Ethics and Information Technology (2019) 21:127–136
https://doi.org/10.1007/s10676-018-9493-1

ORIGINAL PAPER

Reframing biometric surveillance: from a means of inspection to a form of control

Avi Marciano[1,2]

Published online: 6 December 2018

Abstract
This paper reviews the social scientific literature on biometric surveillance, with particular attention to its potential harms. It maps the harms caused by biometric surveillance, traces their theoretical origins, and brings these harms together in one integrative framework to elucidate their cumulative power. Demonstrating these harms with examples from the United States, the European Union, and Israel, I propose that biometric surveillance be addressed, evaluated and reframed as a new form of control rather than simply another means of inspection. I conclude by delineating three features of biometric technologies—complexity, objectivity, and agency—that demonstrate their social power and draw attention to the importance of studying biometric surveillance.

Keywords Surveillance · Biometric technologies · Social sorting · Identity management · Privacy · Algorithms

Introduction

Surveillance practices and policies have undergone a dramatic increase in number and intensity over the past two decades, most notably in the post-9/11 Western world. Some scholars suggest that such growth constitutes one of the most far-reaching social changes of the past 50 years (Rule 2012), having become a key organizing principle of late modernity (Lyon et al. 2012). The academic community, particularly in English-speaking countries, has addressed these developments thoroughly by defining new fields (e.g., surveillance studies), establishing academic networks (e.g., SSN and SSC), and issuing new journals (e.g., *Surveillance & Society*). Within this broader context, biometric surveillance has emerged as a sub-field that attracts particular interest.

Biometric research—once the exclusive realm of computer scientists, mathematicians, and engineers—has become increasingly subject to critical research that poses political, cultural and ethical questions. This paper reviews the social scientific literature on biometric surveillance and reframes it around potential harms. Its primary aim consists of mapping the harms of biometric surveillance, tracing their theoretical origins, and identifying the disciplines and fields that explain them; second, it seeks to bring these harms together in one integrative framework. The importance of these efforts is twofold: First, biometric surveillance is becoming more and more prevalent in our everyday lives as the biometric industry keeps expanding. Its annual growth rate was estimated at 28% between 2005 and 2010 (Gelb and Clark 2013), while the biometrics system market is estimated to grow from $16.8 billion by 2018 to $41.80 billion by 2023 (Biometric System Market). Nevertheless, socio-critical inquiries concerning biometric surveillance rarely focus on the harms and when they do address the topic, they usually lack an overarching theoretical framework, thereby limiting discussion to specific aspects such as privacy. Second, including distinct biometric surveillance practices in one integrative framework elucidates their continuity and affinity, thus demonstrating their cumulative power.

In the first part of this paper, I elaborate briefly on what I call the *surveillance network* to contextualize the four suggested harms of biometric surveillance within a broad framework of surveillance. I then introduce these harms, trace their theoretical origins, and provide past and present examples from the United States, the European Union and Israel. In the succeeding two sections, I explain why biometric surveillance should be reframed and evaluated as a new

✉ Avi Marciano
avimarci@bgu.ac.il

[1] Department of Communication Studies, Ben-Gurion University of the Negev, Beer-Sheva, Israel

[2] Information Society Project, Yale Law School, New Heaven, CT, USA

Table 1 Central elements in the surveillance network

Level	1	2	3	4	5
Surveilling agent	States	Institutions	Employers	Corporations	Individuals
Surveilled subject	(Non)citizens	Wards	Employees	Consumers	Subordinate individuals
Surveillance context	National security, border control, public administration, welfare	Prisons, schools, hospitals	Workplaces	Consumerism, marketing	The home

form of control, and suggest three features of biometric technologies—complexity, objectivity and agency—to explain the social power of biometrics and to draw attention to the importance of studying biometric surveillance.

The surveillance network

Biometric surveillance refers to the use of automated systems that measure biological (e.g., fingerprint) or behavioral (e.g., gait) characteristics to identify, monitor, and control individuals and populations. Biometric surveillance is only one part of an extensive *surveillance network*, that I define as the overall social setting in which surveillance occurs. The surveillance network consists of three elements: A surveilling agent, a surveilled subject, and the surveillance context that defines the relationship between them.

Table 1 below lists the most common surveilling agents—states, institutions (e.g., prisons), employers, corporations, and individuals (e.g., parents)—and the respective objects of their surveillance: Citizens, wards (e.g., prisoners), employees, consumers, and individuals (e.g., offspring). The surveilling and the surveilled are connected by a particular surveillance context, such as an agenda (e.g., national security), practice (e.g., marketing), location (e.g., workplace), etc.[1]

Biometric surveillance corresponds with these levels in descending order, as it is widely performed by nation states, less by institutions and rarely by individuals. The harms discussed below are therefore evaluated vis-à-vis state surveillance within particular contexts, such as national security, border control, public administration and so forth.

Four harms of biometric surveillance

Unauthorized use of bodily information

Over the past two decades, scholars have propounded two theoretical concepts that together explain how biometric surveillance might facilitate unauthorized use of personal information. One such concept, *the body as password*, first appeared in Ann Davis' seminal article, in which she presciently observed that "we may be feeding pieces of ourselves into an ever-expanding array of computerized […] databanks" and asked readers if they were "ready for this form of being digital" (Davis 1997). Today, surveillance scholars use this concept to address a relatively new reality in which our bodies serve as gateways to physical and virtual spaces (Lyon 2008; Aas 2006). *The body as password* is a prominent manifestation of a broader idea—the *informatization of the body*. This idea suggests that in our hyper-digital environment, human bodies become substantial carriers of information, challenging the traditional dichotomy between the body and the information imprinted therein (van Der Ploeg 2005).

Corresponding with these two concepts, van Der Ploeg considers how the conversion of our physical existence into a digital code reformulates the ontology of the human body, concluding that biometric technologies redefine bodies as information (2003). This new ontology rationalizes the very workings of biometric technologies, that are designed to bypass the mind and communicate directly with the body as a reliable object providing "objective" information. From this perspective, biometric technologies clearly prioritize the physical body over the (increasingly undervalued?) mind, thus producing a new body-mind hierarchy. In Lianos' words, "what the subject thinks, does or believes […] is simply meaningless for the technological device" (2003). The direct communication between technologies and bodies, paired with the declining prominence of the mind, render human communication and negotiation superfluous. Employment of biometric technologies thus produces mute individuals whose bodies speak for them, and who are not obligated—and sometimes not allowed—to participate, consent, or even speak.

[1] Roger Clarke provides a detailed framework for surveillance analysis, consisting of six forms of surveillance (physical, communications, data, location, body, and omnipresent/omniscient), and seven dimensions of surveillance activity (of what, for whom, by whom, why, how, where, when). http://www.rogerclarke.com/DV/FSA.html#DSA.

These outcomes of the new ontology—prioritizing the body over the mind, obviating human communication, and producing mute individuals with speaking bodies—legitimize unauthorized use of personal bodily information. Within such a climate, we witness a shift from voluntary information disclosure and sharing to involuntary, automatic, and even remote information retrieval by powerful others, without our consent or even our knowledge. The power of biometric technologies, in this sense, lies in their capability to decode the encrypted body and expose data that we might prefer to keep private.

The possibility of unauthorized and unaware use of biometric information was a central argument put forth by Israeli social activists in their battle against the Israel Biometric Project approved by the Knesset (Israel's Parliament) in 2009. This project combines two distinct initiatives: The issuing of biometric ID cards and passports to all Israeli citizens, and the establishment of a mandatory biometric database for storing their bodily information (two index fingers and facial images). In 2013, Israel launched a two-year preliminary experiment to evaluate and assess the project's feasibility and necessity, during which participation had been voluntary. In March 2017, after two controversial extensions of the pilot, the Knesset approved the database and rendered it official (see Author removed 2016; Lebovic and Pinchuk 2010).

The project's opponents put much of their efforts into educating the public about the strategic and unnecessary coupling of the two initiatives. While supporting the issuing of biometric documents, they firmly opposed the establishment of a database, that enables unauthorized use of citizens' biometric information (as facial recognition cameras installed on streets can only identify passersby if an image bank has been compiled). For example, a comprehensive evaluation report published by the Israeli Digital Rights Movement regarding the pilot's performance refers to "one of the most significant dangers of the biometric database—the ability to identify passersby or protesters" (DRM 2017). The report questions the state's preference of fingerprints and facial images to other biometric features such as iris, "which is very difficult to collect without individuals' awareness because it requires […] their cooperation: screening passersby in the streets will not provide useful data about their irises, and therefore it cannot be used to identify or surveil them without their knowledge" (p. 47). The Israeli case—and this report in particular—demonstrate the potential ramifications of this harm, as well as its relevance to policy intervention.

The harm inherent in biometric surveillance is, of course, neither new nor unique to the Israeli project.[2] In fact, the fear of unauthorized use of biometric information underlies, explicitly or implicitly, critical discussions regarding urban surveillance and CCTV deployment (Norris 2012; Fussey and Coaffee 2012). However, based on the most common definition of privacy as the ability of individuals to control their own information (Westin 1967; Altman 1977; Rule 2012), scholars usually frame this harm as privacy violation. I suggest that such framing misses a unique capacity of biometric information. Photographing passersby without their knowledge and storing their face templates for future comparisons far exceed the realm of privacy. In no other context can forced use of the physical body escape the label of body desecration. Framing and discussing this harm in terms of information thus mask its adverse ramification—depriving people of the right to control their own bodies and make decisions accordingly.

So far, I have traced the theoretical origins of the first harm of biometric surveillance and linked them with the new ontology of the human body as information. This ontology facilitates a body-mind hierarchy that rationalizes the reduction of human communication and the production of mute individuals, that together manage to legitimize unauthorized use of bodily information.

Another significant ramification of the above rationale is the technocratization of citizenship. A mandatory biometric database of the kind that Israel is establishing will soon become a central administrative instrument in the work of the state's authorities. As such, the traditional encounter between functionaries and citizens might be replaced gradually by a mediated encounter between citizens and machines. Israel, like most other countries, already maintains a few voluntary and limited biometric databases. For example, unemployed citizens who enroll voluntarily in a biometric database maintained by the National Insurance Institute are required to undergo an automated biometric identification process weekly in order to receive unemployment compensation. In this case, citizen-machine communication replaces human communication. Citizens' personal stories that once might have influenced a given functionary's decisions become surplus information that is simply irrelevant to the new rationale of biometrics. This rationale is facilitated by—and itself facilitates—a technical, alienated, and utilitarian

[2] One well-known public manifestation of this harm occurred in January 2001, when 70,000 football fans gathered at Raymond James Stadium in Tampa, Florida to watch the 35th Super Bowl championship. These fans were unaware that while they were watching the game, they were also being watched. During the game, facial recognition cameras had scanned spectators' faces and produced templates that were immediately searched against a computerized database of criminals (McCullagh 2001).

relationship between the state and its citizens. A mandatory biometric database will render this rationale ubiquitous.

Denial or limitation of access

The primary function of biometrics as a means of sorting people out results in the denial or limitation of access to physical spaces, mostly in the context of border control. The theoretical explanation for this harm can be identified in the intersection of two fields—*citizenship studies* (Isin and Turner 2002) and *identity management* (van Zoonen 2013).

Scholars have long been interested in the relations between citizens and "cultural others". Carl Schmitt (1996) distinguished between friends and enemies, defining the latter as different, alien, or strangers with whom an intense conflict is possible. Bauman (1993) suggested a more nuanced distinction between enemies and strangers, claiming that the latter embody a greater threat than the former because they are neither friends nor enemies and may be both. While enemies are definable—they are usually associated with the outside, negativity and the wilderness—strangers are "the undecidable," those who are neither/nor. The distinction between citizens and "cultural others" is implied in the very concept of citizenship. Identifying citizens has always been a major concern of modern nation states (Torpey 2000) in their attempt to determine and control eligibility for citizenship (Lyon 2007). The modern form of citizenship, therefore, *assumes* identification and maintains the above distinction by excluding the ineligible.

The events of 9/11 are central to the rise of this biometric surveillance harm. While some scholars have suggested that the juxtaposing of citizens and non-citizens is no longer useful (see Ong 2005), the general climate in the post-9/11 Western world proves otherwise. Many studies have shown, for example, how media representations identify asylum seekers and refugees with migration, crime, and terrorism (Williams 2003; Salter 2004), evoking moral panic and fear (Erjavec 2003; Gale 2004). Moreover, the events of 9/11 clearly intensified practices of identification (Monahan 2012), while the heightened mobility that accompanies globalization posed new challenges and encouraged nation states to come up with sophisticated methods of identification and classification (Wilson 2006). Biometric technologies have emerged as the ideal solution in this respect.

Simply stated, as a central means of identification, biometric technologies play a crucial role in determining the boundaries of citizenship (see Ajana 2012), as they label and sort those who should be denied individual rights. On a deeper level, the role of biometric technologies in denying and limiting access has to do with the relatively new field of *identity management*, that addresses the constant efforts of states to authenticate individuals by fixing single and stable identities (van Zoonen 2013).

Biometric technologies play a significant role in practices of identity management (Muller 2004). As they are not programmed to deal with multiple identities, they inevitably reduce the individual to one stable self (see also Martin and Whitley 2013). According to van Zoonen (2013), identity management policies reflect a shift from discourse of multiplicity to discourse of duplicity, assuming that people maintain a fixed, stable and true identity that they *have* rather than *perform*. In this state of mind, the will of "cultural others" to celebrate and even maintain multiple identities arouses suspicion. The critical approach of identity management suggests that biometric identification or authentication should be perceived as an institutionalized means of establishing one's identity rather than as a scientific procedure aimed at revealing a preexisting identity. In other words, biometric technologies have the capacity to *produce* and *construct* particular identities to certain individuals that can be used to justify a denial of access. I demonstrate this point by describing two biometric megaprojects—one concerning US border control policies, and the other addressing major American and European biometric databases. I selected these projects because they represent the first level in the surveillance network (state surveillance) and because they target "cultural others".

Two US biometric projects—the *Immigration and Naturalization Service Passenger Accelerated Service System* (INSPASS, no longer exists) and the *Global Entry*—grant "low-risk travelers" enhanced mobility, fast access and expedited clearance, while detaining and excluding those categorized as "high-risk" (van Der Ploeg 2006; Wilson 2006). van Der Ploeg (2006) challenges the alleged objectivity of these categories, emphasizing the role that biometrics play in their maintenance. She argues that although geographical borders have always had different political significance for different individuals and groups, biometric technologies introduce us to a new level of discrimination. The *informatization of borders* through biometric technologies, she claims, constructs privileged, trusted identities by rendering the border less visible and more easily permeable for specific individuals, while increasing the border's "stopping power" for others. As such, biometric technologies enable "the extension of the function of the border as a selective and discriminating barrier". Bauman further emphasizes the biases underlying the above categories, claiming that biometric technologies enforce the discriminatory division between "the extraterritoriality of the new global elite and the forced territoriality of the rest" (2000).

In 2004, the United States Department of Homeland Security (DHS) established the *U.S. Visitor and Immigrant Status Indicator Technology* (US-VISIT) program to support immigration and border management. For this purpose, the DHS maintains the *Automated Biometric Identification System* (IDENT)—a central biometric database that stores and processes digital fingerprints, photographs, iris scans, and facial images, linking them with biographical information to establish and verify identities of "persons of interest"—primarily individuals who interact with the various agencies operating under the DHS. Large parts of this database consist of two major programs managed by the US Citizenship and Immigration Services (USCIS): The *Refugees, Asylum and Parole Services* (RAPS) and the *Asylum Pre-Screening System* (APSS). IDENT is the largest biometric database in the world, storing more than 130 million records (Lynch 2012; DHS 2012). The European parallel to the American RAPS and APSS is the EURODAC—a centralized fingerprint database of asylum seekers and "irregular migrants" over the age of 14. As of 2013, the database held more than 2.3 million entries, each stored for a period of ten years. The database aims to facilitate coordination among EU countries regarding applications for asylum, as well as achieving better control over illegal movement within the EU (van der Ploeg 1999; EUlisa 2013). Critical reports regarding both databases raise serious concerns, some of which are related to the transformation of these databases into policing tools, enhanced governmental surveillance, perpetuation of racially motivated targeting etc. (Jones 2014; EUlisa 2013).

Discriminating against "cultural others" by denying or limiting their access is not a new phenomenon, but biometric surveillance has made such discrimination explicit and blatant, as is evident in the contrasting categories of high/low-risk travelers. More importantly, biometric discrimination is algorithmic, ostensibly free of human judgment and "purged of the ugly politics of us and them, friends and enemies" (Muller 2004). Consequently, the denial and limitation of access through biometrics are allegedly more legitimate and therefore exempt from the rules of political correctness.

Bodily social sorting

The term *social sorting* describes the classification of individuals and populations according to various criteria, singling out certain groups for "special handling" (Lyon 2003). Social sorting practices are important because they influence people's life chances. In the digital age, these practices reach a new peak with the advent of *statistical surveillance*—data analyses that aim at simplifying our complex, changing environment and more importantly, at enabling stakeholders to make sound decisions that "maximize the benefits and minimize the risks that are associated with managing the behavior of […] individuals" (Gandy 2012).

While traditional surveillance focuses on capturing elusive information to produce an accurate representation of the present, statistical surveillance aims at creating a strategic representation of the future (Gandy 2012). To put it differently, in times of *anticipatory surveillance*, we no longer try to identify unruly subjects, ascribe guilt, and impose punishment, but use different surveillance techniques to sort groups by *a priori* levels of dangerousness (Feely & Simon, in Stalder and Lyon 2003). The use of predictive algorithms that label, sort and prioritize individuals and groups necessarily results in discrimination against unprivileged and socially marginalized individuals, who usually end up at the bottom of the hierarchy as risky citizens (see Gandy 2009) and unprofitable consumers (see Turow 2006). In this sense, statistical surveillance facilitates exclusionary rather than inclusionary goals (Norris et al. 1998), constituting a concrete technology of discrimination that large segments of society experience as *cumulative disadvantage* (Gandy 2012).

When statistical and anticipatory surveillance meet biometrics, the social sorting of people and groups takes a different form and makes its way into the physical realm. The primary purpose of biometric technologies is reading the body to identify people, but as the physical body correlates with other aspects of the self, biometric technologies have the capacity to expose hidden and sometimes sensitive information that can be exploited by different stakeholders.

Bodily features commonly used for biometric identification contain various kinds of information, such as genetic, medical, socioeconomic, and even personality traits. For example, lack of fingerprints might indicate genetic disorders such as Adermatoglyphia (ironically known as "immigration delay disease") (Nousbeck et al. 2011), or reveal that a person uses chemotherapy drugs to treat cancer (Chavarri-Guerra and Soto-Perez-de-Celis 2015).[3] Similarly, worn or distorted fingerprints might be associated with socioeconomic and occupational factors. Puri et al. compared the performance of fingerprint recognition technologies among urban and rural populations and found that the second challenges recognition algorithms because of worn and damaged fingerprint patterns (Puri et al. 2010). Other studies linked damaged patterns with practitioners of working-class occupations, such as plumbers, carpenters, and laborers, who wash their hands frequently (Woodward et al. 2001). Other bodily features, such as iris characteristics, have been found to be related to a variety of behavioral and personality traits (see Larsson et al. 2007).

These kinds of information are valuable for different stakeholders—from state authorities to insurance agencies—in their efforts to hierarchize citizens and potential customers, respectively, according to criteria of profitability. Unprivileged groups that usually end up at the bottom of the hierarchy will pay higher insurance premiums, for example.

[3] From time to time, scientists report on unpleasant encounters between cancer patients with deleted fingerprints and biometric technologies, such as a 62-year-old man who was detained by US customs (Wong et al. 2009) and a 65-year-old woman who was denied service at a bank (Chavarri-Guerra and Soto-Perez-de-Celis 2015).

While the first harm refers to unauthorized retrieval of bodily information, this one addresses a different case—individuals who share their bodily information voluntarily but are not aware of its hidden meanings, let alone the far-reaching implications thereof.

Symbolic ineligibility

As shown earlier, biometric technologies can be discriminatory in many different senses (see also Magnet 2011). The last harm of biometric surveillance goes beyond discrimination *per se*, focusing on its symbolism by addressing the role of biometrics in the construction of marginality and otherness.

Biometric technologies require individuals to enroll in the system and submit their bodily information to produce a biometric pattern. In every subsequent use, whenever identification or authentication is required, the individual once again submits his/her biometric data, which is then compared to the pattern produced earlier. However, certain groups experience a *failure-to-enroll* (FTE) situation, in which the biometric system fails to capture the user's body attributes (Wayman et al. 2005). This phenomenon is explained all too often in terms of technological limitation, yet is actually strongly rooted in social bias. The *illegible bodies*, as Murray (2007) suggests, are mostly colored populations such as African-Americans, Hispanics, and Asians. Indeed, Nanavati and his colleagues (2002) showed that facial-scan technologies fail to enroll dark-skinned persons simply because the cameras are optimized for lighter-skinned users (Introna and Wood 2004). While Nanavati and his colleagues discuss this phenomenon in technical terms, Pugliese attempts to "name the constitutive role of whiteness in setting the operating parameters of these image acquisition technologies" (Pugliese 2005, 2010; see also). Drawing on Richard Dyer, he brings the politics behind these technologies to the fore, claiming that particular biometric technologies are infrastructurally calibrated to whiteness as the normative standard. His description of the symbolism implied in FTE situations is even more telling: "Not to produce a template is equivalent to having no legal ontology, to being a non-being; you are equivalent to subjects who cannot be represented and whose presence can only be inferred by their very failure to be represented" (Pugliese 2005). In other words, in the age of ubiquitous biometrics, one has to be *biometrically recognizable* in order to exist.

Magnet and Rodgers (2011) showed how whole body imaging technologies placed in airports for security purposes perpetuate social inequalities by singling out particular communities for increased searches and harassment. They assess contemporary uses of these technologies as violent acts directed toward what they call *othered bodies*—transgender, disabled, racialized, and overweight people. Murray (2007) elaborates on the symbolic aspect of this procedure, suggesting that biometric technologies label such bodies as abnormal because they do not correspond to the idealized model, thus intensifying their otherness.

The Israel Biometric Project illustrates how biometric technologies are used to produce and intensify marginality and otherness. Many policy documents were published during the pilot period described earlier in order to guide implementation of the project, including detailed methods of addressing FTE situations. The Biometric System Experimentation Protocol stipulates the procedures to be performed during registration and determines that: "every biometric feature will be scanned up to six times […] to attain high quality data; should it fail, an **exceptions procedure** will be executed" (IBDMA 2013). Another document, the first of four semiannual reports published by the Israel Biometric Database Management Authority, lists the causes of failed fingerprint scans, thus revealing the identities of those defined as "exceptions":

> 8.3.3.1. Wounds, burns, and mutilations: Defects caused by wounds and burns, or a complete lack of fingerprint due to hand or finger mutilation; 8.3.3.2. Worn fingerprints, especially of elderly or diabetics who undergo regular pricking; 8.3.3.3. Dermatoses: Severe inflammatory skin diseases; 8.3.3.4. Disabilities: Physical handicap such as shaky hand or paralysis; 8.3.3.5. Oncological treatment: Certain chemotherapeutic medications might reduce fingerprint quality and rarely erase it temporarily; 8.3.3.6. Laborers: Some manual jobs might harm the skin and fingerprints (IBDMA 2014).

According to the report, these "exceptions"—mostly the elderly, the disabled, laborers, and people who suffer from illnesses such as cancer, diabetes and the like—are required to wait for a supervisor's confirmation to register. This results in a disturbing distinction between two groups: Those who have the privilege of registering quickly and efficiently in private cubicles, and the rest—ineligible bodies who literally stand in a separate line, waiting for special confirmation that represents marginality and otherness. Indeed, the privilege to be *biometrically recognizable* separates individuals who enter the national register smoothly and thus perform "successful citizenship" from ineligible citizens whose admission to this register is conditioned.

So far, I elaborated on four principal harms engendered by biometric surveillance. First, defining and using bodies as information facilitate reduction of human communication and the consequent production of mute individuals. Together, they legitimize unauthorized use of bodily information and technocratization of citizenship. Second, biometric technologies determine eligibility for citizenship, but more significantly, they construct and produce rather than simply read social identities that are then subjected to denial or limitation of access. Third, while decoding the physical body for administrative purposes, biometric technologies extract sensitive information that different stakeholders use to hierarchize individuals and populations for profit-making purposes. Finally, biometric technologies set a technical threshold for identification that some people—mostly minorities—cannot meet. This failure produces *ineligible bodies*, resulting in the construction of marginality and otherness.

Considering these harms, it is astounding to learn that less than two decades ago, scholars depicted automated surveillance technologies as a promise of equality and equity. Michaelis Lianos and Douglas (2000), for example, suggested that:

> "It is the first time in human history that we have the opportunity to experience forms of control that do not take into account any category of social division. Age, sex, race, beauty and attire are irrelevant […]. We stand in the middle of a massive development of egalitarian processes which cannot even be suspected to discriminate among their users" .

Including the four harms of biometric surveillance in one integrative framework elucidates their affinity and demonstrates their cumulative power: Although they vary in context, they point in the same direction and suggest that technologies previously perceived as a promise of equality now support and enhance rather than transcend traditional social categories. Consequently, in the remaining parts of the paper, I seek to reframe biometric surveillance as a new form of control and suggest three main features of biometrics to explain their social power.

Biometric surveillance: toward a new rationale

The immediate and visible impact of biometric technologies is mostly quantitative, as unprecedented amounts of data can now be collected, processed, and analyzed easily and rapidly. Nevertheless, the four harms discussed in this paper suggest that new surveillance techniques facilitate a *qualitative change*, as they alter dramatically what we can do with information (also see Graham and Wood 2003). In this respect, the impact of biometric surveillance cannot always be measured or quantified.

To better comprehend this qualitative change and the impact of biometric surveillance on our everyday lives, I reframe biometric surveillance and suggest that it be evaluated not as yet *another means* of inspection, but rather as a *new form* of control. While the first conceptualization perceives biometric surveillance as a technical means, the second offers a new rationale whereby human bodies are redefined as public objects on which state sovereignty can be enacted. Accordingly, bodies may be legitimately subjected to unauthorized use without the consent or knowledge of the individuals involved, read and decoded to expose hidden information and even translated into concrete ineligibility.

This does not imply that biometrics are inherently bad. In the first of his six laws of technology, Melvin Kranzberg wrote that "technology is neither good nor bad; nor is it neutral" (Kranzberg 1986). Winner's (1986) *theory of technological politics* also suggests that technologies are political (as opposed to neutral) in the sense that certain technologies are likely to have a specific impact when operating within certain political contexts. Following this line of reasoning, the adverse ramifications of biometrics appear to be rooted in the neo-liberal politics in which they are designed and employed, that legitimize categorization and hierarchization of individuals, as well as their subjugation to powerful forces.

The social power of biometrics: complexity, objectivity, and agency

The suggested conceptualization of biometric surveillance as a new form of control should be evaluated vis-à-vis three prominent features that they share with other algorithmic machines and that explain their social power: Complexity, objectivity, and agency. This argument does not imply that biometric technologies are deterministically powerful, but rather, that these features are exploited to allow certain uses of biometrics (see Winner 1986).

The combination of technical expertise and social theory is uncommon. Engineers and algorithm experts rarely take on critical social research; conversely, social scientists are not likely to delve into the technicalities that usually lie outside their proficiency. Consequently, not only laymen but even social scientists and surveillance scholars rarely understand how biometrics actually work. Their technological complexity, that remains a mystery in more ways than one, may well be among the most prominent characteristics of algorithmic technologies. Biometrics, in this context, are part of a growing array of *enigmatic technologies* that shape our black box society, according to Pasquale (2015). Technological complexity matters because it has the capacity to discourage examination, thus reinforcing the black box status of enigmatic technologies. It is thus hardly surprising that algorithms only became the focus of critical social scientific work in the last decade (Kitchin 2017).

Second, biometric technologies are strongly related to the contested concept of objectivity. In the most basic sense, they quantify selves and represent bodies numerically as a digital code. Human registrants stored in biometric systems are thus managed in terms of calculation, comparison, match, assessment, and similar conceptions. The combination of machines, numbers, and biology legitimizes a technical, scientific, and objective discourse around biometrics (Muller 2004), which is significant because it plays a crucial role in the production of 'truths' (Beer 2017). In this sense, biometric technologies are political, *inter alia*, because they are purported to represent 'only' what they actively produce (Murray 2007).

Third, biometric technologies are increasingly involved in automatic decision-making, with no or little human intervention. As biometrics often operate within particular contexts such as border control, law enforcement, and crime prevention, they are used to evaluate and judge people. Such *encoded extension of human agency* (Introna 2011), or the displacement of agency from humans to machines, raises ethical questions about mediated social sorting and discrimination. Technological agency is consequently of significance not only because it appropriates reasoning from human agents, but also because automated decision making, unlike the human variety, is said to be unbiased (and it is clearly not so).

The social power of biometrics resides in the interrelations among these three features. Briefly, technological agency, despite its questionable outcomes, if not adverse ramifications, is rarely challenged because of its perceived objectivity and complexity. When robots who judge a beauty contest prefer white contestants, it is hard to challenge their decision with convincing arguments—not only because it is based on "objective factors such as facial symmetry and wrinkles" (Levin 2016), but also because few experts can open and challenge this technical black box effectively. For the same reason, human agents have little chance of success if their narratives contradict the verdict of biometric machines, as "by definition, robust identification systems have the virtue of producing fewer errors," supporting the "presumption that the computer is right and the objecting individual is wrong" (Gelb and Clark 2013). Overall, the complexity-objectivity-agency triangle reinforces biometrics' status as uncontested and perhaps even impervious to challenge.

Policy solutions to balance harms and benefits of biometric surveillance are beyond the scope of this paper as they involve law, regulation and education. However, adopting a basic *approach of neutral politics*, both by policymakers and publics, is a first step toward educated use and implementation of algorithmic technologies. This approach suggests that while algorithmic technologies are political as socio-technical systems because they draw on, operate in, and potentially shape political contexts, they are nevertheless neutral because their functioning as socio-technical system is never pre-determined but should be constantly considered and negotiated. The juxtaposition of politics and neutrality points out the potential ramifications of biometrics but at the same time subjects these ramifications to informed societal decision.

Acknowledgements This article draws on my doctoral dissertation, which I wrote at the Department of Communication at the University of Haifa, under the supervision of Dr. Rivka Ribak. I want to thank her for the dedicated mentorship and guidance.

References

Aas, K. F. (2006). 'The body does not lie': Identity, risk and trust in technoculture. *Crime, Media, Culture, 2*(2), 143–158. https://doi.org/10.1177/1741659006065401.

Ajana, B. (2012). Biometric citizenship. *Citizenship Studies, 16*(7), 851–870. https://doi.org/10.1080/13621025.2012.669962.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues, 33*(3), 66–84. https://doi.org/10.1111/j.1540-4560.1977.tb01883.x.

Bauman, Z. (1993). *Modernity and ambivalence*. Cambridge: Polity.

Bauman, Z. (2000). Social issues of law and order. *British Journal of Criminology, 40*(2), 205–221. https://doi.org/10.1093/bjc/40.2.205.

Beer, D. (2017). The social power of algorithms. *Information, Communication & Society, 20*(1), 1–13. https://doi.org/10.1080/1369118X.2016.1216147.

Biometric System Market. Biometric System Market by Authentication Type (Single-Factor and Multifactor), Functionality Type (Contact, Non-Contact, and Combined), Component (Hardware and Software), Application, and Geography - Global Forecast to 2023. http://www.goo.gl/y2Q9K6.

Chavarri-Guerra, Y., & Soto-Perez-de-Celis, E. (2015). Loss of fingerprints. *New England Journal of Medicine*. https://doi.org/10.1056/NEJMicm1409635.

Davis, A. (1997). The body as password. *Wired*.

DHS (2012). *Privacy impact assessment for the Automated Biometric Identification System (IDENT)*. In U. S. D. O. H. Security (Ed.): San Francisco: The Electronic Frontier Foundation.

DRM (2017). *Analysis of the pilot's summarizing reports of the biometric database management authority* (4th edition).

Erjavec, K. (2003). Media construction of identity through moral panics: Discourses of immigration in Slovenia. *Journal of Ethnic and Migration Studies, 29*(1), 83–101. https://doi.org/10.1080/1369183032000076731.

EUlisa (2013). Annual report on the 2013 activities of the Central Unit of Eurodac pursuant to Article 24(1) of Regulation (EC) No 2725/2000. The European Commission.

Fussey, P., & Coaffee, J. (2012). Urban spaces of surveillance. In K. Ball, K. D. Haggerty & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 201–208). Abingdon: Routledge.

Gale, P. (2004). The refugee crisis and fear: Populist politics and media discourse. *Journal of Sociology, 40*(4), 321–340.

Gandy, O. H. (2009). *Coming to terms with chance: Engaging rational discrimination and cumulative disadvantage*. Farnham: Ashgate.

Gandy, O. H. (2012). Statistical surveillance: Remote sensing in the digital age. In K. Ball, K. D. Haggerty & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 125–132). Abingdon: Routledge.

Gelb, A., & Clark, J. (2013). *Identification for development: The biometrics revolution, Working paper 315*. Washington, DC: Centre for Global Development.

Graham, S., & Wood, D. (2003). Digitizing surveillance: Categorization, space, inequality. *Critical Social Policy, 23*(2), 227–248. https://doi.org/10.1177/0261018303023002006.

IBDMA (2013). The protocol for the experimentation of the biometric system.

IBDMA (2014). The first IBDMA's periodical report.

Introna, L. D. (2011). The enframing of code: Agency, originality and the plagiarist. *Theory, Culture & Society, 28*(6), 113–141. https://doi.org/10.1177/0263276411418131.

Introna, L. D., & Wood, D. (2004). Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance & Society, 2*(2/3), 177–198.

Isin, E. F., & Turner, B. S. (2002). Citizenship studies: An introduction. In E. F. Isin & B. S. Turner (Eds.), *Handbook of citizenship studies* (pp. 1–10). London: Sage.

Jones, C. (2014). Analysis: 11 years of Eurodac. (Vol. 16): Statewatch Analyses.

Kitchin, R. (2017). Thinking critically about and researching algorithms. *Information, Communication & Society, 20*(1), 14–29. https://doi.org/10.1080/1369118X.2016.1154087.

Kranzberg, M. (1986). Technology and history: "Kranzberg's laws". *Technology and Culture, 27*(3), 544–560.

Larsson, M., Pedersen, N. L., & Stattin, H. (2007). Associations between iris characteristics and personality in adulthood. *Biological Psychology, 75*(2), 165–175. https://doi.org/10.1016/j.biopsycho.2007.01.007.

Lebovic, N., & Pinchuk, A. (2010, The State of Israel and the biometric database law: Political centrism and the post-democratic state. *The Israel Democracy Institute*.

Levin, S. (2016). A beauty contest was judged by AI and the robots didn't like dark skin. *The Guardian*.

Lianos, M. (2003). Social control after Foucault. *Surveillance & Society, 1*(3), 412–430.

Lianos, M., & Douglas, M. (2000). Dangerization and the end of deviance: The institutional environment. *British Journal of Criminology, 40*(2), 261–278.

Lynch, J. (2012). *From fingerprints to DNA: Biometric data collection in US immigrant communities and beyond*. San Francisco: The Electronic Frontier Foundation

Lyon, D. (2003). Surveillance as social sorting: Computer codes and mobile bodies. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk, and digital discrimination* (pp. 13–30). London: Routledge.

Lyon, D. (2007). National ID cards: Crime-control, citizenship and social sorting. *Policing, 1*(1), 111–118. https://doi.org/10.1093/police/pam015.

Lyon, D. (2008). Biometrics, identification and surveillance. *Bioethics, 22*(9), 499–508. https://doi.org/10.1111/j.1467-8519.2008.00697.x.

Lyon, D., Haggerty, K. D., & Ball, K. (2012). Introducing surveillance studies. In K. Ball, K. D. Haggerty & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 1–11). Abingdon: Routledge.

Magnet, S., & Rodgers, T. (2011). Stripping for the state: Whole body imaging technologies and the surveillance of othered bodies. *Feminist Media Studies, 12*(1), 101–118. https://doi.org/10.1080/14680777.2011.558352.

Magnet, S. A. (2011). *When biometrics fail: Gender, race, and the technology of identity*. Durham: Duke University Press.

Martin, A. K., & Whitley, E. A. (2013). Fixing identity? Biometrics and the tensions of material practices. *Media, Culture & Society, 35*(1), 52–60. https://doi.org/10.1177/0163443712464558.

McCullagh, D. (2001). Call it Super Bowl face scan I. Wired.

Monahan, T. (2012). Surveillance and terrorism. In K. Ball, K. D. Haggerty & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 285–291). Abingdon: Routledge.

Muller, B. J. (2004). Dis)qualified bodies: Securitization, citizenship and 'identity management'. *Citizenship Studies, 8*(3), 279–294. https://doi.org/10.1080/1362102042000257005.

Murray, H. (2007). Monstrous play in negative spaces: Illegible bodies and the cultural construction of biometric technology. *The Communication Review, 10*(4), 347–365. https://doi.org/10.1080/10714420701715415.

Nanavati, S., Thieme, M., & Nanavati, R. (2002). *Biometrics: Identity verification in a networked world (Wiley tech brief series)*. New York: Wiley.

Norris, C. (2012). The success of failure: Accounting for the global growth of CCTV. In K. Ball, K. D. Haggerty & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 251–258). Abingdon: Routledge.

Norris, C., Moran, J., & Armstrong, G. (1998). Algorithmic surveillance: The future of automated visual surveillance. In C. Norris, J. Moran & G. Armstrong (Eds.), *Surveillance, closed circuit television, and social control* (pp. 255–275). Aldershot: Ashgate.

Nousbeck, J., Burger, B., Fuchs-Telem, D., Pavlovsky, M., Fenig, S., Sarig, O., et al. (2011). A mutation in a skin-specific isoform of SMARCAD1 causes autosomal-dominant adermatoglyphia. *The American Journal of Human Genetics, 89*(2), 302–307. https://doi.org/10.1016/j.ajhg.2011.07.004.

Ong, A. (2005). (Re)Articulations of Citizenship. *Political Science and Politics, 38*(4), 697–699. https://doi.org/10.1017/S1049096505050377.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge: Harvard University Press.

Pugliese, J. (2005). In silico race and the heteronomy of biometric proxies: Biometrics in the context of civilian life, border security and counter-terrorism laws. *The Australian Feminist Law Journal, 23*, 1–32.

Pugliese, J. (2010). *Biometrics: Bodies, technologies, biopolitics*. New York: Routledge).

Puri, C., Narang, K., Tiwari, A., Vatsa, M., & Singh, R. (2010). On analysis of rural and urban Indian fingerprint images. In A. Kumar, & D. Zhang (Eds.), *Ethics and policy of biometrics: Third international conference on ethics and policy of biometrics and international data sharing, ICEB 2010, Hong Kong, January 4–5, 2010: Revised selected papers* (pp. 55–61, Lecture notes in computer science, Vol. 6005). Berlin: Springer.

Rule, J. B. (2012). "Needs" for surveillance and the movement to protect privacy. In K. Ball, K. D. Haggerty & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 64–71). Abingdon: Routledge.

Salter, M. B. (2004). Passports, mobility, and security: How smart can the border be? *International Studies Perspectives, 5*(1), 71–91. https://doi.org/10.1111/j.1528-3577.2004.00158.x.

Schmitt, C. (1996). *The concept of the political*. Chicago: University of Chicago Press.

Stalder, F., & Lyon, D. (2003). Electronic identity cards and social classification. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk, and digital discrimination* (pp. 77–93). London: Routledge.

Torpey, J. (2000). *The invention of the passport: Surveillance, citizenship, and the state (Cambridge studies in law and society)*. Cambridge: Cambridge University Press.

Turow, J. (2006). *Niche envy: Marketing discrimination in the digital age*. Cambridge: The MIT Press.

van der Ploeg, I. (1999). The illegal body: `Eurodac' and the politics of biometric identification. *Ethics and Information Technology, 1*(4), 295–302. https://doi.org/10.1023/A:1010064613240.

van Der Ploeg, I. (2003). Biometrics and the body as information: Normative issues of the socio-technical coding of the body. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk, and digital discrimination* (pp. 57–73). London: Routledge.

van Der Ploeg, I. (2005). *The machine-readable body: Essays on biometrics and the informatization of the body*. Maastricht: Shaker Publishing.

van Der Ploeg, I. (2006). Borderline identities: The enrollment of bodies in the technological reconstruction of borders. In T. Monahan (Ed.), *Surveillance and security: Technological politics and power in everyday life* (pp. 177–193). New York: Routledge.

van Zoonen, L. (2013). From identity to identification: Fixating the fragmented self. *Media, Culture & Society, 35*(1), 44–51. https://doi.org/10.1177/0163443712464557.

Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). An introduction to biometric authentication systems. In J. Wayman, A. Jain, D. Maltoni & D. Maio (Eds.), *Biometric systems: Technology, design and performance evaluation* (pp. 1–20). London: Springer London.

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.

Williams, M. C. (2003). Words, images, enemies: Securitization and international politics. *International Studies Quarterly, 47*(4), 511–531. https://doi.org/10.1046/j.0020-8833.2003.00277.x.

Wilson, D. (2006). Biometrics, borders and the ideal suspect. In S. Pickering & L. Weber (Eds.), *Borders, mobility and technologies of control* (pp. 87–109). The Netherlands: Springer.

Winner, L. (1986). *The whale and the reactor: A search for limits in an age of high technology*. Chicago: University of Chicago Press.

Wong, M., Choo, S.-P., & Tan, E.-H. (2009). Travel warning with capecitabine. *Annals of Oncology*. https://doi.org/10.1093/annonc/mdp278.

Woodward, J. D., Webb, K., Newton, W., Bradley, E. M., M., & Rubenson, D. (2001). *Army biometric applications: Identifying and addressing sociocultural concerns*. Santa Monica: Rand.