Three Sides of the Same Coin

Datafied Transparency, Biometric Surveillance, and Algorithmic Governmentalities

Albu, Oana Brindusa; Krause Hansen, Hans

Three Sides of the Same Coin: Datafied Transparency, Biometric Surveillance, and Algorithmic Governmentalities

Oana B. Albu*
Hans Krause Hansen**

Abstract

This article explores how datafied transparency resulting from the use of facial recognition technologies creates different risks and dynamics of power and control. Theoretically, the article draws on Foucauldian studies and assemblage theory and analyzes how the power specific to facial recognition technologies rests on algorithmic governmentalities and interaction of humans and technologies in surveillant assemblages. Empirically, the article examines facial recognition legislation and its use in different corporate and institutional sectors around the world. The article concludes that datafied transparency is inseparable from the operation of surveillant assemblages and algorithmic governmentalities, and that algoactivism could be one form of resistance to counter such forms of power and control.

I. Introduction

Transparency powerfully communicates democratic values but also raises intricate questions about knowledge, power, and control in contemporary societies.[1] While transparency has a prominent place in both academic and public discourses as a marker of accountability and participation, fairness, and justice, it is also complicit with technological developments that easily challenge democratic values.[2] Digital environments provide ample illustrations of this ambiguity. The footprints left by people using smart phones make human conduct visible and thus honor values of accountability and justice, which are especially important in the judicial system but also in other domains such as health and education. At the same

[*] Associate Professor at the Department of Management, Society and Communication, Copenhagen Business School. We thank Ida Koivisto for her useful editorial help.

[**] Professor at the Department of Management, Society and Communication, Copenhagen Business School.

[1] Hans Krause Hansen & Richard Weiskopf, From Universalizing Transparency to the Interplay of Transparency Matrices: Critical Insights from the Emerging Social Credit System in China, 42 Org. Stud. 109 (2021).

[2] Mike Ananny & Kate Crawford, Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability, 20 New Media & Soc'y 973 (2018).

ISSN 2291-9732

time, such digital footprints are harvested and turned into the raw material of surveillance capitalism used by political elites to gain more control over individuals and populations.[3]

Scholarly and public debates on transparency and surveillance indicate the central role of observation in the exercise of power and control in any type of political regime. Indeed, it is difficult to distinguish between what Bernstein calls "control-focused, purposeful observation"[4] in his study of "transparency" in management and organizations, and Lyon's classical definition of "surveillance" as "systematic attention to personal details, with a view to managing or influencing the persons and groups concerned."[5] But in digital environments, the questions of who observes whom, why, and to what effect are of a somewhat different breed than in the traditional analog world. In digital contexts, the production of transparency and/or surveillance relies largely on what is termed datafication, i.e., the transformation of human experience into machine-readable "big data,"[6] which is driven by algorithms. Due to technological advancements, algorithms are not simply rule-based procedures for transforming input data into a desired output.[7] Algorithms can independently resolve specific tasks through the application of machine-learning systems. Like conventional rule-based algorithms designed by humans to follow particular steps, machine learning algorithms are fed with data—but in addition, they are trained to automatically define the rules and steps themselves, usually in ways that are opaque if not inaccessible even to highly specialized human programmers.[8]

Decision-makers in state institutions and corporations increasingly rely on datafication and algorithmic processing to transform previously invisible or unmarked human activities into "datafied subjects."[9] This article argues that datafication and the ensuing production of datafied subjects are both fueled by and standing in an ambiguous, if not uneasy, relationship with the classical transparency ideals shaping democratic societies and modern market economies.[10] Not only is it difficult to comprehend how algorithms are created and what they do, it is also unclear in what sense datafied subjects are actually made "transparent" and subject to control, even if this happens in the name of democracy and justice.

[3] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for Human Future at the New Frontier of Power (2019).

[4] Ethan S. Bernstein, Making Transparency Transparent: The Evolution of Observation in Management Theory, 11 Acad. Mgmt. Annals 217 (2017).

[5] David Lyon, Surveillance as Social Sorting: Computer Codes and Mobile Bodies, in Surveillance as Social Sorting 13 (David Lyon ed., 2003).

[6] Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think (2013).

[7] Tarleton Gillespie, The Relevance of Algorithms, in Media Technologies: Essays on Communication, Materiality, and Society 167 (Tarleton Gillespie et al. eds., 2014).

[8] Hannah Fry, Hello World: How to Be Human in the Age of the Machine (2018).

[9] David Lyon, The Culture of Surveillance: Watching as a Way of Life (2018).

[10] Marion Fourcade & Kieran Healy, Seeing Like a Market, 15 Socio-Econ. Rev. 9 (2017).

This article draws on insights from Foucauldian studies and assemblage theory[11] to scrutinize these ambiguities, and it takes the growing use of facial recognition technologies as a paradigmatic example of the fundamental dilemmas pertaining to the transparency ideal in contemporary societies.

Facial recognition is a biometric technology enabling measurements of bodily characteristics,[12] and thus it resembles iris recognition and fingerprinting. In contrast to the latter two, however, facial recognition can operate anonymously in the background and without the consent or participation of those targeted by it.[13] As such, the use of facial recognition technologies reflects an expansion of the repertoire of surveillance technologies developed throughout modernity. The next section develops a conceptual framework to help understand how and why this is the case, followed by an analysis of selected facial recognition examples and the regulatory interventions addressing them.

II. The Power of Biometrics: Surveillant Assemblages and Algorithmic Governmentalities

Surveillance has been famously theorized with reference to the Panopticon, an architectural idea developed by British philosopher Jeremy Bentham in the late eighteenth century. Foucault's influential *Discipline and Punish* focused on Bentham's design of the prison-Panopticon, which would ensure the self-discipline of the inmates through the illusion of continuous surveillance by the inspector located in the central tower.[14] For Foucault, the Panopticon was a diagram for the relationship between power, surveillance, and discipline in modern society, in which power is largely hidden and dispersed. Later scholarship has extended these insights and speaks of *post-panoptic* surveillance,[15] which also includes horizontal and synoptic bottom-up forms of surveillance. Neoliberal globalization, the proliferation of digital technologies, and the post-9/11 emphasis on "security" have come to embed surveillance into digital networks and infrastructures, which entangle state, private, and civil society actors in new ways and form wider so-called "surveillant assemblages."[16]

The idea of the "surveillant assemblage" seeks to address how people, discourses and material objects are brought together within and across contexts for purposes of control, and has its roots in assemblage theory. Assemblage theory[17] comes in a variety of

[11] Kevin Haggerty & Richard Ericson, The Surveillant Assemblage, 51 Brit. J. Soc. 605 (2000).

[12] Kelly A. Gates, Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance (2011).

[13] Lizzie Dearden, UK's largest police force spends over £200,000 on facial recognition trials that resulted in no arrests, The Independent, Jan. 19, 2019 (https://www.independent.co.uk/news/uk/home-news/facial-recognition-uk-police-met-arrests-london-cost-false-positives-accuracy-a8723756.html).

[14] Michel Foucault, Discipline and Punish: The Birth of the Prison (Alan Sheridan trans., 1977).

[15] Maša Galič et al., Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation, 30 Phil. & Tech. 9 (2017).

[16] Haggerty & Ericson, supra note 11.

[17] Manuel DeLanda, Assemblage Theory (2016).

forms[18] but generally questions the taken-for-granted nature of concepts such as state,[19] society,[20] and agency,[21] and suggests the usefulness of investigating the historically contingent relations and linkages between humans and their material surroundings, including technologies.[22] Assemblages can take on various expressions and shape people's behavior in different ways. Consider for example the contemporary proliferation of video cameras set up by police, security companies and citizens themselves. These technologies not only enable centralized forms of surveillance that (re)invoke Bentham's Panopticon and later social theorizing on the policing of society and its citizens, but also more decentralized forms of surveillance. Because post-panoptic surveillance is networked in character and comes to form assemblages, it also contains spaces that allow for "synoptic" forms of surveillance, including "sousveillance" (surveillance "from below") and "peer-"or "co-surveillance."[23] Panoptic and post-panoptic forms of surveillance rarely pertain to distinct political regimes in contemporary societies, but can overlap, support, or work against one another in specific contexts.[24]

The concept of surveillant assemblage allows us to understand how human bodies are abstracted from their territorial settings and turned into data flows. Such flows are then "reassembled into distinct 'data doubles' which can be scrutinized and targeted for intervention."[25] With the accelerating convergence of databases across governmental and commercial sectors, the accumulation and analysis of personal biometric data, ranging from fingerprints, health records and blood samples, to flying habits and shopping patterns, have become easier.[26] These data-gathering processes are infused with "pre-emptive mentalities that drive organizational orientations towards the goal of scanning and imagining the future."[27] The future-orientation and significance of these pre-emptive mentalities can be further understood by drawing on insights from studies of governmentality. Here,

[18] Aihwa Ong & Stephen Collier, Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems (2008).

[19] Claudia Aradau & Tobias Blanke, The (Big) Data-Security Assemblage: Knowledge and Critique, 2 Big Data & Soc'y 1 (2015).

[20] David Murakami Wood, What is global surveillance? Towards a relational political economy of the global surveillant assemblage, 49 Geoforum 317 (2013).

[21] Rita Abrahamsen & Michael C. Williams, Security Beyond the State: Global Security Assemblages in International Politics, 3 Int'l Pol. Soc. 1 (2009).

[22] Bruno Latour, Reassembling the Social: An Introduction to Actor-Network-Theory (2007).

[23] Aaron Doyle, Revisiting the Synopticon: Reconsidering Mathiesen's "The Viewer Society" in the Age of Web 2.0, 15 Theoretical Crim. 283 (2011).

[24] Krause Hansen & Weiskopf, supra note 1.

[25] Lyon, supra note 9.

[26] Laura Sydell, Storing Health Records on Your Phone: Can Apple Live Up to Its Privacy Values?, NPR, Feb. 27, 2019 (https://www.npr.org/2019/02/27/697026827/storing-health-records-on-your-phone-can-apple-live-up-to-its-privacy-values).

[27] Jude McCulloch & Dean Wilson, Pre-crime: Pre-emption, Precaution and the Future 78 (2016).

government is a form of power that refers to the "conduct of conduct," which structures "the possible field of action of others."[28] Government relies on representing the world in terms of "problems" to be identified and in need of amelioration through the mobilization and intervention of technologies of various sorts. Governmental "rationalities" inform the diagnosis of "problems" and the exercise of government, which also includes the governing practices of actors and authorities beyond the state. "Technologies of government" are the actual mechanisms through which authorities, be they public, private, or in-betweens, seek to "shape, normalize and instrumentalize the conduct, thought, decisions and aspirations of others in order to achieve the objectives they consider desirable."[29] Importantly, authorities exercise government "at a distance," and technologies such as facial recognition can be used to align economic, social and personal conduct with authorities' socio-political and economic objectives.

Taken together, then, the concepts of *algorithmic governmentalities* and *surveillant assemblages* enable us to understand how power operates in a world where attempts to create transparency are shaped by datafication. Before the advent of the Internet, the focus was on the governing practices of and by the offline individual. Algorithmic governmentalities expand the focus to the surveilling operations of multiple assemblages comprised of biometric technologies, algorithms and machines, and supervisory bodies. Biometric surveillance involves automated monitoring methods to recognize people based on their behavioral and physiological characteristics,[30] and it aggregates and analyzes fragmented online data footprints left by individuals for purposes of evaluation and profiling (potential criminal, customer, voter, etc.).

The surveillance processes inherent to governmentality in the pre-Internet age have traditionally been understood as dyadic processes between a discrete human observer and the human being observed. Under algorithmic governmentalities, surveillance becomes a computational process in which the human is largely absent. An "algorithmic gaze" largely replaces human observation and decision making, giving way to an illusion of objectivity as human judgment is largely bypassed.[31] Being a kind of machine rationality based on the automated harvesting, aggregation, and analysis of massive quantities of data, algorithmic governmentality thus promises to anticipate and affect possible future behaviors.[32]

The deployment of facial recognition embodies insidious algorithmic governmentalities that affect how people live, both in the present and in the future. While algorithms

[28] Michel Foucault, Afterword by Michel Foucault: The Subject and Power, in Michel Foucault, Beyond Structuralism and Hermeneutics 208 (Hubert Dreyfus & Paul Rabinow eds., 2d ed. 1983).

[29] Peter Miller & Nikolas Rose, Governing Economic Life, 19 Econ. & Soc'y 1 (1990).

[30] Mark G. Milone, Biometric Surveillance: Searching for Identity, 57 Bus. Law. 497 (2001).

[31] Gemma Newlands, Algorithmic Surveillance in the Gig Economy: The Organization of Work Through Lefebvrian Conceived Space, Org. Stud., Feb. 20, 2020 (https://journals.sagepub.com/doi/full/10.1177/0170840620937900).

[32] Antoinette Rouvroy & Thomas Berns, Gouvernementalité algorithmique et perspectives d'émancipation, 177 Réseaux 163 (2013).

work in simple rule-based programs, they can also be set to work on big data sets with the help of machine learning systems. In contrast to conventional statistical practices, which contain hypotheses about the world anchored on quantification and classifications, algorithms powered by machine learning generate hypotheses and classification criteria from big data harvested and potentially acted upon in real time. These algorithms can both operate instantaneously and create a predictable computational sequence of that which is to come. These operations help reduce the sense of uncertainty. Algorithmic governmentalities are, in other words, informed by constantly generated expectations to the future that become cause and justification for action in the present, including pre-emptive interventions[33] based on the automatic evaluation of what bodies potentially could do rather than what people are actually doing.[34]

What biometric surveillance, surveillant assemblages and algorithmic governmentalities ultimately show us is that the current use of digital technologies supplements if not changes traditional "fixed" forms of surveillance. Contemporary forms of surveillance are more "liquid"[35] than their predecessors because they mix soft- and hardware, such as novel apps run on "smart" mobile devices. For example, the watching of physical spaces through traditional technologies like video cameras is combined with the algorithmic monitoring of digital spaces. Institutional actors, public and private, capture massive data from a growing number of data points, including smart phones, biometric scanners, sensors and facial recognition technologies. The data are stored, aggregated, and analyzed by machine learning algorithms for political, commercial and entertainment purposes. These data travel between domains and can be repurposed as databases become increasingly integrated. The machine-generated mathematical correlations revealed through the analysis of data cannot offer any proof of causality or conclusive reasoning about future behaviors. But policy- and decision-makers often take such correlations as indicative of expected behaviors. The forecasts that emerge from the analysis of data come with an aura of objectivity and are based on honorable transparency ideals, as we next discuss, while nurturing anticipatory and preemptive aspirations.[36]

[33] Ben Anderson, Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies, 34 Progress Hum. Geo. 777 (2010).

[34] Antoinette Rouvroy, The End(s) of Critique: Data-Behaviourism vs. Due-Process, in Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology 143 (Mireille Hildebrandt & Katja de Vries eds., 2013).

[35] David Lyon, Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies, 4 Int'l Pol. Soc. 325 (2010).

[36] Louise Amoore, The Politics of Possibility: Risk and Security Beyond Probability (2013).

III. Face as an Assemblage: Towards Datafied Transparency

In both critical legal[37] and social studies[38] it has been widely shown that efforts to create transparency involve much more than the provision of information,[39] and are rather a matter of managing information and associated visibilities[40] than providing insight and clarity. We add to these conversations by showing how biometric surveillance is inseparable from the pursuit of transparency in the current digitalized environment. As we show in the following sections, corporations and governments attempt to reach transparency ideals by gathering and processing data, and these practices have boosted the variety and the depth of biometric surveillance.[41] Transparency is often characterized by different logics (e.g., market, fame or civic), objectives (to generate evidence, collaboration, popularity or positive reputation), and practices (consultations, information dissemination campaigns or surveillance tactics).[42] In the case of facial recognition, institutions and organizations that use biometric technologies are driven by civic and market logics of transparency with the objective of making citizen behavior visible. As such, the use of biometric technologies is saturated with politics. They frame what is to be governed and they rest on the programmed set of rules and codes that assign a particular "identity." For instance, an algorithm "might disadvantage some data while privileging others, through either technological failure and/or an innate bias of the algorithm's authors. What can be seen is what can be made intelligible, and what can be intelligible determines who we can be."[43] The identification of skin color and gender by HP's facial recognition software is a case in point, as this algorithm was unable to identify Black faces because whiteness was reified as "normal" and Blackness as "abnormal."[44]

The quality of cameras in laptops and smartphones has improved, and access to relatively cheap software and apps offering device-based facial recognition has expanded. In turn, individuals and organizations increasingly use facial recognition technologies. As we discuss at length in section V, such examples are of a great variety. Facial recognition is

[37] Mark Fenster, The Opacity of Transparency, 91 Iowa L. Rev. 885 (2006).

[38] Oana B. Albu & Mikkel Flyverbom, Organizational Transparency: Conceptualizations, Conditions, and Consequences, 58 Bus. & Soc'y 268 (2019).

[39] Andrea Bianchi, On Power and Illusion: The Concept of Transparency in International Law, in Transparency in International Law 1 (Andrea Bianchi & Anne Peters eds., 2013).

[40] Hans Krause Hansen, Policing Corruption Post- and Pre-Crime: Collective Action and Private Authority in the Maritime Industry, 25 Ind. J. Global Leg. Stud. 131 (2018); Krause Hansen & Weiskopf, supra note 1; Mikkel Flyverbom, The Digital Prism: Transparency and Managed Visibilities in a Datafied World (2019).

[41] Lucas Introna & David Wood, Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems, 2 Surveillance & Soc'y 177 (2004).

[42] Lee Edwards, Transparency, Publicity, Democracy, and Markets: Inhabiting Tensions Through Hybridity, Am. Behav. Sci. (2020).

[43] John Cheney-Lippold, We Are Data: Algorithms and the Making of Our Digital Selves 15 (2017).

[44] Brian X. Chen, HP Investigates Claims of "Racist" Computers, Wired, Dec. 22, 2009 (https://www.wired.com/2009/12/hp-notebooks-racist/).

often heralded in many countries around the world as a beacon of hope because of the "transparency" it creates and the overly optimistic promises of efficiency and effectiveness. However, this type of *datafied transparency* is always shaped by facial recognition technologies themselves and the normative arrangements surrounding their deployment. When these technologies and arrangements are linked, and operate together, they result in facial assemblages, a subtype of the surveillant assemblages we discussed above. Understanding the face as an assemblage is important because it allows us to relativize and historicize the face.[45] In other words, the importance of the face does not arise from some necessary or innate condition, but from a certain assemblage of power, a certain politics.[46]

The forms of power and control specific to datafied transparency are therefore based on the ability to aggregate and associate data about the individual and the population. While these abilities of biometric data collection and processing are given by machine learning algorithms,[47] it is important to understand facial recognition not solely from a technical point of view. We need to also consider the broader social and political-economic contexts in which the use of facial recognition is undertaken.[48] Especially relevant are the more recent developments of deep neural networks, big data, and machine learning technologies where the capabilities of algorithms to recognize visual patterns and perform complex large-scale operations of observation, recording and profiling have developed significantly.

In most cases, facial recognition is based on two processes happening in real time:[49] facial identification (i.e., linking the image of a face to a concrete individual) and facial analysis (i.e., extracting facial information from an image). These processes are algorithmically computed by machine learning algorithms that are trained to set their own rules to identify from a facial image information such as race, gender, age, emotion, sexual orientation or the predisposition to commit a crime.[50] This happens as, in the first step, the algorithm is fed a labelled data set which contains the information that the algorithm needs to learn to identify (e.g., gender of a subject in an image). In the second step, the algorithm eventually learns incrementally to adjust its values and increase accuracy by performing statistical calculations of optimization and a process of trial and error. It has been asserted, for instance, that the accuracy of an algorithm used to detect sexual orientation from facial images reached 91 percent for men and 83 percent for women when given five facial images of a person, in comparison to human judges that achieved much lower accuracy

[45] Gilles Deleuze & Felix Guattari, A Thousand Plateaus: Capitalism and Schizophrenia (Brian Massumi trans., 1987).

[46] Jenny Edkins, Face Politics (2015).

[47] Cheney-Lippold, supra note 43.

[48] Gates, supra note 12.

[49] Claudio Celis Bueno, The Face Revisited: Using Deleuze and Guattari to Explore the Politics of Algorithmic Face Recognition, 37 Theory, Culture & Soc'y 73 (2020).

[50] Jacob Hood, Making the Body Electric: The Politics of Body-Worn Cameras and Facial Recognition in the United States, 18 Surveillance & Soc'y 157 (2020).

(respectively, 61 percent for men and 54 percent for women).[51] Due to such popularity of machine learning and biometrics applications in different areas such as law enforcement, medicine, and engineering, many countries have developed regulatory measures favorable for facial recognition use. A brief analysis is provided in the next section.

IV. Analysis of Legal Measures Targeting Facial Recognition

Given that facial recognition technologies are technologies of government, there is widespread agreement around the world that regulatory measures are needed, even though lawmakers, advocates, law enforcement, and other stakeholders often disagree on exactly what that looks like. Yet many countries have legislative measures favorable to the use of facial recognition technologies. For example, in China, facial recognition is part of the social credit system, which authorities use to monitor residents in public places, incentivize "good" behavior and verify their identities for many services including traveling or new mobile phone subscriptions.[52] In Russia, the deployment of facial recognition systems during public assemblies is a common practice by law enforcement to identify participants to public protests that are considered unlawful.[53] In Israel, border authorities use a deep neural network software (i.e., Better Tomorrow by Any Vision) that allows them to perform facial recognition, gait recognition and object identification at checkpoints.[54] In the UK, law enforcement can use facial recognition in public places through a procedure referred to as "sensitive processing," which involves the processing of biometric data for the purpose of uniquely identifying an individual.[55] These examples show that legislative measures favorable to facial recognition technologies enable "hegemonic" actors to exercise government at a distance by making it possible for different bodies to identify individuals and objects in any live camera feed, such as a security camera or a smartphone, and then track these targets as they move between different feeds. Such biometric surveillance that takes the human body and its movements as the focal points is therefore a technique of population management in complex and uncertain times in which security has become a high priority.

[51] Yilun Wang & Michal Kosinski, Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation from Facial Images, 114 J. Person. & Soc. Psych. 246 (2018); cf. Andrew Gelman et al., Gaydar and the Fallacy of Decontextualized Measurement, 4 Soc. Sci. 10 (2018).

[52] Krause Hansen & Weiskopf, supra note 1; Catherine Stupp, EU Plans Rules for Facial-Recognition Technology, Wall St. J., Feb. 20, 2020 (https://www.wsj.com/articles/eu-plans-rules-for-facial-recognition-technology-11582219726).

[53] Amnesty International, Russia: Intrusive facial recognition technology must not be used to crackdown on protests, Jan. 31, 2020 (https://www.amnesty.org/en/latest/news/2020/01/russia-intrusive-facial-recognition-technology-must-not-be-used-to-crackdown-on-protests/).

[54] Daniel Estrin, Face Recognition Lets Palestinians Cross Israeli Checkposts Fast, But Raises Concerns, NPR, Aug. 22, 2019 (https://www.npr.org/2019/08/22/752765606/face-recognition-lets-palestinians-cross-israeli-checkposts-fast-but-raises-conc?t=1598980306343).

[55] Information Commissioner Office, Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places, Oct. 31, 2019 (https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf).

The European Union (EU) has more nuanced legislative measures for facial recognition. The EU General Data Protection Regulation (GDPR) highlights the importance of the precautionary principle, which may even justify a ban or temporary freeze on some uses of these technologies where its impact on society and the rights and freedoms of individuals is uncertain. The GDPR specifically covers the processing of biometric data, which includes facial images: "elements relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person."[56] However, while the GDPR generally forbids the processing of biometric data for uniquely identifying purposes, legislation permits facial recognition if one can rely on one of the ten exemptions.[57] As a result, different corporate actors can regulate life and exercise power. For instance, companies in the EU use advanced facial image processing technologies to run deep learning models in real-time directly on smartphones and track movement patterns and queues in buildings without falling under the camera monitoring law or GDPR (modcam.com, aimmatter.com).

Similarly, in the United States, the lack of consistent regulatory guidelines (e.g., about footage storage time, public access to footage, and guidelines for camera usage) has led to a situation where different facial recognition technologies are simultaneously used by a wide variety of actors to create datafied transparency for purposes of surveillance and pre-emptive policing.[58] Since these technologies can modify and complement each other, they become tools to steer both individual and collective behavior. Resistance to these techniques of power is scarce and encountered only at a state or city level. For example, legislators in San Francisco have voted to ban the use of facial recognition across local agencies, including transport authority and law enforcement.[59] Following this direction, in California, a moratorium on law enforcement's use of face recognition was passed for a period of three years under the Body Camera Accountability Act.[60] As a result, police departments and law enforcement agencies across the state of California ended any existing use of facial recognition on body-worn cameras (BWC) by January 1, 2020. Echoing the dystopian repercussions of mass surveillance, the moratorium indicates how datafied transparency, algorithmic governmentalities and biometric surveillance are all sides of the same coin: "Facial and other biometric surveillance would corrupt the core purpose of officer-worn body-worn cameras by transforming those devices from transparency and accountability tools into roving surveillance systems."[61] Similarly, the city of Somerville and Oakland

[56] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Art. 2(14).

[57] Id.

[58] Hood, supra note 50.

[59] Dave Lee, San Francisco is first US city to ban facial recognition, BBC News, May 15, 2019 (https://www.bbc.com/news/technology-48276660).

[60] H.R. 3364, 116th Congress: Federal Police Camera and Accountability Act of 2019.

[61] Id.

also passed their own ban on city use of facial recognition.[62] While several bills are proposed to regulate corporations engaged in population management through collecting and re-sharing facial data for the purpose of identifying individuals without their consent,[63] passing such initiatives through the U.S. Congress might take several years.

The problems that happen when regulation takes place only after facial recognition systems have become technologies of government are illustrated by the case of India's controversial Aadhaar biometric identity project.[64] Aadhaar works as "a centralized database that would store biometric information (fingerprints, iris scans, and photographs) for every individual resident in India, indexed alongside their demographic information and a unique 12-digit 'Aadhaar' number." The program ran for years without proper legal guardrails, generating marginalization and undermining privacy rights through its security vulnerabilities.[65] In the end, instead of using new regulations to roll back the system or address its data breaches, lawmakers adapted legislation to fit its current use, thereby preserving its current flaws.[66] As discussed in the following section, the lack of consistent regulatory measures of facial recognition coincides with the rapid expansion of biometrics and its applications in many institutional and corporate settings due to decreasing costs of hardware and software. Such a vicious circle between favorable or inconsistent regulation and a wide range of surveillant assemblages working in the name of transparency leads to the normalization of biometric surveillance and the biopolitical management of populations.

V. Institutional and Corporate Cases

Numerous institutions and law enforcement bodies build upon democratic ideals of transparency and technological betterment in their usage of remote biometric recognition. For instance, in the U.S. the criminal justice information services division of the Federal Bureau of Investigation (FBI) called Facial Analysis, Comparison and Evaluation routinely conducts facial recognition searches on a software called Next Generation Identification (NGI).[67] This technology allows the FBI and some state and local agencies to cross-reference surveillance camera footage and other photographs with its collection of candidate photos, and can access external partners' facial recognition systems to support FBI active

[62] Rachel Metz, Beyond San Francisco, more cities are saying no to facial recognition, CNN, July 17, 2019 (https://edition.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html).

[63] Pam Hrick & Farhang Heydari, The Growing World of Face Recognition Legislation: A Guide to Enacted and Proposed Legislation (https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5d9f7965391b2358bdccda63/1570732405589/The+Growing+World+of+Face+Recognition+Legislation.pdf).

[64] Unique Identification Authority of India, Aadhaar Authentication (https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf); Payal Arora, Benign Dataveillance? Examining Novel Data-Driven Governance Systems in India and China, 24 First Monday (2019).

[65] Human Rights Watch, India: Top Court OK's Biometric ID Program, Sept. 27, 2018 (https://www.hrw.org/news/2018/09/27/india-top-court-oks-biometric-id-program).

[66] Amba Kak, Regulating Biometrics: Global Approaches and Urgent Questions, AI Now Institute, Sept. 1, 2020 (https://ainowinstitute.org/regulatingbiometrics.html).

[67] Federal Bureau of Investigation (2020), Next Generation Identification (NGI) (https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi).

investigations.[68] Similarly, police departments in the U.S. rely on facial recognition technologies. For instance, the Washington county sheriff office and the Orlando Police Department tested Amazon's Rekognition system between 2016-2019.[69] BWC are still used by many large police departments in the U.S.[70] One notable exception is Baltimore, which is one of the only large departments to limit BWC data from being used to "create a database or pool of mug shots" in "photo arrays" or "be searched using facial recognition software"[71] for the systematic biometric surveillance of populations.

Echoing related transparency and preemptive policing rationalities, the U.S. Department of Homeland Security recently expedited the completion of another remote facial recognition system labelled the "Biometric Entry-Exit Tracking System." As a result, facial recognition systems are planned to be installed at the top 20 airports in the U.S. through a Presidential executive order that aims to protect the nation "from terrorist activities by foreign nationals admitted to the United States."[72] Similarly, live facial recognition is being trialed by police forces in many parts of the world, including the UK[73] and India.[74] Indian law enforcement relies, for instance, on Innefu Labs' facial recognition software, where AI Vision also includes gait and body analysis promising 98.3 percent accuracy by leveraging machine learning based on neural networks.[75]

The development of facial recognition solutions in the private sector is rising equally steeply and is driven by similar ideals of datafied transparency. For instance, supermarket chains such as Target and Walmart have already experimented with facial recognition in their stores to identify shoplifters.[76] Social media conglomerates often cite transparency ideals of openness and "free data sharing" but use facial recognition technologies to develop new products that rely entirely on biometric surveillance. For example, the algorithm behind Facebook's app Moments could identify someone even when they are not looking at the camera, through the creation of facial templates in combination with gait

[68] Sam Thielman, FBI using vast public photo data and iffy facial recognition tech to find criminals, The Guardian, June 15, 2016 (https://www.theguardian.com/us-news/2016/jun/15/fbi-facial-recognition-software-photo-database-privacy).

[69] American Civil Liberties Union Foundation, Public Records Request Related to Amazon Facial Recognition Service (https://www.aclunc.org/docs/20180522_ARD.pdf#page=1).

[70] Hood, supra note 50.

[71] Baltimore Police Department, Body Worn Camera, Jan. 1, 2018 (https://www.baltimorepolice.org/sites/default/files/Policies/824_Body_Worn_Cameras.pdf).

[72] Exec. Order No 13769, 82 Fed. Reg. 8977 (Jan. 27, 2017).

[73] Dearden, supra note 13.

[74] Abhinandan Mishra, India to have world's largest auto facial recognition system in 2021, Sunday Guardian Live, Mar. 7, 2020 (https://www.sundayguardianlive.com/news/india-worlds-largest-auto-facial-recognition-system-2021).

[75] Innefu, AI Vision (https://www.innefu.com/ai-vision/).

[76] BBC News, Walmart uses AI cameras to spot thieves, June 21, 2019 (https://www.bbc.com/news/technology-48718198).

recognition.[77] Such facial templates are created from photographs uploaded by users and grant unwarranted surveillance, as noted in one of the important privacy laws in the U.S., the Illinois Biometric Information Privacy Act (BIPA):

> [T]he facial-recognition technology at issue here can obtain information that is "detailed, encyclopedic, and effortlessly compiled," which would be almost impossible without such technology. . . . Once a face template of an individual is created, Facebook can use it to identify that individual in any of the other hundreds of millions of photos uploaded to Facebook each day, as well as determine when the individual was present at a specific location. Facebook can also identify the individual's Facebook friends or acquaintances who are present in the photo. . . . [It] seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building. Or a biometric face template could be used to unlock the face recognition lock on that individual's cell phone.[78]

Given the lack of consistent regulation, social media conglomerates often prepackage and sell facial data to companies that use them for commercial purposes. For example, a Filipino startup built a "smart advertising platform" for commercial vehicles, which employs facial recognition technologies to analyze client personas, based on age, gender, and other factors (e.g., admov.tech). Based on control techniques such as *geo-fencing*, individuals are targeted at a certain location and at a particular time and shown advertisements. Furthermore, facial recognition technologies are also used in the private education sector. Here biometric surveillance has become normalized for disciplinary purposes and data-driven simulations are increasingly mobilized to support transparency in education interventions.[79] For instance, in its aim to make attendance transparent, the Indian startup Clofus built a platform for schools that screens social media data from students' profiles and utilizes facial recognition to capture the emotions of students during classes. By analyzing the captured emotions, Clofus argues that educators gain "valuable insights" into any unusual behavior so that school counselors receive an early warning and can schedule a meeting with a student considered problematic (see clofus.com).

This chilling and dizzying array of biometrics applications shows that nation-states, institutions and corporations world-wide are elated by the potentiality of creating transparency and virtuous behavior. In order to counter these forms of power and transform existing algorithmic governmentalities, techniques of resistance are needed. Since a thorough treatment of resistance is impossible here, we only address one such potential technique in the next section.

[77] Aviva Rutkin, Facebook can recognise you in photos even if you're not looking, New Scientist, June 22, 2015 (https://www.newscientist.com/article/dn27761-facebook-can-recognise-you-in-photos-even-if-youre-not-looking/#ixzz6ZoLj0CLo).

[78] Patel v. Facebook, Inc., 932 F.3d 1264, 1273 (9th Cir. 2019) (citations omitted).

[79] Mark Andrejevic & Neil Selwyn, Facial Recognition Technology in Schools: Critical Questions and Concerns, 45 Learn., Media & Tech. 115 (2020).

VI. Towards Algoactivism

A central task in this article was to identify how datafied transparency pursued by regulators, institutional and corporate actors is based on different algorithmic governmentalities and surveillant assemblages. But techniques of resistance are emerging and help cultivate practices to counter surveillant assemblages, and they may, gradually, engender new designs of algorithmic "mentalities."[80]

Specifically, *algoactivism* is an individual and collective form of resisting algorithmic control, and it amounts to practical action (e.g., whistleblowing), employee empowerment, knowledge sharing and legal mobilization (Freedom of Information requests, etc.) in the corporate sector.[81] In the case of social movements and civil society groups, algoactivism is pursued through the use of lasers to interfere with facial recognition cameras. It also involves counter-algorithmic software which feeds "junk" data into systems to throw off their predictive calculations,[82] as well as cyber encryption technologies to avoid being indexed by classification systems.[83] Algoactivism is fueled by algorithmic anxiety which is the pervasive concern about the extent to which we live our lives as imagined, self-transparent subjects in relation to resisting the data collection performed by facial recognition technologies.[84] Algorithmic anxiety is, of course, not simply a sentimental subjectivity, or a personal pathology related to one's feelings regarding algorithms. Instead, it represents a technique of resistance that allows one to position herself or himself in today's algorithmic culture and continuously interrogate the normative effects of such culture on individuals immersed in a regime of transparency that itself remains largely opaque.

The oppressive nature of transparency regimes is often exposed by acts of algoactivism. For example, in China, a data leak from Shenzhen-based SenseNets, a Chinese company that carries out facial recognition surveillance, revealed the personal details of 2.5 million residents (GPS coordinates, ID numbers, home addresses, photos, and employers),[85] unveiling the mass biometric surveillance that takes place under the rationale of transparency. In the UK, citizen journalists and activists have shown that the Metropolitan Police's facial recognition technology had an error rate of 81 percent, and such deployment

[80] Nancy Ettlinger, A Relational Approach to an Analytics of Resistance: Towards a Humanity of Care for the Infirm Elderly, 23 Foucault Stud. 108 (2017).

[81] Katherine C. Kellogg et al., Algorithms at Work: The New Contested Terrain of Control, 14 Acad. Mgmt. Annals 366 (2020).

[82] Aaron K. Martin et al., Understanding Resistance to Digital Surveillance: Towards A Multi-Disciplinary, Multi-Actor Framework, 6 Surveillance & Soc'y 213 (2009).

[83] Oana Albu, Dis/Ordering: The Use of Information and Communication Technologies by Human Rights Civil Society Organizations, in Dis/organization As Communication: Exploring the Disordering, Disruptive and Chaotic Properties of Communication 151 (Consuelo Vasquez & Timothy Kuhn eds., 2019).

[84] Patricia de Vries & Willem Schinkel, Algorithmic Anxiety: Masks and Camouflage in Artistic Imaginaries of Facial Recognition Algorithms, 6 Big Data & Soc'y (2019).

[85] Yuan Yang & Madhumita Murgia, Data leak reveals China is tracking almost 2.6m people in Xinjiang, Financial Times, Feb. 16, 2019 (https://www.ft.com/content/9ed9362e-31f7-11e9-bb0c-42459962a812).

was likely to be found "unlawful" if challenged in court.[86] Similarly, in the U.S., the American Civil Liberties Union (ACLU), a civil society group, has shown based on a FOIA request that the FBI has done very minimal testing on the accuracy of their internal NGI system.[87] Similarly, a test was conducted by ACLU on Amazon's Rekognition and the system incorrectly matched twenty-eight members of Congress, identifying them as other people who had been arrested for a crime.[88] Although Amazon responded that the confidence threshold used in those tests should be set to higher values to match their recommendations for law enforcement scenarios,[89] it still raised concerns about possible harms from racial biases and whether such facial recognition tools are accurate and reliable enough for deployment. As a result of algoactivism and the pressure on investors and employees due to the "enabling [of] a surveillance system readily available to violate rights and target communities of color,"[90] Amazon announced a one-year break on selling the software to governmental agencies.

In short, there is a need for robust algoactivism because the use of facial recognition technologies to identify an individual among many individuals in a public place is far more intrusive than a local, one-to-one face authentication to unlock a smartphone. Once a digital infrastructure for biometric identification is in place, it can easily be used for other purposes ("function creep", i.e., the face will be treated not just as a form of biometric identification, but also as a new source of demographic and psychographic data).[91] These surveillant assemblages and algorithmic governmentalities are conducive of racial discrimination based on erroneous categorization and classification systems.[92] Such disproportionate misidentifications have already led to the over-policing of ethnic minorities on the premise of technological "objectivity"[93] and the undermining of privacy rights through biometric surveillance and control.

[86] Rachel England, UK police's facial recognition system has an 81 percent error rate, Engadget, July 4, 2019 (https://www.engadget.com/2019-07-04-uk-met-facial-recognition-failure-rate.html).

[87] Neema Singh Guliani, American Civil Liberties Union Foundation, The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database, June 7, 2019 (https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through).

[88] Jacob Snow, Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots, American Civil Liberties Union Foundation, July 26, 2018 (https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28).

[89] Matt Wood, Thoughts on Machine Learning Accuracy, AWS, Amazon, July 27, 2018 (https://aws.amazon.com/blogs/aws/thoughts-on-machine-learning-accuracy/).

[90] Amazon Prohibit Sales Resolution (2019) (https://static1.squarespace.com/static/57693891579fb3ab7149f04b/t/5c2cf4f86d2a73e6a9cfd391/1546450246520/Amazon+Prohibit+Sales+Resolution).

[91] Andrejevic & Selwyn, supra note 79.

[92] Fabio Bacchini & Ludovica Lorusso, Race, Again: How Face Recognition Technology Reinforces Racial Discrimination, 17 J. Info. Comm. & Ethics Soc'y 321 (2019).

[93] Big Brother Watch, Face Off: The lawless growth of facial recognition in UK policing, May 2018, (https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf).

VII. Conclusion

This article has built on Foucauldian studies and assemblage theory to highlight how the power specific to facial recognition technologies emerges from algorithmic governmentalities and surveillant assemblages in which automation and pre-emptive rationalities play a key role in the "conduct of conduct." The datafied transparency resulting from the deployment of facial recognition technologies comes with significant yet varying effects of power, control, and risks which are relative to the characteristics of the institutional and social contexts in which these technologies are used, including the legislation addressing facial recognition technologies in specific corporate and institutional settings. While datafied transparency is inseparable from the operation of surveillant assemblages and algorithmic governmentalities, algoactivism is appearing as an emerging form of contestation if not resistance to these forms of power and control. Such algoactivism reveals that facial recognition technologies are dangerous when they fail and can be harmful when they work, and, in a wider sense, that datafied transparency can be a highly treacherous pursuit.[94]

[94] Kate Crawford, Regulate Facial-Recognition Technology, 572 Nature 565 (2019).