Toward a critique of algorithmic violence

Bellanova, R.; Irion, K.; Lindskov Jacobsen, K.; Ragazzi, F.P.S.M.; Saugmann, R.; Suchman, L.

Note: To cite this publication please use the final published version (if applicable).

Toward a Critique of Algorithmic Violence

Rocco Bellanova [iD] and Kristina Irion [iD]
University of Amsterdam, The Netherlands

Katja Lindskov Jacobsen [iD]
University of Copenhagen, Denmark

Francesco Ragazzi [iD]
Leiden University, The Netherlands

Rune Saugmann [iD]
Tampere University, Finland

and

Lucy Suchman [iD]
Lancaster University, UK

Questions about how algorithms contribute to (in)security are under discussion across international political sociology. Building upon and adding to these debates, our collective discussion foregrounds questions about *algorithmic violence*. We argue that it is important to examine how algorithmic systems feed (into) specific forms of violence, and how they justify violent actions or redefine what forms of violence are deemed legitimate. Bringing together different disciplinary and conceptual vantage points, this collective discussion opens a conversation about algorithmic violence focusing both on its specific instances and on the challenges that arise in conceptualizing and studying it. Overall, the discussion converges on three areas of concern—the violence undergirding the creation and feeding of data infrastructures; the translation processes at play in the use of computer/machine vision across diverse security practices; and the institutional governing of algorithmic violence, especially its organization, limitation, and legitimation. Our two-fold aim is to show the potential of a cross-disciplinary conversation and to move toward an interactional research agenda. While our approaches diverge, they also enrich each other. Ultimately, we highlight the critical purchase of studying the role of algorithmic violence in the fabric of the international through a situated analysis of algorithmic systems as part of complex, and often messy, practices.

Les questions concernant la manière dont les algorithmes affectent l'(in)sécurité deviennent de plus en plus courantes en sociologie politique internationale. Notre discussion collective s'appuie sur ces débats et les enrichit en abordant les questions portant sur la *violence algorithmique*. Nous soutenons qu'il est important d'analyser et de discuter de la manière dont les systèmes algorithmiques alimentent (et entretiennent) des formes spécifiques de violence, ainsi que de la façon dont ils justifient des actes violents ou redéfinissent les formes de violence jugées légitimes. Cette discussion collective réunit différents points de vue disciplinaires et conceptuels

Corresponding author e-mail: r.bellanova@uva.nl

pour ouvrir un débat sur la violence algorithmique en se concentrant à la fois sur des exemples spécifiques et sur les défis à relever pour la conceptualiser et l'étudier. Cette discussion se concentre sur trois sujets de préoccupation : la violence qui sous-tend la création et l'alimentation des infrastructures de données, les processus de conversion en jeu dans l'utilisation de la vision informatique/machine à travers diverses pratiques de sécurité, et la gouvernance institutionnelle de la violence algorithmique, en particulier son organisation, sa limitation et sa légitimation. Notre double objectif est de montrer le potentiel d'une discussion interdisciplinaire et d'avancer vers un programme de recherche interactionnel. Bien que nos approches divergent, elles s'enrichissent mutuellement. Notre but est de mettre en évidence les possibilités analytiques ouvertes par l'étude de la violence algorithmique et de son role dans la fabrique des relations internationales, par le biais d'une étude des systèmes algorithmiques dans le cadre de pratiques complexes et désordonnées.

Las preguntas acerca de cómo afectan los algoritmos a la (in)seguridad son cada vez más comunes en la Sociología Política Internacional. A fin de construir y sumar a estos debates, nuestro Debate Colectivo pone en primer plano las preguntas sobre la violencia algorítmica. Sostenemos que es importante abrir el debate acerca de cómo los sistemas algorítmicos alimentan (en) formas específicas de violencia, cómo justifican las acciones violentas o redefinen qué formas de violencia se consideran legítimas. A partir de la reunión de diferentes puntos de vista disciplinarios y conceptuales, este Debate Colectivo abre una conversación sobre la violencia algorítmica centrándose tanto en sus instancias específicas como en los desafíos de su conceptualización y estudio. En general, el debate converge en tres áreas de interés: la violencia que sustenta la creación y alimentación de las infraestructuras de datos, los procesos de traducción en juego en la utilización de la visión de la computadora/máquina a través de diversas prácticas de seguridad y el gobierno institucional de la violencia algorítmica, especialmente su organización, limitación y legitimación. Nuestro doble objetivo es mostrar el potencial de una conversación interdisciplinaria y avanzar hacia una agenda de investigación interactiva. Si bien nuestros abordajes divergen, se enriquecen mutuamente. Finalmente, destacamos la adquisición fundamental del estudio de las funciones de la violencia algorítmica en el tejido de lo internacional a través de un análisis situado de los sistemas algorítmicos como parte de prácticas complejas y, a menudo, desordenadas.

Technology-based responses to the COVID-19 "crisis" intersect with knowledge practices, digital technologies, and security visions that the six researchers participating in this collective discussion have been studying for some time, from different disciplinary and conceptual perspectives. The rush toward the creation of contact-tracing applications casts light on how data that are being collected, stored, circulated, and processed matter. As the Google/Apple contact-tracing collaboration reminds public authorities and scholars (Ilves 2020), the design and deployment of even seemingly basic data and computing infrastructures does not happen in a socio-material and economic vacuum (Kitchin 2014). Big Tech companies—be they widely known firms like Microsoft and Huawei or niche ones like Palantir—emerge as key security actors across a wide range of domains from public health to law enforcement. The COVID-19 pandemic has been used to legitimate as well as expand uses of technologies such as delivery drones carrying medical supplies to "a remote British isle under a COVID-19 trial program" (Reagan 2020). On Paris public transport, there are plans to use facial recognition to check whether people are wearing masks (Leloup 2020). At the same time, new facial recognition systems are being

developed to enable face recognition even when people are wearing masks, and "touchless" biometrics is now a market set for huge growth. What is common to many of these technologies is that algorithms play a key role in their functioning.

Scholars working in international political sociology (IPS) writ large have for some time focused on how algorithms come to affect security practices, from border controls to warfare (Amoore 2009; Bigo 2014; Wilcox 2017; Huelss 2019; Suchman 2020). Similarly, discussions about the spread of digital surveillance and intelligence-led policing often revolve around the (ab)use of algorithmic systems for tracking, assessing, and steering human behavior (Lyon 2003; Bonditti 2004; Amoore and de Goede 2005; Amicelle and Iafolla 2017; Johns 2017; Aradau and Blanke 2018). Alongside these works, there is a fast-growing interdisciplinary literature questioning the adoption of algorithmic systems as if they were "mechanical[ly] objective" solutions (Daston and Galison 1992, 83) to any issue that may arise in largely datafied societies. Indeed, algorithmic systems are seen as powerful allies by those who aim at taming an emergent world into a seemingly rational and thus more predictable reality (Rouvroy 2013, 146-147), often with claims for their unparalleled accuracy (Suchman, Follis, and Weber 2017). The promise of artificial intelligence (AI) and neural networks—not unlike the mathematical and statistical tools of positivism in the late nineteenth/early twentieth century (Hacking 1990)—is to offer technical solutions to complex sociopolitical problems (Morozov 2013). Recent critical scholarship, in contrast, has unpacked some contentious features and limits of algorithmic systems. Among them are the peculiar forms of knowledge and ignorance that these systems generate (Hildebrandt 2008; Introna 2016), their ethical problematics (Zarsky 2016; Yeung 2018), their political consequences (Cheney-Lippold 2011; Eubanks 2018), and their feedback onto the shaping of a reality that they are supposed to "simply" read (Muller et al. 2016; Amoore and Raley 2017).

This collective discussion is concerned with *algorithmic violence.* We argue that it is important to foreground, unpack, and examine critically how algorithmic systems feed (into) specific forms of violence, and how they justify violent actions or redefine which type of violence is considered legitimate. The instances of algorithmic violence that we discuss below are about the *force of computation.* That is, paraphrasing Derrida (1990, 925), the force needed to make computation possible and the force that computation leverages, and thus ultimately how computation relates to justice. As Amoore (2020, 5–6) notes, "what matters is not primarily the identification and regulation of algorithmic wrongs, but more significantly how algorithms are implicated in new regimes of verification, new forms of identifying a wrong or of truth telling in the world." Thinking in terms of "cloud ethics" (Amoore 2020, 7) thus means unpacking "the propensities and possibilities that algorithms embody." Such an approach—while important—might not be enough. Through our collective discussion we insist on the significance of focusing not only on the algorithms' transformative force, but also on how algorithmic systems are forced and enforced. This broader approach invites finding situated points from which to highlight when and how tensions between justice and violence arise, and from which to pose critical questions about how certain forms of violence are deemed legitimate by state authorities and private companies, as well as how those forms of violence are justified, become the object of political contestation, and impact individual and political rights. To think about algorithmic violence in terms of the force of computation permits us to shift "attention to [the algorithm's] pragmatic functioning," that is, "to consider the way that algorithms work as part of a broader set of processes" (Goffey 2008, 19). Resituating algorithms in practice allows us to "unknow them," "to mak[e] the familiar slightly more unfamiliar" (Bucher 2018, 46). In other words, it permits us to observe how algorithmic systems always involve humans and technologies, albeit in different ways, and to see how human–technology entanglements are made integral to a chain of decision and command (de Goede 2018).

Our collective discussion brings together colleagues from international relations, science and technology studies (STS), and law. Each short text is interrupted and enriched by comments from and exchanges with co-authors. These interactions are included in the text as block quotes using a different font. Overall, the discussion converges on three areas of concern—the violence undergirding the creation and feeding of data infrastructures; the translation processes at play in the use of computer/machine vision across diverse security practices; and the institutional governing of algorithmic violence, especially its organization, limitation, and legitimation. Our aim is to show the potential of a cross-disciplinary conversation, and potentially move toward an interactional research agenda: a conversation that will not only add to the literature presented above but also push the research agenda across disciplinary boundaries. We make explicit our different lines of research and epistemic–methodological approaches. In the process, it becomes evident that we come to this conversation with diverse understandings of what both *algorithmic* and *violence* mean, opening the question of upon what common ground—if any—we *imagine* what algorithmic violence is and does, and thus how we can build a critique of algorithmic violence. As this is also the case for other key terms mobilized in the conversation, we were not able—nor are we keen—to resolve all differences and produce a manifesto-like text. Rather, in the spirit of a collective discussion, we decided to keep both cracks and scaffoldings visible.

Bellanova and Lindskov Jacobsen: Algorithmic—Violence—Imagining

Our shared assumption is that computation does not happen in a vacuum. In order to think about the violence of algorithmic systems, we need to understand them as made of more than "[a] series of instructions ... used by a computer, or a program, to carry out a specific task or solve a problem" (Lister et al. 2009, 418). As Suchman notes:

> This definition performs the trick so pervasive in discourses of computing, that is, the rhetorical elision of "the instruction" as understood in relation to human action with machine-readable, executable code (see McDermott 1976; Broussard 2019). As I've argued elsewhere (Suchman 2007, 2016), building upon the insights of ethnomethodology, instructions share with other forms of prescriptive representation (recipes, plans, laws, etc.) a kind of irremediable incompleteness. More specifically, they presuppose capacities necessary to their enactment that they do not, and crucially cannot, fully specify. The contingent work of finding the relevance of an instruction to the circumstances in which it needs to be carried out, fundamentally differentiates an instruction from a line of code; what it means to execute the latter must be unambiguous in relation to a correspondingly sensored and encoded "world." A corollary of this is that the computer or program does not, strictly speaking, "use" the instruction, nor does it carry out a "task" or solve a "problem"; it only executes code when activated to do so.

Questioning the force of computation requires broadening our focus as well to investigate the forms of violence going on at the level of data infrastructures. As Lindskov Jacobsen powerfully shows, some of the instances of algorithmic violence sketched below remind us that algorithms need data(fication) to operate (Fuller and Goffey 2012, 83). Thus, a critique of algorithmic violence is inseparable from political and legal questions about big data (Madsen et al. 2016), data colonialism (Thatcher, O'Sullivan, and Mahmoudi 2016) and data justice (Dencik, Hintz, and Cable 2016). These questions could aptly be articulated as questions about what visions and values are inscribed into data and computing infrastructures (Hellberg and Grönlund 2013).

In framing our questions, this collective discussion has benefited most clearly from encounters between IPS and STS. This is not, per se, a novelty, as conceptual

traffic with STS is becoming common within IPS (Best and Walters 2013; Lisle and Bourne 2019; Bellanova et al. 2020). Yet, as Ragazzi notes:

> IPS has been looking at technologies for decades, but has never bothered to look at what they actually *do*. STS has allowed IPS scholars to open the black box—and now the work that is left is to make the connections across the "walls" of the black box between macro and meso social processes (structural violence, field effects, etc.) and micro-processes (computational logics, affordances).

At the same time, critical literatures on algorithms already insist on the need for resituating algorithms as part of messy practices. As Goffey (2008, 19) argues, "[a]lgorithms act, but they do so as part of an ill-defined network of actions upon actions" (see also Gillespie 2014; Ziewitz 2016). This is a promising step toward understanding algorithmic force. It also invites us to focus on the "human–machine reconfigurations" enacted through algorithmic systems (Suchman 2007). Finally, engaging with public law offers to IPS writ large the occasion to question what criticality may be needed to counter specific forms of algorithmic violence (Johns 2017; Irion 2021). It also suggests unpacking the institutionalization of some of these critical tools, especially data protection, and their effects on international security practices (Bellanova and de Goede 2020).

We face the question as well of how we can delimit the scope of a critique of algorithmic violence. This becomes a crucial issue when studying how datasets circulate across different knowledge practices. For instance, some machine-readable data processed by algorithms to identify "legitimate" military targets, for example in Somalia, may have been collected by non-military agencies, yet subsequently accessed by and used for military purposes.[1] Humanitarian actors collect and store increasing amounts of biometric data on vulnerable subjects, also in contexts characterized not only by humanitarian needs but also by the security concerns of states engaged, for example, in counterterror (Lindskov Jacobsen and Fast 2019). Critical scholarship has also highlighted how algorithmic systems negatively affect already vulnerable or marginalized groups in the Global North (Eubanks 2018). Noble's (2018, 10) work pinpoints how "algorithmic oppression" does not end with the use of specific algorithmic systems but has far-reaching, if not structural, effects. As she puts it, "algorithms are serving up deleterious information about people, creating and normalising structural and systemic isolation, or practicing digital redlining, all of which reinforce oppressive social and economic relations" (Noble 2018, 10). So, we need to ask in what sense is violence implied at the level of data infrastructures different from, and yet related to, algorithmic violence in the narrower sense of the term? These are crucial questions to contemplate and attend to as we strive to develop analytical vocabularies to explore the associated forms of violence with which algorithmic systems and processes are intimately linked.

> *Irion*: I would like to make three comments in relation to how we use violence with respect to datafication and algorithms; broadly speaking about the ambivalence, the ubiquity and the mitigation of violence. *First*, how can the social sciences meaningfully interact with the ambivalence of violence? From our collective discussion it emerges that violence can mean physical harm, discrimination, semantic force, impalpable effects, and so many different forms and expression. Oftentimes, it is not the algorithm that is violent but the actors and processes, and still we summarize it as algorithmic violence. Sometimes the violence is clearly perceptible, sometimes microscopic but amplified in its totality. Should we not reserve violence to the algorithms that mean and do harm and use other categories to label unfairness, marginalization and exploitative practices? Should there not be a meaningful and flexible taxonomy of

---

[1] See "Violence and the Making of Machine-Readable Data Infrastructures" section. Also, see Katja Lindskov Jacobsen, "Shadowy Conjunctions in the War on Terror," conference presentation, EASST/4S 2020, panel organized by Claudia Aradau and Annalisa Pelizza, UCL Institute for Global Prosperity (IGP), February 6, 2020. https://www.eventbrite.co.uk/e/directors-seminar-katja-lindskov-jacobsen-tickets-86571149639.

violence that involves socio-technical algorithmic systems? *Second*, if most practices of datafication and digitalization are deemed inherently violent, it would appear that algorithmic violence is ubiquitous and inevitable. Just as physical infrastructures can condition human affordances, computation and algorithms also tend to condition how humans can interact with them. Is there not a risk that a critique of algorithmic violence becomes meaningless if there is no non-violent alternative? How can a critique of algorithmic violence do justice to the many benefits and the positive impacts of algorithms for human flourishing? If we do not nuance algorithmic violence better, are we not falling into an all too convenient posture of criticism without being constructive about non-violent alternatives? *Third*, before any mitigation of violence we need to establish the existence of a violent practice. This is where law and policy are often way too binary in their analyses. Classical tort law, for example, needs a manifested harm that can be causally linked to someone's action in order to afford damages. European Union (EU) data protection law protects individuals' privacy and personal data but is also meant to enable the circulation of personal data in the EU (Granger and Irion 2018). How any future regulation of algorithms conceptualizes harm will be key to the level of protection it affords. Here, the discourse on algorithmic violence will be helpful but also requires better contours to be meaningful for public policymaking.

Saugmann: I understand the aim of your comments (as limiting ambiguity and encouraging practical uptake of our idea of algorithmic violence), but I think it is difficult in practice. Here, I think of, for example, Google building the radicalization machine that is YouTube after 2013, while "not being evil" or intending harm, but nevertheless playing a role in "infrastructuring" extremism (NYT Editorial Board 2018). And reading your third comment, aren't we then sticking to the "familiar categories" you describe below, if we keep to a more conventional, and often largely pre-digital, understanding of harm/violence? To me, the critical added value in algorithmic violence is that it can point out practices that are not violent in the "traditional" sense, and thus cannot be held to account if we look to fulfil that criterion.

From drone attacks based on the tracking of SIM cards to anti-riot police using face recognition systems, the violence of algorithms is becoming part of our common imaginary. We soon realized that many of us were thinking with images, albeit with different understandings about what *thinking with* and *images* both mean.

Ragazzi: I think here it is important to clarify what we mean by thinking with images. Is it thinking with images produced by the algorithms, fed into the algorithmic logic, or themselves the result of algorithmic processing? All these images occupy specific positions, and conflating them could blur the argument.

Saugmann: Thinking about how images are changing is another way of thinking about algorithms, as it soon becomes clear that digital images are digital maybe even before they are visual, computational objects before representational objects (cf. Seppänen 2017). This change suggests a wider ontological change affecting "known" social science concepts like communication in the digital society. We need to carefully avoid thinking that we already know what images are, what violence is, to be open to reconfigurations taking place through and around such concepts.

Thinking algorithmic violence with images means acknowledging that different kinds of imaginaries are at play. It also means attending to what algorithms do to, and with, images differently, not least at the level of ontology. Finally, it invites us to explore the "security collages" underpinning computational imaginaries (Leander 2019, 327), and the "security compositions" produced with digital data (Bellanova and González Fuster 2019, 351-ff).

Suchman: Helping to Keep Humans Away from Danger?

My engagement with the problem of algorithmic violence is an extension of an anti-militarism rooted in my position as a citizen of the United States, a nation that

takes its strategic interests as justification for interventions wherever those are asserted to be under threat. Annual US "defense" spending equals that of the ten next most heavily armed countries, with 54 percent of the federal discretionary budget going to the military (Bacevich 2020; Tian et al. 2020). Current calls in the United States to "defund the police" are echoed by affiliated calls for demilitarization (Benjamin and Davies 2020), tied to histories of white supremacy and colonization, both of which mark the country's founding and its ongoing claims for exceptionalism. This location tethers me to questions of war and militarism (Stavrianakis and Stern 2017), even amid the invaluable movement toward a more expansively feminist articulation of what peaceful coexistence might look like (Wibben et al. 2018).

Two images frame my contribution to our discussion (figures 1 and 2), both imagining a computationally based situational awareness which simultaneously enables and justifies the exercise of violent action at a distance.

REMOTELY CONTROLLED Some armed robots are operated with video-game-style consoles, helping to keep humans away from danger. David Walter Banks for The New York Times

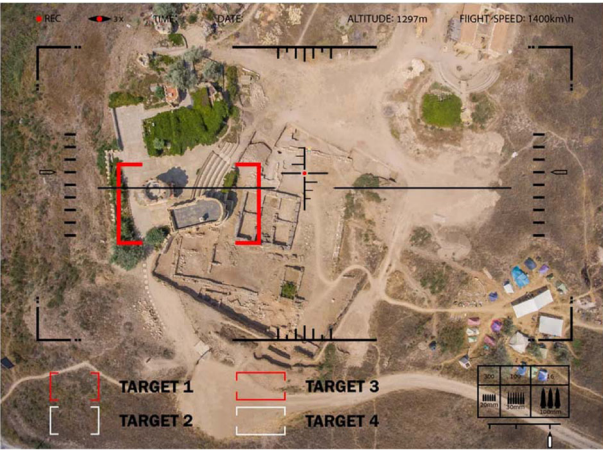**Figure 1.** Remote Control, Ft Benning, Georgia, 2010.

Figure 2. The Kill Chain, Yemen, 2018.

In 2010, technology reporter John Markoff wrote an article in the New York Times titled "War Machines: Recruiting Robots for Combat."[2] The accompanying photo (figure 1) shows a control console branded with the logo of UK defense contractor, QinetiQ. We view the console from the position of its (white, male) operator, whose lower arms and hands are in view at the bottom of the frame. The console rests on bare earth, signaling its readiness for use "on the ground," and serves as an icon for new lines of research and development among military contractors in remotely controlled weapon systems. Most stunning to me is the caption that narrates the image, and particularly its closing phrase. It reads: "Remotely controlled: some armed robots are operated with video-game-style consoles, *helping to keep humans away from danger.*"

The implied universality of the category "human"—read in this case, of course, as those of "us" who affiliate with the body whose hands we see—and the associated erasure and effective dehumanization of those who will be the targets of this device, tie it to my larger critical engagement with the trope of "situational awareness." More specifically, in thinking about situational awareness as both precondition and aspiration for the use of legally sanctioned violent force, my focus is on the interfaces that configure war fighters to achieve "recognition" of relevant subjects and objects, and in particular the discriminations that are a prerequisite for defensible killing under international humanitarian law (Suchman 2015, 2016, 2020).

> *Lindskov Jacobsen and Saugmann*: It is interesting here to note how "recognition," "means," and "obligations" interrelate in armed conflict. In a study of collaborative air war practice, we found that in Western air interventions there is acute attention to how some targets can be legal for some nations, while not for others. So-called Red Card Holder Teams have been introduced, for example during Operation Inherent Resolve,[3] in order to determine whether "engaging" (i.e., killing) a given target falls within the mandate of a contributing nation. The ethics of collaboration that underlies the wars is one of "efficiency" or permissibility. Often, national mandate restrictions do not mean that a task which such mandates do not permit will not be carried out. Rather, it often means that instead "collaborators will do what a given contributor isn't allowed to" because of mandate restrictions (Lindskov Jacobsen and Saugmann 2019, 352).

> *Bellanova*: I like your comment because it insists on how the *algorithmic scopic regime*—if one were to mobilize Jay's (1988) notion—does not give way to an immediately actionable reality. Contrary to a certain rhetoric suggesting that governing with algorithmic is a frictionless practice, it becomes evident that any given algorithmic scopic regime actually encounters, and may enter into conflict with, other scopic regimes (be they algorithmic or not) already used by modern institutions. Often, a negotiation between scopic regimes imposes itself and, as your work (Lindskov Jacobsen and Saugmann 2019) work shows, this happens even when public authorities engage in warfare.

Here's another indicative image (figure 2), a frame from a full-motion video taken by a so-called unmanned aerial system, a drone hovering over an area currently under surveillance by the US military.

The image accompanies an article in The Guardian in 2018 titled "The Kill Chain: Inside the Unit that Tracks Targets for US Drone Wars," which describes the distributed system of drone operators, video analysts, and associated military personnel who look for persons deemed to be threats to the US homeland under the so-called war on terror.[4] This image is a drone's eye view of a desert area in Yemen, one of the locations, named by the US military, of "active hostilities," along with

---

[2] The full article can be found at https://www.nytimes.com/2010/11/28/science/28robot.html.

[3] *Operation Inherent Resolve* is the US-led military intervention against ISIL, including both a campaign in Iraq and a campaign in Syria. https://www.inherentresolve.mil/.

[4] Accessed January 15, 2021. https://www.theguardian.com/world/2018/jan/23/the-kill-chain-inside-the-unit-that-tracks-targets-for-us-drone-wars.

Somalia and Afghanistan. The frames indicate objects automatically identified as prospective targets.

For the purposes of this discussion, we can think of algorithmic systems as technologies of data processing and techniques of analysis that take some kind of input (e.g., full-motion video images) rendered in a machine-readable format (as patterns of screen pixels in the case of images), and generate human-readable output (e.g., the marking of a particular pattern in the image as a building, or in other applications as a face).

> *Lindskov Jacobsen*: Beyond the focus on police and military are also questions about the role of humanitarian and development agencies in collecting and storing data, which risks feeding into the data processing upon which "targets" are identified. In places like Afghanistan and Somalia, humanitarian actors collect and store biometric data, which raises questions about their role in the process of rendering subjects in these locations into "a machine-readable format" (while mandated to ensure the protection of vulnerable individuals). How does the issue of algorithmic violence look when considering the potential exposure of biometric data collected by the World Food Programme, knowing for example the decision by WFP to partner with Palantir (WFP 2019)?

Importantly, automated pattern recognition is based not on recognition in the human sense, but on statistical correlations that, however meaningless, selectively produce results that are legible, or recognizable as meaningful, to humans. From designation of the training data for so-called machine learning algorithms to assessment of the results, it is humans who select the input and who evaluate the output of the algorithmic system's operations. And it is humans who must take responsibility for the assumptions and interests that inform those operations, and for the real life, and death, consequences that follow.

Those life and death consequences are what I am exploring here under the rubric of violent algorithms. By thinking about these systems in terms of their visual politics, we are looking at the ways in which seeing is never a simple biological or perceptual process, but is always mediated through specific cultural, historical, professional, and increasingly technical practices. Securitization, whether in "the homeland," at borders, or in sites of armed conflict, is a mediated practice, or complex of practices, which are also profoundly political. So, we are interested here in what we are calling the visual politics of technologically mediated practices of seeing.

The recent insurgency within the United States against racialized profiling of Black Americans, understood as a continuation of the legacy of settler colonialism and slavery that enabled the country's founding, has contributed to a growing awareness of the inseparability of policing and militarism. Another form of algorithmic violence that has come into focus in this context is so-called facial recognition, sold by its purveyors as an infrastructure for policing at a distance. Facial recognition algorithms, like all forms of data analytics, require the rendering of features legible to human perception as computationally detectable features (e.g., edges, pixel densities, and normal distributions). These techniques support the mobilization of practices of racial/ethnic/gender profiling, while erasing constitutive relations of power and histories of injustice. While critical demonstrations of the limits and injuries of facial recognition technologies have at least temporarily interrupted their adoption in domestic policing in the United States,[5] the investment in profiling as a proxy for awareness remains a substrate for US militarism.

The profile, by definition a stereotype of a posited category, is a crucial element of the *operative image* of knowledge/ignorance that informs technologies deployed in the service of identifying/designating a threat. The operative image is a term introduced by Harun Farocki to describe "images that do not represent an object, but rather are part of an operation" (Farocki 2004, 17)—a concept that Ragazzi and

---

[5] https://www.nbcnews.com/tech/security/tech-worker-group-calls-facial-recognition-ban-citing-technical-ethical-n1232591.

Saugmann discuss further below. Profiling operates on the premise that another can be recognized in the absence of familiarity. This should alert us to the limitations and dangers of visualities, and of the image as a ground truth of security imaginaries, attentive to the multiple sites at which images/imaginaries underwrite the continuation of securitization's violent methods. Machine visions are, in this respect, generatively subject to material-discursive analysis, as translations that promise to ground relations of power through the operations of computational machinery in legacies of injurious discrimination. This line of research requires engagement, not with the algorithm narrowly defined, but with algorithmic systems *in situ*, in their historical, geopolitical deployments, and attention to the possibilities opened by that which continues to escape them (Ansems de Vries et al. 2017).

Bellanova: Thinking with Tweets and Cookies

Take a tweet posted by the US Immigration and Customs Enforcement (ICE) agency in late October 2019 (figure 3 above). The person in the picture is handcuffed—their arms locked behind their back. An ICE agent is pushing a biometric reader against the person's fingers, to identify and process the arrested individual. I am not sure where this tweet should sit in the topology of algorithmic images suggested above by Ragazzi. Insofar as a social network platform included this tweet in my feed, I consider it to be partially the result of algorithmic processing (cf. Saugmann 2017). I read it together with the accompanying text and the information that Twitter provides me about the user. It is circulated as promotional visual material, in support of ICE's own security practices. In figure 3, algorithmic violence is a situated, all too material and coercive use of force—not only the claimed reaffirmation of a monopoly of violence by state authorities, but also the computational force of the infrastructure that supposedly enables "targeting illegal aliens with criminal records who pose a threat to public safety." On the one hand, as Lindskov Jacobsen discusses below in greater detail, resituating algorithmic systems as part of sociotechnical data infrastructures permits us to see how violence is exerted even before any profile is generated or used to target people. For instance, the collection of fingerprints or DNA samples is often a moment where authorities—especially state authorities—can materially force datafication to feed the algorithm. On the other hand, the fingerprint reader at the center of the image invites us to think about how data infrastructures, bringing together databases across boundaries, inform actors' power relations. For large-scale data systems to function smoothly, fairly complex infrastructures must be put and kept in place (Bellanova and Glouftsios 2020), often with a key role played by companies such as Palantir (Knight and Gekker 2020).

Figure 3. Screenshot taken by Bellanova of a tweet posted by the official account of the US ICE (@ICEgov) on October 24, 2019.

We may lack such clear images of other forms of algorithmic violence. It is hard to visualize more subtle ways in which algorithms inform, and justify, decisions that discriminate.

> *Ragazzi*: This raises the question of the existence of different modalities of knowledge and how to access them.

> *Bellanova*: It seems to me that there are at least three different practices of knowledge (and non-knowledge) at stake. First, how we (as scholars from different backgrounds and with different approaches and methods) come to know (or not) the algorithmic (Bucher 2018), that is, scholarly knowledge practices. Second, how algorithmic systems are expected to produce a specific kind of knowledge for decision-makers in different sites of a "security chain" (de Goede 2018), that is, algorithmic-driven knowledge practices. Third, how those affected by algorithmic systems come to know (or not) whether and how the algorithmic played a role in a decision affecting them, that is, "decoding" the algorithmic practices (cf. Lomborg and Kapsch 2020).

Besides now classic examples such as travelers' risk-assessment, the analysis of dialect inflections during asylum procedures provides a challenging case of algorithmic imaginary. In this case, imagining is disconnected from the visual, as these algorithmic systems operate through the sampling and codification of audio material, and then the datafication of whatever "asylum speakers" (Abu Hamdan 2016) say during interviews to assess whether their inflection matches the one from the place of origin they previously declared (see also Bellanova and González Fuster 2019). As I have learned working with González Fuster, a colleague and a friend particularly attentive to the sonic, the social sciences and humanities are not unaware of the fact they might suffer from a sort of visualism (Ihde 2009). A much-needed attention to the visual (Bleiker 2018) risks us becoming deaf to other forms of computational imaginaries. We may end up having a hard time in imagining less visually based surveillance operations (but, see Weitzel 2018).

> *Irion:* The invisibilities of computerized surveillance and algorithmic intermediation in the public and in the private sectors also take a toll on their perception, acceptance and resistance by users and netizens. Creating awareness, providing information, and designing images as part of an algorithmic narrative can be really challenging, and need to be imaginative in the way the message is conveyed.

With her work "Listening Back," artist and scholar Jasmine Guffond takes a different path to foreground data-driven surveillance and opens it to question. Rather than visualizing computation, she developed "an add-on for the Chrome and Firefox browsers that sonifies Internet cookies in real time as one browses online" (Guffond 2020).[6] This is a form of artistic intervention that critiques by turning into sound what largely escapes users' visual perception. As she explains: "Listening Back functions to expose real-time digital surveillance and consequently the ways in which our everyday relationships to being surveilled have become normalised" (Guffond 2020). As such, this intervention becomes a form of "digital parasitism" (Aradau, Blanke, and Greenway 2019), as it ultimately requires the installation of a small algorithm. To some extent, thinking with cookies the way in which Guffond does bring together the first and third knowledge practices I mentioned above— the scholarly and the decoding ones. In both cases, the goal is not to get a better understanding of the inner workings of a given algorithmic system. The sonification just makes the browsing—an all too familiar activity—stranger, and often difficult to carry out due to the persistent sound (akin to a noise, for my ears) produced by the cookies. In other words, it promises no direct access to a higher truth, but potentially opens up a space of play.

---

[6] Irion: Another good example next to sonifying internet cookies would be the art project, *The Smell of Data*. https://smellofdata.com/.

Lindskov Jacobsen: Violence and the Making of Machine-Readable Data Infrastructures

Addressing the question of algorithmic violence from a perspective of contemporary security and intervention technologies, two intertwined moves seem crucial. First, the importance of moving beyond or rather "before" algorithmic processing, to also explore in our research how machine-readable data, and indeed machine-readable bodies, are made (van der Ploeg and Sprenkels 2011) and become available for algorithms to subsequently process (see also Bellanova and González Fuster 2019). Second, to move beyond, and to add to, critical analyses of data infrastructures in Western contexts[7] (with the crucial issue of "DIY surveillance" mentioned below by Ragazzi), to explore how associated forms of violence at the level of data infrastructures play out in the global "periphery," with attention to power relations, hierarchies, and difference.

Put differently, algorithmic violence begins much before the biased and discriminatory processing of data, with all its tacit injustices and violence. Moreover, the type of violence implied at the level of the very making of machine-readable data infrastructures looks different if we shift attention to the global periphery. Accordingly, exploring the force needed to make computation possible must include attention to force and violence at different points and different contexts of data "collection" and infrastructuring. Introducing contemporary security and intervention technologies as a lens onto the making of digital infrastructures and increasingly pervasive forms of data collection, as key elements when discussing algorithmic violence, enables much-needed attention to global power relations, beyond racial biases in algorithms.

Various contemporary intervention technologies—be they military or humanitarian—entail the transformation of fingerprints, iris patterns or other "unique physical characteristics" into digitalized, machine-readable data. Biometric fingerprint or iris scan technologies are used not only by the US military to register Afghan citizens encountered in Afghanistan, but also by numerous other intervention actors, including humanitarian and development agencies (Johns 2017; The Engine Room and Oxfam 2018; Lindskov Jacobsen 2019). Sometimes the setting in which such non-military agencies collect biometric data from individuals is a setting where the US military is also conducting counterterror operations, as in Afghanistan or Somalia.

Looking at the widespread use of intervention technologies like biometrics offers illustrative examples of practices in the global periphery that entail the making of enormous amounts of machine-readable data, including sensitive data from vulnerable populations seeking aid and protection from humanitarian agencies. Beyond the US military, a wide range of agencies use intervention technologies that more or less explicitly partake in the production of a data infrastructure that then enables subsequent algorithmic processing aimed, for example, at identifying targets or suspects.

Besides extending the analysis "before" algorithmic processing, it is also important to extend our critique to one that engages with, and makes visible how, the making of machine-readable data plays out in the global periphery, including critical differences in "data generating" conditions and how such differences translate into specific expressions of violence. While for some the cost of declining to give up your biometric data could simply be the convenience of accessing your phone only by the touch of your finger(print), even this is misleading as machine-readable data may be collected even if you do not access your phone using fingerprint biometrics. Yet, the point to stress here is the importance of recognizing that analyses that look

---

[7] "Western" is a problematic descriptor. It should not distract attention from violence within, nor should it indicate inherent cohesion or a "given" entity or set of actors. Rather, it is meant to allude to two things: global power structures and differences in how algorithmic violence, including at the level of machine-readable data-making, is encountered.

at "Western" contexts are not representative of the multiple forms of violence related to data gathering, data retention, etc. (see also Jacobsen 2012; Frowd 2017). Empirical evidence from two types of intervention contexts illustrates this point.

In some intervention contexts, declining to give up biometric data entails much more than foregoing convenience. In most intervention contexts, the cost of declining to give up personal data like biometrics is far more consequential than for "Western citizens." Imagine being a refugee in need of assistance, with nowhere else to turn than to UNHCR. Yet, UNHCR has decided to make biometric registration a standard procedure when assisting refugees (Lindskov Jacobsen 2017; Madianou 2019). Thus, declining to give up biometric data (which algorithms may later process) might in such cases entail far more than giving up convenience. It could potentially have fatal implications, if it results in individuals being denied assistance or in individuals deciding not to register because of data sharing concerns. The point to stress here is the different circumstances under which machine-readable data are being generated in various intervention contexts in the global periphery. Besides differences in meaningful opt out possibilities, another issue is the difference in age limit. The example that most vividly illustrates this is the recent trialing of fingerprint biometrics for infants in various intervention contexts in the global periphery, sometimes involving humanitarian agencies (Parker 2019). In the EU, as another example, the age at which fingerprints are required for visa applications is currently twelve years.

Further illustrative of differences—differences with potentially violent implications—between the making of machine-readable data in "Western" contexts, is the fact that once collected by UNHCR, the policy is to keep biometric data indefinitely, even once an individual ceases to be a refugee. Not only does this policy differ significantly from restrictions on biometric data retention in, for example, the EU, these examples also illustrate crucial differences at the level of the very making of machine-readable data infrastructures. These are differences that a critique of algorithmic violence must help make visible, with attention to how they translate into a differential distribution of security/insecurity.

Moreover, even in cases where an individual agrees to give up biometric data, this too risks bringing added insecurity, for example, in the form of risks of retaliation from Al Shabaab in Somalia. If Al Shabaab gains access to biometric data showing exactly which individuals have received aid from Western organizations (that Al Shabaab sees as an enemy), this could have fatal repercussions for individuals, who cannot readily deny their iris pattern or fingerprint. Data collection may also entail violence in other ways, as when implicitly encouraging illegal border crossings as part of the very journey required for persons to have their data collected: "Almost a year after submitting his application for family reunification, Abdul was informed by the Immigration Service that his wife and children had to be DNA tested at a Danish embassy in order to validate relations of kinship in the family. His family therefore paid an 'agent' to help them undertake an illegal cross-border journey to an embassy in a different country" (Olwig et al. 2019, 194).

In short, there are important forms of violence at the very point of data collection that need to be included, made visible, and understood as part of our critique of algorithmic violence. Indeed, even if these forms of violence happen before the algorithmic processing, they are crucial given that the making of machine-readable data (e.g., the iris patterns of millions of refugees) is a precondition for subsequent algorithmic processing. These data, generated in the context of various contemporary intervention settings (military and humanitarian), form part of a broader data infrastructure. That infrastructure itself entails violence even before adding the algorithmic processing of data, simply at the very point of insisting on its massive collection, sometimes justified in the name of humanitarian protection. Put differently, there is violence in the form of immediate disqualification and resulting insecurity as well as in the form of future uncertainty (for what purposes may these

data be accessed and algorithmically processed) that we need to attend to when thinking about questions of algorithmic violence. Appreciating that the generation of accessible, digitalized data is a precondition for algorithmic processing, these examples should make clear why, when thinking about algorithmic violence, we need to attend to questions about the differential conditions under which such data are generated, collected, stored, and shared. What violence goes into the making of the digitalized data infrastructures that computer-implementable instructions can then tacitly process—sometimes with fatal consequences—as for the individual whose fingerprint was allegedly lifted off an improvised explosive device in Somalia, and recognized at a border-crossing point as he was trying to enter the United States from Mexico (Kimery 2018)?

Saugmann: The Semiotic Violence of Computer Vision

There are too many digital images in the world for anyone to see; this observation has long been repeated across both security and civilian debates. So perhaps the importance of images is not in what they could show us—show me, and you, dear readers, and collaborators in this collective discussion—if we saw them. Computer vision algorithms present not an extension of, but an alternative to, seeing, one that is highly sought after by security bureaucracies and commercial actors alike, as in the case of the US project MAVEN, which seeks to deploy computer vision systems to overcome the problem that the US military produces too many aerial surveillance images for even the US security bureaucracy to analyze (Saugmann 2019).

> *Suchman*: What informs the US military's "algorithmic warfare"? Very little has been made public about the training data—the "38 categories of objects"—that informed the initial project named MAVEN (Biddle 2019). We do know that the data to be analyzed were rendered as such from full motion video feeds recorded as part of US drone surveillance operations, and that the "objects" to be detected included buildings, vehicles, and humans (presumably those not inside either buildings or vehicles). Gregory (2018) has called upon scholars not to be captured by the view from above, focusing our analyses only on the military gaze, but to attend as well to life on the ground. It's here that algorithmic warfare sources the data that feed it, in the violent transformation of everyday activity into "patterns of life" seen as "anomalous" and so threatening to US interests. The violence continues in its aftermath, moreover, as the injured and dead become the body count. Witnessing and testimony, not turning away, are vital countermeasures.

Algorithms are tricky to study for many reasons. Many of the algorithms that are important to daily life are frequently changing, technically impenetrable even for those with the technological insight to scrutinize them, closely guarded business secrets, and not very meaningful without knowing the data that they operate on (Gillespie 2014). Add that the algorithms immediately important to security are shrouded in additional layers of secrecy (Pasquale 2015), and that the decisions they make are often at best indirect—decision support, rough content filtering, flagging for review, etc.—and you have your work cut out for you as a critically minded social scientist.

Algorithms, as we indicated above, do not do much on their own. They treat data, so one approach is to look at that data. And in the case of "AI," "deep learning," or "neural networks," the technologies dominating computer vision today, they are also trained with data and integrate past performance (Wang and Deng 2018). In the case of computer vision, these training data consist of images and descriptions of what they contain.

Algorithms as a governance technique, even computer vision algorithms, are many things, more like "meetings" or "statistics" than something on which you can put your finger firmly and pronounce a verdict. Even so, there are some effects
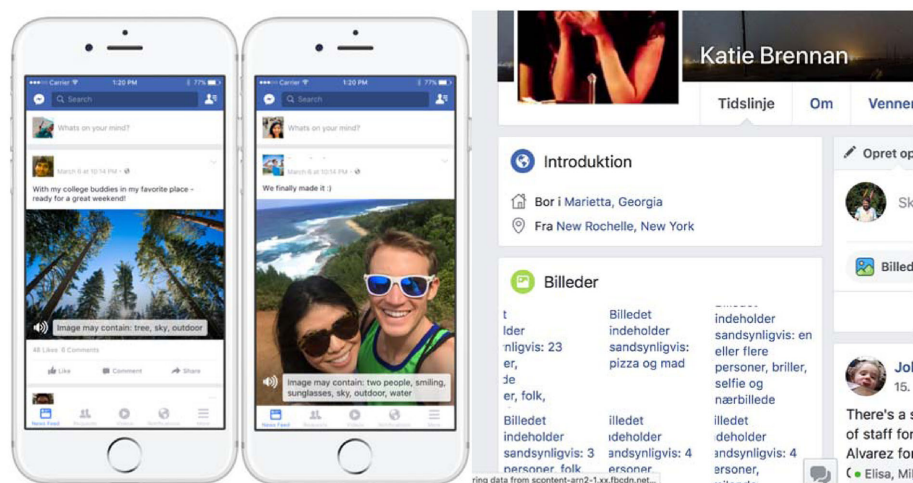
Figure 4. Machine vision-generated descriptions of images. Left: from an illustration in the paper developing the feature (Wu et al. 2017). Right: in use on the Facebook platform of the author, showing image descriptors while loading images. Descriptors help the platform load quickly, and help it track which kinds of image descriptors correlate with user interest. Screenshot taken by Saugmann, October 2018.

that—again like governance through statistics—are similar across dissimilar computer vision systems or different applications of computer vision. The key issue here is what I will call *semiotic violence*,[8] that is, the violence done unto the visual meaning-making process by computer vision systems.

> *Ragazzi*: My own intervention is an additional reflection/variation on Saugmann's notion of semiotic violence (a term I am happy to adopt). While their contribution focuses after this paragraph more on the effects of the violence, my intervention is more focused on thinking about what these operations of semiotic violence are, in particular what are the epistemic operations that are at stake in semiotic violence, and how the notion of translation between multiple modalities of knowledge allows us to shed light on how it works.

This violence is the foundation upon which the force of computation rests when it comes to computer vision tasks, and it has two crucial elements. First, the capture of something that is considered reality in digital storage formats; this part is done with digital cameras, perhaps even by you and me when we post a video or image on a social network platform from where it can be appropriated and used without our knowledge. Second, the conversion of those images into other data formats by computer vision systems, be that unique descriptors, captions, matches with faces in a known database, face recognition data, color description, or some other parameter that the system is developed to produce. Facebook, which I am sure many of you have used, deploys machine vision in many forms, for example, to recognize faces (not in all jurisdictions) and to lighten data load and thus speed up page loading by initially replacing images with descriptions, as shown in figure 4. The computer vision algorithm reduces the images to a set of descriptors. It appears to have been initially developed to help the visually impaired, but also offers what Facebook calls "possib[ilities] to leverage all that rich content to create better experiences for everybody on Facebook" (García García, Wu, and Paluri 2016) and is implemented

---

[8]This concept came up in a discussion with the always-inspiring Gitte du Plessis, which began from her work on white imaginaries of the arctic, environmentalism, and race (du Plessis 2020).

widely as an unseen background operation only visible if images are slow at loading (see figure 4). Computer vision algorithms "see inside images and videos to understand what they depict ... Specifically, we can detect objects, scenes, actions, places of interest, whether an image/video contains objectionable content" (García García, Wu, and Paluri 2016).

We often hear how machine learning systems are better at recognizing objects in images (since 2014) or better at playing mathematical-like games (since 2015), or, more dubiously, can categorize emotions and people's sexuality, etc. This does not mean that machine learning systems/algorithms/AI can see or play games, or have any idea about what sex and erotic attraction is. It means that they can find regularities in data that produce a smaller margin of discrepancy compared to the "true" labels attached to the data when people are asked to do the same categorization on that data (Hayles 1993; Ranjan et al. 2018).

> *Bellanova*: Here you insist, rightly so, that many tend to conflate how machines and humans think (especially when it comes to AI). I would be interested in a brief discussion about the fact that we may think in different ways, but that we have to be careful in not reifying a human way of thinking (and producing meaning) that would be pure, as in not machinic at all. This has political implications because it risks assuming that there has been a lost paradise where humans were able to think without any external aid and that this anti-computational imaginary is a more just projection for the future.

> *Saugmann*: I see how you read me here, and am largely supportive and should probably be more careful in making clear that what I am trying to point out is that semeiosis and data analysis are not equivalent, not that semeiosis is politically innocent or benign. What I am after is closer to what McDermott, in 1976, called "wishful mnemonics," the equivalence constructed in talking about algorithmic systems in anthropomorphizing terms like intelligence, vision, and analysis (McDermott 1976). Noel Sharkey and Lucy Suchman (2013, 18) dig up this concept to warn against assuming that "computational mechanisms actually support the functions named, in other than name only." I try here to show how such support needs to look not only at outcomes but also at the processes by which human faculties are mimicked. If the computational system is evaluated as analogue but superior to human performance, the evaluation may favor computational logics over human ones, such as productive or purposeful misunderstanding or misinterpretation.

Seen from this perspective, it is logical that the areas in which AI excels or is mostly used are datafied social relations like those that we find in online media, where algorithms curate news feeds or data-ready social relations such as chess or other games that lend themselves to description in numbers.

The problem I am interested in here is how algorithmic systems understand us when we are not already acting in data, as we are when we press buttons or scroll through feeds in social media systems. The issue here is how the social world becomes available to algorithms, which read not emotions or faces but structured data, tabulations that can be contained in a data file. This is, increasingly, the work of the digital camera. Far from producing images, what digital cameras produce is not only standardized data files containing data that enable a data reader to display an image, but also metadata that apart from specifying how to read the file and possibly containing a thumbnail preview of its contents enables open tagging as well as geo-tags, timestamps, equipment tags, and a myriad of other operations of describing and or classifying the files. The creation of files follows standardized protocols that date back decades and ensure readability across billions of devices. What is most important for me here is that the resulting image is treated as a photograph that adequately depicts something external to the camera (or at least has the possibility of doing so), that is, that the camera is seen as storing an external reality in digital images, a reality that can then be seen and analyzed through looking at the images.

This is not to say that we are unaware of the myriad of ways in which images can be deceptive, but to say that we are ready to deny the non-equivalence Magritte points to in *la trahison des images*, which holds that the image of a pipe is not a pipe.

> *Ragazzi*: In his work, Pantenburg (2015) explains that the history of cinema is divided between those who posit that the image always lies (*film constructivists* such as Vertov, Eisenstein, and Kuleshov) and those who believe that the image never lies (*film realists* such as Kracauer and Bazin). He shows convincingly that Farocki and Godard took both propositions as true, namely that the image always and never lies at the same time, depending on how it is used. This is what allows both directors to conceptualize a film-based form of theoretical reflection (the essay film), in which images are pitted against others, and some second-order images are presented as "meta-images," which undermines the "realism" of the first-order images. But the construction of the essay film relies on the assumption that these second-order, meta-images carry some degree of truth. This is a similar discussion to the one that we find in social science between foundationalists and anti-foundationalists, one critique against radical anti-foundationalists being that to make their point they still need to assume that there is a "truth" in the claim of anti-foundationalism.

Despite everything, we are ready to treat the digital image as evidence of the actual existence of that which it depicts. This trust often extends to non-visual metadata like time or location stamps, showing how the camera is a trusted device for datafication, rather than a picture-capturing device. The fixation of a past social world in a digital image file is the first step in what I call semiotic violence.

> *Lindskov Jacobsen*: Paradoxically, this issue of trust "despite everything" is sometimes evident even in contexts where, for example, iris recognition cameras are deployed "experimentally" (in humanitarian settings). Still, under such conditions, there is a tendency to trust the camera as a device for datafication. Indeed, an important question to add is perhaps to explore how consequences following from such trust may differ between different subject categories. For example, in humanitarian contexts, this aspect of semiotic violence may come with specific kinds of risks, including the risk that trust in (experimentally applied) iris recognition cameras might imply that, in case of doubt, "refugee status" may be "called into question sooner than the technology" (Hosein and Nyst 2013, 41).

> *Bellanova*: Indeed, the role of metadata within security practices deserves more of our attention. Research in IPS has already insisted on how metadata, such as traffic and location data generated by mobile phones, give private and public authorities detailed information, and this despite their seemingly less privacy-intrusive nature (Bauman et al. 2014). As Saugmann argues here, actors afford metadata the ability to stabilize other captured data as a trustworthy and reliable representation of reality. Metadata also provide precious, if not essential, hints to an algorithmic system to characterize digital objects as something present in a database. From these perspectives, we may want to further unpack how metadata affect computational imaginaries and ultimately security practices and their governance.

> *Irion*: I would like to add that the pervasive logic is that a certain feature is useful for a given individual, for example geolocation data on a digital image can show your vacation trip on a map. At the same time, this usefulness is not exclusive but exploitable for a myriad of other ends that are no longer in the interest of the individual.

The second step is the training of computer vision systems to read these files for the reality they are held to contain and accurately perform tasks like labeling objects, or feelings, or identifying faces from a database. In systems based on machine learning, this takes place through training the algorithm on datasets of training images, that is, images that are labeled with what is, in machine vision engineering, called "ground truth," a description of the objects found in the image or of the accurate face. This is where the semiotics come in. The process underpinning machine learning and machine vision seems semiotic in its nature, difference and

relationality being the key to "learning." In semiotic terms, you would say that the machine vision system learns how this or that signifier (e.g., a face or the shape of a car) does not connect to that signified (e.g., George Clooney or the word cat) just as semiotic theory would have it, by associating the labeled "ground truth" with image elements. Yet, the idea that this connection is "truth" is what is antithetical to semiotics. As semiotics is not the discovery but the making of meaning, the outcome cannot be known in advance, just waiting to be found (as in de Saussure's theory). Thus, the making gets lost when meaning is reimagined as truth. Semiosis, as anybody living in a language community knows well, is fluid, always changing. The visual expressions of peacefulness, anger, sexual preference, gender, etc. are all dynamic and, for example, signifiers of sexual orientation or identity can both change rapidly and also be very specific to particular subcultures. Weber (2017) pointed to the fluidity of sexuality itself to rightly point out the violence in claiming that machine vision can identify sexual preference, and the violence such categorization can all too easily facilitate. On top of this, ground truth denies the dynamic and intersubjective agency of making meaning in interpreting images, and even if deep learning machine vision systems can use the feedback from past categorizations to calibrate future ones (Wang and Deng 2018), this learning is still based on the fallacy of "out-thereness" (Law 2004, 24), of meaning existing as external and anterior to the act of interpretation.

Kittler, von Mücke, and Similon (1987, 117) asserts that as media history moved "from the Remington, via the Turing machine, to microelectronics; [it moved] from mechanization, via automatization, to the implementation of a writing which is cypher and not sense." This is a process that with standardized digital images and computer vision algorithms extends to encompass not just our writing but our visual being. The force of computer vision systems is predicated on a semiotic violence that is the suppression of the always dynamic intersubjectivity on which visual social relations develop by a vision that is cypher and not sense. To a machine vision algorithm, there is nothing strange in you being, for example, 73 percent female. Elsewhere in this discussion, Ragazzi thematizes the translation that takes place after such a calculation, to render it useful for doing security work.

What I have tried to show here is how the force of computation to act on the social world is predicated on a double "fixing" that constitutes what I call semiotic violence. The social past is fixed as evidence contained in image data files and, by the training of machine vision algorithms within regimes of visual truth, the meaning of visual signifiers is fixed, denying that interpretation is indeed interpretation, that meanings can and do change every time we invoke them.

Irion: Retracing the Genesis of De-territorialized Algorithmic Systems

My law and technology background necessarily influences my appreciation of algorithmic violence; however, through our interdisciplinary discussion I have come to realize how important the social sciences have been, and will be, for deconstructing powerful imaginaries on algorithms and AI. Shared perceptions about the predictive capabilities of algorithms or the acceptance of how algorithms pre-structure human experience influence the way, and the conditions in which, our societies continue to embrace algorithmic agents. Where code is capable of regulating conduct in much the same way that legal code does (Lessig 2006), algorithmic systems by extension enforce their version of "reality" from patterns and probabilities derived from data. It is the logic and practices that imbue digital technology (Zuboff 2019) that implicate algorithmic design as always political but never neutral (Gillespie 2014). Hence, every algorithmic system constitutes a highly contextualized vehicle to achieve complex organizational goals. This is where law traditionally comes in to formulate and guarantee the conditions of human freedom in relation to algorithmic predictions. Or so it should be.

From a legal perspective, the de-territorialization of algorithmic agents proves highly problematic for their human-centric governance (Irion 2020). All components—training data and machine learning code—can be moved across today's digital ecosystem and predictive outcomes can be applied at a distance. Take a look at the Crawford and Joler's (2018) "Anatomy of an AI System." It depicts Amazon Echo, colloquially known as Alexa, as an anatomical map of human labor, data, and planetary resources. Algorithmic systems can be deployed in ways that are fairly location-independent, for example, in algorithmic warfare as pictured by Suchman above, foreign interference with democratic elections with computational propaganda (Brundage and Shahar 2018; Howard 2020), or the pervasive mass surveillance of internet users by digital platforms (Zuboff 2019). All three examples embody different degrees of violence; the point I am trying to make, however, is that an algorithm's transboundary provision, even where they form part of relatively mundane digital services, affects the societies and individuals it interacts with.

> *Suchman*: I think we need to understand these systems as always location-dependent and track very closely the claims for their portability, the actual practices through which they're made to travel from one site to another, and the associated material and semiotic violence that enables and results from algorithmic scaling. Following Google's withdrawal from the MAVEN program due to employee protests and accompanying negative publicity, former Google CEO Eric Schmidt has resigned from Google's board of directors to devote himself more fully to funding start-ups like Rebellion Defense, devoted to "modern, scalable products that use artificial intelligence to analyze, secure, and transport national security and defense data," products that, we are assured, all serve democracy, humanitarian values and the rule of law (Conger and Metz 2020).

> *Ragazzi*: I think the decision of the EU Court of Justice (2020) against the Privacy Shield framework is one additional strong argument in favor of the idea of territory-dependent rule over technology. It's important to be explicitly critical of the metaphor of the "cloud" that is in fact a very location-dependent set of networked server farms, which all have their specific geographies of power.

> *Lindskov Jacobsen*: Including a focus on underlying data infrastructures may call attention to an additional, yet different kind of boundary that we need to attend to when exploring issues of algorithmic violence. Some data are collected during military intervention (in Iraq, Afghanistan, and Somalia for example), yet often such data (e.g., biometrics collected by the US military in Iraq) are kept by the US military after a military intervention has ended. This arguably means that when thinking about "boundaries," the war/peace boundary is also an important site to include in analyses of violence at the level of the data infrastructure that underwrites algorithmic systems.

The problem with transnational algorithms can be best described as the fittingness of the algorithmic prediction to the situation where it is applied. A sociotechnical–legal mismatch can be the result of the development genesis of an algorithm or of the transplant effect (Berkowitz, Pistor, and Richard 2003) when an algorithm is deployed in different contexts. Buttarelli (2018) cautions that computer algorithms, when they are developed "in countries with the least protection for fundamental rights, controlled by authoritarian regimes, will not provide us with a sustainable and viable future infrastructure." Take facial recognition systems, for example, which are state policy in China but have prompted calls for strict regulation in Western democracies (Stark 2019). The question here arises whether a given algorithmic system's genesis should be taken into account for its legitimate and ethical adoption in Europe and elsewhere. The other issue is that transnational transplants of algorithms might prove problematic if they do not correspond to the social and legal contexts of the society they interact with (Chander 2021). Often, algorithms and training datasets come from jurisdictions different from those where the algorithmic system is later used. Societies by contrast have diverse setups

of rights, freedoms, and indeed also ethics that are increasingly and deliberately meshed together by transnational technologies and planetary-scale computation. Individuals and societies will be confronted with transnational algorithms whose design modulates values and violence external to the local contexts that carry the risk of normative arbitrage between societies.

> *Lindskov Jacobsen*: These points about the genesis of both data and algorithmic systems are crucial, adding attention to the differential circumstances, including discriminatory elements and ethical challenges, that are often forgotten when data and technology circulate back to contexts.

> *Bellanova*: I agree that the genesis of a given algorithmic system is important, not only in territorial but also in temporal terms. Bucher (2018, 42) invites us to think about the agency of algorithms, not merely in terms of "where" but also, and foremost, in terms of "when." For instance, what about the use of algorithmic systems initially developed for retailing purposes and then deployed, with minor adjustments and tweaking, in law enforcement contexts?

> *Lindskov Jacobsen*: Perhaps an important question is whether the introduction of new regulation in certain locations entails a risk of shifting the gathering of training data and the testing of new algorithms to different, less stringently regulated locations.

The speed with which the algorithmic interdependency of societies increases is not met by an equally rapid formation of international cooperation mechanisms that would mitigate the negative consequences (UN Secretary-General's High-Level Panel on Digital Cooperation 2019). The international community is actually very far from universal principles for governing algorithmic systems. OECD (2019) Principles on Artificial Intelligence are a significant step forward, but they are non-binding and flexible to domestic articulations. As was affirmed by the UN Human Rights Council (2016, 2018), human rights must be protected offline and online regardless of frontiers. However, unlike digital technologies, human rights do not simply flow across borders. Instead, human rights wield universal protection from their geopolitically fragmented implementation by states. Put differently, international human rights protection is founded on constitutional pluralism that provides for variation between societies' human rights frameworks.

Simultaneously, transnational algorithmic flows erode the paradigms that used to underpin a society's conventional right to self-governance. Characteristic of the demise of the Westphalian nation state in the era of digital globalization, domestic legal institutions often turn out to be unfit to govern transnational technologies (Irion 2020). The disintermediation of human rights in transnational settings is well documented in the cases of online data privacy, but will become equally persistent in relation to the right to non-discrimination (Barocas and Selbst 2016) and the guarantee of personal autonomy (Pasquale 2015). Policymakers in the EU and elsewhere take legislative action based on the presumption that algorithmic governance at the domestic level can be assertive on transnational algorithmic systems. This poses the real risk of not seeing the forest for the trees, because transnational algorithms can bypass even the best catalogue of prescriptive requirements with which algorithms should comply. Left to its own devices, top-down regulation based on conferring rights and obligations does not stand a chance of coping with algorithmic systems that flow into our societies from abroad, unless there are means to scrutinize them.

One way to handle the cross-border supply of algorithmic predictions would be to insist on a healthy measure of transparency contributing to human rights accountability. Public knowledge about global data value chains, involved actors, and the geographic distribution of the parts of a transnational algorithmic system are key for any risk assessment. Moreover, social scientists argue that algorithmic governance would benefit from "regulation toward auditability" (see Sandvig et al. 2014)

that privileges public scrutiny over internal audits. There will be areas of important public interest, such as political micro-targeting and computational propaganda, where only radical transparency at the level of algorithmic code, data inputs and outputs, and application programming interfaces would provide for public scrutiny and mitigate the risk of normative arbitrage. Operational transparency would be a precondition for the development of automated tools to hold transnational algorithms accountable, for example, in the field of consumer protection and public sector decision-making (Lippi et al. 2020).

> *Bellanova*: While I can see the merit of politically insisting on the need for further transparency, there is a risk of focusing only on some (albeit important) aspects of algorithmic governance and sidelining others. As Ananny and Crawford (2018, 974, italics in original) note, "[t]he implicit assumption behind calls for transparency is that *seeing* a phenomenon creates opportunities and obligations to make it accountable and thus to *change* it." When we try to see what algorithmic violence does, much depends on who casts what kind of light on what, and against which background. For instance, the value of Crawford and Joler's (2018) work on Alexa is the ability to go beyond the classical foci on transparency as understood by public law, and to unpack the multiple relations—including violent relations of exploitation of human and nature—that make possible the material existence of an algorithmic system such as Alexa.

Ragazzi: Learning to Study (Algorithmic) Translations

I would like in this short intervention to address one of the key paradoxes of algorithmic violence as sketched in the introduction of this article. Surveillance, security, and war apparatuses, empowered through modern digital technologies, have never been so pervasive as they are today (Bauman et al. 2014). At the same time, rarely has such a precise and overarching degree of surveillance been able to impose itself without violence on the broader population (Zuboff 2019). Comparisons of digital surveillance with the years of the communist East German Stasi or the Romanian Securitate are somewhat unconvincing: our contemporary condition, in modern democracies, is a far cry from the level of generalized fear and suspicion that prevailed in those dictatorships. In democracies, algorithmic security is implemented with a great degree of indifference at best, active volunteering of personal data and "DIY surveillance" at worst (Bauman and Lyon 2013, 59). There are, of course, small pockets of contestation among academics, human rights organizations, and activists. But their impact has been, so far, marginal. Occasionally, the opposition to practices of algorithmic violence gains popularity, crystalizing around the use of specific technologies. Advocacy groups have, for example, been successful in mobilizing against facial recognition in the context of the recent demonstrations against police brutality in the United States (Coldewey 2020; Fowler 2020). But overall, for the general public, including many critical academics and activists, Gmail, Yahoo, YouTube, Google Docs, Facebook, Instagram, WhatsApp, and Skype are services that bear no apparent connection with CIA terrorist kill lists and drone operations in Afghanistan–Pakistan (Heller 2013), databases of alleged "radicalized" individuals in Europe (Heath-Kelly 2016), or surveillance mechanisms deployed in the south of the Mediterranean to prevent undocumented migrants from reaching Europe (Fisher 2018).

> *Irion*: I would like to add that for the purpose of serving online ads to internet users the adtech industry has built the largest online surveillance infrastructure in history. How could an entire industry be allowed to spiral out of control, invade and trespass to such a pervasive degree on individuals' online lives, thereby increasingly refining their algorithmically supported infrastructures? I believe one of the reasons is the invisibility and secrecy of the violence and our lack of imagination. Zuboff (2019, 12) explains that "[w]hen we encounter something unprecedented, we automatically

interpret it through the lenses of familiar categories, thereby rendering invisible precisely that which is unprecedented." Endemic online surveillance is emblematic for the enduring regulatory crisis in information law and policy, which is moreover ill equipped to scrutinize algorithmic systems.

There are many reasons behind this disconnect. Even though the Snowden revelations have highlighted clear relations between these two realities, and even though several academic and advocacy projects work relentlessly to publicize the relations between them, most people chose to ignore them, because of laziness, lack of technical skills, convenience, or network effects. But I would like to suggest that there is a further fundamental reason, of an epistemological nature. Algorithmic violence is largely accepted because unlike the various modes of state surveillance and violence of the past, it is for the most part invisible, inaudible and impalpable for the vast majority of people. Algorithmic violence is indeed located not only in the acts of collecting or processing data, but rather in the technical operations of translation (Goodwin 1994, Bourne, Johnson, and Lisle 2015) that render the world computable. On the one hand, these are the operations of datafication, that is, of transformation of the world captured through various sensors into computational data (Aradau and Blanke 2015). On the other hand, it is located in operations of textualization, visualization, auralization, or tactilization, that is, operations that translate those computational products back into discursive and sensorial outputs that can be acted upon by professionals of security and warfare. Saugmann has captured this idea in the notion of *semiotic violence* in his above intervention. It is this specific characteristic that renders algorithmic violence largely intangible to scrutiny because it escapes our traditional categories of social scientific knowledge production and thus political mobilization. We know indeed how to study data collection. We know how to study algorithms. But we know very little about how to study those operations of translation that allow discourse, images, sounds, and data to be computed and made actionable.

> *Suchman*: As promoter of algorithmic warfare, Eric Schmidt himself has remarked that algorithms for machine learning require "millions of entries in the matrices, billions of pieces of data"; he draws a contrast between applications like traffic analysis and the hunt for "terrorists" (Scharre et al. 2017). Along with the respective frequency of car traffic versus terrorism, the difference turns on what comprise our units of analysis. For traffic flow, a "piece" of data would be a vehicle, about which we would in the first analysis require no knowledge of where it was going, who was inside it, and so forth. But what would be the comparable unit in, for example, the class "member of ISIS"? The latter requires rendering persons as standardized units through the use of profiling, with the effect that we have a highly sophisticated technology reliant upon the crudest forms of stereotyping. Done responsibly, Crawford and Paglen (2019, not paginated) observe: "the project of interpreting images is a profoundly complex and relational endeavor. Images are remarkably slippery things, laden with multiple potential meanings, irresolvable questions, and contradictions."

How can we therefore address this blind spot? A growing body of literature, located at the convergence of critical security studies (Saugmann 2013; de Goede, Simon, and Hoijtink 2014; Amicelle, Aradau, and Jeandesboz 2015; Amoore and Raley 2017; Saugmann 2017) and STS (Bellanova and González Fuster 2013; O'Grady 2015; Suchman 2015; Saugmann 2019) has started to lay the conceptual foundations of a sociological analysis of such processes. But it is interesting to notice that one of the emerging concepts around which this literature is starting to be organized—the notion of "operative image," cited in several recent texts (Dijstelbloem, van Reekum, and Schinkel 2017; Gregory 2018; Bousquet 2018; Suchman above)—does not come from the work of a social scientist, but that of a filmmaker, Farocki (2004), who coined it a decade earlier than today's discussions, to explain the purpose of his cinematographic and theoretical research. Farocki

has indeed largely anticipated the scholarly question of the translation of the image into operative decisions and routines of algorithmic violence: from his early work on computer vision *Auge/Machine I–III* (Farocki 2001–2003) to his later work on simulation and 3D renderings of war in *Serious Games I–IV*.[9] As Thomas Elsaesser put it:

> in the more recent installations … Farocki seems to ask: How do we meet the challenge of visibility and visualization, when more and more phenomena that govern our lives are not visible to the human eye, because they are either too big or too small, too fast or too slow, or they deal in magnitudes and quantities we cannot comprehend other than in diagrams or mathematical equations? (Elsaesser and Alberro 2014, 8)

What is at stake, in work like Farocki's, is thus precisely the question that social science is revisiting more than a decade later, namely how to seize the image theoretically: not only conceptually, but through a cinematographic practice aimed at making visible and tangible the tensions and translations between discourse, images and algorithms. Farocki is, of course, not the only artist to have put their finger precisely on the question of translation between different modalities of knowledge and perception (one can think, for example, of recent work by Steyerl, Paglen, and Crawford or the Forensic Architecture project). But he is certainly one of the first to have proposed a theoretical approach to algorithmic violence that does not rely on propositional, text-based analysis, but instead on a practice-based theorizing, interested as he was in exploring the ways in which embracing the complex relations that images against images, images against text, and images against algorithms bring to our understanding of the processes of translation and the violence that can be embedded in them (Deleuze 1986 [1983]; Pantenburg 2015).

> *Saugmann*: I think the concept of the operative image is useful but also deceptive, essentializing or ontologizing a difference that is not a difference in the image, but in how it is used. As I try to show above with something as mundane as Facebook pictures, any image can be subjected to machine vision, categorized in terms useful to the operator, and thus operationalized. So, whereas I very much appreciate how Farocki calls attention to the potentially violent uses of images, I think the concept runs the danger of suggesting that this is somehow related to the image that, for example, a "surveillance image" is inherently operative while a cat picture is not. This is only the case until a cat image becomes useful for those with the computational resources to categorize and relate the cat picture. And since difference and patterns are what advanced computational systems are establishing as security in enormous datasets (Kaufmann, Egbert, and Leese 2018), the data that are *not* pointing to anything abnormal are also "operative" in the sense of participating in establishing, for example, a norm against which outliers can be flagged. So, speaking of the "operative image" rather than image operationalization, may burden the image with the misuse made of it. I have tried to show how this is an issue in the appropriation of images taken by civilians in war zones (Saugmann 2020). There may perhaps be some images, like Paglen's "limit tele-photography" series of photos of secret sites that I have earlier worked on, which come close to being "non-operative" or at least seek to be so close to the "limits of visibility" that it is hard to imagine how they could be operationalized (Saugmann and Möller 2013). But I am skeptical as to whether this is really the case, not least as metadata can still be made operational even if the image is not visually intelligible. So for me, the operative image is any image, or at least any digital image.

Where does this leave us social scientists and international political sociologists more specifically? Does it mean that algorithmic violence can only be truly uncovered through artistic, cinematographic practices? Of course, not. The point of my intervention is not to oppose what we can call non-propositional reasoning to propositional, argumentative reasoning (MacDougall 2006). It is instead to argue that IPS, critical security studies, and STS have much to gain in embracing novel modalities of audio–visual, sensorial theorizing (Taylor 1994; Vuori and Saugmann

---

[9] https://www.moma.org/collection/works/143767.

Andersen 2018). Analyzing algorithmic violence solely through text places the analysis already at the endpoint of the process of translation as reducing images, sounds, and computational processes to text is already a process of translation in itself. If what is to be studied is the translation, then what is needed is a dialogue with different methods that allow us to put methods of digital and audio–visual tinkering, reverse engineering, visualization, auralization, audio–visual recording, and editing in dialogue with propositional knowledge at the center, so as to uncover how these processes of translation work: as a fruitful analysis and critique can come from making these processes once again visible, audible, and palpable.

Conclusion: Algorithmic Violences

Computing played an important role in bringing together this collective discussion: not only as a subject matter, given that the algorithmic, in all of its diverse instantiations and multiple understandings, is a recurring research object for each of us. While we were able to meet in person on a few occasions, most of the conversation took place online, on platforms such as Zoom and Google Docs. These are run by private actors involved, as data sources or algorithm providers, in security practices ranging from law enforcement to warfare, including practices that we have been questioning in this very collective discussion. Such an irony is not lost on us. It actually highlights even further the urgency of discussing how, through what digital means, a critique of algorithmic violence can be carried out. Currently, a massive digitalization of education, from elementary schools to universities, is happening at unprecedented speed. The question of how we, as teachers, colleagues, and intellectuals, navigate and negotiate computation is indeed becoming paramount in view of "mediating" critique, as in "work[ing] as one link in a chain of meaning-making that stretches across diverse actors and domains of life" (Austin, Bellanova, and Kaufmann 2019, 4). Hence, rather than offering firm conclusions, this discussion puts forward a number of issues that we are particularly concerned to see highlighted in future debates.

This collective discussion shows that it is vital to attend to the multiplicity and ambiguity of algorithmic violence, as well as to the effects of seemingly innocent necessities like the fixation of the past into fact/data as necessary to fix the social for computational treatment, and thus to enable such computation to make the future actionable, something security can intervene in. When thinking about more conventional, often largely pre-digital, forms of violence, as the subject of much international relations scholarship, it is increasingly important to add a note on algorithmic violence in the analysis. Doing so is necessary in order not to lose sight of practices that are not violent in a more traditional sense (see also Amoore and de Goede 2014). This is an empirical point (e.g., about blind spots vis-à-vis instances of algorithmic violence), as well as a methodological argument (e.g., about translation processes at play in the use of computer/machine vision and hence about the value of moving beyond text when analyzing algorithmic violence), and a normative sensitivity (e.g., about invisibilized forms of algorithmic violence not being held to account). Indeed, the invisibility of many algorithmically supported infrastructures poses numerous challenges, including accountability and governance challenges, hence the importance of thinking differently about the issue of algorithmic violence. Attention must be paid to an algorithmic system's genesis in terms of data provenance, geography, culture, time and space, resources, and actors involved for its governance. This is particularly crucial for issues arising from the transnational deployment of algorithmic systems for the protection of human rights and other domestic forms of redress against algorithmic violence.

In the security domain, violence is often implied in the very making of the data infrastructures needed for algorithms to work. Violence thus starts before algorithms produce profiles or provide targeting information. Semiotic violence can also

happen when datasets move from one practice to another, crossing not only geopolitical borders but also sociopolitical settings and temporal boundaries, for example, between civilian and military practices. Accordingly, we need to attend to questions of algorithmic violence happening not only in the initial moments of datafication and data collection, but also when datasets become (in)security data. Focusing on data infrastructures and their making in diverse security contexts can help resituating algorithms as part of complex and messy practices, and thus avoid disembodying them (which would end up cautioning the same frictionless discourse that promotes algorithmic governance). It may offer IPS-inspired research a way to grasp the force of computation *in media res*, that is, studying how algorithms affect and are shaped by other things (see also Chun 2011, 177). This means no clear-cut foundational ground on which critique can be built and leveraged once and for all, but rather a continuous work of attention and intervention.

References

Abu Hamdan, Lawrence. 2016. *[Inaudible] A Politics of Listening in 4 Acts.* Berlin: SternbergPress.
Amicelle, Anthony, Claudia Aradau, and Julien Jeandesboz. 2015. "Questioning Security Devices: Performativity, Resistance, Politics." *Security Dialogue* 46 (4): 293–306.
Amicelle, Anthony, and Vanessa Iafolla. 2017. "Suspicion-in-the-Making: Surveillance and Denunciation in Financial Policing." *The British Journal of Criminology* 58 (4): 845–63.
Amoore, Louise. 2009. "Algorithmic War: Everyday Geographies of the War on Terror." *Antipode* 41 (1): 49–69.
———. 2020. *Cloud Ethics.* Durham, NC: Duke University Press.
Amoore, Louise, and Marieke de Goede. 2005. "Governance, Risk and Dataveillance in the War on Terror." *Crime, Law & Social Change* 43 (2/3): 149–73.
———. 2014. "What counts as violence?." In *Global Politics. A new introduction,* edited by Jenny Edkins and Maja Zehfuss, 496–518. Oxon: Routledge.
Amoore, Louise, and Rita Raley. 2017. "Securing with Algorithms: Knowledge, Decision, Sovereignty." *Security Dialogue* 48 (1): 3–10.
Ananny, Mike, and Kate Crawford. 2018. "Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability." *New Media & Society* 20 (3): 973–89.
Ansems de Vries, Leonie, Lara Montesinos Coleman, Doerthe Rosenow, Martina Tazzioli, and Rolando Vázquez. 2017. "Collective Discussion: Fracturing Politics (Or, How to Avoid the Tacit Reproduction of Modern/Colonial Ontologies in Critical Thought)." *International Political Sociology* 11 (1): 90–108.

Aradau, Claudia, and Tobias Blanke. 2015. "The (Big) Data-Security Assemblage: Knowledge and Critique." *Big Data & Society* 2 (2): 1–12.

———. 2018. "Governing Others: Anomaly and the Algorithmic Subject of Security." *European Journal of International Security* 3 (1): 1–21.

Aradau, Claudia, Tobias Blanke, and Giles Greenway. 2019. "Acts of Digital Parasitism: Hacking, Humanitarian Apps and Platformisation." *New Media & Society* 21 (11–12): 2548–65.

Austin, Jonathan Luke, Rocco Bellanova, and Mareile Kaufmann. 2019. "Doing and Mediating Critique: An Invitation to Practice Companionship." *Security Dialogue* 50 (1): 3–19.

Bacevich, Andrew J. 2020. "Defund the Police. And the Military, Too." *The Nation*, June 24. Accessed January 4, 2021. https://www.thenation.com/article/society/defund-police-military/.

Barocas, Solon, and Andrew D. Selbst. 2016. "Big Data's Disparate Impact." *California Law Review* 104 (3): 671–732.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and Rob B.J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8 (2): 121–44.

Bauman, Zygmunt, and David Lyon. 2013. *Liquid Surveillance: A Conversation.* Cambridge: Polity Press.

Bellanova, Rocco, and Marieke de Goede. 2020. "The Algorithmic Regulation of Security: An Infrastructural Perspective." *Regulation & Governance.* doi:10.1111/rego.12338.

Bellanova, Rocco, and Georgios Glouftsios. 2020. "Controlling the Schengen Information System (SIS II): The Infrastructural Politics of Fragility and Maintenance." *Geopolitics.* doi:10.1080/14650045.2020.1830765.

Bellanova, Rocco, and Gloria González Fuster. 2013. "Politics of Disappearance: Scanners and (Unobserved) Bodies as Mediators of Security Practices." *International Political Sociology* 7 (2): 188–209.

———. 2019. "Composting and Computing: On Digital Security Compositions." *European Journal of International Security* 4 (3): 345–65.

Bellanova, Rocco, Katja Lindskov Jacobsen, and Linda Monsees. 2020. "Taking the Trouble: Science, Technology and Security Studies." *Critical Studies on Security* 8 (2): 87–100.

Benjamin, Medea, and Nicolas Davies. 2020. "Defund the Police, Defund the Military." openDemocracy. Accessed January 12, 2021. https://www.opendemocracy.net/en/oureconomy/defund-police-defund-military/.

Berkowitz, Daniel, Katharina Pistor, and Jean-Francois Richard. 2003. "The Transplant Effect." *The American Journal of Comparative Law* 51 (1): 163–204.

Best, Jacqueline, and William Walters. 2013. ""Actor-Network Theory" and International Relationality: Lost (and Found) in Translation. Introduction." *International Political Sociology* 7 (3): 332–34.

Biddle, Sam. 2019. "Pentagon Says All of Google's Work on Drones Is Exempt from the Freedom of Information Act." *The Intercept*, March 25. Accessed January 14, 2021. https://theintercept.com/2019/03/25/google-project-maven-pentagon-foia/.

Bigo, Didier. 2014. "The (In)securitization Practices of the Three Universes of EU Border Control: Military/Navy—Border Guards/Police—Database Analysts." *Security Dialogue* 45 (3): 209–25.

Bleiker, Roland, ed. 2018. *Visual Global Politics.* London: Routledge.

Bonditti, Philippe. 2004. "From Territorial Space to Networks: A Foucaldian Approach to the Implementation of Biometry." *Alternatives* 29 (4): 465–82.

Bourne, Mike, Heather Johnson, and Debbie Lisle. 2015. "Laboratizing the Border: The Production, Translation and Anticipation of Security Technologies." *Security Dialogue* 46 (4): 307–25.

Bousquet, Antoine. 2018. *The Eye of War. Military Perception from the Telescope to the Drone.* Minneapolis, MN: University of Minnesota Press.

Broussard, Meredith. 2019. *Artificial Unintelligence: How Computers Misunderstand the World.* Cambridge, MA: MIT Press.

Brundage, Miles, and Avin Shahar. 2018. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.* Oxford: University of Oxford.

Bucher, Taina. 2018. *If … Then. Algorithmic Power and Politics.* Oxford: Oxford University Press.

Buttarelli, Giovanni. 2018. "What Do We Learn from Machine Learning?" European Data Protection Supervisor. Accessed January 13, 2021. https://edps.europa.eu/press-publications/press-news/blog/what-do-we-learn-machine-learning_en.

Chander, Anupam. 2021. "AI and Trade." In *Big Data and Global Trade Law*, edited by Mira Burri. Cambridge: Cambridge University Press.

Cheney-Lippold, John. 2011. "A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control." *Theory, Culture & Society* 28 (6): 164–81.

Chun, Wendy Hui Kyong. 2011. *Programmed Visions.* Cambridge, MA: MIT Press.

Coldewey, Devin. 2020. "IBM Ends All Facial Recognition Business as CEO Calls Out Bias and Inequality." *TechCrunch*, June 9. Accessed January 14, 2021. https://techcrunch.com/2020/06/08/ibm-ends-all-facial-recognition-work-as-ceo-calls-out-bias-and-inequality/?guccounter=1.

Conger, Kate, and Cade Metz. 2020. "'I Could Solve Most of Your Problems': Eric Schmidt's Pentagon Offensive." *New York Times*, May 2. Accessed January 13, 2021. https://www.nytimes.com/2020/05/02/technology/eric-schmidt-pentagon-google.html?utm_source=morning_brew.

Crawford, Kate, and Vladan Joler. 2018. *Anatomy of an AI System.* New York: The AI Now Institute and Share Lab.

Crawford, Kate, and Trevor Paglen. 2019. *Excavating AI. The Politics of Images in Machine Learning Training Sets.* New York: The AI Now Institute.

Daston, Lorraine, and Peter Galison. 1992. "The Image of Objectivity." *Representations* (40): 81–128.

de Goede, Marieke. 2018. "The Chain of Security." *Review of International Studies* 44 (1): 24–42.

de Goede, Marieke, Stephanie Simon, and Marijn Hoijtink. 2014. "Performing Preemption." *Security Dialogue* 45 (5): 411–22.

Deleuze, Gilles. 1986 [1983]. *Cinema I: The Movement-Image.* New York: The Athlone Press.

Dencik, Lina, Arne Hintz, and Jonathan Cable. 2016. "Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism." *Big Data & Society* 3 (2): 1–12.

Derrida, Jacques. 1990. "Force de loi: le 'fondement mystique de l'autorité' [Force of Law: The 'Mystical Foundation of Authority']." *Cardozo Law Review* 11 (Special Issue): 920–1045.

Dijstelbloem, Huub, Rogier van Reekum, and Willem Schinkel. 2017. "Surveillance at Sea: The Transactional Politics of Border Control in the Aegean." *Security Dialogue* 48 (3): 224–40.

du Plessis, Gitte. 2020. "Invisibility, Colors, Snow: Arctic Biosemiotics and the Violence of Climate Change." *Theory, Culture & Society.* doi:10.1177/0263276420976793.

Elsaesser, Thomas, and Alexander Alberro. 2014. "Farocki: A Frame for the No Longer Visible: Thomas Elsaesser in Conversation with Alexander Alberro." *e-flux* 59 (November): 1–10.

Eubanks, Virginia. 2018. *Automating Inequality.* New York: Picador.

EU Court of Justice. 2020. *The Court of Justice Invalidates Decision 2016/1250 on the Adequacy of the Protection Provided by the EU–US Data Protection Shield.* Luxembourg: Court of Justice of the European Union.

Farocki, Harun. 2001–2003. Auge/Machine I-III (Eye/Machine I-III).

———. 2004. "Phantom Images." *PUBLIC* 29: 12–22.

Fisher, Daniel X.O. 2018. "Situating Border Control: Unpacking Spain's SIVE Border Surveillance Assemblage." *Political Geography* 65 (July): 67–76.

Fowler, Geoffrey. 2020. "Black Lives Matter Could Change Facial Recognition Forever—If Big Tech Doesn't Stand in the Way." *The Washington Post*, June 12. Accessed January 15, 2021. https://www.washingtonpost.com/technology/2020/06/12/facial-recognition-ban/.

Frowd, Philippe M. 2017. "The Promises and Pitfalls of Biometric Security Practices in Senegal." *International Political Sociology* 11 (4): 343–59.

Fuller, Matthew, and Andrew Goffey. 2012. *Evil Media.* Cambridge, MA: The MIT Press.

García García, Darío, Shaomei Wu, and Manohar Paluri. 2016. "Under the Hood: Building Accessibility Tools for the Visually Impaired on Facebook." *Facebook Engineering*, December 18. Accessed January 15, 2021. https://engineering.fb.com/2016/04/04/ios/under-the-hood-building-accessibility-tools-for-the-visually-impaired-on-facebook.

Gillespie, Tarleton. 2014. "The Relevance of Algorithms." In *Media Technologies. Essays on Communication, Materiality, and Society,* edited by Tarleton Gillespie, Pablo J. Boczkowski, and Kirsten A. Foot, 167–93. Cambridge, MA: The MIT Press.

Goffey, Andrew. 2008. "Algorithm." In *Software Studies. A Lexicon,* edited by Matthew Fuller, 15–20. Cambridge, MA: The MIT Press.

Goodwin, Charles. 1994. "Professional Vision." *American Anthropologist* 96 (3): 606–33.

Granger, Marie-Pierre, and Kristina Irion. 2018. "The Right to Protection of Personal Data: The New Posterchild of European Union Citizenship?" In *Civil Rights and EU Citizenship,* edited by Sybe de Vries, Henri de Waele, and Marie-Pierre Granger, 279–302. Cheltenham: Edward Elgar.

Gregory, Derek. 2018. "Eyes in the Sky–Bodies on the Ground." *Critical Studies on Security* 6 (3): 347–58.

Guffond, Jasmine. 2020. "Listening Back. Browser Add-On for Firefox and Chrome." Accessed June 20, 2020. http://www.jasmineguffond.com/?path=art/Listening+Back.

Hacking, Ian. 1990. *The Taming of Chance.* Cambridge: Cambridge University Press.

Hayles, N. Katherine. 1993. "Virtual Bodies and Flickering Signifiers." *October* 66: 69–91.

Heath-Kelly, Charlotte. 2016. "Algorithmic Autoimmunity in the NHS: Radicalisation and the Clinic." *Security Dialogue* 48 (1): 29–45.

Hellberg, Ann-Sofie, and Åke Grönlund. 2013. "Conflicts in Implementing Interoperability: Re-operationalizing Basic Values." *Government Information Quarterly* 30 (2): 154–62.

Heller, Kevin Jon. 2013. ""One Hell of a Killing Machine": Signature Strikes and International Law." *Journal of International Criminal Justice* 11 (1): 89–119.

Hildebrandt, Mireille. 2008. "Defining Profiling: A New Type of Knowledge?" In *Profiling the European Citizen. Cross Disciplinary Perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 17–45. Dordrecht: Springer.

Hosein, Gus, and Carly Nyst. 2013. "Aiding Surveillance. An Exploration of How Development and Humanitarian Aid Initiatives Are Enabling Surveillance in Developing Countries." Privacy International. Accessed October 2013. https://privacyinternational.org/sites/default/files/2017-12/Aiding%20Surveillance.pdf.

Howard, Philip N. 2020. *Lie Machines*. New Haven, CT: Yale University Press.

Huelss, Hendrik. 2019. "Norms Are What Machines Make of Them: Autonomous Weapons Systems and the Normative Implications of Human–Machine Interactions." *International Political Sociology* 14 (2): 111–28.

Ihde, Don. 2009. "From da Vinci to CAD and Beyond." *Synthese* 168 (3): 453–67.

Ilves, Ieva. 2020. "Why Are Google and Apple Dictating How European Democracies Fight Coronavirus?" *The Guardian*, June 16. Accessed January 15, 2021. https://www.theguardian.com/commentisfree/2020/jun/16/google-apple-dictating-european-democracies-coronavirus.

Introna, Lucas D. 2016. "Algorithms, Governance, and Governmentality. On Governing Academic Writing." *Science, Technology, & Human Values* 41 (1): 17–49.

Irion, Kristina. 2021. "Panta Rhei: A European Perspective on Ensuring a High-Level of Protection of Digital Human Rights in a World in Which Everything Flows." In *Big Data and Global Trade Law*, edited by Mira Burri. Cambridge: Cambridge University Press.

Jacobsen, Elida Kristine Undrum. 2012. "Unique Identification: Inclusion and Surveillance in the Indian Biometric Assemblage." *Security Dialogue* 43 (5): 457–74.

Jay, Martin. 1988. "Scopic Regimes of Modernity." In *Vision and Visuality*, edited by Hal Foster, 3–23. Seattle, WA: Bay Press.

Johns, Fleur. 2017. "Data, Detection, and the Redistribution of the Sensible in International Law." *American Journal of International Law* 111 (1): 57–103.

Kaufmann, Mareile, Simon Egbert, and Matthias Leese. 2018. "Predictive Policing and the Politics of Patterns." *The British Journal of Criminology* 59 (3): 674–92.

Kimery, Anthony. 2018. "Biometrics Play Significant Role in New US Army Intelligence Doctrine." BiometricUpdate.com. Accessed January 14, 2021. https://www.biometricupdate.com/201809/biometrics-play-significant-role-in-new-us-army-intelligence-doctrine.

Kitchin, Rob. 2014. *The Data Revolution. Big Data, Open Data, Data Infrastructures & Their Consequences*. London: Sage.

Kittler, Friedrich, Dorothea von Mücke, and Philippe L. Similon. 1987. "Gramophone, Film, Typewriter." *October* 41: 101–18.

Knight, Emma, and Alex Gekker. 2020. "Mapping Interfacial Regimes of Control: Palantir's ICM in America's Post-9/11 Security Technology Infrastructures." *Surveillance & Society* 18 (2): 231–43.

Law, John. 2004. *After Method. Mess in Social Science Research*. London: Routledge.

Leander, Anna. 2019. "Sticky Security: The Collages of Tracking Device Advertising." *European Journal of International Security* 4 (3): 322–44.

Leloup, Damien. 2020. "La RATP va tester des caméras « intelligentes » pour mesurer le taux de port du masque dans la station Châtelet." *Le Monde*, May 7. Accessed January 15, 2021. https://www.lemonde.fr/pixels/article/2020/05/07/ratp-des-cameras-intelligentes-pour-mesurer-le-taux-de-port-du-masque-dans-la-station-chatelet_6039008_4408996.html.

Lessig, Lawrence. 2006. *Code Version 2.0*. New York: Basic Books.

Lindskov Jacobsen, Katja. 2017. "On Humanitarian Refugee Biometrics and New Forms of Intervention." *Journal of Intervention and Statebuilding* 11 (4): 529–551.

———. 2019. "Biometric Voter Registration: A New Modality of Democracy Assistance?" *Cooperation and Conflict* 55 (1): 127–48.

Lindskov Jacobsen, Katja, and Larissa Fast. 2019. "Rethinking Access: How Humanitarian Technology Governance Blurs Control and Care." *Disasters* 43 (S2): S151–68.

Lindskov Jacobsen, Katja, and Rune Saugmann. 2019. "Optimizing Coalition Air Warfare: The Emergence and Ethical Dilemmas of Red Card Holder Teams." *Global Policy* 10 (3): 349–53.

Lippi, Marco, Giuseppe Contissa, Agnieszka Jablonowska, Francesca Lagioia, Hans-Wolfgang Micklitz, Przemyslaw Palka, Giovanni Sartor, and Paolo Torroni. 2020. "The Force Awakens: Artificial Intelligence for Consumer Law." *Journal of Artificial Intelligence Research* (67): 169–90.

Lisle, Debbie, and Mike Bourne. 2019. "The Many Lives of Border Automation: Turbulence, Coordination and Care." *Social Studies of Science* 49 (5): 682–706.

Lister, Martin, Jon Dovey, Seth Giddings, Iain Grant, and Kieran Kelly. 2009. *New Media. A Critical Introduction*, 2nd ed. Oxon: Routledge.

Lomborg, Stine, and Patrick Heiberg Kapsch. 2020. "Decoding Algorithms." *Media, Culture & Society* 42 (5): 745–761.

Lyon, David, ed. 2003. *Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination*. London: Routledge.

MacDougall, David. 2006. *The Corporeal Image*. Princeton, NJ: Princeton University Press.

Madianou, Mirca. 2019. "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies." *Television & New Media* 20 (6): 581–99.

Madsen, Anders Koed, Mikkel Flyverbom, Martin Hilbert, and Evelyn Ruppert. 2016. "Big Data: Issues for an International Political Sociology of Data Practices." *International Political Sociology* 10 (3): 275–96.

McDermott, Drew. 1976. "Artificial Intelligence Meets Natural Stupidity." *SIGART Bulletin* (57): 4–9.

Morozov, Evgeny. 2013. *To Save Everything, Click Here*. New York: Public Affairs.

Muller, Benjamin, Thomas N. Cooke, Miguel de Larrinaga, Philippe M. Frowd, Deljana Iossifova, Daniela Johannes, Can E. Mutlu, and Adam Nowek. 2016. "Collective Discussion: Ferocious Architecture: Sovereign Spaces/Places by Design." *International Political Sociology* 10 (1): 75–96.

Noble, Safiya Umoja. 2018. *Algorithms of Oppression. How Search Engines Reinforce Racism*. New York: New York University Press.

New York Times Editorial. 2018. "Opinion: The New Radicalization of the Internet." Accessed July 17, 2020. https://www.nytimes.com/2018/11/24/opinion/sunday/facebook-twitter-terrorism-extremism.html.

OECD. 2019. "OECD Principles on AI." Organisation for Economic Co-operation and Development. Accessed January 13, 2021, https://www.oecd.org/going-digital/ai/principles/.

O'Grady, Nathaniel. 2015. "Data, Interface, Security: Assembling Technologies that Govern the Future." *Geoforum* 64: 130–37.

Olwig, Karen Fog, Kristina Grünenberg, Perle Møhl, and Anja Simonsen. 2019. *The Biometric Border World*. London: Routledge.

Pantenburg, Volker. 2015. *Farocki/Godard Film as Theory*. Amsterdam: Amsterdam University Press.

Parker, Ben. 2019. "Betting on Biometrics to Boost Child Vaccination Rates." *The New Humanitarian*. Accessed July 20, 2020. https://www.thenewhumanitarian.org/news-feature/2019/07/18/betting-biometrics-boost-child-vaccination-rates.

Pasquale, Frank. 2015. *The Black Box Society. The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.

Ranjan, Rajeev, Swami Sankaranarayanan, Ankan Bansal, Navaneeth Bodla, Jun Cheng Chen, Vishal M. Patel, Carlos D. Castillo, and Rama Chellappa. 2018. "Deep Learning for Understanding Faces: Machines May Be Just as Good, or Better, than Humans." *IEEE Signal Processing Magazine* 35 (1): 66–83.

Reagan, Jason. 2020. "UK Trials Medical Delivery Drones for COVID-19 Supply Runs." Accessed July 22, 2020. https://dronelife.com/2020/04/30/medical-delivery-drones-uk/.

Rouvroy, Antoinette. 2013. "The End(s) of Critique." In *Privacy, Due Process and the Computational Turn*, edited by Mireille Hildebrandt and Katja de Vries, 143–67. Oxon: Routledge.

Sandvig, Christian, Kevin Hamilton, Karrie Karahalios, and Cedric Langbort. 2014. "An Algorithm Audit." In *Data and Discrimination: Collected Essay*, edited by Seeta Peña Gangadharan, Virginia Eubanks, and Solon Barocas, 6–10. Washington, DC: New America Foundation.

Saugmann, Rune Andersen. 2013. "Epistemic Authority, Lies, and Video: The Constitution of Knowledge and (in)Security in the Video/Security Nexus." *JOMEC Journal* 4: 1–19.

Saugmann, Rune A. 2017. "Video, Algorithms and Security: How Digital Video Platforms Produce Post-Sovereign Security Articulations." *Security Dialogue* 48 (4): 354–72.

Saugmann, Rune. 2019. "Military Techno-vision: Technologies between Visual Ambiguity and the Desire for Security Facts." *European Journal of International Security* 4 (3): 300–21.

———. 2020. "The Security Captor, Captured. Digital Cameras, Visual Politics and Material Semiotics." *Critical Studies on Security* 8 (2): 130–44.

Saugmann, Rune Andersen, and Frank Möller. 2013. "Engaging the Limits of Visibility: Photography, Security and Surveillance." *Security Dialogue* 44 (3): 203–21.

Scharre, Paul, Anthony Cho, Gregory C. Allen, and Eric Schmidt. 2017. "Eric Schmidt Keynote Address at the Center for a New American Security Artificial Intelligence and Global Security Summit." CNAS. Accessed January 13, 2021, https://www.cnas.org/publications/transcript/eric-schmidt-keynote-address-at-the-center-for-a-new-american-security-artificial-intelligence-and-global-security-summit.

Seppänen, Janne. 2017. "Unruly Representation: Materiality, Indexicality and Agency of the Photographic Trace." *photographies* 10 (1): 113–28.

Sharkey, Noel, and Lucy Suchman. 2013. "Wishful Mnemonics and Autonomous Killing Machines." *Proceedings of the AISB* 136: 14–22.

Stark, Luke. 2019. "Facial Recognition Is the Plutonium of AI." *XRDS* 25 (3): 50–55.

Stavrianakis, Anna, and Maria Stern. 2017. "Militarism and Security: Dialogue, Possibilities and Limits." *Security Dialogue* 49 (1–2): 3–18.

Suchman, Lucy. 2007. *Human–Machine Reconfigurations: Plans and Situated Actions*, revised ed. New York: Cambridge University Press.

———. 2015. "Situational Awareness: Deadly Bioconvergence at the Boundaries of Bodies and Machines." *Media Tropes* 5 (1): 1–24.

———. 2016. "Situational Awareness and Adherence to the Principle of Distinction as a Necessary Condition for Lawful Autonomy." In *Lethal Autonomous Weapon Systems: Technology, Definition, Ethics, Law & Security*, edited by Robin Geiss and Henning Lahmann, 273–83. Berlin: Federal Foreign Office, Division Conventional Arms Control.

———. 2020. "Algorithmic Warfare and the Reinvention of Accuracy." *Critical Studies on Security* 8 (2): 175–87.

Suchman, Lucy, Karolina Follis, and Jutta Weber. 2017. "Tracking and Targeting: Sociotechnologies of (In)Security." *Science, Technology, & Human Values* 42 (6): 983–1002.

Taylor, Lucien, ed. 1994. *Visualizing Theory: Selected Essays from V.A.R., 1990–1994.* London: Routledge.

Thatcher, Jim, David O'Sullivan, and Dillon Mahmoudi. 2016. "Data Colonialism through Accumulation by Dispossession: New Metaphors for Daily Data." *Environment and Planning D: Society and Space* 34 (6): 990–1006.

The Engine Room, and Oxfam. 2018. *Biometrics in the Humanitarian Sector.* Oxford: Oxfam.

Tian, Nan, Alexandra Kuimova, Diego Lopes Da Silva, Pieter D. Wezeman, and Siemon T. Wezeman. 2020. *Trends in World Military Expenditure, 2019.* Stockholm: SIPRI.

UN Human Rights Council. 2016. *The Promotion, Protection and Enjoyment of Human Rights on the Internet, Resolution A/HRC/RES/32/13.* Geneva: United Nations.

———. 2018. *The Promotion, Protection and Enjoyment of Human Rights on the Internet, Resolution A/HRC/38/L.10/Rev.1.* Geneva: United Nations.

UN Secretary-General's High-Level Panel on Digital Cooperation. 2019. *The Age of Digital Interdependence.* New York: UN Secretary-General.

van der Ploeg, Irma, and Isolde Sprenkels. 2011. "Migration and the Machine-Readable Body: Identification and Biometrics." In *Migration and the New Technological Borders of Europe*, edited by Huub Dijstelbloem and Albert Meijer, 68–104. London: Palgrave Macmillan.

Vuori, Juha A., and Rune Saugmann Andersen, eds. 2018. *Visual Security Studies: Sights and Spectacles of Insecurity and War.* London: Routledge.

Wang, Mei, and Weihong Deng. 2018. "Deep Face Recognition: A Survey." arXiv:1804.06655.

Weber, Cynthia. 2017. "The Face of Sexuality: Why Do AI-Generated Sexual Orientations Matter?" The Disorder of Things. Accessed June 20, 2020. https://thedisorderofthings.com/2017/09/25/the-face-of-sexuality-why-do-ai-generated-sexual-orientations-matter/.

Weitzel, Michelle D. 2018. "Audializing Migrant Bodies: Sound and Security at the Border." *Security Dialogue* 49 (6): 421–37.

WFP. 2019. "Palantir and WFP Partner to Help Transform Global Humanitarian Delivery." World Food Programme. Accessed July 20, 2020. https://www.wfp.org/news/palantir-and-wfp-partner-help-transform-global-humanitarian-delivery.

Wibben, Annick T.R., Catia Cecilia Confortini, Sanam Roohi, Sarai B. Aharoni, Leena Vastapuu, and Tiina Vaittinen. 2018. "Collective Discussion: Piecing-Up Feminist Peace Research." *International Political Sociology* 13 (1): 86–107.

Wilcox, Lauren. 2017. "Embodying Algorithmic War: Gender, Race, and the Posthuman in Drone Warfare." *Security Dialogue* 48 (1): 11–28.

Wu, Shaomei, Jeffrey Wieland, Omid Farivar, and Julie Schiller. 2017. "Automatic Alt-text: Computer-Generated Image Descriptions for Blind Users on a Social Network Service." In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, Portland, Oregon.

Yeung, Karen. 2018. "Algorithmic Regulation: A Critical Interrogation." *Regulation & Governance* 12 (4): 505–23.

Zarsky, Tal. 2016. "The Trouble with Algorithmic Decisions. An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making." *Science, Technology, & Human Values* 41 (1): 118–32.

Ziewitz, Malte. 2016. "Governing Algorithms. Myth, Mess, and Methods." *Science, Technology, & Human Values* 41 (1): 3–16.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power.* New York: Public Affairs.