Kronman, L 2023 Hacking Surveillance Cameras, Tricking AI and Disputing Biases: Artistic Critiques of Machine Vision. *Open Library of Humanities*, 9(2): pp. 1–35. DOI: https://doi.org/10.16995/olh.10181

Open Library of Humanities

Hacking Surveillance Cameras, Tricking AI and Disputing Biases: Artistic Critiques of Machine Vision

Linda Kronman, University of Bergen, NO, linda.kronman@uib.no

In the field of AI, troublesome machine behaviour is a recurring problem, and is particularly worrying when the governance of populations is externalised to machines. This article will focus on machine vision and explore whether hacking as a concept, a method and an ethic, as it has been appropriated by artists, makers and designers, offers ways for citizens to resist surveillant vision. By combining distant and close readings of art hacks in the 'Database of Machine Vision in Art, Games and Narratives' this article demonstrates a shift in resisting machine vision from hacking sensorial devices to tricking intellectual seeing. I call it the 'intuition machine shift' and argue that emergent with this shift is an art hacking strategy which specifically challenges biased machine vision. Drawing from critical making, tactical media and feminist theorisation of hacking, and adopting Mareille Kaufmann's understanding of hacking as a form of disputing surveillance, this article outlines three artistic approaches to hacking machine vision: hacking surveillance cameras, tricking AI and disputing biases. The conceptual contribution of disputing biases is developed further to offer new nuanced understandings of risks and potentials of art hacks to resist biased machine vision.

1. Introduction

AI audits evaluating machine vision applications such as facial recognition repeatedly expose problematic machine behaviour (Bandy, 2021). Several studies show how biased technologies lead to harmful outcomes, while biased machine vision is increasingly recognised as a problem in AI (Myers West et al., 2019; Srinivasan and Chander, 2021; Suresh and Guttag, 2021). In this article I am particularly interested in approaches challenging such harmful biases. The intersection of hacking and art, called art hacks, provides numerous examples of resistance to surveillant machine vision. What kind of artistic approaches to hacking machine vision exist? Are there art hacks that challenge biased machine vision which could potentially provide tactics for citizens to resist oppressive machine vision?

Hacking machine vision implies a certain agency to resist surveillant vision. Hacking might first bring to mind 'teenagers in their bedrooms', because this is how hackers were depicted in early influential hacker movies; or we think of hacking as a criminal act, because the mainstream media typically represent hackers as cyber terrorists (Gordon, 2010; Vegh, 2005). Even though few people have direct experience of hacking state or corporate surveillance, some may have experienced it as part of digital gameplay (Solberg, 2022). Hacking as a concept, a method and an ethic has also been appropriated by artists, makers and designers in nuanced ways, which has transformed the meaning of hacking (Bogers and Chiappini, 2019; Bradbury and O'Hara, 2019). In media art since the 1990s, hybrid groups and individuals identifying themselves to varying degrees as artists, scientists, technicians, craftspersons, theorists and activists have performed hacking-related interventions, such as alteration, reverse engineering, digital hijacking, mutation and subversion under the loose umbrella term of tactical media (Lovink, 2002; Raley, 2009). We can also find multiple artworks critiquing machine vision that can be defined as hacks in the 'Database of Machine Vision in Art, Games and Narratives'[1] (hereafter Machine Vision Database). This is a database which primarily collects creative works that use or reference different types of machine vision technologies. As this article will demonstrate, art comes with a rich variety of hacking tactics, and thereby offers an opportunity to explore ways of resisting machine vision bias.

[1] The Machine Vision Database is a collection of 500 creative works that were collected, interpreted and annotated with metadata as part of the Machine Vision in Everyday Life project at the University of Bergen, to explore the database visit https://machine-vision.no/. For an archived version of the database, see (Rettberg et al., 2022a). The Machine Vision in Everyday Life project website can be found here: https://www.uib.no/en/machinevision. For datasets exported from the Machine Vision Database see (Rettberg et al., 2022b). For detailed descriptions of the database and exported data see: 'Representations of machine vision technologies in artworks, games and narratives: A dataset' (Rettberg et al., 2022c).

To define what counts as hacking machine vision, the first part of this article establishes what hacking in a media art context entails. In addition, I introduce Mareille Kaufmann's proposal to understand hacking as a form of disputing surveillance (2020). By arguing that hacking can be an approach to dispute biases in machine vision, this article contributes a different angle to how we think about bias in the field of AI.[2] After it situates hacking as a media art practice, the second part of this article combines different methods of reading art, thereby contributing to the field of Digital Humanities and Art History by exemplifying an approach to the analysis of artworks which 'simultaneously takes into consideration macro and micro perspectives, that is, a combination of distant and close reading' (Sekelj, 2020: 170).

I start my analysis with a distant reading of art hacks in the Machine Vision Database by asking: which machine vision technologies are hacked in art? A key finding reveals a shift from hacking hardware to tricking software, which is presented in a timeline visualisation (**Figure 1**). This resonates with what Surveillance Studies scholar Andrea Mubi Brighenti observes as a 'shift from sensorial to intellectual seeing' when discussing the paradigm of 'visibility of control' in surveillance assemblages (2010: 138). This means that cameras equipped with AI-powered perception are doing more than capturing and recording; they are also tracking, tracing and making sense of data. Surveillance assemblages are now capable of processing vast amounts of data and of rapid decision-making and, as I argue elsewhere, these machines are equipped with cognitive capacities and operate as 'intuition machines' producing 'technical intuitions' (Kronman, 2020). I thus call this the 'intuition machine shift' as it entails a gradual change from cameras as recording devices to intuition machines. This article highlights that this shift requires new tactics to hack machine vision. Material practices of hacking surveillance camera signals turn into tactics of tricking AI; and what is particularly interesting in this shift is the potential of art hacks to resist machine vision biases.

The intuition machine shift is further examined through a bricolage of network analysis and example art hacks from the database. Acknowledging the 'disbalanced cultural authority of data visualizations' as a 'blind spot', this article uses visualisations as just one step in the research process (Drucker, 2020: 27). The advantage of distant reading of artworks as network visualisations is that this method allows for three hacking machine vision tendencies to be outlined in the Machine Vision Database: hacking surveillance cameras, tricking AI and disputing biases. However, it is important to note that the analysis in this article is constrained by the methodological choice of using the Machine Vision Database. The database primarily collects creative works that either

[2] In this article, AI is understood in the narrow sense as machine learning algorithms.

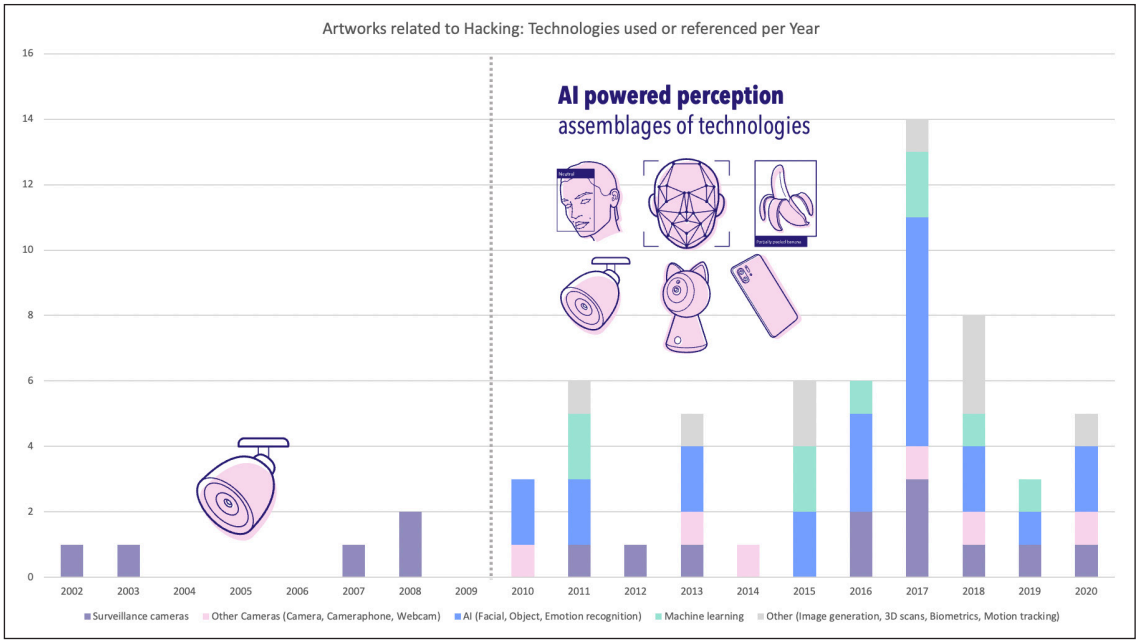

Figure 1: Technologies used or referenced in hacking-related artworks. The grey line indicates the intuition machine shift. The shift also marks a gradual change in hacking tactics. Before 2010, surveillance cameras were hacked as sensory recording devices; thereafter, art hacks have engaged more often with assemblages of AI-powered perception. Figure by author, data source: 'creativeworks.csv' exported from the Machine Vision Database (Rettberg et al., 2022b).

use or reference machine vision. Initially, the categorisation of the Machine Vision Database draws from a broader set of research questions investigating how machine vision is represented in art, games and narratives. Consequently, the perspective this article builds upon comprises critiques of machine vision which are initially recognised as artworks and thereafter as forms of hacking. Many of what would be considered seminal hacking interventions in media art and tactical media are not included in this article because they do not involve machine vision. Grassroots hacktivist projects, if not exhibited in an art context, are also excluded from the database. In addition, this analysis must be understood as a snapshot in time, since 80% of the creative works collected in the database are from 2011 to 2021.

That said, recognising the constraints of chosen methodologies opens new directions for further research, and the topic of hacking machine vision would advance from more multifaceted perspectives such as analysing machine vision hacks collected in an academic database of activist projects. By acknowledging the limitations of chosen methodologies, I wish to clarify that my objective is by no means to present an exhaustive categorisation or a representative list of machine vision hacks in art. Rather, the categorisation is intended to be a context in which to introduce disputing biases as

an emergent art hack tactic and to discuss the potential of art hacks to resist biases in machine vision, as well as the ethical tensions that arise from hacking as an aesthetic.

The first two categories—hacking surveillance cameras and tricking AI—are exemplified by selected artworks in each category. Jill Magid's *System Azure Security Ornamentation* (2002), !Mediengruppe Bitnik's *CCTV – A Trail of Images* (2008) and Helena Nikonole's *deus X mchn* (2017) present different approaches to hacking surveillance cameras. In the Machine Vision Database there is a great variety of 'anti-surveillance artefacts' (Madison and Klang, 2019: 2), which can be described as camouflaging or obfuscating wearables used to trick AI. I have chosen to discuss three artworks that each exemplify slightly different tactics to trick AI: *CV Dazzle* (2010), a camouflage make-up concept by Adam Harvey, and *URME Personal Surveillance Identity Prosthetic* (2013) masks, designed to obfuscate facial recognition, by Leo Selvaggio are both extensively debated in surveillance studies (Brunton and Nissenbaum, 2015; Madison and Klang, 2019; Monahan, 2015; Selvaggio, 2015; de Vries, 2017), while Simone C Niquille's *REALFACE Glamoflage* (2013) is an early example of adversarial patches, now gaining popularity in the fashion industry. Sections on hacking surveillance cameras and tricking AI frame the artistic strategies of hacking machine vision as an evolving practice. The shift from hacking hardware to tricking software provides the context to introduce disputing biases as an emergent hacking strategy. To exemplify how hacks are disputing biases, I have chosen two influential, yet distinctively different, approaches to resisting facial recognition technologies: Joy Buolamwini's viral video poem *The Coded Gaze: Unmasking Algorithmic Bias* (2016a), advocating for algorithmic justice, and Paolo Cirio's *Capture* (2020), a provocative subversion of facial recognition technology.

Since the artworks discussed in this article hack machine vision technologies deployed in different kinds of 'surveillant assemblages', the works discussed in this article can be considered 'surveillance art' (Haggerty and Ericson, 2000; McGrath and Sweeny, 2010). Surveillance is a repeated topic in art, and in surveillance studies art has been examined as a collective imaginary of security, insecurity and control (Arns, 2011; Brighenti, 2010). Surveillance art has also been used to raise awareness of 'the risks posed by surveillance technologies in social and political spheres' (Morrison, 2015). The question of whether surveillance art is 'effective and evoking' in engaging with audiences is still under debate. Whether art provides opposing counter-visualities to totalising regimes of visuality, or enables space for resisting surveillance in other ways (Barnard-Wills and Barnard-Wills, 2012; Hogue, 2016; Madison and Klang, 2019; Monahan, 2015, 2018, 2020). By discussing surveillance art through the lens of hacking machine vision, this article contributes new nuanced understandings of art's capability to resist surveillant vision, and to critique AI-powered perception to these debates.

2. What Counts as Hacking Machine Vision? Drawing from a Hybrid of Hacking Cultures

Initially, hacking was connected to hackers, who were usually described as either skilful programmers invested in understanding how a computer system works, or criminals circumventing computer systems. In 'A Genealogy of Hacking' Tim Jordan describes how hacking emerged with networked computer communication, with a sense that cyberspace has its own values (2017). In these early days, hacking meant manipulating technologies and modifying them to do things they were not intended to do. On the one hand, clever uses and subversions of technologies, a do-it-yourself ethos and sharing knowledge amongst peers were central to the ethos of early hacker communities; on the other, though, in the 1990s hacking became tied to criminalised cybercrime as 'illicitly breaking into someone else's computer' (Jordan, 2017: 534). This definition has stuck to hacking as a term, although hacking practices have developed into various strands.

Hacking is predominantly linked to computing, but can also be applied to non-computing artefacts, and what is produced through hacking can manifest as artefacts, as well as sociality. Examples of this are presented in Christina Dunbar-Hester's study of feminist Free/Libre Open Source Software (FLOSS) collectives, which depict hacking as a practice that 'is uniquely renewable, modifiable, and "versionable" – this is what makes it hacking' (Dunbar-Hester, 2022). Indeed, depending on the context, what is meant by hacking ranges from a narrow definition of hacking as breaking into computer systems, to an extended understanding of hacking as a social practice in which hacking equals change. However, there is concern that the term is watered down when used for any clever practice, such as IKEA hacks.[3] Tim Jordan criticises such uses of the term hacking, arguing that this is a way to diffuse and diminish hacking as a practice which should be reserved for activities that specifically engage with information technologies (2017).

In contrast to Jordan, Otto von Busch interprets McKenzie Wark's 'A Hacker Manifesto' as a new class struggle arguing for opening up the term 'hacking' to include any transformative action, be it physical, semantic or spiritual (von Busch and Palmås, 2006; McKenzie, 2004). He and Karl Palmås suggest the term 'abstract hacktivism' to describe a wider range of hacking cultures and include craftivism, urban hacks and fan fiction as examples. Hacktivism implies that hacking embodies political agency. Initially, it referred to 'exploiting network infrastructure's technical and ontological features, with the final goal of reaching a sociopolitical change in society' (Romagna, 2020).

In media art, hacktivism is closely tied to the genre of tactical media. Tactical media, as 'a deliberately slippery term' (Lovink, 2002: 271), was coined in the 1990s and is inclusive of a wide range of situationist-inspired interventions by practitioners such

[3] IKEA hacks are designs that repurpose IKEA products for use in non-intended ways.

as the Electronic Civil Disobedience movement, the Electronic Disturbance Theatre, Critical Art Ensemble, Institute for Applied Autonomy, Yes Men and Surveillance Camera Players; or, as Geert Lovink described them while theorising tactical media, a 'temporary alliance of hackers, artists, critics, journalists and activists' (2002: 271). In her book *Tactical Media*, Rita Raley describes how this 'politico-aesthetic engagement' of media artist-activists in a network society includes a range of 'practices such as reverse engineering, hacktivism, denial-of-service attacks, the digital hijack, contestational robotics, collaborative software, and open-access technology labs' (Raley, 2009: 6, 25). Lovink describes at length how tactical media practitioners differed in their concerns about the effectiveness and ethics of tactics, particularly when it came to hacktivism activities such as using the Floodnet software, developed by the Electronic Disturbance Theatre for 'virtual sit-ins' (Lovink, 2002: 268). As for hacking, abstract hacktivism supplemented the more disruptive tactical media version with a less confronting version of hacktivism which stands for opening, sharing and exposing the insides of any system which is designed as a black box.

Nevertheless, for many of the artworks discussed in this article the influence of early tactical media is apparent. Tactical media interventions by Surveillance Camera Players can be counted as a precursor for the more recent machine vision art hacks discussed in this article. Surveillance Camera Players was founded in New York in 1996 as an early example of an anti-surveillance group taking a political stance towards machine vision and drawing attention to surveillance cameras in urban settings. Activities of Surveillance Camera Players included mapping CCTV cameras in US cities and ad hoc adaptations of novels like George Orwell's *Nineteen Eighty-Four* in front of security cameras.[4] These acts, directed to unknown control room operators, were repeatedly confronted by security guards or the police and the public could 'witness the spectacle and perhaps the absurdity of modern surveillant relations' (Monahan, 2006: 526). The concept that the ubiquity of surveillance cameras needs to be exposed and that the surveillance of public spaces 'violate[s] our constitutional right to privacy' was already articulated by Surveillance Camera Players (n.d.). Making the invisible layers of surveillance technology visible continued to be one of the main objectives of hacking surveillance cameras in the early 2000s.

Hacking is also defined as activities that take place in hackerspaces. Such spaces are not uniform, however, and they promote a multiplicity of values, issues and tactics (Bazzichelli, 2011; Grenzfurthner and Schneider, 2009). Hacking thus means different things in different hackerspaces. In one hackerspace, hacking can refer to commercial,

[4] Maps by Surveillance Camera Players are available online: https://www.notbored.org/the-scp.html.

techno-positive and innovation-focused making. While another hackerspace may have emerged as a feminist response to experiences of sexism and discrimination in male-dominated hackerspaces (Fox et al., 2015; Toupin, 2014). In feminist hackerspaces, the playfulness of hacking is connected with inclusion, intimacy, care and repair, which challenges the stereotype of hacking as something necessarily masculine, destructive or competitive (Dunbar-Hester, 2022; Savic and Wuschitz, 2018; SSL Nagbot, 2016). Feminist hacking involves tactics of (mis-)use and reverse engineering, which encourages a 'fearless relation to technology' (Savic and Wuschitz, 2018). In a feminist and new materialist critique of hacking, Gareth Foote and Eva Verhoeven discuss local forms of hacking such as 'jugaad'—a hacking practice from India—which can be described as a sort of making that involves augmenting, repairing, improving and subverting designed systems, which is 'driven by environmental and economic conditions of necessity, rather than leisure or profit-driven innovation' (2019: 77).

In many hackerspaces, making and hacking converge into a material practice of hacking. Making in maker culture has been described as a 'sanitised' version of hacking, cleansed of the politics, activism, tactics, history, economics and social issues associated with hacking and hacktivism (Hertz, 2012). In mainstream maker culture, hacking is understood as a creative engagement with technologies. To infuse critical thinking back into hacking and making, the term 'critical making' has been suggested to bridge practices such as critical design, critical engineering and media art, along with other critical practices (Hertz, 2012; 2020; Ratto, 2011; Ratto and Hertz, 2019). Critical making encompasses a variety of approaches that combine material engagement with technologies and cultural reflectivity (Bogers and Chiappini, 2019). In feminist hackerspaces, for example, critical reflection on norms and values is coupled with designing and building objects which 'above all fosters the bending of normalized gender performance' (Savic and Wuschitz, 2018).

What this short summary of different hacking cultures depicts is that hacking can be understood as a broad variety of technology-based approaches and interventions. The art hacks discussed in this article cannot be placed within one of these hacking cultures, nor do they represent a specific set of hacking practices or ethics. Hacking machine vision involves hybrid approaches, in which hacking and making converge. In this article, hacking machine vision includes material practices such as hacking the hardware and signals of surveillance cameras, as well as the designing of anti-surveillance artefacts to trick AI-powered perception. In addition, hacking refers to interventions that subvert the deployment of machine vision. With more focused (yet still somewhat broad) definitions of hacking and art hacks established, we can move forward to discuss how hacking can be a way of resisting and disputing surveillant vision.

3. Hacking as an Approach to Dispute Biases in Machine Vision

In the article 'Hacking Surveillance', Mareile Kaufmann theorises hacking through the notion of dispute rather than hacking as a diverse set of ethics and practices in different hacker cultures (2020). Kaufmann takes the vantage point that there are actors with agency to challenge the totality of surveillance as implied by dominantly ocular-veillance metaphors such as Bentham's 'panopticon' theorised by Foucault, Mathiesen's 'synopticon', an Orwellian 'all-seeing eye', or even Mann's 'sousveillance', referring to watching from below, thereby assuming a hierarchy with a view from above (Foucault, 1979; Mann et al., 2003; Mathiesen, 1997; Orwell, 1977). Inspired by Boltanski's and Thévenot's 'sociology of the dispute' that 'acknowledges the critical capacity of everyday situations', and by analysing interviews with hackers, Kaufmann proposes that hacking accomplishes 'small but continuous resistance' (Boltanski and Thévenot, 1999; Kaufmann, 2020). If hacking is thought about through the dynamics of disputing, then

> Hacking also tends to have a temporality that is not aimed at a final resolution. As a form of dispute, it is more a playful back-and-forth between surveillance mechanisms and those who hack them. Disputes also inspire a re-thinking of norms and practices — something that is in fact a major aspect of hacking (Kaufmann, 2020).

Hacking as a form of dispute is a continuum of interactions in which people and objects are brought together to settle injustice. As an artistic critique, hacking aesthetics are not necessarily aimed at undoing technologies, but negotiating how technologies are designed and deployed. Like tactical media interventions, they are 'never perfect, always in becoming, performative and pragmatic, involved in a continual process of questioning the premises of the channels they work with' (Lovink, 2002: 264). Most of the art hacks in the database dispute naturalised surveillance practices or the loss of privacy.

The key contribution of this article is to recognise an emergent group of machine vision hacks which are disputing biases in machine vision. These hacks present tactics to resist 'oppressive algorithms' (Noble, 2018). The term 'bias' in AI comes with a multiplicity of meanings which themselves are embedded with values and power relations 'that inform what counts as bias and what does not' (Miceli et al., 2022: 2, 34). In this article, aligned with the concept of machine vision bias in the Machine Vision Database, bias comes with negative connotations (Kronman, 2023). Harmful biases come in the form of discrimination, distortion, exploitation, or misjudgement (Bandy, 2021). Such biases propagate inequality by oppressing populations that are already systematically marginalised.

However, there is nothing inevitable about how machine vision is designed or deployed so that art hacks disputing biases are set to challenge harmful and discriminating AI. Artworks disputing biases subvert and reverse surveillant assemblages and bring long histories of discrimination to the surface which are perpetuated in contemporary machine vision technologies (Browne, 2015; Dubrofsky and Magnet, 2015; Gates, 2011; Magnet, 2011). Art hacks exposing historical biases are closely related to two types of machine learning bias, which I will discuss in this article: representation bias and deployment bias. Representation bias (also called sample bias) occurs when a dataset used for machine learning underrepresents a certain population. Consequently, machine vision products fail to generalise accurately: for example, they fail to detect faces or misclassify gender (Suresh and Guttag, 2021: 4). Deployment bias arises when machine vision is deployed to solve a problem, ignoring that 'in reality, it operates in a complicated sociotechnical system moderated by institutional structures and human decision-makers' (6). Even though representation bias can be 'fixed' by balancing out the sample of images in a training set, it will still be harmful if machine vision is deployed by racially biased police enforcement. A 'power-oriented perspective' on bias thereby acknowledges that bias machine vision does not occur in a vacuum and is not merely about technical systems. Bias is 'fundamentally entangled with naturalized ways of doing things' (Miceli et al., 2022: 2, 34). Both biased datasets and deployment biases that occur when machine vision is, for example, used to govern populations, are entangled with human biases and historical biases reflecting 'the world *as it is* or *was*' (Suresh and Guttag, 2021: 4, original emphasis) and a 'debiased' dataset can still lead to discriminatory outcomes.

Disputing biases in this sense is to resist machine vision which inflicts 'allocative harms' (in the form of lost opportunities or resources), or representational harms (e.g., reinforcing a stereotype) on a particular population (Barocas et al., 2017; Suresh and Guttag, 2021). At their best, art hacks disputing biases can succeed in imagining failures of AI by '[f]oreseeing failures and harms that one has not observed before or that occur in new contexts … even when they seem like they should have been predictable in hindsight' (Boyarskaya et al., 2020). However, before moving forward to discuss art hacks disputing machine vision biases, we need an overview of such hacks.

4. Hacking Surveillance Cameras, Tricking AI and Disputing Bias: an Analysis of Art Hacks in the Machine Vision Database

The previous part of this article contextualised what hacking machine vision and disputing biases entails. In this part of the article, I take data visualisations as an initial

method to identify which technologies are hacked by artworks in the Machine Vision Database, and furthermore, what type of hacking-related actions are repeated when artists interact with machine vision. These data visualisations serve a dual purpose: first, I want to draw attention to a shift from hacking surveillance cameras to tricking AI-powered perception. This key finding, the *intuition machine shift*, points towards a change in how we perceive machine vision in surveillance assemblages. The second purpose is to outline three categories of hacking machine vision: hacking surveillance cameras, tricking AI and disputing biases. The first two categories are outlined to support my main argument of an emergent third category of art hack strategies which dispute biases in machine vision. This categorisation of machine vision hacks in the database is by no means exhaustive, and the limited length of this article, for example, excludes discussion about a type of art hack in the database that appropriate machine vision technologies.[5]

I focus on the artworks in the datasets exported from the Machine Vision Database, leaving the games, novels and movies aside. Of the 190 artworks in the database, 36 are related to hacking and they were all created between 2002 and 2020. A sample of 36 hacking-related artworks is by no means representative. However, **Figure 1**—which shows the technologies used or referenced in hacking-related artworks and distributes these on a timeline—clearly marks the intuition machine shift. Out of the 26 machine vision technologies defined in the database, art hacks in the early 2000s are solely about hacking surveillance cameras. As **Figure 1** illustrates, around 2010 there was a shift from hacking surveillance cameras to assemblages of machine vision technologies that enable AI-powered perception. These assemblages usually involve machine learning software such as facial or object recognition, and some type of camera. To explore further what the intuition machine shift encompasses, I turn to a network visualisation of 'Machine Vision Situations' in the Machine Vision Database (depicted in **Figures 2** and **3**) and discuss this intuition machine shift from hacking surveillance cameras to tricking AI through a series of chosen art hacks.

---

[5] A few examples in the database of appropriating machine vision in art hacks are: *MaskID* (2018) by artist collective Peng!, which is an image generation software used to trick facial recognition by combining facial vectors of two individuals into one passport photo. *MakID* can be found in the Machine Vision Database archive (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/maskid/. In *The Other Nefertiti* (2015) Nora Al-Badri and Jan Nikolai Nelles smuggled a 'hacked Kinect', an Xbox 360 sensor which can (among other things) capture depth and full-body 3D, into Neues Museum Berlin and made a 3D scan of Nefertiti's bust. The 'Nefertiti hack' disputes the appropriation of cultural heritage by institutions in the Global North. *The Other Nefertiti* can be found in the Machine Vision Database archive (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/other-nefertiti/.

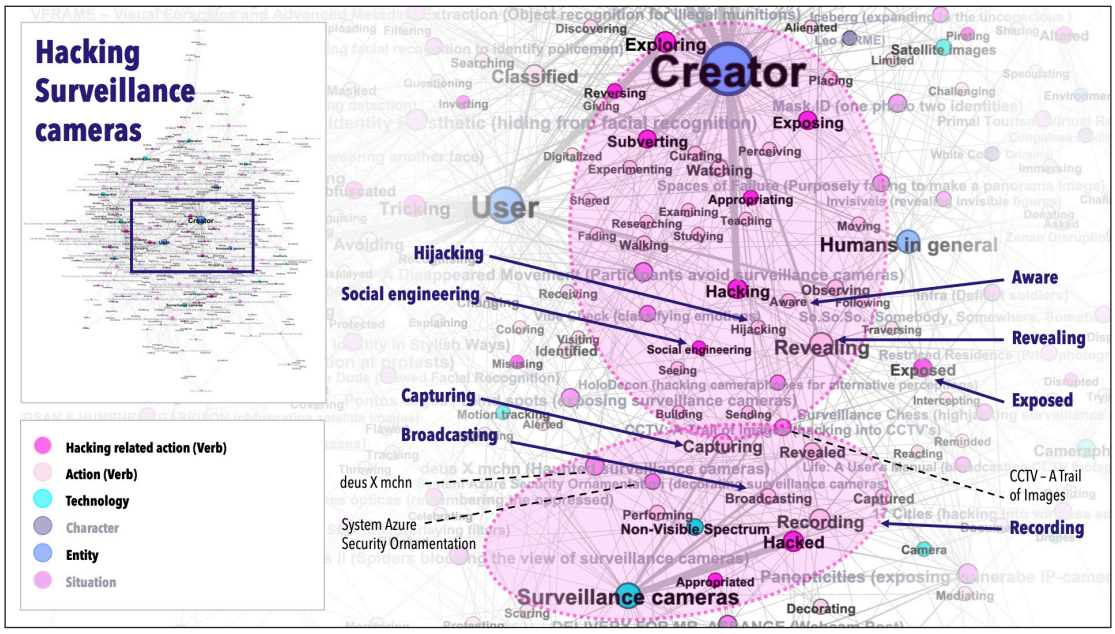

Figure 2: Screenshot of a network visualisation made in Gephi by author, depicting Machine Vision Situations from artworks with hacking or hacking-related verbs like tricking and subverting. The screenshot depicts the emergent assemblage: Creator-Hacking/Surveillance Cameras Hacked. Data source: 'situations.csv' exported from the Machine Vision Database (Rettberg et al., 2022b).

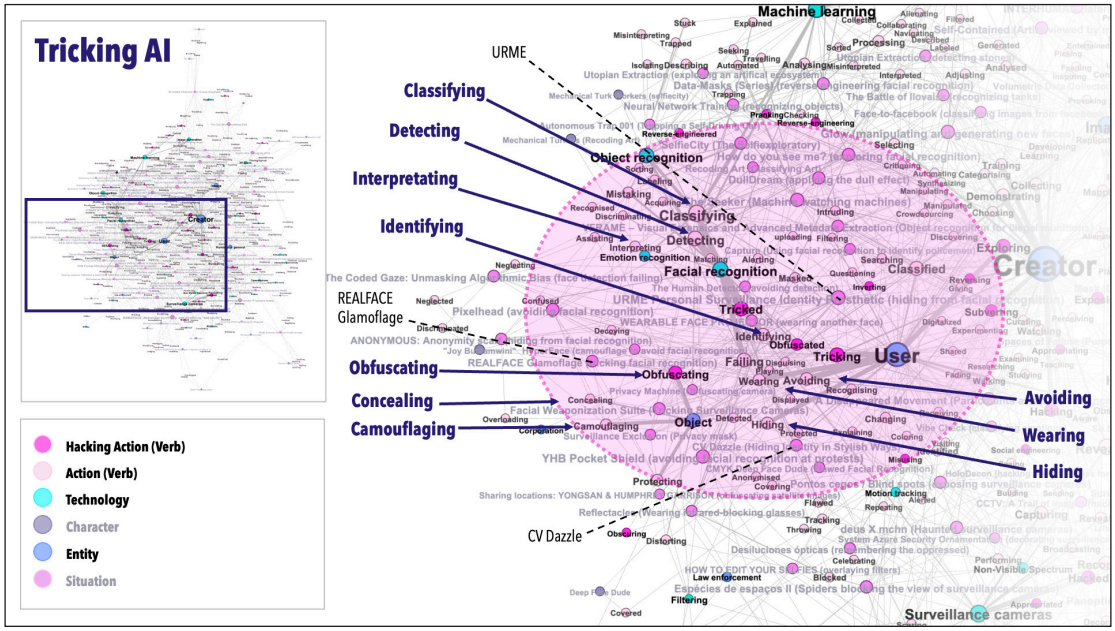

Figure 3: Screenshot of a network visualisation made in Gephi by author, depicting Machine Vision Situations from artworks with hacking or hacking-related verbs like tricking and subverting. The screenshot depicts that several artworks in the database are anti-surveillance artefacts, objects designed to trick and obfuscate AI-powered perception. Data source: 'situations.csv' exported from the Machine Vision Database (Rettberg et al., 2022b).

4.1 Hacking Surveillance Cameras

In the Machine Vision Database, agent interactions in relation to machine vision technologies are described with verbs in Machine Vision Situations (Rettberg et al., 2022a). **Figure 2** shows a network visualisation with the agents, verbs and situations which relate to hacking. In the network visualisation, a strong connection (thick edge) is depicted between the agent node 'Creator' (i.e., artists) and the verb node 'hacking' (i.e., action). Likewise, the visualisation shows that surveillance cameras are predominantly hacked. This means that there are multiple situations in the database which depict artists hacking surveillance cameras.

If we look at other actions in proximity of this emergent—artists hacking surveillance cameras assemblage—we find verbs like 'social engineering' and 'hijacking' that indicate hacking interventions. One example of using the tactic of social engineering is Jill Magid's *System Azure Security Ornamentation* (2002).[6] This hack involved gaining access to Amsterdam Police Headquarters' surveillance cameras and decorating their cases with jewels. Building video transmitters and hijacking signals transmitted by surveillance cameras is another repeated hacking tactic found in the database.[7] Present participle verbs such as 'capturing', 'recording' and 'broadcasting' that cluster with surveillance cameras in the network visualisation (**Figure 2**), is a sign that surveillance cameras are perceived as sensorial devices. *CCTV – A Trail of Images* (2008) by !Mediengruppe Bitnik exemplifies how hacking surveillance cameras is primarily experienced as a material practice and a form of critical making.[8] *CCTV – A Trail of Images* engaged participants in a series of workshops to build surveillance camera sniffers (!Mediengruppe Bitnik, 2009b). With the DIY video transmitters, !Mediengruppe Bitnik then led participants for walks in the city, capturing CCTV signals. The artist duo describes the materiality of captured CCTV signals as images that were displayed by the DIY transmitters:

> Static. When we were kids, we used to call it 'snowstorm' when black and white dots flickered on the TV screen at night after the broadcasting programme had come to an end. We continue on our way, but then the static on the small screen changes

---

[6] *System Azure Security Ornamentation* can be found in the Machine Vision Database archive, (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/system-azure-security-ornamentation/.

[7] Michelle Teran uses a video transmitter to capture CCTV camera signals in her performance *Life: A User's Manual* (2003) and created video installations from the captured video footage *Life: A User's Manual* can be found in the Machine Vision Database archive (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/life-users-manual/. !Mediengruppe Bitnik uses the same tactic in several artworks, including *CCTV – A Trail of Images* (2008), *Militärstrasse 105* (2009a) and *Surveillance Chess* (2012) that can be found in the Machine Vision Database archive (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/surveillance-chess/.

[8] *CCTV – A Trail of Images* (2008) can be found in in the Machine Vision Database archive (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/cctv-trail-images/.

> imperceptibly from flickering specks into grey lines; the sh-sh-sh sound gets softer, stops altogether. Suddenly soft music, first barely audible, then louder: muzak. At the same time, the grey lines ever more distinctly draw the image of an austere interior: bare, functional, a column at the centre, in the background a glass door, to the right a notice board. At first the scene is black and white, then gradually takes on colour, a bit too yellow, a bit too bright (2014).

This description clearly depicts that in early art hacks surveillance cameras were still perceived as sensory devices, mainly capturing recording and transmitting signals.

After the 9/11 terror attacks in 2001, hacking CCTV cameras was a response to the exponential increase in surveillance cameras in public spaces. Surveillance, which had been considered a minority activity undertaken by specific persons or organisations, had gradually turned into a way of life as 'watching and being watched are hard-wired into the smart city' (Lyon, 2018). However, artists like the members of the Security Camera Players group (the previously mentioned tactical media practitioners who had been mapping CCTV cameras since the mid-1990s) argued that installing more cameras would not prevent terrorism or crime. In their opinion, 'surveillance cameras failed to do anything but violate basic human rights', and thus the group would continue disputing 'irrational calls for the installation of *more* surveillance cameras and for the increased use of face recognition software to '"enhance" the performance of these cameras' (2001). Mapping cameras and exposing their whereabouts was a way to oppose the loss of privacy.

Actions like 'revealing', 'exposed' and being 'aware' close to the verb 'hacking' in the network visualisation indicate that one key objective of artists hacking surveillance cameras is to render visible the increase in surveillance technologies in public spaces. Resonating with the concepts of surveillant vision of Surveillance Camera Players, artworks from the early 2000s were created with the specific intention of drawing the audience's attention to surveillance cameras. The *System Azure Security Ornamentation* project exemplified this, exposing surveillance cameras hidden in plain sight by decorating them to stand out (Magid, 2002). Hacking and hijacking surveillance feeds have been conceptualised by artists as explorations of invisible layers of a city. In this context, hacking is a way of exposing, for example, that people are watching 'what they want to protect' (Teran, 2003). In the early 2000s, CCTV infrastructure was costly in relation to today's cheap, easy-to-install, networked IP cameras. Surveillance cameras connected to the Internet of Things have since enabled remote art hacks into spaces which are emotionally or economically valued and worth watching over.

Several art hacks in the Machine Vision Database provoke reflection on the vulnerabilities of networked surveillance technologies,[9] demonstrating how 'security cameras are not quite living up to their name' (Kronman and Zingerle, 2019). Third party access to networked cameras can be surprisingly easy. Helena Nikonole's *deus X mchn* (2017) is only one example of hacking networked cameras in the Machine Vision Database.[10] Most IP cameras are insecure by design, which means that camera manufacturers do not prompt the customer to change the default password. If the password is not changed, anyone can check out the hard-coded default password from a manual and remotely access and operate networked cameras. In *deus X mchn*, the hack also involves converting IP-camera microphones into loudspeakers and then using them to broadcast AI-generated texts. While tactical media interventions by Surveillance Camera Players were spectacles directed at unknown eyes behind CCTV cameras, in *deus X mchn* the attention of those being surveilled is turned to the unknown AI emanating from the camera. Video documentation of people's bewildered reactions to the AI-haunted surveillance cameras in *deus X mchn* shows that in these situations, cameras are suddenly perceived as more than sensorial devices: they have some level of cognitive capacity.

4.2 Tricking AI

Surveillance cameras have gradually turned into intuition machines equipped with machine learning software such as facial, emotion or object recognition. Machine vision is no longer perceived as sensorial recording devices but as a form of intellectual seeing, with cognitive capacities to analyse, predict and classify. This intuition machine shift, which occurred around the 2010s (as depicted in **Figure 1**), also presents new tactics to hack machine vision. Instead of material practices like decorating casings or working with hardware to hack camera signals, art hacks turn into tactics of tricking AI. In **Figure 3**, we see the same network visualisation as earlier, but this time the screenshot focuses on AI technologies such as facial, emotion and object recognition. The hacking-related verb forms clustered with AI technologies are *tricking* and *tricked*. Near to this cluster of AI technologies we also find operations like 'detecting', 'identifying', 'interpreting' and 'classifying', which indicate forms of cognition.

---

[9] Artworks in the Machine Vision Database archive (Rettberg et al., 2022a) that hack networked IP cameras are, for example: *America is Bleeding* (2005) by STANZA https://machinevisionuib.github.io/creative-work/america-bleeding/, and *Panopticities* (2018) by KairUs https://machinevisionuib.github.io/creative-work/panopticities/.

[10] *deus X mchn* (2017) can be found in the Machine Vision Database archive (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/deus-x-mchn/.

What emerges in **Figure 3** is a strong connection between the 'User' and 'tricking' nodes. Close by, we also find the 'Object' entity, which in turn is linked to actions like 'obfuscating', 'concealing' and 'camouflaging'. Halfway between 'User' and 'Object', we find 'wearing'. Indeed, in the Machine Vision Database there is a multiplicity of anti-surveillance artefacts (objects) that artists have designed for users to wear which can trick AI. These designs include masks, make-up and hairstyles, scarves, t-shirts and other wearables. Actions in proximity to 'wearing', like 'avoiding' and 'hiding', entail that anti-surveillance artefacts are intended for a 'play of avoidance' and are worn to avoid detection; to hide from the algorithmic gaze (Monahan, 2015). Perhaps the most well-known example of such play of avoidance is Adam Harvey's *CV Dazzle* (2010).[11] Over a decade ago, Harvey worked with creative directors, make-up artists and models to create fashionable looks which blocked algorithmic face detection. In the title, 'CV' stands for computer vision and 'Dazzle' refers to a camouflage technique used extensively in the First and Second World Wars.

Obfuscation is another tactic used to trick AI. While camouflage tactics like *CV dazzle* block or disrupt the detection of a face, obfuscation is based on sending false signals to confuse facial recognition (Brunton and Nissenbaum, 2015: 8). Often, the algorithm is tricked to identify the individual as someone or something else. *URME Personal Surveillance Identity Prosthetic* (2013) by Leo Selvaggio is an example of obfuscation translated into a contemporary surveillance landscape.[12] Selvaggio offers his own face to be worn as a mask, which comes in two versions: either as a photo-realistic 3D-printed prosthetic or as a printable paper mask. Facial recognition identifies wearers of URME masks such as Leo Selvaggio. Tricked by the false face, the user's 'true' identity is concealed. URME masks are encouraged to be used simultaneously by several people; a multiplicity of Selvaggios recognised at the same time in different places challenges the logic of surveillant vision.

Other wearables, like Simone C Niquille's *REALFACE Glamoflage* (2013) t-shirts trick facial recognition with adversarial attacks.[13] Distorted images of celebrities printed on Niquille's *REALFACE Glamoflage* t-shirts were designed to cause classification errors and 'fool' machine vision (Lee, 2018). The *REALFACE Glamoflage* designs were specifically developed to confuse Facebook's auto-tagging function. Adversarial patches have been

[11] *CV Dazzle* (2010) can be found in the Machine Vision Database archive (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/cv-dazzle/.

[12] *URME Personal Surveillance Identity Prosthetic* (2013) can be found in the Machine Vision Database archive (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/urme-personal-surveillance-identity-prosthetic/.

[13] *REALFACE Glamoflage* (2013) can be found in the Machine Vision Database archive (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/realface-glamoflage/.

further commodified by the fashion industry, for example, a fashion start-up selling patterned knitted clothing claimed to confuse recognition algorithms and misclassify humans as animals (Marks, 2023). The designs are advertised to protect users from the collection of biometric data without the need to cover one's face.

Tricking AI without covering one's face is a response to anti-mask legislation in Europe and North America, which in certain situations prohibits masks and other anti-surveillance designs that block an individual's identification. In places like Hong Kong, banning masks was a direct response from the government to protesters who were circumventing biometric identification (Madison and Klang, 2019: 5). In their awareness of such laws, artists like Selvaggio warn protesters that wearing his masks at protests might be regionally banned and directs readers to 'community resources' with more information about anti-mask laws and a list of alternative interventions to trick AI (Selvaggio, n.d.). As these examples illustrate, if anti-surveillance designs become too practical and popular they might be prohibited by legislation, or risk solidifying surveillance practices by propelling advances in machine vision.

Hille Koskela and Liisa A. Mäkinen understand surveillance through game metaphors like hide-and-seek (2016). Playing the game of avoidance and tricking AI with anti-surveillance designs is a type of urban hide-and-seek. There are some parallels that can be drawn between today's play of avoidance and a more sinister game of hide-and-seek which took place during the First and Second World Wars. During wartime, camouflage artists like British marine artist Norman Wilkinson who is credited for the original Dazzle designs, developed innovative camouflage designs in order to hide battleships and aircraft. The response was to develop new machine vision technologies like infrared night vision; thus, the hide-and-seek game was instrumental in propelling advances in machine vision (Bousquet, 2018).

In contemporary surveillance assemblages, AI-powered perception is developed to serve the desire for control, governance and security. This desire pushes rapid advances in AI technologies. Clever hacks and anti-surveillance artefacts can, at best, buy time with their camouflaging and obfuscating designs (Brunton and Nissenbaum, 2015). On his webpage, Adam Harvey addresses how facial recognition algorithms have evolved since he designed *CV Dazzle* in 2010 (latest update March 1, 2023). The looks—created over a decade ago from the publication of this article—were designed to block face detection with the Viola-Jones algorithm widely used at that time. However, the success of deep convolutional neural networks has made the Viola-Jones algorithm obsolete. Consequently, *CV Dazzle* designs from a decade ago do not work on today's facial recognition algorithms. Harvey stresses that *CV Dazzle* is to be understood as a

concept, rather than a pattern or a product, and that each design needs to be adapted to work for a specific algorithm and with each unique face.

Tactics of tricking AI, which involve anti-surveillance artefacts like *CV Dazzle* or *URME*, have been characterised as hyper-individual approaches that fail to provide meaningful resistance towards dominating regimes of visuality in surveillance (Monahan, 2015; de Vries, 2017). While tactical media practitioners differ in their opinions about the effectiveness of hacking strategies like Denial of Service (DoS), in Surveillance Studies the critiques of anti-surveillance designs question whether such tactics to trick AI manage to oppose surveillant vision in any meaningful way. For example, anti-surveillance artefacts have been critiqued as failures due to their 'hyper-visible invisibility — invisible to recognition technology, but hyper visual on the street' (de Vries, 2017). They are described as 'an *aestheticization of resistance*, a performance that generates media attention and scholarly interest without necessarily challenging the violent and discriminatory logics of surveillance societies' (Monahan, 2015: 160, original emphasis).

However, as exemplified, anti-surveillance designs are not intended to be practical mass market products used on a large scale on the streets. Nor are they intended as solutions for overthrowing the fundamental structural violence embedded in discriminatory surveillance societies. This is similar to how Rita Raley writes about tactical media practioners: 'these artist-activists may not necessarily be invested in the idea of a fundamental structural transformation, but they are invested in cultural critique, itself invested with a transformative power that may not be immediately perceptible but in which one must place a certain belief' (2009: 14). Whether an art hack succeeds or fails is perhaps the wrong question to begin with and we should rather be asking, as Raley suggests, 'to what extent it strengthens social relations and to what extent its activities are virtuosic' (29). By the mention of virtuosity, Raley is referring to the traces a tactical media campaign leaves, and to what extent it is witnessed and recorded into memory as an achievement. In other words, the potential of such art hacks does not lie in developing anti-surveillance products that successfully protect the individual from the unsolicited collection of biometric data. Rather, their success should be evaluated based on how they invite different audiences to join the dispute and to negotiate everyday uses of machine vision technologies.

CV Dazzle, as a concept, has inspired new anti-surveillance designs; it is referenced in science fiction and numerous anti-surveillance makeup tutorials circulating

on YouTube replicate Harvey's concept.[14] As discussed above, artists engage with communities that inform others about legislation, raise awareness of developments in computer vision and develop new artworks. For example, *CV Dazzle* is only one project among many in which Adam Harvey tricks AI or continues to dispute problematics in computer vision (Harvey, undated).[15] The potential of anti-surveillance artefacts like *CV Dazzle* to resist surveillance arises from the way they circulate as a concept, then transform and become part of everyday digital resistance, carving space for critical discourse both online and on the street (Madison and Klang, 2019). In the Machine Vision Database, together with anti-surveillance artefacts, there are art hacks that directly challenge the discriminatory logics of facial recognition. I will now turn to this third type of art hacks called 'disputing biases' to ask: can such art hacks, in a similar way to *CV Dazzle*, carve out space for discourse and consequently present approaches to dispute biased machine vision?

4.2 Disputing Biases

The large number of anti-surveillance artefacts in the Machine Vision Database is clearly apparent from **Figure 3**'s screenshot of the network visualisation. Less apparent in the network visualisation, however, are art hacks which—by tricking AI or subverting the deployment of machine vision—challenge discriminating machine vision; in essence, these are disputing biases. Similar nodes cluster together in network visualisations, and it is therefore sometimes meaningful to look at artworks which are at the fringes of such clusters. By looking at the fringes of the anti-surveillance artefacts cluster, one can find Joy Buolamwini's viral video poem *The Coded Gaze: Unmasking Algorithmic Bias* (2016a), highlighted in **Figure 4**.[16]

---

[14] For example, in Leo Selvaggio's *The YHB Pocket Shield* (2020), the 'H' in the initialism refers to Harvey, whose work among other things has inspired the design of this DIY face shield. It is intended to provide wearers with protection against spreading viruses, and facial recognition. *The YHB Pocket Shield* can be found in the Machine Vision Database (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/yhb-pocket-shield/. Future use of dazzle make-up is imagined, e.g., in Cory Doctorow's science fiction novel *Attack Surface* (2020) as cited in the Machine Vision Database (Rettberg et al., 2022a): https://machine-vision.no/situation/attack-surface-dazzle-makeup. A search query on YouTube for 'anti-surveillance make-up' lists several tutorials guiding viewers to make and test new fashion designs that block facial recognition.

[15] For example, Adam Harvey collaborated with Hyphen-Labs to create *HyperFace* (2017), a scarf which obfuscates facial recognition with faces. *HyperFace* can be found in the Machine Vision Database (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/hyperface/. Stealth Wear (2013), inspired by Islamic dress, is designed to block detection by thermal cameras. Harvey's whole body of work problematises aspects of computer vision: https://ahprojects.com.

[16] *The Coded Gaze: Unmasking Algorithmic Bias* (2016a) can be found in the Machine Vision Database archive: https://machinevisionuib.github.io/creative-work/coded-gaze-unmasking-algorithmic-bias/.

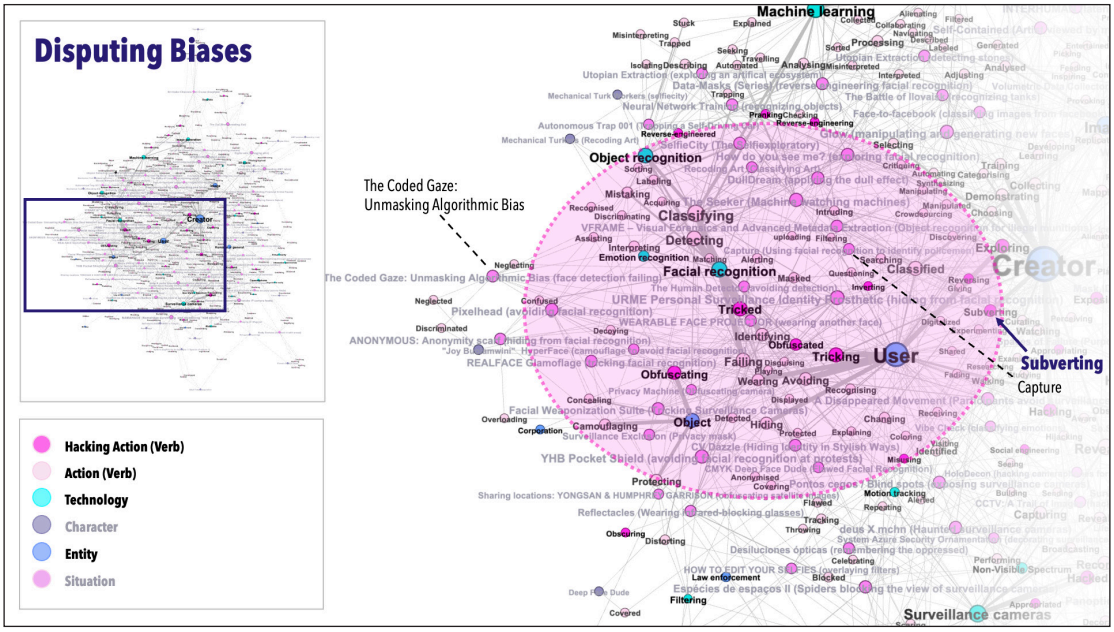

Figure 4: Screenshot of a network visualisation made in Gephi by author, highlighting works disputing biases in machine vision. Data source: 'situations.csv' exported from the Machine Vision Database (Rettberg et al., 2022b).

In *The Coded Gaze* video there is a scene in which the artist tricks AI. As with many anti-surveillance hacks, Joy Buolamwini also wears a mask. Yet as a black woman, she needs to wear a *white* mask—not to avoid detection, but to be visible to 'The Coded Gaze'. As the video poem further explains, Buolamwini's face is only recognised when she wears a white mask, because facial detection software has been trained on a dataset of faces that is disproportionally white. Due to this type of representation bias, Buolamwini is by default invisible to 'The Coded Gaze'. What emerges is a need to trick AI, although in contrast to previously discussed anti-surveillance designs, Buolamwini's trick is to become visible.

Buolamwini has influentially used this scene from *The Coded Gaze* to campaign against discriminating machine vision. The scene also appears in Buolamwini's TED talk and Shalini Kantayya's documentary *Coded Bias* (2020), in which Buolamwini, together with scholars like Meredith Broussard, Cathy O'Neil, Safiya Noble, Timnit Gebru and Virginia Eubanks, discusses forms of oppressive AI (Buolamwini, 2016b; Kantayya, 2020). Thus, Buolamwini's wearing of a white mask to trick AI becomes a symbol of discrimination. In contrast to masks as anti-surveillance artefacts designed to dispute the loss of privacy in public places, Buolamwini's intervention is an art hack that disputes biases in machine vision: it has successfully made visible a certain type

of machine vision bias and carved out space for a discourse which acknowledges that AI-powered perception is experienced differently at the intersections of gender, race and class. With the intuition machine shift, historically discriminatory surveillance practices are amplified by representation and deployment bias.

Discriminatory surveillance practices have a long record and technologies ingrained into surveillance have never been neutral (Browne, 2015; Gates, 2011; Magnet, 2011). Racialised surveillance structures both centre on and ignore black bodies, trapping them between regimes of hypervisibility and invisibility (Benjamin, 2019). With the intuition machine shift, racial bias has been externalised to machines. While enslaved people mandated by 'lantern laws' in 18th-century New York had to carry lit candles to illuminate their faces after dark, Joy Buolamwini had to illuminate her face with a white mask because it was too dark (Browne, 2015: 78).

Historical bias, rooted in eugenics and colonial techniques of population control, codes blackness as a suspicious and criminal other (Sekula, 1986). On the one hand, machine vision algorithms intended to sort populations based on appearance can render othered bodies hypervisible; on the other, AI-powered perception repeats media histories of normalising whiteness and ignoring black and brown bodies. A historical example of this is how photographic film was first calibrated for white skin, with 'Shirley Cards' (Benjamin, 2019: 139). In a similar way, as demonstrated in *The Coded Gaze,* today's biometric technologies are calibrated to privilege a light skin colour, which can be understood as the continuous practice of 'prototypical whiteness' in machine vision (Browne, 2015: 110). For the majority of the world's population, when faces are not detected due to prototypical whiteness, everyday interaction becomes bothersome and such invisibility is undesirable. In *The Coded Gaze*, Buolamwini addresses a different kind of invisibility than anti-surveillance artefacts. Whereas anti-surveillance artefacts strive for privacy, Buolamwini challenges inequalities and ignorance in the ways machine vision systems are designed.

Since bias in machine vision comes in multiple layers; art hacks alone are not a sufficient enough drive for change. Buolamwini thus disputes biases in multiple domains. As an artist in the cultural domain, Buolamwini's viral poems are created with the intention to draw attention to the ways in which AI technologies are experienced differently at the intersections of race and gender. In *The Coded Gaze*, Buolamwini wears the white mask to trick AI. Another of Buolamwini's viral poems, *AI, Ain't I A Woman?*, is what I call an 'artistic audit' which exposes intersectional bias in gender classification products (Buolamwini, 2018; Kronman, 2023). Further, to support creative ways of disputing algorithmic oppression, Buolamwini launched the Algorithmic Justice League: an organisation which raises awareness of biases in

AI systems. As a computer scientist at MIT, Buolamwini disputes machine vision in the technical domain by auditing facial recognition and drawing attention to a lack of diversity in datasets. Buolamwini's project *Gender Shades* is a seminal intersectional audit in the field of computer vision (Buolamwini and Gebru, 2018). Resonating with *AI, Ain't I A Woman?*, *Gender Shades* delivers proof that studied gender classification products were more accurate in predicting the gender of white-skinned males, yet performed poorly for dark-skinned females. The *Gender Shades* project has been highly influential and many computer vision audits stem from this study. In addition, as a researcher and AI expert in the field of computer vision, Buolamwini advises on legislation and witnessed at US Congress on the impact of facial recognition on our civil rights and liberties (Buolamwini, 2019).

Machine vision bias is not solely a technical issue. As a multifaceted problem, machine vision bias can and should be disputed from various angles. Art hacks exposing representation bias, such as *The Coded Gaze*, must be seen as one contribution to this dispute. However, focusing solely on representation bias fosters a concept that the problem can be solved simply by debiasing machine vision with technical fixes to add diversity to datasets and to develop more accurate models. However, such fixes do not prevent discriminating use of technologies. In an ongoing negotiation of how machine vision is designed and used in everyday life, art hacks such as Paolo Cirio's artwork *Capture* (2020) question the ways in which machine vision technologies (for example, facial recognition) are deployed.[17]

In the network visualisation (**Figure 4**), actions such as 'subverting' and 'inverting' also imply the use of hacking tactics. Among artworks connected to the verb 'subverting', Cirio's artwork *Capture* is another art hack which disputes biased machine vision.[18] Consisting of cropped photographs and bearing similarities to facial training sets, *Capture* was presented as a speculative first step in developing a facial recognition application to identify police violence at protests (Burt, 2020). This subversive hack turns facial recognition 'against the same authorities that urge the use of it' (Cirio, 2020). A planned exhibition of *Capture* at Le Fresnoy in Tourcoing provoked media

[17] *Capture* (2020) can be found in the Machine Vision Database archive (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/capture/.

[18] Another example of an art hack disputing biases is Iyo Bisseck's *The Human Detector* (2018) and can be found in the Machine Vision Database archive (Rettberg et al., 2022a): https://machinevisionuib.github.io/creative-work/human-detector/. As a kind of parody on the game of avoidance, Bisseck disputes biases by turning the discriminating AI into a game in which she can 'win every time'. The aim of the game is to move through a room and push a red button without being detected by a huge surveying eye on the screen. The hack is subversive because the sample bias arising from the underrepresentation of black women in the machine learning datasets is turned into a positive situation by the rules of the game.

attention because it coincided with the so-called 'Global Security Law' (N°3452) in France (Bakker, 2020; Beswick, 2020; Loi Sécurité globale, 2020). *Capture* was in particularly disputing Article 24 in the bill that was proposing to ban journalists from publishing images of police officers. Even though the photographs Cirio planned to exhibit did not display any metadata such as names, times or locations, the collected images of police officers incited strong responses. The most prominent response was a tweet from French Minister of the Interior, Gérald Darmanin, who condemned Cirio's work as 'unbearable pillorying of women and men who risk their lives to protect us' (Ní Mhainín, 2020). Darmanin demanded the removal of *Capture* because the published images could be misused and cause harm to the exposed individuals and their families. Perceptibly, the art hack aroused ethical tensions.

Risking legal prosecution, the artwork was withdrawn from the exhibition at Le Fresnoy. Cirio responded with an open letter addressed to Roselyne Bachelot, French Minister of Culture, in opposition to the censuring of his artwork. As intended, the dispute caught people's attention. According to Cirio, '[a]rt provocations are successful when they generate public shock, critical reactions, and strong responses to raise awareness and warn about danger' (Cirio, interviewd in Bishara, 2020). In this sense, *Capture* succeeded: the hack provoked tensions that rose from an ethical dichotomy between privacy and transparency. The media attention was directed at a petition that advocated for the banning of certain types of deployment of facial recognition technologies in Europe. *Capture* clearly managed to draw attention to the topic and around 50,000 signatures were collected for the petition. Although Cirio was cautious not to expose the identity of the police officers in the images, the art hack still exposed them to the public. Nevertheless, the dispute to regulate facial recognition in Europe is still ongoing, although France's legislation to ban journalists from publishing images of the police has since been discarded (Bishara, 2020).

Capture provoked attention because it broke rules, intervening in the normalised use of machine vision at protests. What Cirio challenges is the unjust power asymmetries that arise when facial recognition is deployed to identify individuals at protests. This takes place by conceptually positioning the art hack in a situation where protesters facing police brutality are subject to facial recognition by law enforcement, yet at the same time they lack the rights and means to identify the violent officers they are confronted by. In this case, bias stands for the unfair deployment of machine vision. *Capture* subverts the unfair power asymmetries in the deployment of facial recognition. Somewhat contradictory unjust power asymmetries are reproduced by using the same technology to identify police officers; at the same time, this strategy was the key to drawing attention to this tactical media intervention.

5. The Risks and Potentials of Art Hacks Disputing Biases

The works in the Machine Vision Database clearly show that there is increasing interest among artists in challenging biased machine vision. In this article, I have discussed Joy Buolamwini's *The Coded Gaze* and Paolo Cirio's *Capture* to present two distinctly different approaches to disputing biases in machine vision. Buolamwini advocates changes in how technologies are designed by raising awareness of algorithmic oppression. Cirio provokes the audience to recognise the unfair deployment of machine vision by drawing attention to a campaign to ban certain uses of facial recognition technology. But what are the risks and potentials of the use of hacking as a strategy to dispute machine vision biases?

Kaufmann's examples of disputative engagement with surveillance are based on interviews with self-identified hackers opposed to online dataveillance. Artists are not necessarily identified as hackers; nevertheless, because 'hacking itself is part of a power game', artists hacking surveillance cameras, tricking AI and disputing biases experience similar ethical tensions to hackers working with surveillance (Kaufmann, 2020). There is a risk that art hacks may be counterproductive to an artist's cause. Like hacking online, art hacks might 'reinforce injustices', 'solidify surveillance practices' or 'lead to more encompassing legislation' (Kaufmann, 2020). Hacks like *deus X mchn*, which expose vulnerabilities of networked cameras to challenge surveillance technologies as a solution to our anxieties, risk reproducing cybercrime anxieties. Hacking surveillance cameras and crossing private, personal boundaries by using highjacked surveillance footage in artworks risks the recreation of the very power structures they resist. By individualising the surveillance encounter, a subversive hack like *Capture* 'conflates individuals with the institutions of which they are a part' and, at worst, exposes individuals to '"data violence" … material, symbolic, and other violences inflicted by and through data technologies and their purveyors' (Hoffmann, 2021: 2; Monahan, 2006).

In contrast to most self-identified hackers, artists make their disputes public. Debates and discourse concerning hacktivist tactics have evoked a critical and reflective approach to hacking aesthetics among tactical media practitioners themselves. In an analysis of interviews with 'data artists', Luke Stark and Kate Crawford describe how artists who work with surveillance and hacking are aware that they risk replicating the very same power structures they critique in their art (2019). Artists confronted with ethical and moral justifications for their actions are aware of the ethical dilemmas that hacking aesthetics provoke (Gurses et al., 2010; Romagna, 2020; Stark and Crawford, 2019). Confronted with the 'ethics of ambiguity', and facing critiques of reproducing the unethical dynamics of digital technologies, artists have become more cautious

of their practices and more ‘reflective of their own role and agency as ethical actors’ (Stark and Crawford, 2019: 450).

On the other hand, artists also see a need for expressions which contest societal ethics, and carve out space for discourse by intentionally provoking media attention. Joy Buolamwini’s approach exemplifies a more cautious tactic, as she disputes AI by shifting between being a computer scientist, artist, activist and expert advocating for the regulation of facial recognition. Paolo Cirio, as an acclaimed tactical media practitioner, has used hacking aesthetics successfully in several of his works and intentionally provokes ethical tensions to evoke media attention. He then successfully uses this attention to make room for discourse outside the exhibition space; for example, to debate the dangers of deploying facial recognition. While Cirio, in the role of artist, can take the privileged route and navigate the riskier grey areas of ethics and legality, Buolamwini, who navigates the world of legislation witnessing for US congress to advance her cause, must proceed with caution so as not to be perceived as a threat or to lose credibility (Buolamwini, 2022).

However, an overly cautious approach can easily be subsumed into a growing industry of AI ethics to form a ‘new economy of virtue — a massive network of actors variously situated across industry, civil society, and universities producing and circulating ethics as a service and as a product’ (Phan et al., 2022). If our ‘very understanding of bias and debiasing is inscribed with values, interests, and power relations’, then AI ethics are increasingly adjusted to serve the tech companies that gain from a definition of debiasing which is restricted to technical fixes (Miceli et al., 2022: 2, 34). Even though technical fixes are important steps in thinking about how we design technologies, corrective measures for datasets, the erasure of problematic categories, and human moderators training the models to be fairer can also serve as a form of ‘ethical washing’; a ‘performative façade’ to cover the historical and structural discrimination embedded in AI-powered machine vision (Bietti, 2020). When AI ethics risk becoming a performative façade, art hacks with a more provocative approach can potentially incite reflection and urge a rethinking of biases in AI. Perhaps the next step of disputing bias in machine vision is to hack AI ethics; to challenge asymmetric power relations which emerge through this new economy of virtue, and the narratives enabling tech companies to continue with business as usual.

5. Conclusion

I started this article by situating art hacks as hybrid hacking practices drawing on different hacker cultures. This contextualised artistic interventions of hacking machine

vision within a broad definition of art hacks as exposing, exploring and modifying any type of black boxed systems. After defining what hacking machine vision entails, I used methods of distant reading artworks to render visible the key finding of this article: the intuition machine shift. First depicted in a timeline visualisation that brings to attention that early art hacks in the Machine Vision Database solely engage with surveillance cameras, a change—the intuition machine shift—takes place around 2010, when artworks related to hacking start to involve cameras equipped with AI technologies, such as facial recognition. This change implies that the shift in technology requires new approaches to hacking machine vision. However, a timeline visualisation is limited in scope and tells us little about what this shift entails.

The article thus continues to explore the intuition machine shift through an analysis of a network visualisation depicting the interaction between machine vision technologies and other actors in 'Machine Vision Situations'. The network visualisation is used to outline three partly overlapping approaches of hacking machine vision: hacking surveillance cameras, tricking AI and disputing biases. Acknowledging the limits of data visualisations and analysing art as nodes and edges, the article takes up examples of art hacks in each category, bringing more depth to the analysis. By applying a bricolage of distance and close reading methods, this article demonstrates that early material approaches of hacking surveillance cameras as sensorial recording devices have shifted to performative interventions of tricking machine vision equipped with AI technologies. My naming of the term 'intuition machine shift' emphasises that machine vision technologies are not merely sensorial devices anymore. Intuition machines refer to the cognitive capacities embedded in AI technologies and the reason why machine vision equipped with facial recognition is depicted as being tricked, rather than hacked. I have further argued that emergent with the intuition machine shift is a third type of art hacks: those that dispute biases in machine vision. Partly overlapping with the tactics of tricking AI, the art hacks that I consider to be disputing biases specifically challenge the discriminating design of machine vision, or oppose the oppressive deployment of such technologies.

Returning to the initial question of the potential of art hacks to resist surveillant vision and challenge biases in machine vision, I have made explicit that one art hack alone is not enough to catalyse change. Art hacks are not and should not be seen as a resolution that settles a dispute. Hacking does not revolutionise forms of surveillance, nor does it undo the technologies that it disputes. Hacking, like disputing, is a practice that 'leads to a change with its own temporality, a slow one that builds on ongoing interaction' (Kaufmann, 2020). All types of art hacks—hacking surveillance cameras, tricking AI and disputing biases—thus take part in an ongoing negotiation

of how machine vision is designed and deployed in our everyday lives. Art hacks, such as tactical media interventions, are performative in their nature, leaving traces of a dispute rather than providing solutions. Their potential lies in carving out space for, and even provoking discourse and ethical concerns, thereby bringing new perspectives to the ways of designing and deploying machine vision.

I have exemplified that hacking approaches to disputing biases in machine vision can be distinctively different. Ethically cautious tactics of disputing biases avoid the reproduction of power imbalances which are under critique. In contrast to the cautious approach, a rather risky, yet potentially successful tactic evokes existing power imbalances to draw attention to them. If artists are reflective of their aesthetic choices and aware of the ethical tensions that might arise, then art hacks disputing biases can be seen as a way of negotiating the world views and values embedded in AI. To take art hacks a step further, artists could engage with hacking the definition of machine vision bias itself, and carve out a space for discourse on how technical debiasing is not enough when technologies are deployed in unjust ways.

Acknowledgements

I am grateful to the Machine Vision team for reflective collaboration on the Machine Vision Database and creation of the datasets used in this article. Special thanks for feedback and support goes to my supervisor Jill Walker Rettberg and co-supervisor Audrey Samson, as well as to Nicolas Malevé, who provided valuable critique in the framework of a PhD masterclass which helped me to shape the direction of this article. In addition, I am grateful to the anonymous peer reviewers who provided helpful feedback to develop this article. The research for this article took place as part of the *Machine Vision in Everyday Life: Playful Interactions with Visual Technologies in Digital Art, Games, Narratives and Social Media* project, which is funded by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement no. 771800).

Competing Interests

The author is also an editor of this Special Collection and has been kept entirely separate to the peer review process of their article.

References

Al-Badri, N and **Nelles, J N** 2015 *The Other Nefertiti*. https://alloversky.com/puzzlepieces/the-other-nefertiti [Last Accessed 14 November 2022].

Arns, I 2011 Transparent World: Minoritarian Tactics in the Age of Transparency. In: Pold, S B and Andersen, C U (eds.) *Interface Criticism – Aesthetics Beyond Buttons*. Aarhus, Denmark: Aarhus University Press. pp. 253–276. DOI: https://doi.org/10.2307/jj.608168.15

Bakker, A 2020 *France's Global Security Law: Article 24 and the Right to Information*. London: Public International Law & Policy Group. https://www.publicinternationallawandpolicygroup.org/lawyering-justice-blog/2020/12/13/frances-global-security-law-article-24-and-the-right-to-information [Last Accessed 10 June 2023].

Bandy, J 2021 Problematic Machine Behavior: A Systematic Literature Review of Algorithm Audits. In: *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1): 74:1–34. DOI: https://doi.org/10.1145/3449148

Barnard-Wills, K and **Barnard-Wills, D** 2012. Invisible Surveillance in Visual Art. *Surveillance & Society*, 10(3/4): 204–214. DOI: https://doi.org/10.24908/ss.v10i3/4.4328

Barocas, S, Crawford, K, Shapiro, A and **Wallach, H** 2017 The problem with bias: from allocative to representational harms in machine learning. Presented at the *9th Annual Conference of the Special Interest Group for Computing, Information and Society (SIGCIS)*. Philadelphia, October 29 2017.

Bazzichelli, T 2011 Networked Disruption. Rethinking Oppositions in Art, Hacktivism and the Business of Social Networking. PhD, Aarhus University. https://www.academia.edu/4297418/Networked_Disruption_Rethinking_Oppositions_in_Art_Hacktivism_and_the_Business_of_Social_Networking [Last Accessed 7 December 2022].

Benjamin, R 2019 *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity. DOI: https://doi.org/10.1093/sf/soz162

Beswick, E 2020 Why is France's new national security bill controversial? *euronews*, 28 November. https://www.euronews.com/2020/11/28/why-is-france-s-new-national-security-bill-controversial [Last Accessed 10 June 2023].

Bietti, E 2020 From ethics washing to ethics bashing: a view on tech ethics from within moral philosophy. In: *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, FAT* '20. Association for Computing Machinery*. pp. 210–219. DOI: https://doi.org/10.1145/3351095.3372860

Bishara, H 2020 Massive Protests Sparked by Proposed Ban on Publishing Photographs of French Police. *Hyperallergic*, 1 December. http://hyperallergic.com/604637/massive-protests-sparked-by-proposed-ban-on-publishing-photographs-of-french-police/ [Last Accessed 2 June 2023].

Bisseck I 2018 *The Human Detector*. https://vimeo.com/347283293 [Last Accessed 6 October 2023].

Bogers, L and **Chiappini, L** (eds.) 2019 *The Critical Makers Reader: (Un)learning Technology* (INC Readers). Amsterdam: Institute of Network Cultures.

Bousquet, A 2018 *The Eye of War: Military Perception from the Telescope to the Drone*. Minneapolis, London: University of Minnesota Press. DOI: https://doi.org/10.5749/j.ctv6hp332

Boyarskaya, M, Olteanu, A and **Crawford, K** 2020 Overcoming Failures of Imagination in AI Infused System Development and Deployment. *ArXiv*, abs/2011.13416. https://browse.arxiv.org/pdf/2011.13416.pdf [Last Accessed 6 October 2023].

Bradbury, V and **O'Hara, S** (eds.) 2019 *Art Hack Practice: Critical Intersections of Art, Innovation and the Maker Movement*. New York: Routledge. DOI: https://doi.org/10.4324/9781351241212

Brighenti, A M 2010 Artveillance: At the Crossroads of Art and Surveillance. *Surveillance & Society*, 7(2):175–186. [Last Accessed 14 October 2022]. DOI: https://doi.org/10.24908/ss.v7i2.4142

Browne, S 2015 *Dark Matters: On the Surveillance of Blackness*. Durham: Duke University Press Books. DOI: https://doi.org/10.1515/9780822375302

Brunton, F and **Nissenbaum, H** 2015 *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge: MIT Press. DOI: https://doi.org/10.7551/mitpress/9780262029735.001.0001

Buolamwini, J 2016a *The Coded Gaze: Unmasking Algorithmic Bias*. https://youtu.be/162VzSzzoPs [Last Accessed 3 March 2021].

Buolamwini, J 2016b *Joy Buolamwini: How I'm fighting bias in algorithms* [TED Talk]. https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms [Last Accessed 24 July 2020].

Buolamwini, J 2018 *AI, Ain't I a Woman*. https://youtu.be/QxuyfWoVV98 [Last Accessed 19 January 2022].

Buolamwini, J 2019 *United States House Committee on Oversight and Government Reform: Hearing on Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties*. Washington: U.S. House of Representatives. https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-BuolamwiniJ-20190522.pdf [Last Accessed 6 October 2023].

Buolamwini, J 2022 Facing the Coded Gaze with Evocative Audits and Algorithmic Audits. PhD, Massachusetts Institute of Technology. https://dspace.mit.edu/handle/1721.1/143396 [Last Accessed 7 July 2023].

Buolamwini, J and **Gebru, T** 2018 Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: *Proceedings of Machine Learning Research. Proceedings of the 1st Conference on Fairness, Accountability and Transparency*. New York. 23-24 February 2018. pp. 77–91. http://proceedings.mlr.press/v81/buolamwini18a.html [Last Accessed 27 May 2020].

Burt, C 2020 Facial recognition utilized by protestors around the world to identify police. *Biometric Update*, 23 October. https://www.biometricupdate.com/202010/facial-recognition-utilized-by-protestors-around-the-world-to-identify-police [Last Accessed 2 June 2023].

Cirio, P 2020 *Capture*. https://paolocirio.net/work/capture/ [Last Accessed 6 October 2023].

de Vries, P B 2017. Dazzles, decoys, and deities: the Janus face of anti-facial recognition masks. *Platform: Journal of Media and Communication*. 8(1): 72–86.

Drucker, J 2020 Blind Spot: Information Visualization and Art History. In: Brown, K (ed.) *The Routledge Companion to Digital Humanities and Art History.* New York: Routledge. pp. 18–31. DOI: https://doi.org/10.4324/9780429505188-4

Dubrofsky, R E and **Magnet, S A** (eds.) 2015 *Feminist Surveillance Studies*. Durham: Duke University Press. DOI: https://doi.org/10.1515/9780822375463

Dunbar-Hester, C 2022 Collectivities and Technological Activism: Feminist Hacking. In: Bruun, M H, Wahlberg, A, Douglas-Jones, R, Hasse, C, Hoeyer, K, Kristensen D B, and Winthereik, B R (eds.) *The Palgrave Handbook of the Anthropology of Technology*. Singapore: Springer. pp. 467–483. DOI: https://doi.org/10.1007/978-981-16-7084-8_24

Foote, G and **Verhoeven, E** 2019 Tactics for a More-Than-Human Maker Culture. In: Bogers, L and Chiappini, L (eds.) *The Critical Makers Reader: (Un)Learning Technology* (INC Readers). Amsterdam: Institute of Network Cultures. pp. 72–85.

Gates, K 2011 *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: NYU Press.

Grenzfurthner, J and **Schneider, F A** 2009 *Hacking the Spaces*. Monochrom Blog. http://www.monochrom.at/hacking-the-spaces/ [Last Accessed 15 July 2022].

Gurses, S, Teran, M and **Luksch, M** 2010 A Trialogue on Interventions in Surveillance Space: Seda Gürses in conversation with Michelle Teran and Manu Luksch. *Surveillance & Society*, 7(2): 165–174. [Last Accessed 14 October 2022]. DOI: https://doi.org/10.24908/ss.v7i2.4141

Harvey, A 2010 (updated March 1, 2023) *CV Dazzle*. https://adam.harvey.studio/cvdazzle/ [Last Accessed 5 October 2023].

Harvey, A 2013 *Stealth Wear*. https://adam.harvey.studio/stealth-wear/ [Last Accessed 6 October 2023].

Harvey, A n.d. *Adam Harvey Studio*. https://adam.harvey.studio/ [Last Accessed 5 October 2023].

Harvey, A and **Hyphen-Labs** 2017 *HyperFace*. https://adam.harvey.studio/hyperface/ [Last Accessed 5 October 2023].

Hertz, G 2012 *Making Critical Making*. In: Hertz, G. (ed.) *Critical Making: Introduction.* Hollywood: Telharmonium Press.

Hertz, G 2020 *Two Terms: Critical Making + D.I.Y. The studio of critical making*. The studio of critical making. http://conceptlab.com/2terms/pdf/hertz-2terms-202011181901.pdf [Last Accessed 12 July 2022].

Hoffmann, A L 2021 Terms of inclusion: Data, discourse, violence. *New Media & Society*. 23(12): 3539–3556. [Last Accessed 2 June 2023]. DOI: https://doi.org/10.1177/1461444820958725

Hogue, S 2016 Performing, Translating, Fashioning: Spectatorship in the Surveillant World. *Surveillance & Society*, 14(2):168–183. 1461444820958725 [Last Accessed 18 October 2023]. DOI: https://doi.org/10.24908/ss.v14i2.6016

Jordan, T 2017 A genealogy of hacking. *Convergence: The International Journal of Research into New Media Technologies*, 23(5): 528–544. [Last Accessed 11 July 2022]. DOI: https://doi.org/10.1177/1354856516640710

KairUs 2018 *Panopticities*. https://kairus.org/portfolio/panopticities-2018/ [Last Accessed 6 October 2022].

Kantayya, S (dir.) 2020 *Coded Bias*. Netflix.

Kaufmann, M 2020 Hacking surveillance. *First Monday*, 25(5). [Last Accessed 3 July 2022]. DOI: https://doi.org/10.5210/fm.v25i5.10006

Koskela, H and **Mäkinen, L A** 2016 Ludic encounters – understanding surveillance through game metaphors. *Information, Communication & Society*, 19(11):1523–1538. [Last Accessed 11 November 2022]. DOI: https://doi.org/10.1080/1369118X.2015.1126330

Kronman, L 2020 Intuition Machines: Cognizers in Complex Human-Technical Assemblages. *A Peer-Reviewed Journal About*, 9(1):54–68. [Last Accessed 17 October 2022]. DOI: https://doi.org/10.7146/aprja.v9i1.121489

Kronman, L 2023 Classifying Humans: The Indirect Reverse Operativity of Machine Vision. *Photographies*, 16(2): 263–289. [Last Accessed 30 June 2023]. DOI: https://doi.org/10.1080/17540763.2023.2189160

Kronman, L and **Zingerle, A** 2019 Panopticities. In: *ARTHEC 2019: Proceedings of the 9th International Conference on Digital And Interactive Arts (ACM)*. Braga, Portugal, 23–24 October 2019. pp. 75–78. DOI: https://doi.org/10.1145/3359852.3359957

Lee, R 2018 Seeing with Machines: Decipherability and Obfuscation in Adversarial Images. In: *Proceedings of the 24th International Symposium on Electronic Art* (ISEA). Durban, South Africa, 24 June 2018. pp. 321–324. https://isea-archives.siggraph.org/wp-content/uploads/2021/02/2018_Lee_Seeing_with_Machines.pdf [Last Accessed 6 October 2023].

Loi Sécurité globale 2020 Proposition de loi n°3452 – 15e législature – relative à la sécurité globale. Paris: Assemblée nationale. https://www.assemblee-nationale.fr/dyn/15/textes/l15b3452_proposition-loi [Last Accessed 6 October 2023].

Lovink, G 2002 *Dark fiber: tracking critical Internet culture, Electronic culture – history, theory, practice*. Cambridge: MIT Press. DOI: https://doi.org/10.7551/mitpress/2272.001.0001

Lyon, D 2018 *The Culture of Surveillance: Watching as a Way of Life*, 1st ed. Cambridge and Medford: Polity.

Madison, N and **Klang, M** 2019 Recognizing Everyday Activism: Understanding Resistance to Facial Recognition [Preprint]. *Journal of Resistance Studies*, 2: 97–113. https://www.researchgate.net/publication/339077140_Recognizing_Everyday_Activism_Understanding_Resistance_to_Facial_Recognition [Last Accessed 6 October 2023].

Magid, J 2002 *System Azure Security Ornamentation*. https://www.jillmagid.com/projects/system-azure-security-ornamentation [Last Accessed 5 October 2023].

Magnet, S A 2011 *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham and London: Duke University Press. DOI: https://doi.org/10.1515/9780822394822

Mann, S, Nolan, J and **Wellman, B** 2003 Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society* 1(3), 331–355. [Last Accessed 10 January 2020]. DOI: https://doi.org/10.24908/ss.v1i3.3344

Marks, A 2023 Cap_able blocks facial recognition software with knitted clothing. *Dezeen*, 7 February. https://www.dezeen.com/2023/02/07/cap_able-facial-recognition-blocking-clothing/ [Last Accessed 2 September 2023].

McGrath, J and **Sweeny, R J** 2010 Editorial: Surveillance, Performance and New Media. *Surveillance & Society*, 7(2): 90–93. [Last Accessed 19 October 2022]. DOI: https://doi.org/10.24908/ss.v7i2.4134

!Mediengruppe Bitnik 2008 *CCTV – A Trail of Images*. https://wwwwwwwwwwwwwwwwwwwwww.bitnik.org/c/ [Last Accessed 28 August 2019].

!Mediengruppe Bitnik 2009a *Militärstrasse* 105. https://wwwwwwwwwwwwwwwwwwwwww.bitnik.org/m/ [Last Accessed 28 August 2019].

!Mediengruppe Bitnik 2009b *CCTV – A Trail of Images – zine*. https://wwwwwwwwwwwwwwwwwwwwww.bitnik.org/media/c/fanzine_london.pdf [Last Accessed 11 September August 2022].

!Mediengruppe Bitnik 2012 *Surveillance Chess*. https://wwwwwwwwwwwwwwwwwwwwww.bitnik.org/s/ [Last Accessed 28 August 2019].

!Mediengruppe Bitnik 2014 Surveillance Chess. *Surveillance & Society*, 12(3): 459–465. [Last Accessed 14 October 2022]. DOI: https://doi.org/10.24908/ss.v12i3.4952

Miceli, M, Posada, J and **Yang, T** 2022 Studying Up Machine Learning Data: Why Talk About Bias When We Mean Power? In: *Proceedings of the ACM on Human-Computer Interaction 6* (GROUP). pp. 34:1–34. [Last Accessed 17 November 2022]. DOI: https://doi.org/10.1145/3492853

Monahan, T 2006 Counter-surveillance as Political Intervention? *Social Semiotics*, 16(4): 515–534. [Last Accessed 10 October 2022]. DOI: https://doi.org/10.1080/10350330601019769

Monahan, T 2015 The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance. *Communication and Critical/Cultural Studies*, 12(2): 159–178. [Last Accessed 19 September 2022]. DOI: https://doi.org/10.1080/14791420.2015.1006646

Monahan, T 2018 Ways of being seen: surveillance art and the interpellation of viewing subjects. *Cultural Studies*. 32(4): 560–581. [Last Accessed 17 October 2022]. DOI: https://doi.org/10.1080/09502386.2017.1374424

Monahan, T 2020 The arresting gaze: Artistic disruptions of antiblack surveillance. *International Journal of Cultural Studies*, 23(4): 564–581. [Last Accessed 17 October 2022]. DOI: https://doi.org/10.1177/1367877920901859

Morrison, E 2015 Surveillance society needs performance theory and arts practice. *International Journal of Performance Arts and Digital Media*, 11(2): 125–130. [Last Accessed 19 September 2022]. DOI: https://doi.org/10.1080/14794713.2015.1084812

Myers West, S, Whittaker, M and **Crawford,** K 2019 *Discriminating Systems Gender, Race, and Power in AI*. New York: AI Now Institute. https://ainowinstitute.org/discriminatingsystems.pdf [Last Accessed 23 Juni 2019].

Ní Mhainín, J 2020 French exhibition on facial recognition cancelled over claims it violates police privacy. *Index on Censorship*. 14 October 2020. https://www.indexoncensorship.org/2020/10/french-exhibition-on-facial-recognition-cancelled-over-claims-it-violates-police-privacy/ [Last Accessed 2 June 2023].

Nikonole, H 2017 *deus X mchn*. http://nikonole.com/deusxmchn [Last Accessed 28 August 2019].

Niquille, S C 2013 *REALFACE Glamoflage*. https://www.wired.com/2013/10/thwart-facebooks-creepy-auto-tagging-with-these-bizarre-t-shirts/ [Last Accessed 6 October 2023].

Noble, S U 2018 *Algorithms of Oppression: How Search Engines Reinforce Racism* [e-book]. New York: New York University Press. DOI: https://doi.org/10.2307/j.ctt1pwt9w5

Peng! 2018 *MaskID*. https://pen.gg/campaign/mask-id-2/ [Last Accessed 6 October 2023].

Phan, T, Goldfein, J, Kuch, D and **Mann, M** 2022 Introduction: Economies of Virtue. In: *Economics of Virtue – The Circulation of 'Ethics" in AI* (INC Theory on Demand). Amsterdam: Institute of Network Cultures. pp. 6–22.

Raley, R 2009 *Tactical Media*. Minneapolis: University of Minnesota Press.

Ratto, M 2011. Critical Making: Conceptual and Material Studies in Technology and Social. *The Information Society*, 27(4): 252–260. [Last Accessed 13 July 2022]. DOI: https://doi.org/10.1080/01972243.2011.583819

Ratto, M and **Hertz, G** 2019 Critical Making and Interdisciplinary Learning: Making as a Bridge between Art, Science, Engineering and Social Interventions. In: Bogers, L and Chiappini, L (eds.) *The Critical Makers Reader: (Un)Learning Technology* (INC Readers). Amsterdam: Institute of Network Cultures. pp. 17–28.

Rettberg, J W, Kronman, L, Solberg, R, Gunderson, M, Bjørklund, S M, Stokkedal, L H, de Seta, G, Jacob, K and **Markham, A** 2022a *Database of Machine Vision in Art, Games and Narratives: Archival Version in HTML and CSS*. [Last Accessed 5 March 2022]. DOI: https://doi.org/10.5281/zenodo.6514729

Rettberg, J W, Kronman, L, Solberg, R, Gunderson, M, Bjørklund, S M, Stokkedal, L H, de Seta, G, Jacob, K, Markham, A 2022b *A Dataset Documenting Representations of Machine Vision Technologies in Artworks, Games and Narratives*. DataverseNO. [Last Accessed 6 October 2023]. DOI: https://doi.org/10.33767/osf.io/pev43

Rettberg, J W, Kronman, L, Solberg, R, Gunderson, M, Bjørklund, S M, Stokkedal, L H, Jacob, K, de Seta, G, Markham, A 2022c Representations of machine vision technologies in artworks, games

and narratives: A dataset. *Data Brief* 42, 108319. [Last Accessed 5 October 2022]. DOI: https://doi.org/10.1016/j.dib.2022.108319

Romagna, M 2020 Evolution of Hacktivism: From Origins to Now. In: Guntarik, O and Grieve-Williams, V (eds.) *From Sit-Ins to #revolutions: Media and the Changing Nature of Protests*. New York: Bloomsbury Publishing. pp. 65–76. DOI: https://doi.org/10.5040/9781501336980.ch-005

Savic, S and **Wuschitz, S** 2018 Feminist Hackerspace as a Place of Infrastructure Production *Ada: a Journal of Gender, New Media & Technology* 2018(13). https://adanewmedia.org/2018/05/issue13-savic-wuschitz/ [Last Accessed 20 July 2020]. DOI: https://doi.org/10.5399/uo/ada.2018.13.10

Sekelj, S 2020 Qualitative Approaches to Network Analysis in Art History: Research on Contemporary Artists' Networks. In: Brown, K (ed.) *The Routledge Companion to Digital Humanities and Art History*. New York: Routledge. pp. 120–134. DOI: https://doi.org/10.4324/9780429505188-12

Sekula, A 1986. The Body and the Archive. *October*, 39(Winter 1986): 3–64. DOI: https://doi.org/10.1021/cen-v064n039.p003

Selvaggio, L 2013 *URME Personal Surveillance Identity Prosthetic*. https://www.urmesurveillance.com/urme-prosthetic [Last Accessed 6 October 2023].

Selvaggio, L 2015 URME Surveillance: performing privilege in the face of automation. *International Journal of Performance Arts and Digital Media*, 11(2): 165–184. [Last Accessed 19 September October 2022]. DOI: https://doi.org/10.1080/14794713.2015.1086138

Selvaggio, L 2020 *YHB Pocket Protest Shield*. https://sites.google.com/view/yhbpocketprotestshield/about [Last Accessed 5 October 2023].

Selvaggio, L n.d. *Resources – URME Surveillance*. http://www.urmesurveillance.com/resources [Last Accessed 6 October 2023].

Solberg, R 2022 (Always) Playing the Camera: Cyborg Vision and Embodied Surveillance in Digital Games. *Surveillance & Society*, 20(2): 142–156. [Last Accessed 24 October 2022]. DOI: https://doi.org/10.24908/ss.v20i2.14517

Srinivasan, R and **Chander, A** 2021 Biases in AI Systems: A survey for practitioners. *Queue*, 19(2): 45–64. [Last Accessed 17 November 2022]. DOI: https://doi.org/10.1145/3466132.3466134

SSL Nagbot 2016 Feminist Hacking/Making: Exploring new gender horizons of possibility. *The Journal of Peer Production*, (#8 Feminism and (un)hacking). http://peerproduction.net/issues/issue-8-feminism-and-unhacking-2/feminist-hackingmaking-exploring-new-gender-horizons-of-possibility/ [Last Accessed 3 July 2022].

Stanza 2005 *America Is Bleeding*. http://www.stanza.co.uk/new_york_stories/index.html [Last Accessed 28 August 2019].

Stark, L and **Crawford, K** 2019 The Work of Art in the Age of Artificial Intelligence: What Artists Can Teach Us About the Ethics of Data Practice. *Surveillance & Society*, 17(3/4): 442–455. [Last Accessed 14 October 2022]. DOI: https://doi.org/10.24908/ss.v17i3/4.10821

Suresh, H and **Guttag, J V** 2021 A Framework for Understanding Sources of Harm throughout the Machine Learning Life Cycle. In: *Proceedings of EAAMO '21: Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO '21)*. New York, October 5 – 9 2021. Article No 17 pp. 1–9. [Last Accessed 17 November 2022]. DOI: https://doi.org/10.1145/3465416.3483305

Surveillance Camera Players 2001 *September 11th 2001*. https://www.notbored.org/change.html [Last Accessed 5 May 2023].

Surveillance Camera Players n.d. *Surveillance Camera Players*. https://www.notbored.org/the-scp.html [Last Accessed 10 May 2023].

Teran, M 2003 *Life: a user's manual*. http://www.ubermatic.org/life/ [Last Accessed 29 August 2019].

Toupin, S 2014 Feminist Hackerspaces: The Synthesis of Feminist and Hacker Cultures. *The Journal of Peer Production*, (5). http://peerproduction.net/issues/issue-5-shared-machine-shops/peer-reviewed-articles/feminist-hackerspaces-the-synthesis-of-feminist-and-hacker-cultures/ [Last Accessed 15 July 2022].

Vegh, S 2005 The media's portrayal of hacking, hackers and hacktivism before and after September 11. *First Monday*. https://firstmonday.org/ojs/index.php/fm/article/download/1206/1126/11411 [Last Accessed 20 May 2022]. DOI: https://doi.org/10.5210/fm.v10i2.1206

von Busch, O and **Palmås, K** 2006 *Abstract hacktivism: the making of a hacker culture*. London: OpenMute.