Bennke, J., (2023) "Media of Verification: An Epistemological Framework for Trust in a Digital Society", *communication +1* 10(1).
doi: https://doi.org/10.7275/cpo.1878

Media of Verification: An Epistemological Framework for Trust in a Digital Society

Johannes Bennke, Hebrew University of Jerusalem, Israel, johannes.bennke@mail.huji.ac.il

The concept of verification is commonly associated with verifying sources in journalism, Open-Source Intelligence, digital forensics, and various digital research methods. In this context, I introduce 'media of verification' as an epistemological framework that encompasses a variety of practices. Through the examination of examples, I elaborate on four modalities: verification in media, apparatuses of verification, verification as consensus-making, and infrastructures of verification. Verification in media involves the pre-reportage verification of sources in journalism. Apparatuses of verification are devices designed to validate authenticity. Verification as consensus-making encompasses decision-making processes, such as negotiations, debt registers, and bookkeeping. Infrastructures of verification pertain to authentication media like certificates, batches, and other mechanisms ensuring the integrity of goods, documents, data, currencies, and sensitive information. I show that different phenomena, practices, and techniques bridging the digital and physical realms are indeed part of the same epistemological framework I call 'media of verification.'

Keywords: verification, apparatus, infrastructure, consensus making, journalism, open-source intelligence, digital forensics

Introduction

Democracies worldwide are under pressure. From within, they are threatened by populism and its various forms of misinformation, lies, and the spread of mistrust and fear. From outside, they face autocracies and war. For decades, there has been an epidemic of distrust in the social fabric of Western democratic societies. And modern technology seems to conspire with these threatening forces. Among other factors, the current traction of generative AI tools in combination with social media seems to be fueling an epidemic of misinformation as well as distrust in science. While a pope in a white puffy jacket might go viral as a funny deepfake meme,[1] the implications are much more serious, and the stakes are much higher when it comes to facts about life and death in war zones, manipulation of elections, and defamations through smear campaigns.

In a world where evidence can be fabricated, real things can be claimed as fake. A recent case in the 2023 Israel-Hamas war is a post on *X*, formerly *Twitter*, which allegedly shows the charred corpse of an Israeli baby lying on a table shown in pixelated form. After it was shared by Prime Minister Netanyahu, an anti-Israeli US politician and influencer claimed that the image was faked using generative AI tools. In order to prove this claim, the influencer attached a screenshot of an AI detector called *AI or not* to his post, classifying it as "This image is generated by AI". An expert in digital forensics at the University of California at Berkeley says that "he could not find any discrepancies in the picture that would indicate an AI fake."[2] Here, an expert can at least rule out certain criteria that it is a fake. Therefore, the badge indicates "FALSE" in the upper right corner of the image (fig. 1). In a world where there are specific tools to verify AI-generated images, you cannot trust your own eyes – even the results of those tools can be mistaken and politically instrumentalized.

But how are truth and trust established *with* technology? A key operation to generate trust, I argue, is verification. Trust has been studied primarily in terms of an interhuman relationship in psychology,[3] as social trust beyond a dyadic

[1] "The Pope Drip," Reddit Post, *R/Midjourney*, March 24, 2023, www.reddit.com/r/midjourney/comments/120vhdc/the_pope_drip/; James Vincent, "The Swagged-out Pope Is an AI Fake — and an Early Glimpse of a New Reality," March 27, 2023, https://www.theverge.com/2023/3/27/23657927/ai-pope-image-fake-midjourney-computer-generated-aesthetic.

[2] Eisele, Ines, and Uta Steinwehr. "Fact Check: AI Fakes in Israel's War against Hamas." *Dw.Com*, November 10, 2023. https://www.dw.com/en/fact-check-ai-fakes-in-israels-war-against-hamas/a-67367744.

[3] Paul Thagard, "Coherence, Truth, and the Development of Scientific Knowledge," *Philosophy of Science* 74 (2007): 28–47.

Figure 1 – A real proof is labeled as a deepfake by an Anti-Israel agitator, Oct 12, 2023, X. https://www.dw.com/en/fact-check-ai-fakes-in-israels-war-against-hamas/a-67367744.

relationship in the political and social sciences,[4] or as cooperation in game theory.[5] But trust is not only an element of the social fabric established by interpersonal interaction and behavior but also by media technologies and their particular operations of verification. The comments of the mentioned alleged deepfake indicates the challenges of everyday journalism and gives a general idea of verification.[6] However, here I broaden the perspective and intend to take what I call *media of verification* as a starting point to think about trust in a society built on digital communication. Here, I talk about trust in the context of media and technology and specify trust even further in particular examples.

While the above-mentioned post comes from recent developments in the field of generative AI and social media with their respective associated uncertainties, there are many other forms of verification. Journalists must verify their sources; internet users must verify their accounts; the state must be able to verify a person's identity to validate his or her right to vote; transactions must be correctly documented in order to track debts and loans; shipping containers must be sealed during transportation to ensure that the cargo has not been tampered with; certificates verify the quality of a product be it a car or code.

Forms of verification are legion. To illustrate the framework and to show how it is embedded in everyday life, I will give a few examples. All these examples differ in the use of media, instruments, devices, rules, and practices. While communication studies have paid a lot of attention to verification in journalism,

[4] Eric M. Uslaner, *The Oxford Handbook of Social and Political Trust* (Oxford University Press, 2018).

[5] Robert M. Axelrod, *The Evolution of Cooperation* (New York, NY: Basic Books, 2006).

[6] Craig Silverman, *Verification Handbook*, accessed November 20, 2023, https://datajournalism.com/read/handbook/verification-1.

media studies go beyond the narrow meaning of verification in the journalistic context. Here, I broaden the perspective and propose to think of 'media of verification' in terms of epistemic practices, operations, apparatuses, consensus-making, infrastructures with their specific methods to establish trust.

From an etymological point of view verification derives from the Latin "verus", meaning "true", "trustworthy", and "facere", meaning "doing", "making". Verification therefore means "making true or trustworthy".[7] Verification is often tied to authentication, legitimation, validation and proof. Verification and validation, for example, are interchangeably used and not always easy to differentiate, unless specified like in the case of the IEEE Standards Association and in hard- and software product development.[8] In quality management, products are verified to determine whether a product meets the defined specifications that a company defined during its development. During validation, it is checked whether the defined usage objectives are achieved and thus the suitability for the customer's requirements is proven. Authenticating something in turn means verifying its truthfulness, for example, by means of a certificate from a third party. But the certification body, its tools and experts must also be authenticated, validated and verified, often with the help of other certificates that are legitimized and validated by another body. This network of references is the basis for something that is considered to be truthful in order to gain trust in information, people, currencies, or goods.

The constructive aspect of verification has become the gateway to an epistemological crisis. The sciences depend on facts *as well as* fictions,[9] facts and objectivity have their own (media) history,[10] and in face of different media, formal, popular, and aesthetic forms of knowledge, knowledge itself has become „promiscuous"[11] in the current information politics. Alternative facts, fake news,

[7] "Verify | Etymology, Origin and Meaning of Verify by Etymonline," accessed November 20, 2023, https://www.etymonline.com/word/verify; "Verification | Etymology of Verification by Etymonline," accessed December 5, 2023, https://www.etymonline.com/word/verification.

[8] Edward Addy, Carl Singer, and Lynn Robert Carter, "IEEE Standard for System, Software, and Hardware Verification and Validation," IEEE Standards Association, 2023, https://standards.ieee.org; pp_pankaj, "Differences between Verification and Validation," *GeeksforGeeks* (blog), April 18, 2019, https://www.geeksforgeeks.org/differences-between-verification-and-validation/.

[9] Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory* (Oxford: Oxford Univ. Press, 2007), 90.

[10] Mary Poovey, *A History of the Modern Fact: Problems of Knowledge in the Sciences of Wealth and Society* (Chicago: University of Chicago Press, 1998). Lorraine Daston and Peter Galison, *Objectivity* (New York, NY: Zone Books, 2010).

[11] Kenneth Cmiel and John Durham Peters, *Promiscuous Knowledge: Information, Image, and Other Truth Games in History* (Chicago London: University of Chicago Press, 2020).

deepfakes, and disinformation are not categorically new.[12] What is new, however, is the fact that credibility no longer depends on honesty and truth. It can even be strengthened by lies. Such a rejection of truth in the name of an alternative truth also rejects a concept of fact that has been a central component of Western science since the Enlightenment. The legal origin of facts takes the courtrooms as "sites of epistemological inquiry".[13] However, as the courtroom has always been part of a larger political power game and is integrated into other legal and administrative bodies such as the Ministry of Justice, the courtroom can become the site of ideological conflicts.[14] Other rules about facts and truths apply outside the courtroom and compete with other claims, alleged truths, and even artistic approaches.[15] The legal system makes use of verification for evidence on the one hand and can regulate verification processes on the other. But the regulations and judgments, especially in international law, are essentially about the recognition of courts as such. Without recognition of the mediating, legislative power, it is difficult to reach a consensus. In most cases, such conflicts are not only based on different interests, but also on different value systems.[16]

In media revolutions like the printing press[17] or digitalization, facts are questioned based on ideology and attention economy. Algorithms in social media promote fakes and ideological messages for revenue, disregarding truth. This toxic cocktail harms social cohesion.[18] The hypothesis is that digital technologies have changed the way we think about truth and trust. Truth and trust are not based on media constructions alone, but they are not possible without them either.

In the history of philosophy, truth has traditionally been viewed as an ideal in the Platonic sense, attainable through Socratic dialogue, questioning, and education. Martin Heidegger, in his commentary on Plato's allegory of the cave, expands on *aletheia* (ἀλήθεια), Old Greek for "truth," emphasizing its

[12] Jacob Soll, "The Long and Brutal History of Fake News," *POLITICO Magazine*, December 18, 2016, http://politi.co/2FaV5W9. Lorenz Engell and Bernhard Siegert, eds., *Schwerpunkt alternative Fakten*, Zeitschrift für Medien- und Kulturforschung, Heft 9, 2 (2018) (Hamburg: Felix Meiner Verlag, 2018);

[13] Barbara J. Shapiro, *A Culture of Fact. England 1550-1720* (Cornell University Press, 1999), 30.

[14] Ibidem.

[15] Milo Rau, *Das Kongo Tribunal*, ed. Eva Bertschy, Rolf Bossart, and Mirjam Knapp (Berlin: Verbrecher Verlag, 2017).

[16] M. N. S. Sellers, Joshua James Kassner, and Colin Starger, eds., *The Value and Purpose of Law: Essays in Honor of M.N.S. Sellers* (Stuttgart: Franz Steiner Verlag, 2019).

[17] Elizabeth L. Eisenstein, *The Printing Press as an Agent of Change: Communications and Cultural Transformations in Early-Modern Europe* (Cambridge: Cambridge University Press, 2009).

[18] Sandra González-Bailón and Yphtach Lelkes, "Do Social Media Undermine Social Cohesion? A Critical Review," *Social Issues and Policy Review* 17, no. 1 (2023): 155–80, https://doi.org/10.1111/sipr.12091. Concha Pérez-Curiel and Rubén Rivas-de-Roca, "Social Cohesion in Times of Crisis: The Role of Communication for Democracies—Editors' Introduction," *Social Sciences* 12, no. 9 (September 2023): 491, https://doi.org/10.3390/socsci12090491.

etymological meaning as "unconcealment."[19] He does not envision truth as a substance accessible through insights gained by philosophers in a vertical ascent from the cave's darkness to the sunlit realm of ideas. Instead, he sees truth as the disclosure or unconcealment of Being. In other words, truth is not about the correspondence between pre-existing facts or ideas and their more or less accurate representations in words (as Plato would have it) but rather about revealing the hidden nature of Being itself.

In contrast to this existential and ontological approach to truth, verification does not occur in the realm of pure ideas; it is practical, achieved through specific techniques, apparatuses, and media. Verification's horizontal movement involves reading traces, transforming them into a symbolic system, and constructing a coherent narrative, relying on diverse perspectives and rhetorical strategies. Here, I also don't intend to investigate verificationism as a method based on empirical observation, logical analysis, and linguistic considerations to assert the meaning of a statement as true or false.[20] Instead, I want to highlight how trust is created through media technologies and how this changes our understanding of trust itself. Four modalities of 'media of verification' are seminal here: *verification in media*, *apparatus of verification*, *verification as consensus-making*, *infrastructures of verification*.

Verification in Media

Probably the most commonly known form of verification happens *in* and *with* media in the field of journalism. Journalists distinguish between fact-checking and verification.[21] Fact-checking takes place "ex post" following claims made by public figures, draws on information from experts, academics, government bodies and other authorities, and leads to a reasoned conclusion about the veracity of the claim. Here, the main question is: "Is what is said true?" Since this work is labor-intensive and can hardly be automated, but is necessary, it leads to a division of labor and specialization in journalism.[22] Fact-check reporters take quotes from public figures, for instance, and classify them as "true", "false", "misleading", or

[19] Martin Heidegger, "Plato's Doctrine of Truth," in *Pathmarks*, ed. William McNeill (New York: Cambridge Univ. Press, 1998), 155–82.

[20] Richard Creath, "Logical Empiricism," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta and Uri Nodelman, Winter 2023 (Metaphysics Research Lab, Stanford University, 2023), https://plato.stanford.edu/archives/win2023/entries/logical-empiricism/.

[21] Alexios Mantzarlis, "Fact-Checking 101," in *Journalism, Fake News & Disinformation*, ed. Cherilyn Ireton and Julie Posetti (Paris: UNESCO, 2018), 85–100, https://unesdoc.unesco.org/ark:/48223/pf0000374458.

[22] Lucas Graves, *Deciding What's True: The Rise of Political Fact-Checking in American Journalism* (New York: Columbia University Press, 2016).

"lacking evidence".[23] Verification, on the other hand, takes place "ex ante", usually based on user-generated content and seeks to obtain primary evidence from eyewitnesses, surveillance cameras, relevant social media posts, reverse image searches, geolocation, and other more or less public sources using specific tools.[24] Here, the main question is: "Do we have to do with a trustworthy source?"

At the time of writing, *The Center for Political Beauty*,[25] a German activist group for human rights, Holocaust memorial, and the fight against anti-Semitism, published a video in which the German Chancellor Olaf Scholz says that he intends to ban the AfD, a radical right-wing party, which is part of the German parliament. The video is a deepfake published on a website that looks like an official German government website.[26] With this "operation", as the Center calls it, they intend to raise awareness of the dangers of deepfakes and right-wing extremism, whose aim is to undermine democracy. In this case, identifying the video as a deepfake was easy. It was framed as such. It was part of an orchestrated "operation" with an exhibition in front of the Chancellery and an elaborate website where users can submit anti-constitutional statements and violations of basic democratic rights committed by AfD politicians. These violations are, in turn, "verified" with references to publicly available sources. A statement of the party on the facts accompanies all "evidences" and reads that the media insinuates these "unconstitutional aspirations" but not the party's representatives.[27] Four bullet points for a ban of the AfD accompany all evidences. Using artistic freedom, a kind of extrajudicial tribunal is being set up here that invokes the Basic Law of the Federal Republic of Germany.

In other instances, this elaborate and obvious framework is not the case. Digital forensics experts are trying to find ways for digital watermarks or other mechanisms,[28] and regulators are enacting laws and policies to hold companies accountable for making deepfakes available almost at the click of a button.[29] This

[23] Linda Qiu, "Fact-Checking Trump's Election Lies - The New York Times," August 17, 2023, https://www.nytimes.com/2023/08/17/us/politics/trump-election-lies-fact-check.html.

[24] Craig Silverman and Rina Tsubaki, "10. Verification Tools," in *Verification Handbook*, accessed December 5, 2023, https://datajournalism.com/read/handbook/verification-1/verification-tools/10-verification-tools.

[25] "Center for Political Beauty," accessed November 30, 2023, https://politicalbeauty.com/.

[26] "AfD-Verbot der Bundesregierung," accessed November 30, 2023, https://afd-verbot.de.

[27] "AfD-Verbot der Bundesregierung | Die Beweise," accessed November 30, 2023, https://afd-verbot.de/beweise.

[28] Larry E. Daniel, Lars E. Daniel, and Sue Spielman, *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom* (Waltham, Mass: Syngress/Elsevier, 2012). Simon Rothöhler, *Medien der Forensik* (Bielefeld: transcript, 2021).

[29] Amanda Lawson, "A Look at Global Deepfake Regulation Approaches," *RAI Institute* (blog), April 24, 2023, https://www.responsible.ai/post/a-look-at-global-deepfake-regulation-approaches; Cass R. Sunstein, "Can the Government Regulate Deepfakes?," *Wall Street Journal*, January 7, 2021, sec. Life, https://www.wsj.com/articles/can-the-government-regulate-deepfakes-11610038590; Adam Satariano and Cecilia Kang, "How Nations Are

cat-and-mouse game involving regulators, programmers, criminals, investigators, and activists has consequences for trust in messages and the media. The images, messages, and the use of different platforms and posts become a battleground. Journalists and the social sciences have shown that in the current Israel-Hamas war, cyberwar is not sci-fi but a reality.[30] Sometimes the verification process itself can become the subject of a story, for example, when there are doubts, contradictory information or unreliable sources. The film *Revision* (Philip Scheffner, GER, 2012) takes a closed criminal case as the subject for a cinematic revision or reenactment, collecting testimonies by people and linking them to places, creating a web of references and perspectives about a crime scene at the border between Germany and Poland. The film shows that there are many unanswered questions and inconsistencies.

Wars are typical cases in which it is difficult to obtain information and put it into a perspective independent of the warring parties. In the fog of war, information given by one of the warring parties often cannot independently be verified. Statements by warring parties are often addressed at the enemy and either exaggerated or contain lies or half-truths, conceal real events, or discredit the other party. For example, ten days into the Israel-Hamas war on October 17, 2023, an explosion at al-Ahli Arab Hospital in Gaza killed and injured an unknown number of civilians. Tensions were high; the events drew the attention of the world public, and the warring parties pointed the finger at each other. Initiatives like Bellingcat,[31] Human Rights Watch, or oryxspioenkop.com go beyond specific tools of fact-checking and the verification of sources. They make use of open-source intelligence (OSINT) like satellite images, social media posts, uploaded videos, patterns of posting, testimonies, and other openly available sources. Others, like truly.media, collaboratively verify user-generated content residing in social networks; yet others use forms of digital forensics to gain information about the what's, the when's, the where's, and the who's that make up journalistic reportage. A little more than a month after the incident at the hospital, Human Rights Watch has verified that the impact resulted from a rocket-propelled munition which is commonly used by Palestinian armed groups. At the time of writing, the investigation is ongoing, in order to determine the exact origin of the

Losing a Global Race to Tackle A.I.'s Harms," *The New York Times*, December 6, 2023, sec. Technology, https://www.nytimes.com/2023/12/06/technology/ai-regulation-policies.html.

[30] Steven Lee Myers and Sheera Frenkel, "In a Worldwide War of Words, Russia, China and Iran Back Hamas," *The New York Times*, November 3, 2023, sec. Technology, https://www.nytimes.com/2023/11/03/technology/israel-hamas-information-war.html.

[31] Charlotte Maher, "Separating Fact from Fiction on Social Media in Times of Conflict," *Bellingcat* (blog), October 26, 2023, https://www.bellingcat.com/resources/how-tos/2023/10/26/separating-fact-from-fiction-on-social-media-in-times-of-conflict/.

rocket, the person responsible, "and whether the laws of war were violated."[32] Verification here takes all available information as a possible trace to give an indication about the event.

My hypothesis is that the main concept in how to think about *verification in media* is the "trace". The trace refers to the Old French "trace" meaning, "mark, imprint, tracks".[33] To trace something does not mean to make the traces, rather to track them down, "follow the trail of something"[34] and interpret them in an environment full of other possible traces. This practice of tracing led Sybille Krämer to think about the trace in terms of ten attributes.[35] To differentiate between traces and non-traces means to identify something which can possibly become part of a symbolic system or narrative.

There are different ways of reading reality in terms of the trace. For instance, the task of a hunter is not only to identify footprints, broken branches, bent blades of grass, or almost unnoticeable displacement of pebbles but to also see other irregularities in the familiar environment and transform them into a coherent image of a narrative. A detective has to be even more creative because criminals often go to great lengths to cover their tracks, making it a challenge to recognize the tracks and their concealment as such in the game of hide-and-seek. Digital forensics are faced with yet another challenge: the sheer amount of available information as metadata, images, social media posts, video and audio recordings, eyewitness reports, and other sources make it a challenge to put it into context. In order to verify what happened, where, when, how, and who was involved, analysts have to be knowledgeable about the technicalities, very creative in how to find possible sources, must draw logical conclusions, and know how to put together the fragments of information into a rather seamless narrative. *Forensic Architecture* for instance, recreated the events of the 2020 explosion of grain silos containing ammonium nitrate at the port of Beirut.[36] They not only used publicly

[32] "Gaza: Findings on October 17 al-Ahli Hospital Explosion | Human Rights Watch," November 26, 2023, https://www.hrw.org/news/2023/11/26/gaza-findings-october-17-al-ahli-hospital-explosion.

[33] "Trace | Etymology of Trace by Etymonline," accessed November 30, 2023, https://www.etymonline.com/word/trace.

[34] Ibidem.

[35] These attributes are: Absence, orientation, materiality, disturbance, unmotivatedness, observer and action dependency, interpretativity/narrative/polysemy, break in time, one-dimensionality/irreversibility and mediality/heteronomy/passivity. Sybille Krämer, "Was Also Ist Eine Spur? Und Worin Besteht Ihre Epistemologische Rolle? Eine Bestandsaufnahme," in *Spur. Spurenlesen Als Orientierungstechnik Und Wissenskunst*, ed. Sybille Krämer, Werner Kogge, and Gernot Grube (Frankfurt a.M.: Suhrkamp, 2007), 11–33.

[36] Eyal Weizman, *Forensic Architecture: Violence at the Threshold of Detectability* (Brooklyn, NY: Zone Books, 2017); Samaneh Moafi, "The Beirut Port Explosion ← Forensic Architecture," 2020, https://forensic-architecture.org/investigation/beirut-port-explosion; Eyal Weizman and Anselm Franke, *Forensis: The Architecture of Public Truth.* (Berlin: Sternberg Press, 2014).

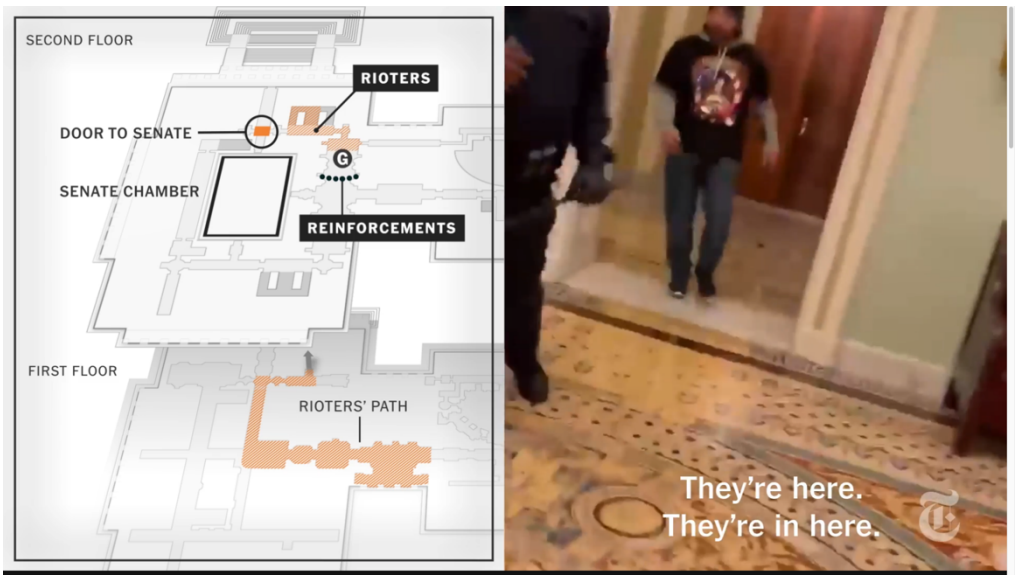

Figure 2 – Screenshot of "Day of Rage" showing a split-screen of a 3D map of The Capitol (left) with rioters entering the building (right).

available information, but also created a 3D model of the port area of Beirut and a large part of the city to locate the video recordings, place them in a chronological order, and find a way to visualize the event. Another example is from the documentary *Bellingcat: Truth in a Post-Truth World* (Hans Pool, NL, 2018) about the shoot-down of Malaysia Airlines Flight 17 (MH17/MAS17) on July 17, 2014. Here, the reporters show evidence that the airplane was shot down by a Russian Buk missile launcher from a separatist-controlled territory in Eastern Ukraine.[37] The New York Times visual investigation about the Capitol Hill Riots on January 6, 2021, goes to great lengths to make plausible the unfolding of the events and the deliberate intention by right-wing extremists to take the U.S. Capitol by force.[38] Here, the film not only uses publicly available information like live broadcasting, social media posts and videos but also shows subtitles, maps, 3D models, and animations especially made for the film which were issued only months after the riots (fig. 2). Organized chronologically, cross-referenced, and edited together, they form a coherent narrative about the ideological motivations and violent intentions of the rioters and ultimately become evidence in hearings.[39]

[37] Eliot Higgins, "MH17 - The Open Source Evidence," bellingcat, October 8, 2015, https://www.bellingcat.com/news/uk-and-europe/2015/10/08/mh17-the-open-source-evidence/.

[38] Dmitriy Khavin et al., "Day of Rage: How Trump Supporters Took the U.S. Capitol," *The New York Times*, June 30, 2021, sec. U.S., https://www.nytimes.com/video/us/politics/100000007606996/capitol-riot-trump-supporters.html.

[39] Luke Broadwater, "'Trump Was at the Center': Jan. 6 Hearing Lays Out Case in Vivid Detail," *The New York Times*, June 9, 2022, sec. U.S., https://www.nytimes.com/2022/06/09/us/politics/trump-jan-6-hearings.html.

Despite the fact that these are different events, taking place at different places, times, and under different circumstances, in all these cases, a potpourri of publicly available information based on differing sources, consisting of different formats, qualities, and perspectives show an investigation into the unfolding of events. Here, verification in media means to geolocate objects on a map, put movements and events into a chronological order on a timeline, and form a coherent narrative by correlating almost invisible traces (voice patterns, shadows, colors, scratch fingerprints on metal, cloths, license plates, perspectives, metadata, etc.).[40] Although, the hunter, the detective, and the digital forensics need a particular skillset of deciphering in their respective metiér, they are part of the same *paradigm of circumstantial evidence*.[41] Such a paradigm takes fragments of reality as clues, turns them into signs in a symbolic system, and funnels them into a network of signs where they are revealed as a trace and related to other more established or conventional signs and representations (portraits, maps, timelines, diagrams etc.). Finally, they are put into a coherent narrative. Verification in media therefore introduces a network of knowledge that generates new narratives in a public discourse. Here, deciphering is a form of reading as a cultural technique in a 'techno-hermeneutics'. Reading and narrating are, therefore, basic elements in the ability to build trust.

To narrate such readings is far from neutral. There is an ethical and epistemological dimension to verification in media with political consequences. Letting the truth tell the story is radical because it is not corrupted. Such a story is neither guided by other interests, nor has it allowed itself to be seduced by desires or carried away by passions. However, this paradigm of circumstantial evidence becomes political the moment it stands in contrast to other statements and supposed truths on the street outside the courtroom and investigative journalism.

But is this already enough to establish trust? Is it enough to read traces, put them into context and relate them to a narrative to establish trust in a person's claim? After all, this form of verification only serves events and narratives but not the instruments themselves or the entities that use these techniques and instruments. What if the institution using these technologies is corrupt or pursuing its own goals? What if the tools used are unreliable, deliberately misleading, or poorly made? Who guards the guardians? Who audits the instruments? How can it be ensured that the information in question is reliable,

[40] Greg Siegel, *Forensic Media. Reconstructing Accidents in Accelerated Modernity* (Durham: Duke University Press, 2014). Bernd Stiegler, "Conan Doyle, Visual History und das Indizienparadigma," in *Grenzen der Bildinterpretation*, ed. Michael R. Müller, Jürgen Raab, and Hans-Georg Soeffner, Wissen, Kommunikation und Gesellschaft (Wiesbaden: Springer Fachmedien, 2014), 79–96, https://doi.org/10.1007/978-3-658-03996-7_5.

[41] Carlo Ginzburg, "Clues: Roots of an Evidential Paradigm," in *Clues, Myths, and the Historical Method* (Hanover, London: University Press of England, 1989), 96–125.

interpreted according to certain guidelines, and translated into a verifiable narrative? Other layers of verification are needed in order to address these questions.

Apparatus of Verification

Another modality here are 'apparatus of verification'. Such apparatus address the tools and instruments that are in play in validating tickets, verifying the identity and transition of a person, or the transport of an object or the transaction of currencies at a particular time and space. Very simple forms of these apparatus are tickets that are torn by the admission staff at the entrance to a concert, movie, or theater. Writing tools like specific paper, ink, or a certain typography with a special design, a number, a time, and date allow for the validity of the ticket. As a gatekeeper, the conductor with the punch needs a trained eye for the limited validity of the ticket.

In more or less automated systems the verification process is more complicated. Digital systems require the scanning of a Quick Response (QR) or barcode at checkpoints. Other cybersecurity systems use dactyloscopy, retinal scanning, voice recognition and other individual body criteria as an authentication method to control passage. Spy and agent films derive a large part of their suspense and their show value from overcoming such technical security systems.[42] The EasyPASS border control system at airports in Germany, for instance, scans passports and uses facial recognition technologies to identify if the person is who they claim to be and if this person is allowed to pass. Here, we have to do with an automated validation process. The border control system verifies the nation which issued the passport, verifies if the passport is valid (expiring date, age etc.), and compares "the information according to the Schengen Borders Code with police databases" as well as compares "the live image 1:1 with the biometric photo stored on the chip."[43] The "collected data is stored for 48 hours" (unless due to a police investigation "the storage period is manually extended to a maximum of 30 days").[44] Each time a checkpoint is passed the exact time and date are registered allowing the border control to verify the crossing of the border.

When withdrawing money from an ATM or paying with a credit card, a Personal Identification Number (PIN) is required, which must be entered into the

[42] Christoph Ernst, "Medien der Zukunft oder Zukunft der Medien?," in *Medien | Zeiten: Interdependenzen*, ed. Sven Grampp, Peter Podrez, and Nicole Wiedenmann (Wiesbaden: Springer Fachmedien, 2023), 331–45, https://doi.org/10.1007/978-3-658-38688-7_18.

[43] "EasyPASS - Homepage - What Data Is Collected during (Partially) Automated Border Control?," accessed November 22, 2023, https://www.easypass.de/EasyPass/EN/Service/FAQ/collected-data.html;jsessionid=07FBE8C52C9CC332D6FF31ADA0660DA4.2_cid379.

[44] Ibidem.

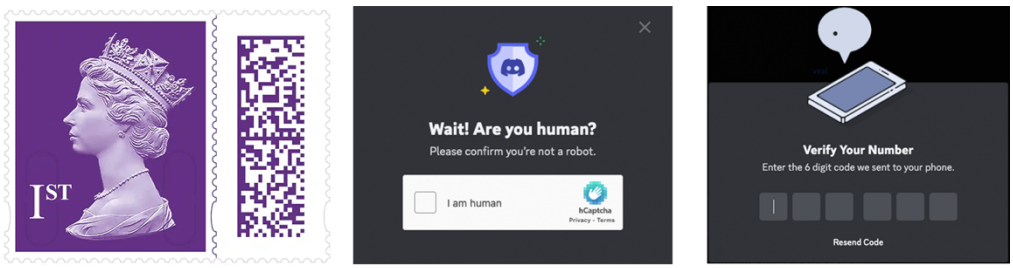

Figure 3 – Stamp with QR-code; hCAPTCHA; Two-Factor-Authentication using SMS.

card reader. Every online account usually requires at least a password and an email address (sometimes accompanied by a username or a mobile number). Two-factor-authentication (2FA) adds another layer of security which has become the new standard in the verification and login procedure of an online account. "Are you who you say you are?" Some platforms make use of a second authenticator app using a Transaction Number (TAN) or a One-Time Password (OTP). During the registration process, the person registering receives a TAN, OTP, or an email which usually contains a link that, when clicked, verifies the user's email address. Very often the user interface shows a green checkmark or thumb up at the end of the process. Such verification entails its own protocols on the side of the system and other programs on the side of the user. Experts test these protocols in terms of efficiency using a verification tool to measure the performance of the security protocol.[45] On the user's side, apps need permissions to get access to other apps, private information need to be managed and password managers have become indispensable little helpers that are implemented as plug-ins in browsers, for example. Other platforms use cognitive-psychological riddles like reCAPTCHA to verify that the user is not a machine ("Verify that you are human!"). Although the protocols of the control and cybersecurity system are in the user's interest to prevent unauthorized access to personal accounts and information, these measures can also be very annoying from the user's perspective, also because they have become a potential gateway for scammers. The shadow history of the Internet consists of spam (WhatsApp messages, emails, SMS) asking for the confirmation of an account or for the details of an address to deliver a supposedly lost package. That way, actors with malicious intentions try to get sensitive information from the unsuspecting recipient. This is why the *FIDO alliance* introduced *FIDO U2F* and in cooperation with the *World Wide Web Consortium* (W3C) *Webauthn*, a passwordless protocol and authentication method using facial recognition and dactyloscopy, which is built directly into the devices.[46] This supposedly makes it more secure and convenient for the user. An *Apple* employee explains it like this:

[45] Kaijun Liu et al., "A Robust and Effective Two-Factor Authentication (2FA) Protocol Based on ECC for Mobile Computing," *Applied Sciences* 13, no. 7 (March 30, 2023): 4425, https://doi.org/10.3390/app13074425.

[46] "FIDO2," *FIDO Alliance* (blog), accessed December 5, 2023, https://fidoalliance.org/fido2/.

"I click the 'sign in' button, Safari prompts me for confirmation, then, boom, Face ID, I'm signed in."[47]

The security measures discussed in this context are designed to utilize the separation and interconnectedness of the physical and digital realms. In fact, these devices serve as evidence of the inseparability of these spheres, while the verification mechanisms guarantee the maintenance of this separation (fig. 3). The mechanisms for verification are pivotal in establishing a secure connection that bridges the physical and digital, but they also ensure that this separation is maintained. These apparatuses ensure that access, interactions, and transactions between the physical and digital realms are verified and protected, thus securing the overall system, and safeguarding the identity and validity of the information provided.

The symbols for these verification measures are different, but the basic principle is the *lock and key*. Any apparatus based on this principle regulates access and denial, therefore it does not only have a security function but also ethical and political implications. Like the postmark,[48] a QR scanner and other validators are embodiments of values and power relations. At best, they are open source, increase safety, are seamlessly and efficiently implemented, decline unauthorized access, at worst, they serve surveillance, exclude minorities and gain profits from it. For this reason, activists, journalists, academics, and other actors use forms of resistance like 'obfuscation'[49] in an attempt to reappropriate one's (digital) life, remain anonymous, and take control of one's personal data. The 'sousveillance movement'[50] specifically tries to subvert such surveillance technologies which threaten individual freedom. The service of a virtual private network (VPN) is a way to gain information outside of state censorship, like in today's Russia, China, and other countries.[51] Other applications like the Tor Browser make use of a network of nodes that allow covering the Internet Protocol (IP) address.

Verification devices therefore validate something as a legitimate entity to pass the register. There is a whole set of apparatus involved in order to allow for

[47] *Meet Face ID and Touch ID for the Web*, 2020, https://developer.apple.com/videos/play/wwdc2020/10670/.

[48] Bernhard Siegert, *Relais: Geschicke der Literatur als Epoche der Post: 1751-1913*, (Berlin: B&B, Brinkmann & Bose, 1993).

[49] Finn Brunton and Helen Fay Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protest* (Cambridge, Massachusetts: MIT Press, 2015). Cory Doctorow, *Homeland*, (New York: Tor Teen, 2013).

[50] Steve Mann and Joseph Ferenbok, "New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World.," *Surveillance & Society* 11, no. 1/2 (July 16, 2013): 18–34, https://doi.org/10.24908/ss.v11i1/2.4456.

[51] Verena Maria Wingerter, "Russia's War on the Internet," *Ukraine Analytica* 1, no. 27 (2022): 53–60. Li Yuan, "China's Information Dark Age Could Be Russia's Future," *The New York Times*, March 18, 2022, sec. Business, https://www.nytimes.com/2022/03/18/business/chinas-russia-information.html.

the transmission of data, the transition of people, and the transaction of currencies and the transportation of goods. High-tech paper, especially with regard to passports[52] and money bills, consists of a mix of different materials (i.e. cotton, paper), specific ink, holographs and almost invisible signs. Other security measures are developed to make the counterfeiters' work more difficult. The issuing entity, like the state, a company, or a validating system, recognizes and validates these documents in a specific context. Lists, paragraphs, and other filing structures are established to access, read, and enforce law, archive protocols, and other files which document transactions.[53]

Apparatus of verification have a key and locking function and include gate keeping entities, their counterparts (tickets, passports, passwords etc.), as well as their filing structure and statistical evaluation. But this is still not a sufficient setup to establish trust. When the alleged true documents and facial features are verified by a control system and when it is cross-referenced with other registries, this does not establish trust but validates the presenting documents and persons for permission to pass. The moment of verification is time stamped; in case of positive validation, an allowance to pass is issued, and the transition, transmission or transaction is registered. A validation of access is necessary, but not yet sufficient to establish trust in a digital society.

Verification as Consensus-Making

All of the above-mentioned examples are based on proof and an authority that recognizes it. What precedes this, however, is a rule-based system that regulates this recognition. Let's take the very basic example of friendship ribbons or bracelets. Usually, all that is needed to put on the friendship bracelets is a verbal agreement. More formal is the case of a legally concluded marriage. Here, a third party is required to perform and witness the act of marrying and the exchange of rings. These social relations are very basic techniques of consensus-making.

It becomes more complicated when the social relation is less intimate, more anonymous, and when a commitment and reliability must be established in a different way. This is the case for passport control, hostage negotiations, and even the relation between filmmakers and their audience. While a third party or an apparatus validates documents, an accountability system is required to enable an agreement between the two (or more) parties. This third instance embodies a system of regulations and testifies to compliance with the rules.

---

[52] Craig Robertson, *The Passport in America: The History of a Document* (Oxford: Oxford University Press, 2012).

[53] Craig Robertson, *The Filing Cabinet: A Vertical History of Information* (Minneapolis London: University of Minnesota Press, 2021); Cornelia Vismann, *Files: Law and Media Technology*, trans. Geoffrey Winthrop-Young, (Stanford, Calif: Stanford Univ. Press, 2008).

Figure 4 – Exchequer Tally Sticks, ca. 1440. The Board of Trustees of the Science Museum, London.

An early form of such a technique is shown by the Lebombo bone. This artifact is more than 40,000 years old and has notches that are interpreted as an early form of correspondence counting. Correspondence is not about counting. It works by checking whether two quantities are equal. Each bone has a corresponding bone, when held together show notches at the same corresponding places. The consensus lies in recognizing that the correspondence of the notches is a truthful and trustworthy form of statement, about a debt relationship for example. Both parties can agree on the debt not by counting but by looking at the corresponding notches. A more sophisticated form of correspondence counting is the bulla. Bulla are an early form of an accounting system. Bulla are clay envelopes often in spherical form with imprints of tokens which they contain. The tokens inside the bulla represent certain goods like animals, grains, or other goods. They could not be removed without destroying the bulla itself. In order to know what tokens were inside the bulla, these tokens were imprinted on the surface of the bulla. The archaeologist Denise Schmandt-Besserat therefore sees the origin of writing in an early accounting system in the Uruk period around 4000–3100 BC.[54]

Other examples of consensus-making include the Tally Sticks (*fig. 4*). In order to document a credit, both parties "would take a hazelwood twig, notch it

[54] Denise Schmandt-Besserat, *From Counting to Cuneiform* (Austin, Tex: University of Texas Press, 1992).

to indicate the amount owed, and then split it in half. The creditor would keep one half, called 'the stock' (hence the origin of the term 'stock holder') and the debtor kept the other, called 'the stub' (hence the origin of the term 'ticket stub')."[55] A further development in accounting is the double-entry bookkeeping which originated in the 13th century in Italy and established by Luca Pacioli in the late 15th century.[56] Double-entry bookkeeping not only documents income and expenses but also documents them in two accounts for debit and credit. One of the aims of double-entry bookkeeping is to 'balance' the books. This accounting equation is a tool for error detection; the sum of the debits must equal the corresponding sum of the credits, otherwise, an error has occurred. The double-entry bookkeeping, therefore, registers not only transactions but has an inbuilt verification mechanism.

At the center of this transaction lies a legal dimension of consensus-making between the different stakeholders (creditor/debtor; civilian/state; hostage taker/negotiating partner). Verification as consensus-making refers to a legal (and often economic) principle to agree on procedural rules, protocols, involved parties, the objects of negotiation, the tokens to be transacted, including the way the transaction takes place. These procedural rules are often the object of dissent and this is where (political) negotiations take place. Notches, entries in a spreadsheet, or paragraphs express the results of these negotiations, sometimes taking the form of a contract that is even notarized with signatures. Once an agreement is reached, a transition, transmission, or transaction takes place.

This type of verification media is not about information or devices, but about the legal dimension of verification based on rules, administrative procedures, and negotiation techniques. Here, trust is established through a consensus as a socio-technical act that is documented in an accessible, legible, and provable way. The truth of the content is verified by the signatures of concerned parties and/or by a third authoritative entity. Eventually, the performative act of the signature takes center stage often documenting date and location as well.

Infrastructures of Verification

Fourth, we have to contend with the integrity of an account, the document or digitized artifact with regard to its content, coherence, readability, and untampered materiality. This is facilitated by authenticating tools like seals, certificates, signatures, coats of arms, stamps, or watermarks.[57] The importance of authenticating documents was recognized very early on. 2,600 years ago seals with

[55] David Graeber, *Debt: The First 5,000 Years*, (Brooklyn: Melville House, 2014), p. 48.

[56] Alan Sangster, "The Genesis of Double Entry Bookkeeping," *The Accounting Review* 91, no. 1 (January 1, 2016): 299–315, https://doi.org/10.2308/accr-51115.

[57] Lisa Gitelman, *Paper Knowledge: Toward a Media History of Documents*, (Durham; London: Duke University Press, 2014).

Figure 5 – Seal of a shipping container.

inscriptions were used to press them into a damp lump of clay that secured the filament tied around a document. This was a sign of ownership, and confirmed the authenticity of the document, as a signature does today.[58] What survived the ages are the seals hardened by the fires, the measures for security, authentication, and ownership but not the documents themselves which often were burned in fires, lost, or withered away.[59] For historians these artifacts are often important evidence of historical figures and their network of correspondence. Just recently the Pope issued a statement authenticating it with an imprint of his seal (Latin "bullum") on hardened liquefied metal on paper.[60] These papal bulls have been issued using seals since the 6th century eventually receiving their name from the seal that authenticates and certifies them as a message issued by the Pope.

A secular and digital form of such a seal can be found in current PDF readers, which you are probably using right now to read this text. They allow for certificate-based signatures. This digital service allows identifying the person signing the document making it "difficult to forge because it contains encrypted

[58] The Israel Museum, Jerusalem, "Inscribed Hebrew Seals," accessed May 14, 2023, https://www.imj.org.il/en/collections/198071-0.
[59] Schmandt-Besserat, *From Counting to Cuneiform*, 13.
[60] "Papal Bull," in *Wikipedia*, November 28, 2023, https://en.wikipedia.org/w/index.php?title=Papal_bull&oldid=1187307773.

information that is unique to the signer."[61] Once the document is signed, recipients can verify any changes in the document. This ensures that the integrity and authenticity of the document remain intact. Similarly, seals used for shipping containers (fig. 5) ensure that the cargo has not been altered during transport (although different international legal norms and common practice undermine effective security).[62]

A special form of digital verification is verified accounts on social media such as *X*, formerly *Twitter*. Between 2009 and 2021, *Twitter* has introduced the blue checkmark three times, each time with different verification policies. In 2009 it was mostly an invitation-only process and there was no way to apply for verification. *Twitter* took the initiative to contact public figures, inviting them to verify their identity for the purpose of obtaining a verified status on their accounts. In 2016[63] a public submission process was installed and closed again in 2017 after public outcry when a white-nationalist and neo-nazi received the badge.[64] Despite the fact that he obviously violated the *Twitter* guidelines the statement issued by *Twitter* addressed another problem: "Verification was meant to authenticate identity & voice but it is interpreted as an endorsement or an indicator of importance. We recognize that we have created this confusion and need to resolve it. We have paused all general verifications while we work and will report back soon", posted *Twitter* on Nov 9, 2017. Twitter users understood verification as an endorsement rather than an authentication of a user's account. One of the intentions of verified accounts was to fight hate speech, fake accounts, and bots which intentionally post misleading information or in the name of others. New guidelines were introduced, and the verification process was reopened in 2021.[65]

After the takeover of *Twitter* by Elon Musk in 2022 and its rebranding to *X*, the verification system "Twitter blue" was changed to an active subscription "X Premium" in three tiers.[66] Now, user accounts with a badge showing a blue checkmark are not verified accounts but subscriptions. Subscribers benefit from certain services such as reduced ads, and in the second tier, also ID verification.

---

[61] Adobe, "Certificate-Based Signatures," 2023, https://helpx.adobe.com/content/help/en/acrobat/using/certificate-based-signatures.html.

[62] Craig Martin, *Shipping Container*, (New York: Bloomsbury Academic, 2016), 87-90.

[63] Nick Statt, "Twitter Now Lets Anyone Request a Verified Account," The Verge, July 19, 2016, https://www.theverge.com/2016/7/19/12227490/twitter-opening-verified-account-user-form.

[64] Phil McCausland, "Twitter Suspends Verifying Accounts after White Nationalist Gets Badge," *NBC News*, November 9, 2017, https://www.nbcnews.com/news/us-news/twitter-suspends-verifying-accounts-after-white-nationalist-gets-badge-n819491.

[65] X, "Relaunching Verification and What's next," May 20, 2021, https://blog.twitter.com/en_us/topics/company/2021/relaunching-verification-and-whats-next.

[66] X, "About X Premium," October 27, 2023, https://help.twitter.com/en/using-x/x-premium.

The only thing that the blue badge with the white checkmark therefore certifies is the fact that we are dealing with a paying customer who uses a social media service. If the ID of the customer is verified is not transparent to the public. Other subscriptions such as *X Verified Organizations*, introduced in November 2023 "enables organizations of all types – businesses, non-profits, and government institutions – to sign up and manage their verification and to affiliate and verify any related account."[67] Such subscriptions come in a gold checkmark for businesses and a grey checkmark for government organizations. How *X* verifies the integrity of the applications for subscriptions is unclear. At the time of writing, "verified organizations" allow for an affiliation of other accounts with the main verified account. Employees or members can become officially affiliated with the companies they work for or the sports clubs they are part of. Verification here takes on the meaning of paid affiliation. Here, at the center of verification is not the identification of a person but a paying client. Like *Twitter*, verification is being rebranded as a paid service.

What can be separated analytically is in practice a hybrid between the apparatus and the infrastructure of verification. This fourth modality of 'media of verification' addresses the infrastructure, the material foundation on which the operations of verification in media, the devices, documents, artifacts, their administrative regulation, and transactions rely.[68] Truth here is ensured using signals, seals, and certificates which authenticate and certify the integrity of documents, currencies, goods, and services. The form of authentication however can relate to very different phenomena like certificates, sworn-in messengers in the postal service during the Middle Ages, or it can relate to security procedures in supply chains securing the provenance and origin of the cargo. It can also relate to current data centers, with its ecological implications of energy consumption and heat production. This means that building trust through digital forms of verification is highly dependent on an authenticating infrastructure that has not only technological but also broader environmental and social implications, takes time, and is labor-intensive, the underlying principles of which still need to be explored.

Conclusion: Beyond Verification

'Media of verification' is a framework that makes it possible to describe different and novel epistemic practices in a digital society. As shown, verification has different epistemological dimensions, therefore taking on different meanings. For once, it describes the trustworthiness and credibility of a source in the media and

[67] X, "Verified Organizations," 2023, https://help.twitter.com/en/using-x/verified-organizations.

[68] Lisa Parks and Nicole Starosielski, eds., *Signal Traffic: Critical Studies of Media Infrastructures*, The Geopolitics of Information (Urbana: University of Illinois Press, 2015).

therefore establishes signs as traces and eventually evidence in a symbolic system. This paradigm of circumstantial evidence is the basic principle underlying all operations of verification. As an apparatus, it validates the permission to pass a gatekeeping device, which by itself heavily relies on a socio-technical consensus between stakeholders. Infrastructures, on the other hand, enable the authenticity and integrity of files or assign a verification badge to paying customers.

The etymological meaning of verification as "finding the truth" therefore says nothing about whether something is trustworthy, nor does it say anything about the concrete epistemic form. However, verification cannot be understood independently of the epistemic practices of finding evidence, regulating access, building consensus and authenticating stakeholders with their tokens.

As the origin of the fact suggests, 'media of verification' are closely linked to the legal field. Like the legal system, verification cannot function without language, its symbolic system, its interpretation and its various meanings, and it cannot function without validating mere signs as reliable evidence. This is most evident in consensus building, because the legal system embodies a rule-based system that can be used as a reference for decision-making processes and eventually legally binding judgments. However, all of this only works under the legitimacy and integrity of the court and the evidence presented in the courtroom.

'Media of verification' do not necessarily try to find the truth. Seals on shipping containers are not there to find the truth, but to ensure the integrity of the cargo. All these operations are certainly necessary means of ensuring trust in anonymous social relationships, but as indicated here, other layers of verification are also needed. This insufficiency might have to do with the dysfunctions that come with the very verification practices that are here to secure traces, regulate access, establish consensus, or authenticate files and accounts. Traces can be flooded with disinformation and misinterpreted. Access can be regulated to exclude minorities or unwanted political dissidents. The rules can be bent or altered altogether not to establish consensus but a dictate. Files can be forged, certificates be corrupted, and accounts be bought.

For this reason, resistance and forms of inoperability are an inherent part of the 'media of verification.' This does not only include obfuscation and other subversive practices but also other frameworks of verification which either need to be translated into each other or do not acknowledge each other at all. The fragmentation of the Internet to a "splinternet"[69], described also with a pejorative connotation as "Balkanization"[70], goes hand in hand with different verification

[69] Clyde Wayne Crews, "On My Mind," *Forbes*, April 2, 2001, https://www.forbes.com/forbes/2001/0402/036.html.

[70] Amaël Cattaruzza et al., "Sovereignty in Cyberspace: Balkanization or Democratization," in *2016 International Conference on Cyber Conflict (CyCon U.S.)*, 2016, 1–9, https://doi.org/10.1109/CYCONUS.2016.7836628.

systems and is profoundly political. It has not only to do with the different legal frameworks for the regulation of the internet but also with the instruments and protocols used to implement these regulations. A digital sovereignty, therefore, necessarily is based on operations and practices of verification which allow for participation in a digital society. If this participation is regarded trustworthy highly depends on political opinions and other factors as well such as a certain literacy. It is necessary to recognize traces, to click the right buttons, to read and write the right documents. A particular ID is mandatory to access nation states, websites, platforms, or the negotiating table. One must be recognized by other stakeholders under a certain set of rules using authentication mechanisms. Without forms of representation none of these actors in this legal framework would be acknowledged.

Is verification primarily a process that creates elements for its own use, or does it rely on pre-established, deemed-verifiable elements? This distinction is crucial for understanding 'media of verification' and approaches to media studies. From a cultural technique perspective, 'media of verification' is rooted in accounting, writing, stamping, signing, and sealing. Media archaeology, however, allows us to connect current verification media to the history of their respective devices and instruments. These media not only generate but also utilize the elements they produce. Verification serves as an illustration of utilization, while the infrastructure represents the broader framework. From a media philosophical perspective, verification is an ongoing activity, requiring multiple layers of cross-references, relations, safeguards, confirmations, certificates, authentications, and expert opinions to create a reliable network of evidence. This 'verifying drift' within media draws attention to the fact that trust goes beyond verification alone.

There are limits to verification. A specific form of verification even has its own iconography. Like the investigative films mentioned above *The Incredulity of Saint Thomas* by Caravaggio (1601/02) makes use of chiaroscuro, a stark contrast of dark and light areas. However, in the image the form of verification very much differs from other such forms. Here, the touch of the finger by Saint Thomas in the spear wound of Jesus is an indexical reference for the veracity of his revelation. The iconography of this gesture can be traced to Lucio Fontana's *Spatial Concept 'Waiting'* (1960) in which an unpainted canvas has been cut once opening up a hole with a dark space behind the canvas. These Tagli (*Cuts*) have been interpreted in different ways, including wounded skin, female genitalia, as a break with representation, and as a spatial rupture blurring the line between two dimensional and three dimensional space. Reduced to the gesture of pointing to an empty space shows the limits of verification and a turn into belief. Signs, stamps, signatures and seals may help to gain trust, but is that really enough to ultimately arrive at a judgment, consent, agreement, conviction, or acceptance? Does a verification system still require a leap of faith? A verification system can be trusted to work

correctly according to the specifications of the product. But this hardly takes into account personal experiences, predictions, and expectations.

I would like to close with a hypothesis about the ambivalence of 'media of verification'. The positivist concept of verification is based on an epistemology of evidence and relates to the concept of fact, which is at the core of Western science. However, different value systems lead to different views on what is recognized as fact and evidence. Like the fact, 'media of verification' has it's foundation in a rule-based legal system. But since this also depends on different value systems, this leads to different judgments about evidence. There are, therefore, certain limits to 'media of verification' when dependent not on evidence and facts but particular values. In this context, a consensus between different value systems (denial of evidence vs. defense of facts) with their respective forms of verification is incompatible. A common discourse is no longer possible when verification is decoupled from a common referentiality. Jean-François Lyotard described this as the "differend,"[71] a situation in which a common discourse is no longer possible. The fragmentation of the internet is, therefore, not only an effect of different value systems but also of different system of referentiality. While verification media in a democracy also imply the protection of minorities and privacy, authoritarian regimes tend to use them to marginalize minorities and control the population. So how 'media of verification' connect the particular to the universal, how these different systems of verification relate to each other, how they interoperate and how differently they deal with trust will have to be explored at another time.

'Media of verification' have consequences for the understanding of verification, truth and trust. Verification here takes on different meanings, be it as a method for reliable evidence, as a validation for passing, as a consensus between stakeholders, or as an authenticating process. Truth here is established using a web of references based on a paradigm of circumstantial evidence, using at least two devices, by agreeing to specific terms and conditions, and by certificates. The concept of 'media of verification' provides an epistemological framework for a comprehensive understanding of the role of media in trust relationships. From this perspective, trust appears as a matter of evidence, based on instruments, rules and a reliable transmission system. Recognizing the limits of 'media of verification', which nevertheless remain open to transcendental aspects, in turn makes it also possible to define the limits of media and communication studies. This enables a clearer account of the media mechanisms, online and offline, that underpin social cohesion.

[71] Jean-François Lyotard, *The Differend: Phrases in Dispute* (Manchester: Manchester Univ. Press, 1988).

Bibliography

Addy, Edward, Carl Singer, and Lynn Robert Carter. "IEEE Standard for System, Software, and Hardware Verification and Validation." IEEE Standards Association, 2023. https://standards.ieee.org.

Adobe. "Certificate-Based Signatures," 2023. https://helpx.adobe.com/content/help/en/acrobat/using/certificate-based-signatures.html.

"AfD-Verbot der Bundesregierung." Accessed November 30, 2023. https://afd-verbot.de.

"AfD-Verbot der Bundesregierung | Die Beweise." Accessed November 30, 2023. https://afd-verbot.de/beweise.

Axelrod, Robert M. *The Evolution of Cooperation*. New York, NY: Basic Books, 2006.

Broadwater, Luke. "'Trump Was at the Center': Jan. 6 Hearing Lays Out Case in Vivid Detail." *The New York Times*, June 9, 2022, sec. U.S. https://www.nytimes.com/2022/06/09/us/politics/trump-jan-6-hearings.html.

Brunton, Finn, and Helen Fay Nissenbaum. *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, Massachusetts: MIT Press, 2015.

Cattaruzza, Amaël, Didier Danet, Stéphane Taillat, and Arthur Laudrain. "Sovereignty in Cyberspace: Balkanization or Democratization." In *2016 International Conference on Cyber Conflict (CyCon U.S.)*, 1–9, 2016. https://doi.org/10.1109/CYCONUS.2016.7836628.

"Center for Political Beauty." Accessed November 30, 2023. https://politicalbeauty.com/.

Cmiel, Kenneth, and John Durham Peters. *Promiscuous Knowledge: Information, Image, and Other Truth Games in History*. Chicago London: University of Chicago Press, 2020.

Creath, Richard. "Logical Empiricism." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta and Uri Nodelman, Winter 2023. Metaphysics Research Lab, Stanford University, 2023. https://plato.stanford.edu/archives/win2023/entries/logical-empiricism/.

Crews, Clyde Wayne. "On My Mind." *Forbes*, April 2, 2001. https://www.forbes.com/forbes/2001/0402/036.html.

Daniel, Larry E., Lars E. Daniel, and Sue Spielman. *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*. Waltham, Mass: Syngress/Elsevier, 2012.

Daston, Lorraine, and Peter Galison. *Objectivity*. New York, NY: Zone Books, 2010.

Doctorow, Cory. *Homeland*. 1st ed. New York: Tor Teen, 2013.

"EasyPASS - Homepage - What Data Is Collected during (Partially) Automated Border Control?" Accessed November 22, 2023. https://www.easypass.de/EasyPass/EN/Service/FAQ/collected-data.html;jsessionid=07FBE8C52C9CC332D6FF31ADA0660DA4.2_cid379.

Eisenstein, Elizabeth L. *The Printing Press as an Agent of Change: Communications and Cultural Transformations in Early-Modern Europe*. 14th ed. Cambridge: Cambridge University Press, 2009.

Engell, Lorenz, and Bernhard Siegert, eds. *Schwerpunkt alternative Fakten*. Zeitschrift für Medien- und Kulturforschung, Heft 9, 2 (2018). Hamburg: Felix Meiner Verlag, 2018.

Ernst, Christoph. "Medien der Zukunft oder Zukunft der Medien?" In *Medien | Zeiten: Interdependenzen*, edited by Sven Grampp, Peter Podrez, and Nicole Wiedenmann, 331–45. Wiesbaden: Springer Fachmedien, 2023. https://doi.org/10.1007/978-3-658-38688-7_18.

FIDO Alliance. "FIDO2." Accessed December 5, 2023. https://fidoalliance.org/fido2/.

"Gaza: Findings on October 17 al-Ahli Hospital Explosion | Human Rights Watch," November 26, 2023. https://www.hrw.org/news/2023/11/26/gaza-findings-october-17-al-ahli-hospital-explosion.

Ginzburg, Carlo. "Clues: Roots of an Evidential Paradigm." In *Clues, Myths, and the Historical Method*, 96–125. Hanover, London: University Press of England, 1989.

Gitelman, Lisa. *Paper Knowledge: Toward a Media History of Documents*. Durham ; London: Duke University Press, 2014.

González-Bailón, Sandra, and Yphtach Lelkes. "Do Social Media Undermine Social Cohesion? A Critical Review." *Social Issues and Policy Review* 17, no. 1 (2023): 155–80. https://doi.org/10.1111/sipr.12091.

Graeber, David. *Debt: The First 5,000 Years*. Brooklyn: Melville House, 2014.

Graves, Lucas. *Deciding What's True: The Rise of Political Fact-Checking in American Journalism*. New York: Columbia University Press, 2016.

Heidegger, Martin. "Plato's Doctrine of Truth." In *Pathmarks*, edited by William McNeill, 155–82. New York: Cambridge Univ. Press, 1998.

Higgins, Eliot. "MH17 - The Open Source Evidence." bellingcat, October 8, 2015. https://www.bellingcat.com/news/uk-and-europe/2015/10/08/mh17-

the-open-source-evidence/.

Khavin, Dmitriy, Haley Willis, Evan Hill, Natalie Reneau, Drew Jordan, Cora Engelbrecht, Christiaan Triebert, Stella Cooper, Malachy Browne, and David Botti. "Day of Rage: How Trump Supporters Took the U.S. Capitol." *The New York Times*, June 30, 2021, sec. U.S. https://www.nytimes.com/video/us/politics/100000007606996/capitol-riot-trump-supporters.html.

Krämer, Sybille. "Was Also Ist Eine Spur? Und Worin Besteht Ihre Epistemologische Rolle? Eine Bestandsaufnahme." In *Spur. Spurenlesen Als Orientierungstechnik Und Wissenskunst*, edited by Sybille Krämer, Werner Kogge, and Gernot Grube, 11–33. Frankfurt a.M.: Suhrkamp, 2007.

Latour, Bruno. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford Univ. Press, 2007.

Lawson, Amanda. "A Look at Global Deepfake Regulation Approaches." *RAI Institute* (blog), April 24, 2023. https://www.responsible.ai/post/a-look-at-global-deepfake-regulation-approaches.

Liu, Kaijun, Zhou Zhou, Qiang Cao, Guosheng Xu, Chenyu Wang, Yuan Gao, Weikai Zeng, and Guoai Xu. "A Robust and Effective Two-Factor Authentication (2FA) Protocol Based on ECC for Mobile Computing." *Applied Sciences* 13, no. 7 (March 30, 2023): 4425. https://doi.org/10.3390/app13074425.

Lyotard, Jean-François. *The Differend: Phrases in Dispute*. Manchester: Manchester Univ. Press, 1988.

Maher, Charlotte. "Separating Fact from Fiction on Social Media in Times of Conflict." *Bellingcat* (blog), October 26, 2023. https://www.bellingcat.com/resources/how-tos/2023/10/26/separating-fact-from-fiction-on-social-media-in-times-of-conflict/.

Mann, Steve, and Joseph Ferenbok. "New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World." *Surveillance & Society* 11, no. 1/2 (July 16, 2013): 18–34. https://doi.org/10.24908/ss.v11i1/2.4456.

Mantzarlis, Alexios. "Fact-Checking 101." In *Journalism, Fake News & Disinformation*, edited by Cherilyn Ireton and Julie Posetti, 85–100. Paris: UNESCO, 2018. https://unesdoc.unesco.org/ark:/48223/pf0000374458.

Martin, Craig. *Shipping Container*. Object Lessons. New York: Bloomsbury Academic, an imprint of Bloomsbury Publishing Inc, 2016.

McCausland, Phil. "Twitter Suspends Verifying Accounts after White Nationalist Gets Badge." *NBC News*, November 9, 2017. https://www.nbcnews.com/news/us-news/twitter-suspends-verifying-

accounts-after-white-nationalist-gets-badge-n819491.

Meet Face ID and Touch ID for the Web, 2020. https://developer.apple.com/videos/play/wwdc2020/10670/.

Moafi, Samaneh. "The Beirut Port Explosion ← Forensic Architecture," 2020. https://forensic-architecture.org/investigation/beirut-port-explosion.

Myers, Steven Lee, and Sheera Frenkel. "In a Worldwide War of Words, Russia, China and Iran Back Hamas." *The New York Times*, November 3, 2023, sec. Technology. https://www.nytimes.com/2023/11/03/technology/israel-hamas-information-war.html.

"Papal Bull." In *Wikipedia*, November 28, 2023. https://en.wikipedia.org/w/index.php?title=Papal_bull&oldid=1187307773.

Parks, Lisa, and Nicole Starosielski, eds. *Signal Traffic: Critical Studies of Media Infrastructures*. The Geopolitics of Information. Urbana: University of Illinois Press, 2015.

Pérez-Curiel, Concha, and Rubén Rivas-de-Roca. "Social Cohesion in Times of Crisis: The Role of Communication for Democracies—Editors' Introduction." *Social Sciences* 12, no. 9 (September 2023): 491. https://doi.org/10.3390/socsci12090491.

Poovey, Mary. *A History of the Modern Fact: Problems of Knowledge in the Sciences of Wealth and Society*. Chicago: University of Chicago Press, 1998.

pp_pankaj. "Differences between Verification and Validation." *GeeksforGeeks* (blog), April 18, 2019. https://www.geeksforgeeks.org/differences-between-verification-and-validation/.

Qiu, Linda. "Fact-Checking Trump's Election Lies - The New York Times," August 17, 2023. https://www.nytimes.com/2023/08/17/us/politics/trump-election-lies-fact-check.html.

Rau, Milo. *Das Kongo Tribunal*. Edited by Eva Bertschy, Rolf Bossart, and Mirjam Knapp. Berlin: Verbrecher Verlag, 2017.

Robertson, Craig. *The Filing Cabinet: A Vertical History of Information*. Minneapolis London: University of Minnesota Press, 2021.

———. *The Passport in America: The History of a Document*. Oxford: Oxford University Press, 2012.

Rothöhler, Simon. *Medien Der Forensik*. Bielefeld: transcript, 2021.

Sangster, Alan. "The Genesis of Double Entry Bookkeeping." *The Accounting Review* 91, no. 1 (January 1, 2016): 299–315. https://doi.org/10.2308/accr-51115.

Satariano, Adam, and Cecilia Kang. "How Nations Are Losing a Global Race

to Tackle A.I.'s Harms." *The New York Times*, December 6, 2023, sec. Technology. https://www.nytimes.com/2023/12/06/technology/ai-regulation-policies.html.

Schmandt-Besserat, Denise. *From Counting to Cuneiform*. Austin, Tex: University of Texas Press, 1992.

Sellers, M. N. S., Joshua James Kassner, and Colin Starger, eds. *The Value and Purpose of Law: Essays in Honor of M.N.S. Sellers*. Archiv Für Rechts- Und Sozialphilosophie, Beiheft 160. Stuttgart: Franz Steiner Verlag, 2019.

Shapiro, Barbara J. *A Culture of Fact. England 1550-1720*. Hardcover | Cornell University Press, 1999. https://www.cornellpress.cornell.edu/book/9780801436864/a-culture-of-fact/#bookTabs=1.

Siegel, Greg. *Forensic Media. Reconstructing Accidents in Accelerated Modernity*. Durham: Duke University Press, 2014.

Siegert, Bernhard. *Relais: Geschicke der Literatur als Epoche der Post: 1751-1913*. Berlin: B&B, Brinkmann & Bose, 1993.

Silverman, Craig. *Verification Handbook*. Accessed December 5, 2023. https://datajournalism.com/read/handbook/verification-1.

Silverman, Craig, and Rina Tsubaki. "10. Verification Tools." In *Verification Handbook*. Accessed December 5, 2023. https://datajournalism.com/read/handbook/verification-1/verification-tools/10-verification-tools.

Soll, Jacob. "The Long and Brutal History of Fake News." *POLITICO Magazine*, December 18, 2016. http://politi.co/2FaV5W9.

Statt, Nick. "Twitter Now Lets Anyone Request a Verified Account." The Verge, July 19, 2016. https://www.theverge.com/2016/7/19/12227490/twitter-opening-verified-account-user-form.

Stiegler, Bernd. "Conan Doyle, Visual History und das Indizienparadigma." In *Grenzen der Bildinterpretation*, edited by Michael R. Müller, Jürgen Raab, and Hans-Georg Soeffner, 79–96. Wissen, Kommunikation und Gesellschaft. Wiesbaden: Springer Fachmedien, 2014. https://doi.org/10.1007/978-3-658-03996-7_5.

Sunstein, Cass R. "Can the Government Regulate Deepfakes?" *Wall Street Journal*, January 7, 2021, sec. Life. https://www.wsj.com/articles/can-the-government-regulate-deepfakes-11610038590.

Thagard, Paul. "Coherence, Truth, and the Development of Scientific Knowledge." *Philosophy of Science* 74 (2007): 28–47.

The Israel Museum, Jerusalem. "Inscribed Hebrew Seals." Accessed May 14, 2023. https://www.imj.org.il/en/collections/198071-0.

"The Pope Drip." Reddit Post. *R/Midjourney*, March 24, 2023. www.reddit.com/r/midjourney/comments/120vhdc/the_pope_drip/.

"The Problem with Facts | Financial Times," n.d., 18.

"Trace | Etymology of Trace by Etymonline." Accessed November 30, 2023. https://www.etymonline.com/word/trace.

Uslaner, Eric M. *The Oxford Handbook of Social and Political Trust*. Oxford University Press, 2018.

"Verification | Etymology of Verification by Etymonline." Accessed December 5, 2023. https://www.etymonline.com/word/verification.

"Verify | Etymology, Origin and Meaning of Verify by Etymonline." Accessed November 21, 2023. https://www.etymonline.com/word/verify.

Vincent, James. "The Swagged-out Pope Is an AI Fake — and an Early Glimpse of a New Reality," March 27, 2023. https://www.theverge.com/2023/3/27/23657927/ai-pope-image-fake-midjourney-computer-generated-aesthetic.

Vismann, Cornelia. *Files: Law and Media Technology*. Translated by Geoffrey Winthrop-Young. Stanford, Calif: Stanford Univ. Press, 2008.

Weizman, Eyal. *Forensic Architecture: Violence at the Threshold of Detectability*. Brooklyn, NY: Zone Books, 2017.

Weizman, Eyal, and Anselm Franke. *Forensis: The Architecture of Public Truth*. Berlin: Sternberg Press, 2014. http://www.sternberg-press.com/?pageId=1360.

Wingerter, Verena Maria. "Russia's War on the Internet." *Ukraine Analytica* 1, no. 27 (2022): 53–60.

X. "About X Premium," October 27, 2023. https://help.twitter.com/en/using-x/x-premium.

———. "Relaunching Verification and What's next," May 20, 2021. https://blog.twitter.com/en_us/topics/company/2021/relaunching-verification-and-whats-next.

———. "Verified Organizations," 2023. https://help.twitter.com/en/using-x/verified-organizations.

Yuan, Li. "China's Information Dark Age Could Be Russia's Future." *The New York Times*, March 18, 2022, sec. Business. https://www.nytimes.com/2022/03/18/business/chinas-russia-information.html.