



Genealogies of online content identification - an introduction

Maria Eriksson, Guillaume Heuguet

► To cite this version:

Maria Eriksson, Guillaume Heuguet. Genealogies of online content identification - an introduction. Internet histories, 2021, 5 (1), pp.1-7. 10.1080/24701475.2021.1878649 . hal-03135501

HAL Id: hal-03135501

<https://hal.sorbonne-universite.fr/hal-03135501>

Submitted on 9 Feb 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Genealogies of online content identification - An introduction

Guillaume Heuguet and Maria Eriksson

In today's digital landscape, cultural content such as texts, films, images, and recorded sounds are increasingly subjected to automatic (or semi-automatic) processes of identification and classification. On a daily basis, spam filters scan swaths of emails in order to separate legit and illegitimate textual messages (Brunton, 2013), algorithms analyze years of user-uploaded film on YouTube in search for copyright violations (Heuguet, 2019), and software systems are deployed to scrutinize millions of images on social media sites in order to detect sexually offensive content (Liao, 2018). These examples reveal how machines and algorithmic systems are increasingly utilized to make complex judgments regarding cultural content. Indeed, it could be argued that the wide-ranging adoption of content identification systems is constructing new ontologies of culture and regimes of truth in the online domain. When put to action, content identification systems are trusted with the ability to separate good/bad and legal/illegal forms of communication and used to secure the singularity, value, authenticity, origin, and ownership of content. Such efforts are deeply embedded in constructions of knowledge, new forms of political governance, and not least global market transactions. Content identification tools now make up an essential part of the online data economy by protecting the interests of rights holders and forwarding the mathematization, objectification, and commodification of cultural productions.

Parallel to their increased pervasiveness and influence, however, content identification systems have also been increasingly contested. Debates regarding automatic content identification tools recently gained momentum due to the European Union's decision to update its copyright laws. A newly adopted EU directive encourages all platform owners to implement automatic content filters to safeguard copyrights (Spangler, 2019) and critics have argued that such measures run the risk of seriously hampering the freedom of speech and stifling cultural expressions online (e.g., Kaye, 2018). A wide range of high profile tech figures (such as Tim Berners Lee, commonly known as one of the founders of the World Wide Web) have even warned that the widespread adoption of pre-emptive content identification systems could effectively destroy the internet as we know it (Cerf et.al., 2018). Content identification systems, then, are not neutral devices but key sites where the moral, juridical, economical, and cultural implications of online surveillance are currently negotiated and put to the test.

This special issue/section traces the lineage and genealogy of online content identification tools and explores how content identification systems enact cultural values. A key point that the issue seeks to make is that content identification tools do much more than simply identify: at a

technical and semiotic level—and under the pretext of "recognizing" singularities—they model, interpret, calculate, classify, and filter. This is especially the case when content identification techniques acquire infrastructural features, become naturalized, and blend into the technological background of the everyday. Here, content identification systems may be described as bringing forth the various *epistémé* described by Foucault in *The Order of Things*; that is, as part of the conditions that ground truth and discourse and thus create possibilities of action in a given place and moment in time (2005 [1966]). Given that content identification tools often make up a (technical) *a priori* that sorts and secretly manages cultural content, they also shape the unfolding of future events in ways that call for scholarly attention.

Google's Content ID system is particularly illustrative of this point. Since 2007, Google has invested more than \$100 million in developing Content ID; an automated tool for tracing and identifying copyright-protected content on YouTube (Google, 2018). Content ID scans all user-generated YouTube videos prior to their publication and matches them against a reference database that contains more than 75 million copyright-protected reference files (YouTube, 2020). If a video is flagged as a suspect case of copyright abuse, rights holders are notified and given the option to either a) block the video from YouTube, b) allow it to remain on the platform without further actions, or c) claim rights to all future ad revenues that the video generates. In 2018, Google claimed that Content ID handled 98% of all copyright disputes that occurred on the platform (Google, 2018), meaning that its algorithmic system for identifying cultural content has a profound capacity to determine *what* and *how* cultural content is displayed on one of the world's largest online platforms.

Born out of a desire to control the circulation of cultural content online—and not least help secure its "commodity potential" (Appadurai, 1988: 13)—Content ID is an excellent example of a content identification system that blends into the technical background and brings about new regimes of truth concerning legal/illegal, fair/unfair, and appropriate/inappropriate forms of cultural expression. Borrowing from Antoinette Rouvrouy, such regimes of truth "result from technological (rather than human) observation, detection, classification, and forward-looking (and thus predictive rather than purely descriptive) evaluation processes" (2011, p. 5). In doing so, they also introduce new modes of governing that fundamentally rely on the capacity for digital systems to detect, sort, evaluate, and predict. This hints at an epistemological shift—or a new "perceptual regime"—that "appears to follow an inductive (rather than deductive) logic" and privileges statistical observations, and pattern

recognition/correlation above subjective evaluations of content and information (ibid., 12; see also Apprigh et.al., 2018 and Ernst in this issue).

On the one hand, the intensified development of algorithmic content identification tools—such as Content ID—can be seen as the culmination of a series of developments in the history of the Internet and the Web, including the privatization and commercialization of online space, the growing importance of corporate governance principles, and the increased political intervention of nation-states in the field of online expression. On the other hand, systems like Content ID extend much older (and analog) techniques of identification. Here, we might for example think of the myriad ways through which human identification techniques such as passports, fingerprints, and DNA scans have been used to control movement, mobilize economic resources, and uphold law and order (e.g. Lyon, 2009; Torpey, 2000; Cole, 2001). In similar ways as these bodily identification techniques, algorithmic content identification is used to regulate the circulation of cultural objects, distribute financial resources, and permit various forms of remote control and policing at a distance. As David Lyon puts it, practices of identification are often the starting point of surveillance: in order for things and people to be governed, their identities and whereabouts first need to be verified (2009). By enabling things to be seen, discovered, and handled in efficient ways, content identification presents a (pseudo) solution to perceived situations of information overload, at the same time as it promises relief from the challenge of constantly training and updating human specialists, whose judgment and trustworthiness is often called into question.

This question of the skillset involved in the programming and use of content identification tools, and the wider division of labor they imply, raise a series of issues: what cultural assumptions become naturalized when content identification work is automated? How can we account for the cultural and political decisions that underline mundane tools of content identification, such as CAPTCHAs, content “IDs” or “fingerprints,” or text filters? And to what extent does the rootedness of content identification tools in specific historical contexts and projects—religious morals, software development routines, economic ventures, knowledge interests, and deeper material genealogies—define their current orientations?

The issue presents four texts that each reflect on how content identification techniques domesticate and establish new systems for the treatment of cultural content. These contributions emphasize the need to not fetishize the algorithmic formulas that provide identificatory “truths” about cultural content since these tools might function less to recognize

entities than to perform and organize information, the web, and its practices in particular ways. By adopting a genealogical approach, our authors shed light on the objectives and practices that guide content identification techniques and in extension also shape online discourses and digital cultural exchanges. Indeed, isolating the theme of content identification allows us to re-situate political and technological debates concerning the freedom of expression in digital environments as a matter of technical strategies of identification, classification, and regulation. This choice of focus ties in with the growing scientific interest in online content moderation (e.g. Gillespie, 2018; Roberts, 2019), but also differs from this body of research in that it insists on staying with the cultural processes and events that often precedes moderation: practices of authentication, validation, and identification.

Article one, written by Gavin Feller and Andrew Ventimiglia, traces the cultural history of religiously motivated media filtering in the United States and highlights interrelations between copyright law, conservative morals, and neoliberal consumer empowerment ideals. By backtracking a series of legal controversies regarding religiously motivated content filtering services in general—and the streaming service VidAngel in particular—the authors reveal how conservative Christian discourse and spiritual/theological logics have shaped content moderation in the U.S. throughout history. Here, content identification tools appear as nodes in struggles and negotiations over good parenting and consumer freedoms, while we are reminded of the cultural embeddedness of content identification tools.

In contrast to the current focus on ideas around “societies of control” (Deleuze, 1992) rather than traditional forms of repression, the VidAngel case helps us realize how moral values and religious projects resonate in current tech culture and the politics of filtering tools. Somewhat surprisingly, it also shows how conservative values and consumer empowerment ideals (i.e., the right to choose *not* to see parts of a program or movie) are intertwined and legitimize each other, rather than being placed in opposition. VidAngel also presents a great place from which to understand identification and filtering tools not so much as an extra-layer in the circulation of cultural content and commodities, but as something that shapes their very fabric. Here, content identification tools even question the boundaries of cultural productions as works of art, as testified by the juridical debates on whether VidAngel was breaching the integrity of movies—and thus the “moral” part of authorship embedded in copyright.

Article two, written by Brian Justie, directs our attention towards the history of CAPTCHA's—a technology that is widely used to identify and separate human beings from programmed scripts online. The article departs from Walter Benjamin's assertion that human meaning-making is profoundly altered and challenged by advances in machinic mediation and asks how our contemporary condition—which is filled with algorithmic automata and artificial intelligence—muddles our conception of the human/non-human. “What is at stake if computers are increasingly proficient at mimicking humans to such an extent that the two indistinguishable?,” Justie asks, as he sets out to explore how the shifting nature of cybersecurity puzzles “provide insights regarding emergent modes of interaction between computers and humans, and the ways in which this relationship becomes codified in our computational infrastructure.”

Justie illustrates how CAPTCHA technologies have gradually shifted from deploying “*realist*” framework toward a *relational* framework of content identification following its introduction in the late 1990s and steady rise to online ubiquity.” By this, he refers to a broader transformation away from situations where human are asked to verify CAPTCHA's that consist of randomly distorted strings of characters and numbers—riddles which are then checked and compared against a database of correct answers—and towards a situation where CAPTCHAs are designed to make users to provide answers to questions that computers do not know.¹ Justie describes the former as a “*realist*” execution of content identifications (given that quizzes and puzzles are matched against existing fact sheets), while the latter is described as a “*relational*” execution, in the sense that computers “recast content identification tasks as a play of the relation *between* relations.” Here, the combined replies of multiple users are used to establish a ground truth and teach machines how to interpret images, for example. Thereby, Justice shows how content identification tools are not just used to separate bots from humans, but also harnessed to crowdsource information that train machine learning models. This shift highlights a broader transition towards the use of machine learning and artificial intelligence in online content identification. As Justie demonstrates, the history of CAPTCHA reveals how authentication techniques have become detached from the epistemological task of reading clues into things and instead become focused on tracking statistical similarities between models of behaviour.

¹ One of the most famous uses of this new form of CAPTCHA is Google's reCAPTCHA, which asks humans to decipher and identify house numbers and street names in pictures, with the aim of implementing the results in Google Maps.

Article three, written by Wolfgang Ernst, presents a commentary on the media epistemic value of sonic analytics tools. Ernst—who has previously written extensively on media archaeology and media history—directs our attention towards the potential for automatic content identification tools to function as instruments in scientific knowledge production. While Ernst recognizes that commercial content identification tools are often tightly linked to issues of surveillance and censorship, it is not the sociopolitical dimensions of content identification tools that are primarily placed in focus in his text. Rather, Ernst asks how algorithmic content identification systems can provide scholarly insights into new forms of machining reasoning, interpretation, and understanding. Automatic content identification tools “redefine what it means to perceive cultural objects in nonhuman ways,” argues Ernst, who therefore also stresses that such tools require scientific attention in their own right.

In particular, Ernst takes a closer look at sound-related identification technologies and explores how they open new orders of insights into archives in general and sonic archives in particular. When sound is digitized and represented in waveforms, it becomes computable in fundamentally new ways—for instance by way of measuring spectral intensity points, melodic similarities, and frequency patterns. What is radically new about these machinic ways of approaching audio content, Ernst suggests, is how they side-step traditional practices of handling archival content with the help of manual content tags (i.e., metadata that is based on categories such as title, genre, author, etc.). Instead, they allow content to be (re)searched and explored *based on the characteristics of the content itself*. Such modes of content identification—and search techniques—are signal-focused and structured around algorithmic systematizations, rather than discursive, hermeneutic, interpretive, and semantic classifications. For Ernst, we would make a mistake if we would not explore the epistemic potential that such tools may carry—articulations that emerge from *within* technical modes of analysis themselves.

Finally, we publish an interview with Aleksandra Kaminska, whose work on analog identification techniques for valuable paper (money, passports, etc.) serves as a historical backdrop to the digital identification techniques otherwise discussed in the issue. Kaminska’s work explores how authenticity, realness, and originality is “inscribed, mediated, and communicated by and through... media artefacts,” and investigates how moments of identification and authentication help regulate movement and translate between different

cultural/economic systems (Kaminska, 2019a, p. 3). Kaminska introduces the concept of “authentication devices” to describe the “mobile technologies that preserve and communicate realness as they move about the world” (ibid., 6). Importantly, this concept shifts our attention from the careful study of “artifacts like books, printed ephemera, or artworks” to those technologies and systems “that work to maintain and secure (social, political, economic) order” (Kaminska, 2019b, p. 601). In her writings, we are also reminded of how divisions between real/unreal, authentic/fake constantly have to be *produced* through techniques and processes of authentication, where every act of classifying something as true, also produces its opposite: forgeries, copies, and frauds.

In the interview, Kaminska reflects on the dialectics of surface and depth, the aesthetic and even ornamental dimensions of authentication devices, and continuities between digital and analog authentication techniques (such as the use of repetitive geometrical patterns on early banknotes). She also highlights the shifting meanings of “trust” and “skill” that occur when authentication techniques are no longer rooted in the human skill of reading clues (but is still very much present in the work of designing them in ways that are copy-proof and machine-readable) and discuss how values like efficiency and speed have shaped the apparent need for content identification.

Taken together, then, the contributions to this special issue highlight the moral/spiritual dimensions of content identification (Feller and Ventimiglia), the material and axiological continuities and discontinuities between security printing and content identification (Kaminska), the destabilizing effects that content identification tools have on our notions of the human/nonhuman (Justie), and the media epistemic potentials that lie hidden in algorithmic identification tools (Ernst). We hope that these texts will invite more research into the complex means by which machines are trained to find, classify, track, and extract meaning and material identities from cultural content.

References:

Appadurai, A. (Ed.). (1988). *The Social Life of Things: Commodities in Cultural Perspective*. Cambridge University Press.

Apprich, C., Chun, W.H.K, Cramer, F., and Steyerl, H. (2018). *Pattern Discrimination*. University of Minnesota Press.

Brunton, F. (2013). *Spam: A Shadow History of the Internet*. MIT Press.

Cerf, V. et.al. (2018). “Article 13 of the EU Copyright Directive Threatens the Internet.” Open letter, June 12. <https://www.eff.org/files/2018/06/13/article13letter.pdf>.

Cole, S.A. (2001). *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Harvard University Press.

Deleuze, G. (1992). Postscript on the Societies of Control. *October*, 59, 3-7.

Foucault, M. (2012 [1966]). *The Order of Things*. Taylor & Francis.

Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.

Google. (2018). “How Google Fights Piracy.” Report. https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/How_Google_Fights_Piracy_2018.pdf.

Heuguet (2019). “Toward a micropolitics of formats.”. In *Revue d’anthropologie des connaissances*, 13-3. <http://journals.openedition.org/rac/3263>.

Kaminska, A. (2019a). “Storing Authenticity at the Surface and into the Depths: Securing Paper with Human- and Machine-Readable Devices.” *Intermédialités*, 32, n.p. <https://doi.org/10.7202/1058474ar>.

_____ (2019b). “Don’t Copy That: Security Printing and the Making of High-Tech Paper.” *Convergence* 25(4), 590–606. <https://doi.org/10.1177/1354856519845748>.

Kaye, D. (2018). "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression A/ACR/38/35." Report, United Nations Human Rights Council, April 6. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement>.

Liao, S. (2018). "Tumblr will ban all adult content on December 17th." *The Verge*. Dec 3.

Lyon, D. (2009). *Identifying Citizens: ID Cards as Surveillance*. Polity Press.

Roberts, S.T. (2019). *Behind the Screen: Content Moderation in the Shadows of Social Media*. Yale University Press.

Rouvroy, A. (2011). "Governmentality in an Age of Autonomic Computing: Technology, Virtuality and Utopia." In *Autonomic Computing and Transformations of Human Agency*, edited by Mireille Hildebrandt and Antoinette Rouvroy. Routledge, 1-32.

Spangler, T. (2019). "EU Approves Revamped Copyright Rules, Which Would Force Internet Companies to Proactively Block Protected Content." *Variety*. Feb 13.

Torpey, J. (2000). *The Invention of the Passport: Surveillance, Citizenship and the State*. Cambridge University Press.

YouTube. (2020). "YouTube About". Website accessed Dec 22.
<https://www.youtube.com/intl/sv/about/press/>. Saved copy in author's possession.