of systems for eliciting or producing spoors, arranging detectability and controlling the registration of an entity or a trace, and the means for assigning the actuality, probability, or likelihood of a trace-bearing relation between things and processes is one of making such traces operate in a self-authenticating way; one that speaks of their own veridiction. In Keenan and Weizman's (2012) account of the forensic analysis of the skull of Mengele, such a challenge was arrived at through what might be called a rhetoric of the thing, in which the bones are called upon to speak by the theatrical means proper to a court of law. In digital conditions, such a rhetoric can be analysed in part by the *exigencies* of software and of data[i]. Such conditions in turn are worked on and worked into by the operations of counter-forensics.

Counter-forensics is of two kinds. Firstly, it include measures to mitigate against the possibility of being traced. Counter-forensics thus generates sets of side-steps and moves that obscure, render unanswerable and prepare materials and processes for interrogation in advance. There is a resonance here with the mode of "black transparency" formulated by the design group Metahaven (2016) in their work on and for Wikileaks, where mechanisms for the achievement of a form of transparency are established by means of encryption and attention to the security that

in turn may be mobilised in attempts to *speak leaks to power*. Secondly, counter-forensics also includes techniques for the tracing of a process of tracing as it occurs, or after the fact. It is an art of recognising the composition of systems, artefacts and processes in relation to their ability to exact the toll or tribute of the spoor from things that pass through them.

Method

In this article we will draw on counter-forensics with an aim to improve aspects of its practice. We examine a recent high-profile case of a leaked video file to map the forensic operations that are both embedded in the file and that operate on it once it is found to be in illicit circulation. We also map the way that forensic techniques concatenate out from the file and from their implementation as preventative and deterrent measures that are built into and arrayed around cultural objects. In order to trace these processes we examine: the video file itself, publically available leaked documents from a number of companies involved in the case, news coverage of the video leak, legal documents, patent documents and corporate brochures advertising forensic techniques and services.

"Following the object" is a method developed in social science, through the work of investigators such as Kopytoff (1986: 64-91) and Lash and Lury (2007), who trace the social force fields that an object bears traces of and that it may transform. As objects designed to act as witnesses to their own misappropriation, the particular materials and techniques that we follow here are unusual in that they are configured to allow for particularly precise kinds of following to occur. That precise following however is not a matter of formulating a public or bringing a forum into being, rather it is a means of closing down dissemination channels for digital media

objects and an attempt at providing inbuilt means to trace the movement of data outside of permitted channels. Indeed, the forensic techniques we will discuss are specifically invented to be sold as measures against what Ravi Sundaram (2015) has called the "circulation engine" of contemporary digital media. This circulation engine is an "unanticipated media ecology" (Sundaram, 2015) in which the spread and storage of official and unofficial documents, files, recordings and other media outstrips the means to both control and to understand it. The objects we study in this article are part and parcel of such a condition. These objects, and the technologies that intervene in them are products of a double movement. On the one hand they exist through digital circulation, on the other, they aim to trace and make difficult, if not impossible, any such circulation, and to render the *post-facto* punishment for involvement in circulation more likely or seem to be so.

In this condition, what we see is that the object is also implicated in sets of anticipated reactions to it and preparations for it. Forensics, as a means of tracing and controlling the movement of digital objects, also enters into them: in visual marks, sound features, timestamps and metadata that may or may not be hidden from the user. Forensic ordering has moved into the very presentation surface of a video file. It also becomes manifest in a set of techniques, regulations and documents, in addition to legal processes and social structures, that are each responsive to certain aspects of the task of forensic control. In the work presented here, we make use of grey media such as forensic manuals, patent applications, company marketing materials, court documents, and trade journals. Grey media are the soul of culture in the contemporary moment, and provide substantial guidance in how to navigate the torsions of the forensic (Fuller and Goffey, 2013). Here, counter-forensics may also operate as a direct critical practice, tracing

both how the statements that act as a forensic argument or component of an argument may come to be made and how eliciting the spoors that they leave in the entities that come under their control may also come to be contested.

Posthumanities and the technical

The emphasis on the forensic contributes to the discussion of the posthumanities in that it exemplifies certain ways in which the operations of the humanities and sciences begin to overlap in terms of their objects of knowledge and the inter-relation amongst the kinds of rigour being employed. This question of communication between kinds of rigour is important, and plays out differentially and generatively in different contexts. In turn it has its own forensic dimension in that it refers to the way in which the means by which an argument or set of proofs are made tends to offer different capacities of resistance to or concurrence with different forms of enquiry attuned to the matching of certain patterns or traces. What it also points to however is that when the location of veridiction or of witnessing moves outside of being simply the property of the knowing subject, and is also found in artefacts, files, timestamping systems, and other things that must be attended to, there is a complex realignment of knowledge and action underway. Such a move is echoed in the development history of computer architectures. Humanist accounts of computing tend to emphasise technology as a means of extending or enhancing what are understood as relatively stable human capacities. These have been important inspirational drivers in the development of technologies such as the Graphic User Interface, the World Wide Web (Berners-Lee, 2000), and Object-Oriented Programming (Fuller and Goffey, 2014). Alongside such accounts however, we can read the history of computing to suggest a way in which humans

increasingly operate as part of informational complexes of which they are an important sub-component, but by no means the central radiant core.

The forensic imagination, in Kirschenbaum's sense, is also a point where, in order to navigate such a condition, previously *technical* knowledge tends to come to the fore. Not simply as a prerogative of nebbishes tucked away in the backrooms of museums or laboratories, but as constitutive of the kinds of knowledge formation that arise when epistemic environments are significantly technological. The technical becomes an intermediary and mobile scale by which other scales are articulated, traced and composed. Nietzsche's (2015) critique of the Prussian education system condemns its role in producing merely technical underlings of an empire, and in critical theory the critique of the technical as the epitome of instrumental reason is well circulated to the point of being an autonomic response. One emollient for such a condition is the way in which the notion of the technical itself is troubled by the forms of knowledge pouring into and reconstituting forensics as a field. The artists, architects, designers, and video-makers whose work is gathered in the *Forensis* volume (Forensic Architecture 2014) employ aesthetic means as modes of forensic analysis. In these cases, the visual sensitivity and training of art schools becomes the technical regime that elicits witnesses who deliver allusive and precise answers. Much of this arises out of attention to minor modes of media – for instance the way in which the processing of images used as evidence results in their degrading or enhancement, the movement from colour to black & white, cropping, the accretion of metadata, the way in which each image becomes part of a mosaic aesthetic of fragments articulating the passage of events through referral to common points of reference (such as arriving at a time of an event, and of an image, via triangulation of the length of shadows across multiple images) all cases in which the

detectability of patterns of detectability themselves come to the fore. These tendencies point to a further aspect of the posthumanities' re-articulation of the technical, in that they tend to recognise the ways in which technologies become points of negotiation, or arise as more or less apt consolidations of tensile relations that might also be described in social and cultural terms. In the case of this article, elements that are designed to have unilateral functions in the control of digital artefacts can also be read and manipulated at a tangent to such purposes if sufficient care is paid. In order to show this, we turn to the trace functions of Digital Rights Management.

The Trace Function

Contemporary forensic techniques in the area of digital media seek to cope with the ever-increasing dispersal of cultural bodies of work and the disintegration of the intellectual property regimes that accompany them. Forensic practice calls not merely for the addition of digital fetters such as Digital Rights Management (DRM) techniques into digital objects and systems, but also the introduction of a unique identifier into each copy of an object, so that its source may be identified after a leak has taken place. In other words, that a given object may escape its technically and legally delineated confines is taken into account prior to the object's initial controlled distribution..

DRM constitutes a broad, "effort to impose power through technology" (Benkler, 2016: 25), such as via the imposition of video playback control mechanisms into web standards (Benkler, 2016: 25), to give but one example out of many (see, e.g. Doctorow et al., 2005). Watermarking and DRM can both be said to function as "[v]ideo protection techniques" (Diehl,

2012: 10), which are in turn "technological tools that enforce excludability of information goods, which otherwise would be public goods" (Diehl, 2012: 10). Our focus here will be on a counter-forensic unraveling of the forensic deployment of watermarking for purposes of source identification. Techniques such as DRM which aim to technologically block the unauthorized distribution of content are augmented in the contemporary forensic landscape with tactics reminiscent of isotopic tracking[ii] which focus on identifying the source of a leak so as to deter future leaks; namely, the forensic practice now often known as *traitor tracing*.

Notably, early taxonomies of forensic fingerprinting[iii] make no mention of an explicit 'traitor' class, instead only delineating the existence of distributors (who supply the content), users (who are authorized to view the content), and opponents (who make "unauthorized use of objects" (Wagner, 1983: 18)). While it is acknowledged that an object may go astray via a user, no specific designation of this sub-class of user is made. The explicit introduction of the term 'traitor' as a particular kind of user who facilitates the access of unauthorized users to given content appears only years later (Chor, 1994: 257-270).

Traitor tracing techniques embed information such as a serial number, (which may in turn relay additional intelligence such as timestamps, location, and source name) within target content (e.g. a film or an ebook) which would in turn facilitate the ready identification or tracing of the originating source of the content, should it appear in an unauthorized distribution channel. If, for instance, a copy of a television show is found to be uploaded to a file-sharing site, and was not knowingly uploaded by the content controllers themselves[iv], traitor tracing would allow for the possibility of identifying where that particular copy of the show originated, so that action may be taken against the source. Though traitor tracing mechanisms may differ in the minutiae of their

operations[v], the underlying commonality of the forensic trace imperative is its ultimate reliance on a binding function. Not only must a unique identifier such as a serial number be embedded somewhere in the target content, but the identifier must explicitly point to a user. The tag must be bound to a source (Diehl, 2012: 36). Despite the fact that a preponderance of content leaks do apparently originate from industry insiders[vi], a traitor trace—whilst ultimately leading to an authorized user—may nonetheless not indicate that this particular user is actually responsible or liable for the leak. For instance, a scenario can readily be imagined in which someone slips an internal document out of someone's briefcase: traitor tracing would lead to the owner of the briefcase (and the document), not to the interloper. Thus while forensic investigators are certainly keen to "assure the reliable tracing of true traitors and avoid framing innocents" (Liu et al., 2005: 9), the potential for the underlying fallibility of the process of trace identification must be kept in mind. Binding is thus not a *de facto* assurance of leak identification and neutralization, particularly in scenarios where the traitor is not within the class of authorized users, and further procures copies from a disparate non-static array of authorized sources (e.g. selecting a new briefcase from which to take documents each time).

Traitor tracing is interesting as a cultural technique in that it identifies a particular object, and attaches an implied authorised user to it on the understanding that the user can be traced should an infraction be mapped back onto it. The technique compensates for the ready dissemination of digital objects in computational networks and implies a disposition of cultural and technical objects *towards* their users. Equally, what the analysis of this particular case makes clear is that alongside the tracing of users and files, techniques and processes are

themselves subject to related forms of tracking and registration via legal forms of the description of interests and ownership.

The Hateful Eight Screener Leak

On December 20, 2015, a copy of director Quentin Tarantino's most recent film, *The Hateful Eight* (2015) materialized online. We can call this Event Alpha[vii]. On December 22, 2015, *The Hollywood Reporter* (*THR*) announced in an exclusive[viii] story (Belloni) that sources had informed them that the source of the leak, or at least the originating copy from which the leak was based, had been identified (Event Beta). The traitor had thus seemingly been traced in less than three days of the content being disseminated. We can undertake a case study of the forensic trace function by conducting a counter-forensic audit trail of the two events. This audit trail will attempt to answer the question of how Event Alpha potentially led to Event Beta via an examination of publicly-available source material (e.g. the leaked content and peripheral materials), news reports, legal documents such as court dockets, patents and patent applications, and finally, leaked confidential corporate documents and internal forensic reports.

While there have certainly been prior legal cases explicitly dealing with the traitor tracing of pre-release cinematic content leaks (see, e.g. United States v. Russell Sprague, 2004; Warner Bros. Entertainment Inc. v. Innovative Artists Talent and Literary Agency Inc. et al., 2016), the depth of analysis afforded by the various and diverse materials pertaining to the leak of *The Hateful Eight* provides the opportunity to construct an unusually extensive counter-forensic audit trail. In other words, given the unique breadth of source documents that have entered the public domain by various means, this case can become particularly illustrative of the potential of

counter-forensics for both revealing and contesting normalised legal forensic narratives and their binding of objects, processes and ideas. It should also be noted that in spite of various subsequent screener leaks in the years following the *Hateful Eight* leak, there have been no visible cases of leaker apprehension, thus suggesting that while there are indeed various cases of screener traitor tracing, they are either not particularly common or not brought to light.

Furthermore, as this case garnered significant media attention and presumable public exposure, the possibility exists that it contributes to a chilling effect on the unbridled dissemination of cultural output, with individuals being afraid to share, for instance, cinematic content for fear of being apprehended for doing so. Such a chilling effect may be demonstrated via the fact that Hive-CM8, the group ostensibly behind the leak of *The Hateful Eight*, subsequently stated "As for Hateful Eight Movie: We feel sorry for the trouble we caused by releasing that great movie before cinedate even has begun. we never intended to hurt anyone by doing that, we didnt know it would get that popular that quickly [...] we wont do another movie before its cinedate, and we def wont go up to 40 as planned, we think we have done enough already" (Hive-CM8, 2015c; Washington, 2016). Thus, a counter-forensic audit trail of the traitor tracing of this particular leak may also function as a foil to the chilling effect the news of a film that was freely shared being traced may have. The unbridled dissemination of content is by no means irrevocably bound to traceability and identification.

An audit trail is simply a "record of system activities to enable the reconstruction and examination of the sequence of events" (Committee on National Security Systems, 2006: 4), generally conducted by forensic examiners (Holley et al., 2010: 76). A counter-forensic audit trail is then a record constructed to disassemble black-boxed forensic events to discover how

they may have occurred (and thus how they may be stymied in the future). In other words, the counter-forensic audit trail examines how a traitor may have been traced, and how future traitors may preempt the forensic trace function by sidestepping the processes which may have come to light during the counter-forensic audit.

Event Alpha was initiated via the uploading of a release[ix] entitled The.Hateful.Eight.2015.DVDScr.XVID.AC3.HQ.Hive-CM8. The release name more or less[x] follows standard conventions that collectively compromise what is known as the release or directory name (Maigret and Roszkowska, 2015: 59), here deploying the specific nomenclatural format:

Title.PublicationYear.Source.VideoCodec.AudioCodec.QualityDenotation.RipperName-GroupAffiliation

From the release name one can decipher that this is a high quality rip of the film *The Hateful Eight* (2015), with the video track encoded with the XviD video codec and the audio track encoded with the AC3 audio codec, sourced from a DVD screener and released by the ripper known as Hive, who is affiliated with the torrent tracker CM8 (a tracker abbreviation for the tracker CrikeyM8). Here, we can see that there is an act of at least ostensive self-identification at the end of the file name.

A DVD screener is an advance, pre-retail copy of a film distributed by studios to parties such as retail merchants or theatre owners (sales screeners), as well as award judges (award screeners) and, at times, film critics (Kroon, 2010: 586). The screener format developed since not all relevant parties could make the special screenings studios organise for new films, necessitating a more portable solution (Guttman, 2015: 226). Following theatrical and

specialized screenings, screeners were deployed via 'For Your Consideration Screenings' showing on a cable TV channel called Z Channel, starting with Francis Ford Coppola's film *The Conversation* (1974) (Guttman, 2015: 227-230). By 1987, screeners were mailed out by publicists on video tape, though they initially included only select scenes rather than the entire film (Guttman, 2015: 547-548). The supposition advanced by news outlets (see, e.g. Khatchatourian, 2015) is that *The Hateful Eight* release in question is sourced from a screener intended for Oscar voters for award consideration, (Leading the release to be classified as an *Academy screener*, a sub-type of *awards screener*, a sub-type of screener.) Today, the Academy screener is viewed by Academy of Motion Picture Arts and Sciences members as a status symbol, demarcating privileged in-group access and membership (Kilday, 2016: 40). The NFO file[xi] accompanying the Hive-CM8 release, however, merely states that this is "DVDScreener 1 of 40" (Hive-CM8, 2015a), and makes no mention of it being sourced from an Oscar-consideration screener. The lack of specificity may be intentional to withhold information that would help identify the source, the result of a lack of knowledge as to that source, or simply a by-product of neglect. What can thus be ascertained, assuming the validity of the release name which may alternately be either a deliberate or unintentional misattribution, is that the Hive-CM8 release is a screener, albeit of uncertain sub-type.

Though screeners have more recently been depicted as quite the caterpillar in the studios' buttermilk (see, e.g. Grossman, 2004: 361-382), to the point where their propensity for being pirated is even highlighted in the standard industry dictionary definition (*viz.* "[s]creeners have historically been a potential source of pirated material" (Kroon, 2010: 70)), discussions of the historical introduction of the concept of screeners tend not to broach the piracy issue, instead

stressing the advantage of a screener in allowing people to become aware of a film's existence (Guttman, 2015: 226-230, 547-548). The apparent potency of piracy has, over time, led to the film industry attempting to adopt various coping strategies ranging from ceasing to distribute screeners altogether (Valenti, 2003), to the deployment of screeners on Flexplay DVDs which oxidize within a set amount of time (e.g. 48 hours) of being taken out of the packaging, rendering the disc unreadable (*Business Wire*, 2004)[xii].

A further aspect of the film industry's attempts at exercising control over screener distribution pivots around the use of watermarks that uniquely identify the recipient of each screener somewhere within the screener itself (Diehl, 2012: 36-37). Watermarks may be broadly classified as being overt or covert (Cox et al., 2008: 5-6), here referring to the viewer's knowledge of a watermark's presence, as well as being either perceptible or imperceptible (Ford et al., 1999: 300), referring to the ease of the viewer's ability to detect the watermark. Overtness may thus be read as a measure of the viewer's awareness of a watermark's existence, whilst perceptibility is a more fine-grained measure of being able to actualize such awareness into actionable detection. The watermark may be overt and perceptible, for instance by inscribing the recipient's name over various frames in the film—thus making the fact that a given work is watermarked both explicitly known to, and readily detectable by, the viewer—which has led in several cases to celebrity personalities being identified as having their screener copies leaked (see, e.g. Fleming, 2011; Gardner, 2014). Conversely, the watermark may instead be covert and imperceptible, with the watermarks neither being readily detectable nor their presence advertised, and the personally identifiable information thus not being immediately apparent to the viewer—who is in this instance further unaware of its being embedded in the media in the

first place—but being readily discernable to the content controllers (Keegan, 2005: B6; Munoz and Healey, 2004). Overt/covert and perceptible/imperceptible watermarks are not necessarily mutually exclusive, with a screener potentially including either, both or neither, mode of watermarking. That is to say, it may be overtly known (by way of an expository disclaimer, for instance) that a screener is watermarked, but said screener could contain both readily perceptible and also imperceptible watermarks.

While covert and imperceptible watermarks may strive for unobservability[xiii] in the service of facilitating streamlined traitor tracing, the role of counter-forensics is to render these processes observable and detectable so as to facilitate the unlinking of any 'traitor' from the leaked content. A subsequent aim of counter-forensics, as is highlighted throughout the given case study, is to contest the forensic claim of being resistant to counter-forensics. In other words, by rendering the forensic trace function detectable or perceptible, paving the way for its removal or manipulation, counter-forensics contests the efficacy of forensic claims of detectability—effectively deploying forensic practices in the service of their own undoing.

Turning now to Event Beta, the aforementioned *THR* article notes that the Hive-CM8 release has been linked to one, "Andrew Kosove, co-CEO of production-finance company Alcon Entertainment" (Belloni, 2015), who had allegedly been sent the screener for awards consideration. The FBI, writes *THR*, was able to identify Kosove as the intended recipient of the screener based on a watermark found on the DVD[xiv]. The *THR* article does not, however, go into any further explication of how the particular watermark was manifest. This information-gap lead to us conducting a counter-forensic audit trail for the purposes of this article. The *THR* article mentions that the *Hateful Eight* DVD that included (some sort of) watermark technology was

manufactured by Deluxe (Belloni, 2015). Deluxe, a large-scale production, post-production, distribution and asset management enterprise (Deluxe Entertainment, 2015a), is apparently trusted by movie studios as "a central bank for their assets" (Keegan, 2005: B6). Deluxe's 'Security Services' website indeed mentions that Deluxe provides "advanced security tracking & reporting", comprising "[s]earch, retrieval and forensics reporting service for pirated content, including cams, telecines, screeners and retail Blu-rays and DVDs", as well as further offering "advanced watermarking and encrypting services" (Deluxe Entertainment, 2015b), thus making Deluxe part of a crowded marketplace of video watermarking providers.[xv] Much like the *THR* article, the Deluxe site does not provide further detail about its watermarking and forensic reporting services. Deluxe's corporate 'about us' page states that "Deluxe knows media" (2009), but likewise refrains from explicitly detailing their watermark operations, albeit stating that "Deluxe successfully launched FCT anti-piracy watermarking technology [in 2003]" (2009). Although Deluxe's own websites do not appear to expand upon the meaning of the FCT acronym, third party sources are more forthcoming, relaying that FCT stands for Forensic Coding Technology (Filmlab, n.d.; Keegan, 2005: B6) .

Whilst news and other third party sources provide a modicum of information, more intelligence is provided via an analysis of leaked documentation. In a leaked presentation entitled "SecureCinema™ Digital Screener Platform" (Deluxe, ca. 2013-2014[xvi]), Deluxe candidly reveals that FCT is a "patented, proprietary watermarking technology", with each copy of a film being "recorded with a hidden and unique watermark" such that, curiously, "no visual artifacts are added to the picture", with the system already having "led to multiple prosecutions". From this, we can say that FCT watermarks can be both covert and overt and do not add visual

artifacts to the video stream. This means that FCT video watermarks function not via the usual modus operandi of the addition of information[xvii], but via the subtraction thereof.

In April 2015, Wikileaks published over 170,000 internal emails from Sony Pictures. An examination of "privileged and confidential" emails sent between Sony executives and Deluxe employees included in this leak, further reveals that Deluxe periodically informs Sony whether a given leak of a film had either "FCT Picture Codes" (e.g. Solon, 2014) or "FCT Sound Codes" (e.g. O'Dell, 2014), thus indicating that FCT watermarking may be both audio- and video-based. The presentation makes mention that the Deluxe subsidiary dealing with content protection, Deluxe Content Protection Services, is based in Toronto. An analysis of an edition of the Canadian *Trade-marks Journal* further reveals that the terms "FCT Data" (Deluxe Laboraties, Inc., 2008a), "FCT Sound" (Deluxe Laboraties, Inc., 2008b), and "FCT Film" (Deluxe Laboraties, Inc., 2008c) were all filed as trademark applications by Deluxe Laboratories, Inc., wherein they were described as being for the service of, e.g., "encoding of audio recordings and sound for use in tracking the source of unauthorized copies thereof" (Deluxe Laboraties, Inc., 2008b), thus lending further evidence to the probability that Deluxe's FCT system operates via the watermarking of both the audio and visual streams of a film.

The original *THR* article further mentions that a "'Web Watch' report [was] produced in response to the leak and shared with THR" (Belloni, 2015), albeit failing to explain what a WebWatch report entails. Although *The Hateful Eight* WebWatch report could not be obtained, a prior WebWatch report sent by Deluxe to Sony for the film *Fury* (2014) was located as an e-mail attachment in leaked corporate correspondence (Jaquez, 2014). The "Watermark Recovery Report" includes a six-digit Watermark ID for both the video ("picture") and audio ("sound")

tracks, as well as the name and ID (which corresponds to the watermark ID) of a "D-Cinema Server" (Deluxe, 2014: 1). The meaning of the server field may be gleaned by turning to additional documentation. Recalling that Deluxe's "SecureCinema™ Digital Screener Platform" presentation mentions that its FCT watermarking technology is patented, a search was performed to identify possible patents and patent applications filed by Deluxe or its subsidiaries. Two relevant patents were found during this discovery stage. The first patent application submitted, filed in 2003 and published in 2005, appears to discuss the aforementioned standard mode of coded symbol-based visual watermarking, a method for incorporating into film frames "images or patterns that appear as unobtrusive defects or artifacts" (Clark and Wary), specifically constituting "a pattern of small, unobtrusive specks" (Clark and Wary). However, as the Deluxe presentation explicitly stated that "no visual artifacts are added to picture" (Deuxe, ca. 2013-2014: 17), it would seem that this was an early prototyping of Deluxe's watermarking technique, as opposed to a mechanism currently in use, at least under the FCT banner. A patent filed in 2004 and published in 2006 (Dewolde), and reissued in 2015 (Dewolde), proposes a video watermarking scheme in which objects in a given frame are themselves augmented, wherein "[i]t is preferred to do this by enlarging an image slightly so that one or more edges of the image is moved relative to the same edge in the video master" (Dewolde, 2015). Given that this technique is in accord with the dictum that no visual artifacts are *added* to the video, as only existent images are manipulated, it would thus seem that this patent is that covering the 'FCT Film' components of Deluxe's FCT watermarking schema. Recalling the mention of the server name in the sample WebWatch report, the patent further notes that the altered (watermarked) video is stored on a given 'modification' server after it is encoded and watermarked from the

master copy on the master server. Thus, the aforementioned server name in the WebWatch report may presumably identify which modification server the given copy of the film was stored on.

A second patent, filed in 2007 and issued in 2008 (Mossman and Wary), deals with the "FCT Sound" component of Deluxe's watermarking scheme and proposes a method for watermarking audio tracks not via the addition of extraneous audio artifacts, but via the removal of existent ones. Specifically, "the analog soundtrack is altered by selectively muting portions of the analog soundtrack at the selected location for the insertion of the identifiable code" (Mossman and Wary, 2008).

Whilst the patent literature is thus more explanatory than Deluxe's official web-facing material and news sources, more explication still may be found in legal proceedings. In 2010, the Swiss company Medien Patent Verwaltung AG filed a complaint in US courts stating that Deluxe had infringed on its (American) anti-piracy watermarking patent, alleging that Deluxe had manufactured film prints which employed Medien's anti-piracy techniques (Medien Patent Verwaltung AG v. Warner Bros. Entertainment, Inc. et al.). Amongst other documents Deluxe filed a reply memorandum contesting Medien's claims which was in turn denied by the court (Medien Patent Verwaltung AG v. Warner Bros. Entertainment, Inc. et al., 2014), centering around the fact that since its audio watermarking system functioned around the subtraction of information not its addition, that its own patent did not infringe upon Medien's patent which only discussed 'markings', not their removal (Medien Patent Verwaltung AG v. Warner Bros. Entertainment, Inc. et al., 2012b). During the course of the various court dockets, however, Deluxe divulged further information about the inner workings of its FCT sound watermarking

procedure, including sample images of watermarked film prints with portions of the film's audio track being obfuscated to create "mutes or micro-second cancellations" (Medien Patent Verwaltung AG v. Warner Bros. Entertainment, Inc. et al., 2012b: 8). In another court docket Deluxe crucially revealed that "[i]mportantly, these codes are hidden in sound effects so that they are not noticeable to the audience" (Medien Patent Verwaltung AG v. Warner Bros. Entertainment, Inc. et al., 2012a: 13). The information extracted from these legal proceedings reveals that the FCT sound watermarks operate via the deletion of micro-second durations of parts of a film's audio track, and may likely occur during sound effects in the soundtrack, so as to attempt to mask their perceptibility.

This audio watermarking patent, however, is designed for forensically marking analog as opposed to digital audio tracks. In fact, the patent explicitly states that in instances where a film otherwise uses a digital audio track, the watermarked portions of the track nonetheless require switching over to an analog audio track[xviii]. This specificity in turn paradoxically opens up a number of possibilities regarding the watermarking of our sample case: that Deluxe deploys alternate technique(s) of audio track watermarking more suited to the digital medium such as echo hiding or spread spectrum coding[xix]—though if so, said techniques do not appear to be patented by Deluxe in contrast to their other audio-visual watermarking techniques which have explicit patents (though Deluxe may deploy watermarking approaches patented by third parties); that Deluxe may use analog film sources to make digital copies of screeners for distribution—as seems to be at least a possibility based on, admittedly dated, company presentation materials (Bergman, 2005: 6)—thus allowing them to use their existent analog method of audio watermarking at a point in the screener production workflow prior to the creation of the digital

screener discs, (although such a workflow would require the expenditure of additional resources in the form of producing analog audio tracks for each eventual screener copy); or, that Deluxe for at least some digital screeners does not use audio watermarking at all, relying instead solely on visual watermarking, as the patent for the latter describes the visual method of selective cropping as being suitable for the "unique encoding of each of a substantial number of distribution video copies" (Dewolde, 2015: 1), and (in not necessitating that an analog source be used) is compatible with digital video sources.

The significance of the ambiguity over audio watermarking for our purposes is that the presence of an audio watermark is then by no means guaranteed. Thus if no audio watermark is found, it may be due to it simply not being present.

Back to the Hive

Returning to the Hive-CM8 release of *The Hateful Eight*, the accompanying NFO file notably states that "[a]ll digital watermarks are removed, were quite a lot even had to crop 10 lines to get it done safely" (Hive-CM8, 2015a). If indeed the originating source of the leak was identified via a watermark present in the release, then it stands to reason that Hive did not in fact successfully remove all the watermarks. Aside from the afore-delineated FCT audio-visual watermarks based on micro-second audio track muting permutations and shifts in object positioning (the presence of which may be made overt via a deterrent disclaimer), respectively, screener copies are also -- as previously mentioned -- commonly watermarked with static visually overt watermarks present throughout the frame with statement akin to 'property of… for promotional/awards consideration only'.

Visual analysis of the video file The.Hateful.Eight.2015.DVDScr.XVID.AC3.HQ.Hive-CM8.avi (Hive-CM8, 2015b) readily reveals an incomplete attempt at overt watermark removal; specifically, the descender[xx] remnants of some sort of visible text message may be seen periodically throughout the duration of the film by simply viewing the AVI file.

~~>>>>INSERT FIGURE ONE HERE~~

Figure 1. Visible descender remnants, left over from a partial overt watermark excision attempt (with arrow emphasis added).

Specifically, the watermark descender remnants appear consistently at approximately ten minute intervals (+/- 10 second drifts), starting at 00:14:22.092 and ending at 02:34:45.357, with each instance lasting for a duration of approximately 14 seconds. If each watermarked copy of the screener had an overt watermark message appear at different intervals (with accompanying differing temporal drifting) and/or for different durations, then the visible watermark remnants may be sufficient to conduct a successful traitor trace, rendering the potential FCT sound/video watermarks irrelevant. Furthermore, if the partially-cropped watermark contains personally identifiable information akin to a name or serial number, the spacings between the visible descender remnants may likewise have been analyzed by Deluxe to find a successful match. Ascertaining whether Deluxe also deployed their FCT video cropping watermarking technique on the screener would entail comparing the screener copy to a later retail or commercial release of the film.

Doubting Veracity

Of course the counter-forensic audit trail undertaken here assigns a presumed truth to the statements expressed in the *THR* article regarding the use of the watermark to identify the original intended recipient of the source screener. The information relayed in the article, however, may solely be an attempt to instill fear, uncertainty and doubt in future pirates, endeavoring to discourage the free sharing of future screener copies, whilst the potential source of the screener may have simply been identified via other means entirely (e.g. by an informant familiar with the source of the file). Finally, recall that it is unclear whether the article erroneously refers to the DVD itself as containing the watermark(s), not the actual AVI file, or

whether this instead amounts to an unintentional slippage, betraying that Deluxe indeed had access to the source DVDR from which the Hive XviD AVI encode was made[xxi]. While this question of the particular source that was analyzed by content controllers in their performance of the traitor trace function may not appear to be immediately relevant as an effective digital watermarking scheme, it would mean that the watermark was sufficiently robust to survive being encoded from one video standard (the DVDR MPEG-2) to another (the AVI XviD MPEG-4), and thus would be present in both versions. It is nonetheless a critical point for two reasons. Firstly, its non-relevance is predicated upon the assumption that Hive-CM8 were not successful in removing the watermark(s) from their encode, whereas perhaps they actually were. Secondly, given that the source DVDR was not openly digitally distributed like the AVI, if Deluxe was indeed able to analyze the source DVDR, this would point to their having insider access to the release group's internal servers. The question of the source is here of pivotal importance -- not necessarily due to questions around the watermark, but instead due to questions of access. However, these musings are entirely hypothetical without openly-available answers. The underlying outcome is that the counter-forensic audit trail, *much like the forensic trace figuration itself* which it strived to disassemble, is provisional and ongoing.

Conclusion

In this case, the forensic means of bringing an entity, the released screener file, to the public inspection of the forum is interwoven with the other case of forensics, that of the construction of the conditions of traceability, the control mechanisms built into material culture. Forensics in Weizman's discussion of the term is a wide means of eliciting spoors that are out in the world, in

the recording and storage capacities of coded and unencoded matter, in triangulating the relations between entities and processes and the spoors that they leave as a remainder. Forensics then takes these entities and capacities for detectability and draws their relations into a process of becoming public, in documents, court materials, testimony and curation, each in turn with its own processes of articulation and capacities for action and reflection. We can say that this is a mode of forensics that starts with the development of means of pattern-recognition, and moves towards the state of pattern-revelation. Counter-forensics is a complementary movement in that it exists by and through the means by which the conditions of traceability are established and rendered slow, troubled, indecisive, or inoperative. The counter-forensic audit is a means of tracing and articulating the conditions of composition of such disturbances to forensics and its systems of implication, a technological approach that takes inversion as the grounds for invention.

As a mode of posthumanities' engagement with technologies, counter-forensics is exemplified by the way in which it takes the composition of matter and means of encoding as a wider field of action in which the work of art, becomes merely a means for the agglomeration of other kinds of spoor. The clotting of technologies that it takes to stabilise something like the film as a form of property, are in turn ramified by and woven into economic conditions that are troubled and worked around by the technologies of leaking and re-routing. The double movement between forensics and counter-forensics operates in part in the conditions of asymmetry between public knowledge and private data silos that in turn articulate patterns of detectability. Developing techniques for inhabiting and leakily-thriving in the torsions exerted by such circumstances is characteristic of the technical sensibility of the conditions that in turn

register as the posthuman. The astute compiler of contradictions will of course observe that there is a certain catch here, that the field of techniques that implies both the leak and the watermark - the state of fluidity of files, and that which imprints upon such liquid – there is a certain similarity between the kinds of actors involved such that they cannot readily be reduced to the identity of the sufferer and of the exerciser of power. Indeed, when it comes to leaks, we find that not only are the tools related, but so too are the persons, where day job and night work conflictually intersect. As such, despite a certain aridity in the vernacular of some of its sources, the counter-forensic audit trail is thus something of a thriller in itself.

Biographical Notes:

Matthew Fuller is author of books including 'How to be a Geek, essays on the culture of software', Polity 2017 and 'How to Sleep, the art, biology and culture of unconsciousness', Bloomsbury, 2018. He is Professor of Cultural Studies at Goldsmiths, University of London.

Nikita Mazurov is a researcher interested in posthuman counterforensics; exploring the intersection of privacy and piracy--specifically in the necessity of the latter for ensuring the former.

Contact info: cup01nm@alumni.gold.ac.uk

Corresponding Author Postal Address:

Matthew Fuller

Media Communications and Cultural Studies

Goldsmiths

London

SE14 6NW

email: m.fuller@gold.ac.uk

References

Andy (2015) The Hateful Eight and The Revenant screeners leaked online. *TorrentFreak*. Available at: https://torrentfreak.com/the-hateful-eight-and-the-revenant-leaked-online-151221/.

Antonellis, Darcy et al. (2007) "Motion Picture Anti-Piracy Coding". Patent No. US7206409B2.

Barr, Merrill (2015) 'Supergirl' pilot leak: Theft or CBS marketing ploy?. *Forbes*. Available at: http://www.forbes.com/sites/merrillbarr/2015/05/22/supergirl-pilot-leak.

Belloni, Matthew (2015) ‘Hateful Eight’ pirated screener traced back to top Hollywood executive. *The Hollywood Reporter*. Available at: https://www.hollywoodreporter.com/news/hateful-eight-pirated-screener-traced-850899.

Benkler, Yochai (2016) Degrees of freedom, dimensions of power. *Daedalus* 145(1): 18–32.

Bergman, Steve (2005) ‘DCI Spec & the Deluxe Motion Picture Content Value Chain’. Deluxe Presentation. International Broadcasting Convention. Available at: http://www.edcf.net/edcf_docs/IBC%202005%20Bergman%20Deluxe%20Presentation.pps.

Berners-Lee, Tim (2000) *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web*. New York: Harper Business.

Business Wire (2004) Thomson provides studios assistance with security services on VHS and DVD screeners for 2003 ACADEMY AWARD season. *Business Wire*: February 16 2004. Available at: http://www.businesswire.com/news/home/20040216005143/en/Thomson-Studios-Assistance-Security-Services-VHS-DVD.

Byers, Simon et al. (2003) Analysis of security vulnerabilities in the movie production and distribution process. In: *DRM '03 — Proceedings of the 3rd ACM Workshop on Digital Rights Management*.

Chor, Benny et al. (1994) Tracing traitors. In: Desmedt, Yvo G. (ed) *Advances in Cryptology — CRYPTO '94: 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994. Proceedings*. Berlin: Springer-Verlag.

Committee on National Security Systems (2006) *National Information Assurance (IA) Glossary*. CNSS Instruction No. 4009.

ContentArmor (2018) Company profile. *ContentArmor*. Available at: https://contentarmor.net/company-profile/.

Cox, Ingemar J. et al. (2008) *Digital Watermarking and Steganography (Second Edition)*. Burlington: Elsevier.

Craig, Paul (2005) *Software Piracy Exposed*. Rockland: Syngress.

Cvejic, Nedeljko and Seppännen, Tapio (2008) *Digital Audio Watermarking Techniques and Technologies: Applications and Benchmarks*. Hershey: Information Science Reference.

Deer, Tova Rabinowitz (2016) *Exploring Typography (Second Edition)*. Boston: Cenage Learning.

Deluxe (2009) Us. *Deluxe Archive Solutions*. Available at: http://www.ruscom.com/deluxe/us.html.

Deluxe (ca. 2013-2014) SecureCinema™ Digital Screener Platform. Presentation. Available at: https://wikileaks.org/sony/docs/05/docs/Anti-Piracy/Screeners/Deluxe_SecureCinema%20v2.pdf.

Deluxe (2014) Watermark recovery report: Fury | FRY007. Available at: https://wikileaks.org/sony/emails/emailid/201910#email_raw.

Deluxe Entertainment (2015a) What we do. *byDeluxe*. Available at: http://www.bydeluxe.com/what-we-do.html.

Deluxe Entertainment (2015b) Asset management. *byDeluxe*. Available at: http://www.bydeluxe.com/what-we-do/asset-management/security-services-practices.html.

Deluxe Laboratories, Inc. (2008a) FCT data. *Trade-marks Journal* 55(2813): 128–129.

Deluxe Laboratories, Inc. (2008b) FCT sound. *Trade-marks Journal* 55(2813): 129.

Deluxe Laboratories, Inc. (2008c) FCT film. *Trade-marks Journal* 55(2813): 130.

Dewolde, Jeffrey H. (2006) "Program Encoding and Counterfeit Tracking System and Method". Patent No. US20060015464 A1.

Dewolde, Jeffrey H. (2015) "Program Encoding and Counterfeit Tracking System and Method". Patent No. USRE45406E.

Diehl, Eric (2012) *Securing Digital Video: Techniques for DRM and Content Protection*. Berlin: Springer-Verlag.

Doctorow, Cory (2007) Warner TV person: I deliberately leaked our pilot episode. *Boing Boing*. Available at: https://boingboing.net/2007/08/03/warner-tv-person-i-d.html.

Doctorow, Cory et al. (2005) Digital rights management: A failure in the developed world, a danger to the developing world. *International Telecommunications Union, ITU-R Working Party*

6M Report on Content Protection Technologies. Available at: https://w2.eff.org/IP/DRM/drm_paper.pdf.

Duffield, David Jay et al. (2006) "Theater Identification System Utilizing Identifiers Projected onto a Screen". Patent No. US20060262280A1.

Filmlab (n.d.) Piracy control. *Filmlab.* Available at: http://www.filmlabindia.com/services/security/.

Fleming, Mike Jr. (2011) Pirated 'Super 8' print points back to Howard Stern Show. *Deadline*. Available at: https://deadline.com/2011/08/pirated-super-8-print-points-back-to-howard-stern-show-154608/.

Fleming, Mike Jr. (2014) Quentin Tarantino shelves 'The Hateful Eight' after betrayal results in script leak. *Deadline*. Available at: https://deadline.com/2014/01/quentin-tarantino-hateful-eight-leak-novel-669066/.

Ford, James et al. (1999) Classification and characterization of digital watermarks for multimedia data. In: Furht, Borko (ed) *Handbook of Multimedia Computing*. New York: CRC Press.

Forensic Architecture (eds) *Forensis: The Architecture of Public Truth*. Berlin: Sternberg Press.

Fuller, Matthew and Goffey, Andrew (2013) *Evil Media*. Cambridge: The MIT Press.

Fuller, Matthew and Goffey, Andrew (2014) The unknown objects of object-orientation. In Harvey, Penny et al. (eds) *Objects and Materials: A Routledge Companion*. London: Routledge.

Gardner, Eriq (2014) Oscars host Ellen DeGeneres linked to leaked 'Walter Mitty' screener. *The Hollywood Reporter*. Available at: https://www.hollywoodreporter.com/thr-esq/oscars-host-ellen-degeneres-linked-669909.

Google News (2015) "Hateful Eight screener link" search query. Available at: https://www.google.com/search?safe=off&tbm=nws&q=hateful+eight+screener+leak (accessed 28 December 2015).

Greenwald, Glenn (2015) *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. London: Penguin.

Grossman, David G. (2004) Screening the screeners. *IDEA - The Journal of Law and Technology* 45(3): 361–382.

Guttman, Dick (2015) *Starflacker: Inside the Golden Age of Hollywood*. Beverly Hills: R. Guttman Associates.

Hayles, Katherine N. (1999) *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*. Chicago: University of Chicago Press.

He, Xing (2012) *Signal Processing, Perceptual Coding and Watermarking of Digital Audio: Advanced Technologies and Models*. Hershey: Information Science Reference.

Hive-CM8 (2015a) The.Hateful.Eight.2015.DVDScr.XVID.AC3.HQ.Hive-CM8.nfo.

Hive-CM8 (2015b) The.Hateful.Eight.2015.DVDScr.XVID.AC3.HQ.Hive-CM8.avi.

Hive-CM8 (2015c) The.Big.Short.2015.DVDScr.XVID.AC3.HQ.Hive-CM8.nfo.

Holley, James O. et al. (2010) Electronic discovery. In: Casey, Eoghan (ed) *Handbook of Digital Forensics and Investigation*. London: Elsevier.

Irdeto (2018) About us. *Irdeto*. Available at: https://irdeto.com/about-us/about-us.html.

Jaquez, Sean (2014) "FW: UPDATED NEW SOURCE WATERMARK RECOVERY: Fury #FRY007 | no rls group | Cam". Email. Available at: https://wikileaks.org/sony/emails/emailid/201910.

Keegan, Terence (2005) The code expands - Deluxe broadens watermark use beyond awards screeners. *Variety* 398(4): B6.

Keenan, Thomas and Weizman, Eyal (2012) *Mengele's Skull: The Advent of a Forensic Aesthetics*. Berlin: Sternberg Press.

Khatchatourian, Maane (2015) "'Revenant,' 'Hateful Eight' screeners leak to huge piracy before theatrical release. *Variety*. Available at: https://variety.com/2015/film/news/hateful-eight-revenant-leak-watch-online-1201666010/.

Kilday, Gregg (2016) The other truth about Academy membership. *The Hollywood Reporter* 02.19.16: 40.

Kirschenbaum, Matthew (2008) *Mechanisms: New Media and the Forensic Imagination*. Cambridge: MIT Press.

Kopytoff, Igor (1986) The cultural biography of things: Commoditization as process. In: Appadurai, Arjun (ed) *The Social Life of Things: Commodities in Cultural Perspective*. Cambridge: Cambridge University Press.

Kroon, Richard W. (2010) *A/V A to Z: An Encyclopedic Dictionary of Media, Entertainment and Other Audiovisual Terms*. Jefferson: McFarland & Company.

Lash, Scott and Lury, Celia (2007) *Global Culture Industry: The Mediation of Things*. Cambridge: Polity.

Liu, K. J. Ray et al. (2005) *Multimedia Fingerprinting Forensics for Traitor Tracing*. New York: Hindawi Publishing Corporation.

Maigret, Nicolas and Roszkowska, Maria (eds) (2015) *The Pirate Book*. Ljubljana: Aksioma - Institute for Contemporary Art.

MarkAny (2018) About us. *MarkAny*. Available at: http://www.markany.com/eng/markany-company/.

Medien Patent Verwaltung AG v. Warner Bros. Entertainment, Inc., Technicolor Inc., and Deluxe Entertainment Services Group, Inc. (2010) Case No. 10 Civ.IV 4119. Complaint and Demand for Jury Trial.

Medien Patent Verwaltung AG v. Warner Bros. Entertainment, Inc., Technicolor Inc., and Deluxe Entertainment Services Group, Inc. (2012a) Case No. 10 Civ. 4119 (CM). Memorandum of Law.

Medien Patent Verwaltung AG v. Warner Bros. Entertainment, Inc., Technicolor Inc., and Deluxe Entertainment Services Group, Inc. (2012b) Case No. 10 Civ. 4119 (CM)(GWG). Reply Memorandum.

Medien Patent Verwaltung AG v. Warner Bros. Entertainment, Inc., Technicolor Inc., and Deluxe Entertainment Services Group, Inc. (2014) Case No. 10 Civ. 4119 (CM)(GWG). Decision and Order.

Metahaven (2016) *Black Transparency: The Right to Know in an Age of Mass Surveillance*. Berlin: Sternberg Press.

Mossman, Colin F. and Wary, Joseph C. (2008) "System and Method for Audio Encoding and Counterfeit Tracking a Motion Picture". Patent No. US7394519 B1.

Munoz, Lorenza and Healey, Jon (2004) Actor must pay studios for sharing film copies. *Los Angeles Times*. Available at: http://articles.latimes.com/2004/nov/24/business/fi-screener24.

NexGuard (2018) Who we are. *NexGuard*. Available at: http://www.nexguard.com/company/.

Nietzsche, Friedrich (2015) *Anti-Education: On the Future of Our Educational Institutions*. Translated by Searls, Damion. New York: New York Review Books.

O'Dell, Steven (2014) "Re: URGENT -Need your immediate action: NEW AUDIO SOURCE WATERMARK RECOVERY: RoboCop #RCP001 | no rls group | Audio only". Email. Available at: https://wikileaks.org/sony/emails/emailid/186024.

Pfitzmann, Andreas and Köhntopp, Marit (2001) Anonymity, unobservability, and pseudonymity—a proposal for terminology. In: Federrath, Hannes (ed) *Designing Privacy Enhancing Technologies (Lecture Notes in Computer Science 2009)*. Berlin: Springer-Verlag.

Risk Based Security (2014) A breakdown and analysis of the December, 2014 Sony hack, 2014. *Risk Based Security*. Available at: https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/.

Roddy, James E. et al. (2005) "Method and Apparatus for Watermarking Film". Patent No. US6882356B2.

Schuppli, Susan (2014) Can the sun lie. In: Forensic Architecture (eds) *Forensis: The Architecture of Public Truth*. Berlin: Sternberg Press.

Schuppli, Susan (forthcoming) *Material Witness: Forensic Media and the Production of Evidence*. Cambridge: MIT Press.

Solmon, Vicki (2014) "FW: UPDATED NEW SOURCE REPORT: The Amazing Spider-Man 2 #TAS026 | BOT | Cam". Email. Available at: https://wikileaks.org/sony/emails/emailid/193543.

Sundaram, Ravi (2015) Publicity, transparency and the circulation engine: The media sting in India. *Current Anthropology* 56(S12): S297–S305.

Trevathan, Jarrod and Ghodosi, Hossein (2003) Overview of traitor tracing schemes. In: *Communications of CCISA, Selected Topics of Cryptography and Information Security 9.4*.

United States v. Russell Sprague (2004) Bryan D. DuChene Affidavit.

Valenti, Jack (2003) Film studios announce end to award screeners: Measure taken to combat piracy". *MPAA*. Press Release, September 30 2003. Available at: https://web.archive.org/web/20031003062927/http://www.mpaa.org/jack/2003/2003_09_30a.htm.

Vee, Annette and Brown, James Jr. (eds) (2016) *Computational Culture* (5): *Rhetoric and Computation*. Available at: http://computationalculture.net/index-issue-five/.

Verimatrix (2018) About us. *Verimatrix*. Available at: https://www.verimatrix.com/.

Vizireanu, Ion et al. (2012) "System and Method for Analyzing and Marking Film". Patent No. US8090145B2.

Wagner, Neal R. (1983) Fingerprinting. In: *Proceedings of the 1983 IEEE Symposium on Security and Privacy*.

Warner Bros. Entertainment Inc. v. Innovative Artists Talent and Literary Agency Inc. et al. (2016) Case No. 2:16-cv-07902. Complaint for Copyright Infringement and Violation of Digital Millennium Copyright Act, Demand for Jury Trial.

Warren-Myers, Fletcher et al. (2015) An industry-scale mass marking technique for tracing farmed fish escapees. *PLoS ONE* 10(3): e0118594.

Washington, Arlene (2016) Piracy group behind 'Hateful Eight' leak releases apology. *The Hollywood Reporter*. Available at: http://www.hollywoodreporter.com/news/piracy-group-behind-hateful-eight-851761/.

Weizman, Eyal (2014) Introduction: Forensis. In: Forensic Architecture (eds) *Forensis: The Architecture of Public Truth*. Berlin: Sternberg Press.

Weizman, Eyal (2015) Presentation of *'Black Friday': Carnage in Rafah during 2014 Israel/Gaza Conflict*. London: Centre for Research Architecture, Goldsmiths.

Weizman, Eyal and Sheikh, Fazal (2015) *The Conflict Shoreline: Colonization as Climate Change in the Negev Desert*. Brooklyn: Steidl/Cabinet.

[i] For a development of this discussion, see a special issue of *Computational Culture* edited by Annette Vee and James Brown Jr. devoted to Computational Rhetoric. (2016).

[ii] E.g. "Farmed fish escape and enter the environment with subsequent effects on wild populations. Reducing escapes requires the ability to trace individuals back to the point of escape, so that escape causes can be identified and technical standards improved. Here, we tested if stable isotope otolith fingerprint marks delivered during routine vaccination could be an accurate, feasible and cost effective marking method" (Warren-Myers et al., 2015: e0118594).

[iii] 'Fingerprints' are here understood to be "characteristics of an object that tend to distinguish it from other similar objects" (Wagner, 1983: 18), with the notion of human fingerprints thus being extrapolated to all manner objects;

however, the associated term ‘fingerprinting’ is not merely a similar extrapolation: in the specific forensic vernacular, ‘fingerprinting’ does not here refer exclusively to the taking of a fingerprint, but may also refer to the *addition* thereof. In other words, if an object is fingerprinted, it may either already possess a fingerprint which would then be subsequently recorded, or notably it may also mean that the act of fingerprinting has added a fingerprint to said object so as to facilitate its identification (Wagner, 1983: 18).

[iv] The qualifier of the upload taking place without authorization of the legally-delineated content controllers is essential, as content controllers have at times intentionally leaked content (or directly facilitated the leaking thereof) as part of a promotional effort for the given product (see, e.g. Doctorow, 2007), and at other times been suspected thereof (see, e.g. Barr, 2015).

[v] E.g. dynamic traitor tracing schemes assign different keys over time, as opposed to static systems which may associate the same key with a given potential traitor throughout the dispersal of various contents thereto (for exhibitory discussions of the various available traitor tracing permutations, see Trevathan and Ghodosi, 2003: 51-63; Liu et al., 2005).

[vi] “We developed a data set of 312 popular movies and located one or more samples of 183 of these movies on file sharing networks, for a total of 285 movie samples. 77% of these samples appear to have been leaked by industry insiders” (Byers et al., 2003: 1).

[vii] The content in question was originally uploaded at 2015-12-20 06:31:28 (GMT) on ***, though news sources did not report on it until at least the following day (see, e.g. Andy, 2015).

[viii] The original *THR* story (Belloni, 2015), much like the leaked content in question (Khatchatourian, 2015), has since its original publication been widely disseminated (*Google News*, 2015); thus the wide-scale propagation of the actual content is mirrored by the similarly wide-scale propagation of news of the potential identification of the content source, indicating dual interests of both content procurement and in the knowledge of where the leak originated from.

[ix] A release is here understood as the pirated content in question and any peripheral associated content (e.g. NFO and sample files); though aside from the quantitative constituent components, a “release is to a cracker what a canvas is to an artist (i.e., an expression of self and a transformation of time into a tangible product) […] Pirates take each release very seriously; it is more than just a release to them, it is an art form” (Craig, 2005: 95-96).

[x] The particular release name here deviates from the norm by including the non-standard, albeit not entirely unused, ‘HQ’ denotation, as well as including both the individual pirate’s handle as well as the affiliated group (or in this case, torrent tracker) (cf. the more standardized standard, albeit once again not sole, practice of only including a singular attribution tag denoting either a single group, individual, or affiliated filesharing site).

[xi] An NFO (information) file is an accompanying text (utilizing ASCII/ANSI standards) document typically included in a release which contains supplementary information about a release not denoted in the release name (Craig, 2005: 96).

[xii] Cf. the case of *Agrippa*, an artwork designed to become unreadable after a single viewing (for discussion, see Kirschenbaum, 2008: 213-248).

[xiii] In deploying the nomenclature of unobservability and unlinkability, we are here drawing upon terminology fine-tuned by Pfitzmann and Köhntopp (2001: 1-9).

[xiv] As the full DVD has not actually appeared publicly, this statement in turn may mean that the FBI or its affiliates have access to an internal group File Transport Protocol (FTP) site which was used to store the full DVDR, or it may instead mean that the article is referring to the Hive-CM8 AVI file, which was sourced from the DVD.

[xv] Other companies in the area are outfits such as ContentArmor (2018) and NexGuard (2018) (see also: Irdeto, 2018; MarkAny, 2018; Verimatrix, 2018)

[xvi] Given that the presentation references case studies from 2013 (Deluxe, ca. 2013-2014: 14), and that the Sony leak initiated in November 2014 (Risk Based Security, 2014), the presentation materials can thus be dated to be between 2013-2014 despite not having an official date (file metadata timestamp data is not present in the PDF document). As the presentation was part of the large dump of internal Sony files (Risk Based Security, 2014), it stands to reason that the presentation may have been intended for Sony officials.

[xvii] As, e.g. would be the case with the insertion of microdots into film frames, as is a common visual film watermarking practice (see, e.g. Antonellis et al., 2007; Duffield et al., 2006; Roddy et al., 2005; Vizireanu et al., 2012)

[xviii] "In one embodiment, the audio soundtrack is altered to ensure that playback of the audio soundtrack reverts from a digital recording on the copy of the motion picture to the analog recording of the soundtrack at the selected location where the identifiable code is inserted into the audio soundtrack" (Mossman and Wary, 2008: 9).

[xix] For detailed discussions of potential digital audio watermarking techniques, see Cvejic and Seppännen, 2008; He, 2012.

[xx] A typographical descender is the component of a character which protrudes below the given font baseline, extending below other letters; a visible descender may be commonly demonstrated in lowercase letters such as 'g' or 'y' (Deer, 2016: 253).

[xxi] This is not an unlikely scenario, given that internal emails (e.g. O'Dell, 2014) betray the fact that Deluxe has access to at least one release group's internal FTP server, which they monitor for new pre-release uploads of leaked content. Thus it is both possible and plausible that the Hive release had indeed been successfully rendered watermark-free, and that Deluxe instead readily acquired the watermarks from the original copy, which may have been uploaded by the supplier with the intention of having another party remove the markings prior to encoding the resultant AVI file.