ACME An International Journal for Critical Geographies

Second Generation Biometrics and the Future of Geosurveillance: A Minority Report on FAST

David Swanlund

PhD Student, Department of Geography
Simon Fraser University
dswanlun@sfu.ca

Nadine Schuurman

Professor, Department of Geography
Simon Fraser University
nadine@sfu.ca

Abstract

Biometrics are technologies that measure the body and are typically seen as existing for the purposes of identity verification. However, they are rapidly moving towards a new paradigm of behavioural analysis and prediction. The Department of Homeland Security's Future Attribute Screening Technology (FAST) is one example of this shift. In this article, we use FAST to explore the implications of new biometric technologies for geosurveillance. We argue that second generation biometrics mark a major shift in the application of geosurveillance due to their spatial and topological nature, and that they are motivated in part by a desire to make bodies more legible. More importantly, we argue that second generation biometrics both intensify and extend geosurveillance of already marginalized bodies. Finally, we call for more geographical research into biometrics given their rapid development and oncoming proliferation.

Keywords

Surveillance; privacy; future attribute screening technology; second generation biometrics; security

Introduction

> "Why Homeland Security's Pre-Crime Prevention Technology Is a Terrible Idea" (Bosch & Canfield, 2012)
>
> "Terrorist 'pre-crime' detector field tested in United States" (Weinberger, 2011)
>
> "Homeland Security's 'Pre-Crime' Screening Will Never Work" (Furnas, 2012)
>
> "DHS Begins Testing Controversial Pre-Crime FAST System (On the Willing)" (Loftus, 2011)

There is a striking resemblance between the Department of Homeland Security's (DHS) advanced biometric project and the film *Minority Report*. The film, which centers on the notion of stopping crime before it happens (so-called 'pre-crime'), is referred to with near ubiquity in media discussions of Future Attribute Screening Technology, or FAST, a DHS project that employs an array of biometric technologies in order to protect against terrorism. In fact, even the DHS recognizes the connection: when assessing the risks of FAST, the DHS wrote that "Risks are largely based on perception of 'Big Brother,' 'Minority Report,' or other nefarious technique [sic] being used to unnecessarily intrude upon the traveling public's privacy" (U.S. Department of Homeland Security, 2015, p. 47). The more one learns about FAST, the more accurate this comparison appears.

Indeed, FAST's goal is to flag individuals who may harbour 'malintent', which the DHS defines as "the mental state of an individual intending to cause harm to [American] citizens or infrastructure" (U.S. Department of Homeland Security, 2014). Flagged individuals may be taken aside for further screening and interrogation, despite having neither committed a crime nor having declared clear intent to commit a crime. This is not a case of an individual clearly being jittery as they pass through the security check at an airport being pulled aside for further questioning. This is a case wherein a machine wirelessly senses not only visible characteristics such as eye movement and facial twitches, but also hidden characteristics such as heart rate, respiration, and body temperature (pheromones have also been considered) to "identify deception and hostile intent in real time", presumably through mathematical calculation (Milgrom-Levin et al., 2008, p. 22; U.S. Department of Homeland Security, 2008). Amoore & Hall describe biometrics

as taking the body apart and visualizing them in a form of 'digitised dissection', a process that FAST only intensifies (Amoore & Hall, 2009).

This article interrogates FAST to provide insight into imminent technological changes to geosurveillance. While a similar article could most assuredly be written within the wider, aspatial context of surveillance, we direct our sights to the geographical aspects of FAST because, as we demonstrate, it is in part these geographical aspects that make projects like FAST so troubling. FAST is particularly interesting because it is emblematic of the modern security state insofar as it is built around the fear of the unknown. For instance, in a kind of bodily 'Total Information Awareness', FAST combines as many sensors as possible that may *potentially* predict malintent, fearing that any given factor will not sufficiently evaluate a given individual (Markoff, 2002). FAST is also interesting because it takes multiple independent surveillance projects, such as facial recognition and wireless heartbeat sensing (which can be used to infer mood), and draws them into a single project that could operate beyond the highly securitized spaces where we would expect to encounter them, such as airports (Milgrom-Levin et al., 2008).

Of course, we do not intend to claim that FAST in its current and literal form will face widespread deployment in the near future. Instead, we wish to evoke its chimeric technological form, its predictive purpose, and its spatial and topological characteristics to sketch a hologram of the impact that biometrics might have on geosurveillance – in the absence of technological restraint or opposition. Thus, this discussion serves as a case study into the potential future impacts of biometrics on geosurveillance.

Recent advances in biometrics constitute a particularly potent form of geosurveillance, due in part to how they operate spatially. Indeed, the deployment of biometrics in geosurveillance operations marks a significant, and in many ways unavoidable, intensification and extension of surveillance that challenges not only notions of privacy and consent, but of control over one's own body and mind. As we illustrate later in the article, these ramifications are also more likely to be felt by those that are already marginalized due to the methods that new biometrics use to assess risk. While biometrics' uneven effects on marginalized (particularly transgender) individuals have been the subject of several articles over the last decade, it nevertheless demands revisiting given recent advances and research directions in biometrics research and development (Currah & Mulqueen, 2011; Magnet, 2011; Magnet & Rodgers, 2012; Murray, 2007; Vélez, 2012).

This paper consists of four parts. First, we briefly review biometrics in the geographical literature and differentiate between first and second generation biometrics. The second section provides an overview of the FAST program. The third section situates FAST in a larger landscape of geosurveillance technologies to understand both its innovations and shortcomings. Finally, the last section of the article theorizes biometric projects like FAST in terms of legibility and argues that

they both intensify and extend geosurveillance to the detriment of their subjects, particularly those with already marginalized bodies.

It is worth noting that we treat the accuracy or calculability of these technologies as secondary within the scope of this article. While this issue is central to the algorithmic and biometric literatures, it remains secondary here for three reasons: *(1)* accuracy and calculability have been covered extensively, such as in Amoore (2014), Magnet (2011) and Pugliese (2012); *(2)* the inaccuracy of a given technology does not necessarily preclude authorities from using that technology; and *(3)* over the long term, critiques of accuracy can be responded to by an application of further engineering. Biometrics are a burgeoning industry, and there is no doubt that the capabilities of such technologies will continue to rapidly progress, perhaps far beyond our expectations; as this article will illustrate, we cannot afford to restrict our critiques to their current limitations.

Geography and Biometrics

Although the study of biometric technologies is not a major research area in geography, they have not gone unnoticed. Geographers have expressed significant concern about their use, and frequently contextualize their rising popularity within the security apparatus that emerged following the 9/11 terrorist attacks (Amoore, 2006, 2009; Häkli, 2007; Pero & Smith, 2014). Within this context, biometrics are largely viewed as biopolitical tools used to regulate human mobilities in the name of security (Amoore, 2006; Amoore & Hall, 2009; Häkli, 2007; Nguyen, 2015). While these types of tools and practices have been primarily examined along borders, it has also been acknowledged that their deployment has crept inwards to other 'spaces of enclosure', such as schools (Amoore, Marmura, & Salter, 2008; Nguyen, 2015), where they have been characterized in terms of both racism and violence (Amoore & Hall, 2009; Häkli, 2007; Nishiyama, 2015).

Geographers have primarily engaged with what are now being termed *first generation biometrics*. First generation biometrics are those that are built around identity verification, and that use "simple sensors, able to capture and store some physical features of the object to recognize", such as facial recognition (Ghilardi & Keller, 2012, p. 30). As geographical work on biometrics has tended to focus on the use of biometrics at the border, the technological emphasis has primarily been on fingerprint and retinal scanning (Amoore, 2006; Häkli, 2007; Pero & Smith, 2014), as well as on the use of full body scanners (Amoore & Hall, 2009). Additionally, analysis of how biometrics are implicated in judging or sorting individuals tends to primarily engage with how biometrics are used to identify individuals and link them to other information from which to sort them, rather than how biometric measurements themselves can be used for sorting (Amoore, 2006; Häkli, 2007; Nguyen, 2015; Pero & Smith, 2014).

However, as Sutrop & Las-Mikko rightly claim, "it has become abundantly clear that knowing a person's identity is not sufficient to prevent a threat" (Sutrop

& Laas-Mikko, 2012, p. 27). Therefore, second generation biometrics take measuring the body a step further:

> Second generation biometrics progress from asking who you are (the focus of first generation biometrics) to asking how you are; they are less interested in permanent data relating to a pure identity, and more propelled by an individuals' relationship with their environment. What are your intentions and how do you manifest these? (Mordini, Tzovaras, & Ashton, 2012, p. 11)

Examples of second generation biometrics can include "gait, face dynamics, signature dynamics, human computer interfacing, voice and even odour" (Mordini & Ashton, 2012, p. 262). Moreover, the results of second generation biometric scans can be analyzed to uniquely identify an individual, a practice often performed in gait analysis (analysis of how people walk). In fact, gait has been used by those in both industry and academia to uniquely identify individuals with 99 percent accuracy under favourable conditions (Castro, Marin-Jimenez, Guil, & de la Blanca, 2016; Horizon, 2016). When accuracy is lower, multiple second generation biometric readings can be combined to increase their reliability of unique identification. Alternatively, second generation biometrics, such as wireless heartbeat analysis (which can be used to infer mood) could be paired with first generation biometrics, such as facial recognition, to anchor intents into identities. Significantly, however, aside from facial recognition, many first generation biometrics require some form of active contact, such as placing a finger on a fingerprint scanner or looking into a retinal scanner, whereas second generation biometrics can largely operate passively from a distance without contact or user interaction (Sutrop & Laas-Mikko, 2012). These passive biometrics are "high on the [research and development] agenda today, enabling the design of systems that can be applied without people even being aware that they are being identified, registered, or assessed" (Van Der Ploeg, 2012, p. 294). Enter FAST.

Future Attribute Screening Technology

FAST's first notable mentions in the media were in September 2008 (ABC News, 2008; Angeles, 2008; Barrie, 2008). Since then, various details about the project have trickled out through sources including Freedom of Information Act requests, meeting transcripts, privacy impact assessments, and press releases. Much of the project, however, is still shrouded in secrecy, particularly with regard to its developments over the last few years.

A 2008 privacy impact assessment crafted by the DHS revealed some details about the project that raised a number of questions. According to the assessment, FAST featured at the time:

> (1) A remote cardiovascular and respiratory sensor to measure heart rate and respiration, which allows for the calculation of heart rate, heart rate variability, respiration rate, and respiratory sinus arrhythmia.

(2) A remote eye tracker, which is a device that uses a camera and processing software to track the position and gaze of the eyes (and, in some instances, the entire head) of a subject. Most eye trackers will also provide a measurement of the pupil diameter.

(3) Thermal cameras that provide detailed information on the changes in the thermal properties of the skin in the face will help assess electrodermal activity and measure respiration and eye movements.

(4) A high resolution video that allows for highly detailed images of the face and body to be taken so that image analysis can determine facial features and expressions and body movements, and an audio system for analyzing human voice for pitch change.

(5) Other sensor types such as for pheromones detection are also under consideration. (U.S. Department of Homeland Security, 2008, p. 4)

Unfortunately, there is no recent indication of what 'other sensors' are currently under consideration.

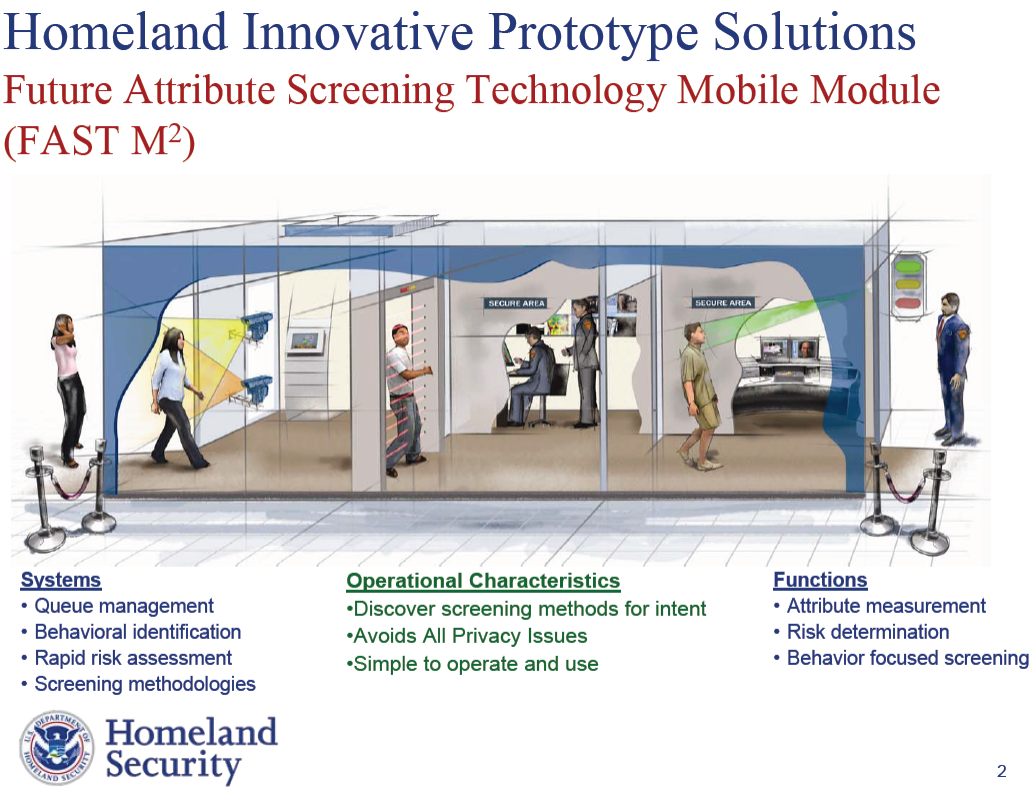

Figure 1: a slide from a DHS presentation providing a visual representation of FAST and outlining its use-cases and capabilities. Source: (U.S. Department of Homeland Security, 2007).

Visual representations of FAST (Figure 1) show it to be a series of rooms that an individual passes through while being interviewed along the way (PublicIntelligence, 2012; U.S. Department of Homeland Security, 2007). Whether in the future FAST, or any other derivative projects, will be able to process a single individual, several individuals, or a crowd simultaneously is difficult to know for certain. It is likely that certain aspects of FAST, such as facial or body movement recognition, could be scaled up significantly if deployed in more open environments, but that other aspects could not, such as pheromones or vocal response. Obviously, scaling the technology such that it does not utilize personal interviews would lower the stress response that FAST relies on, thereby reducing its accuracy.

The trade-off between screening depth versus speed could be adjusted based on the where the technology is deployed, as the ultimate purpose of FAST is to bring airport-level security to public events. This is revealed by a transcript of a DHS workshop, where the then Under Secretary of the DHS Science and Technology Directorate said that in developing FAST "the goal here is in a public event, like the Super Bowl or the Olympics, to go ahead and see if, can we do this noninvasive screening that will give us indication of hostile intent so that we can take an individual to secondary screening?" (Milgrom-Levin et al., 2008, p. 25). The transcript also alludes to using FAST to secure transit infrastructure such as trains and buses. Again, whether this happens with FAST itself is unknown, but these statements certainly shed light on the perspective and motivations of the DHS in its desire to deploy second generation biometrics in wider, more public settings.

Finally, the DHS sells FAST as a "gender, culture and age-neutral" technology that "does not connect physiological data to an individual, nor does it permanently store collected data once the analysis is complete" (U.S. Department of Homeland Security, 2014). It is worth noting that this statement leaves open the potential to store data for a limited duration (which could mean that data is stored for hours, months, or years, so long as it is not 'permanent'), and that physiological data is inherently tied to the individual from which that data is derived. With these openings in mind, it is worth questioning how data collected through FAST may be used in the event of a terror attack, or how it may be used to train the algorithms behind the technology. Nevertheless, if this attempt to distance the technology from "perception[s] of 'Big Brother,' 'Minority Report,' or other nefarious technique[s]" were to be believed (U.S. Department of Homeland Security, 2015, p. 000047), FAST still fits within David Lyon's definition of surveillance "as any focused attention to personal details for the purposes of influence, management, or control" (Lyon, 2010, p. 1). In this case, FAST is an attempt to manage and control individuals who pass through the system as they enter an airport, Olympic game, etc. Indeed, the DHS is developing a powerful set of technologies that could have significant consequences if ever abused.

Situating FAST

In order to understand what makes FAST so concerning, it is important to understand the technological landscape in which FAST exists. To do this, we briefly outline a schema of geosurveillance technology by exploring two distinctions within it, one topological and one spatial, which are exemplified in Table 1. Our understanding of topology in this context aligns with GIScience and mathematics, and we therefore focus our attention to the configuration of links and nodes at work in geosurveillance (Bian, 2009; University of Waterloo, 2015). As such, the topological distinction is between what we call technometric vs biometric geosurveillance. Technometric geosurveillance technologies do not measure an individual's actual location, but rather indirectly infer this information by measuring a separate technology that is *assumed* to be representative of their location (a cell phone, for instance). Biometric geosurveillance, on the other hand, directly measures the individual's body itself to determine their location. As we will illustrate, this small topological difference has significant consequences.

The spatial distinction we have made is between types of geosurveillance that operate *within* space versus those that operate *over* space, which we will also refer to as spatial versus spatialized forms of geosurveillance, respectively. These are types of surveillance that geolocate an individual to a discrete location versus those that operate continuously over space. Importantly, we focus our attention here not to the respective ranges of various geosurveillance technologies, but rather to the fact that they have a range at all, a difference that drastically changes how they operate. While these two cross-cutting dichotomies may be obvious for some, we must clearly and systematically delineate them to emphasize how they could amplify the operation of geosurveillance. Additionally, unpacking the spatial and topological characteristics of surveillance technologies may help to understand the spatial form that tactics and strategies for resistance may take (Swanlund & Schuurman, 2018).

Table 1: Examples of the cross-cutting topological and spatial categories of geosurveillance. Cells with a darker shade represent the most topologically efficient and spatially powerful forms of geosurveillance.

	WITHIN SPACE	**OVER SPACE**
TECHNOMETRIC GEOSURVEILLANCE	GeoIP; Debit/Credit Card Transactions; Social Media Check-ins;	Cell Phone; Radio-Frequency Identification (RFID); Global Positioning Systems (GPS)
BIOMETRIC GEOSURVEILLANCE	Fingerprint Scanners; Retinal Scanners	Gait Analysis; Facial Recognition; Heartbeat Detection

Technometric geosurveillance encompasses most geosurveillance technologies that we are familiar with. Those that operate in space might be exemplified by debit or credit card transactions. These infer individuals' locations based on a single and discrete point of contact, the store at which the transaction occurred, with active participation on the part of an individual. A less active, but still ultimately voluntary example may include GeoIP, which approximates an internet user's location based on a variety of measurements but does so in both discrete physical and virtual space. Indeed, this is a fairly mundane form of geosurveillance: while it generates massive volumes of data, this data is sporadic and bound to a single location (e. g., a store at which a purchase was made or an approximate location at which a computer accessed the internet). Also note that these examples do not directly point to a given individual's location, only the location of an event where that individual is assumed to be (for instance, a stolen credit card may generate location tracks far away from an individual's actual location).

On the other hand, those forms of technometric geosurveillance that operate *over* space can generate much more detailed and continuous data that are not bound to a single location, and instead can be measured remotely. For example, a cell phone can be tracked continuously over space so long as it has reception. Other devices that utilize GPS or RFID technologies can also be tracked over space in a similar fashion, such as smart-phones, vehicles, and ID tags. However, the indirect nature of technometric geosurveillance makes it easy to subvert, as its operation is contingent on the technology that is being surveilled: an individual can pay with cash to avoid creating an electronic record, can hide their IP address using Tor or a VPN, or can simply turn off their phone. Of course, there are many social constraints and forces that can prevent this subversion, and these constraints play out differently depending on context and social difference. For instance, a wealthy individual can much more easily use cash to make purchases than a marginalized person reliant on credit to afford groceries between paycheques. It is in part for this reason that geosurveillance already has uneven effects for those that are marginalized. From a mere technical perspective, however, subversion is straightforward.

Biometric geosurveillance, however, is much more difficult to subvert. Here, examples of biometric technologies that operate within space include fingerprint and retinal scanners, where any locational information that is derived from them will refer only to a specific and singular location in space, such as a particular airport that an individual may travel through. These examples are extremely difficult to subvert from a technical perspective due to their measurement of the body itself. As a result of this topological advantage, the only practical method of subversion is to completely avoid the technology.

The difficulty of subversion posed by the topological efficiency of biometrics is drastically amplified when spatialized biometrics enter the field. With spatialized biometrics, practical subversion is nearly infeasible due to their ability

to operate passively at a distance (over space) and on the body itself. This combined topological efficiency and spatial power effects nearly total surveillance over the areas in which spatialized biometrics are positioned. For example, to avoid facial recognition one would have to wear a mask (which may not be possible, such as in banks) or heavy make-up (Harvey, 2017), and even then, gait recognition may be able to identify them.

When spatialized biometrics are using second generation technologies, the infeasibility of subversion becomes far more problematic due to the added stakes involved. Again, second generation biometrics work on the body so that they can detect physiological attributes (including heart rate, respiration, gait, and vocal frequency) that enable calculated inferences, including mood. However, these measurements could also be used to detect certain medical conditions. According to Mordini & Ashton, second generation biometrics could potentially detect mental illnesses such as depression or anxiety, as well as physical conditions such as joint disorders (Mordini & Ashton, 2012). Surely the ability to identify people with potentially stigmatized illnesses could result in those people suffering negative effects, a problem exacerbated by the fact that they may already be marginalized due to those illnesses. In short, spatialized second generation biometrics are not only incredibly difficult to subvert, they also put our own health privacy at risk of exposure, which itself has significant consequences.

Given the dangers of spatialized biometrics, we must also be aware of the related developments being made in both the public and private sector. One active project at MIT aims to infer an individual's mood by using WiFi signals to monitor their respiration and heart rate. This method can "detect emotions with 70 percent accuracy even when it hadn't previously measured the target person's heartbeat", with accuracy rates rising to 87% with prior data (Conner-Simons, 2016). Another project called AutoEmotive, also at MIT, uses both contact and non-contact sensors to detect drivers' physiological traits in order to measure stress. This information is then used to compensate for the added risk of a stressed out driver, such as by increasing headlight strength, warning the driver of their stressful state, or playing relaxing music (AutoEmotive, n.d.). Even churches are beginning to deploy facial recognition to track who is skipping out on the Sabbath (Hill, 2015), while music festivals use the same technology to track spending (Pulliam-Moore, 2015). All the while, the FBI has repurposed photos from drivers licenses to feed into its facial recognition database of over 400 million photos (Kravets, 2016). There is little doubt that these technologies are popular and will be retained and expanded in the near future.

Theorizing Second Generation Biometrics

At their core, biometrics are tools that render bodies legible. Indeed, a legible subject is one that is knowable, predictable, and therefore able to be managed accordingly (Martin, 2010). An illegible subject, on the other hand, is dangerous, unpredictable, and difficult to manage. As Lauren Martin's (2010) work

argues, legibility has become a staple of airport security, where first generation biometric systems, including retinal and fingerprint scanners, are now familiar technologies. These make subjects legible largely by authenticating their identity and tying it to known information about them. In other words, most first generation biometrics operate by anchoring individuals' bodies into their data-doubles (Amoore, 2006). One possible exception to this is full body scanners, which, instead of asking 'who' we are, tend to ask 'what' we are: what are the boundaries of the body and what dangerous objects are potentially hidden around it? 'Who' and 'what' we are, however, provide highly incomplete assessments of risk.

Second generation biometrics mark a new, intensified level of legibility by shifting the question from 'who' or 'what' to 'how' (Mordini et al., 2012). In this way, the information to be read off an individual's body significantly increases in descriptive power; 'who' someone is or 'what' they carry is less descriptive compared to 'how' they are feeling in a given moment as a determination of the potential threat they pose to public safety. For instance, in relation to the modern 'war on terror', mere knowledge of someone's identity is not enough to stop a terrorist attack; identification must be combined with other useful information about a given individual for it to be an effective counter-terrorism tool (Sutrop & Laas-Mikko, 2012). On the other hand, knowing that they are nervous or anxious because of their heart rate, respiration, and/or body temperature is enough information on its own to prompt further interrogation. Nothing external is required.

Biometric technologies that operate over space – including both first generation and second generation biometrics – extend the reach of surveillance such that more bodies can be made legible. This is seen in the DHS' intended use-cases for FAST, that involve, for example, higher security screening at sporting events without sacrificing throughput. In terms of prospective uses for these technologies, however, their operation over space makes it possible to not just screen individuals faster, but to screen multiple individuals simultaneously. Therefore, second generation biometrics mark not just an *intensification*, but an *extension* of geosurveillance.

At a broader scale, this desire for legibility can be understood through what Rachel Hall calls the *aesthetics of transparency*:

> The aesthetics of transparency belong to a rationality of government that understands security in terms of visibility. The aesthetics of transparency is motivated by the desire to turn the world (the body) inside-out such that there would no longer be any secrets or interiors, human or geographical, in which our enemies (or enemy within) might find refuge (Hall, 2007, pp. 320–321).

These interiors can include not only the inside of a backpack or oral cavity within which dangers might lurk, but the interiors of minds where malintent might slither. Moreover, Hall writes that "the aesthetics of transparency establishes a binary opposition between interiority and exteriority and privileges the external or visible surface over the suspect's word" (Hall, 2007, p. 321). Trust then is placed only in the sterile, quantitative composite that is our biometric profile. (Hall, 2007, p. 323).

Understood in this context, second generation biometrics turn the interior inside-out such that it becomes externally visible, allowing the aesthetic of transparency to extend its operation into the previously untrusted and inaccessible territory of the mind. With these internal and invisible characteristics of ourselves reified, any attendant security risks become patently apparent. This is accomplished not only by making visible our heart rate, respiration, body temperature, minute vocal fluctuations, gait, and/or minute facial movements, but by analyzing those data using algorithms that quantify and classify our internal emotions such that they too are external and visible. With these at hand, we become legible and transparent, without dangerous interiors or secrets. We become securable insofar as we can be controlled and regulated, but also securitized, insofar as our bodies become mere subjects of security.

Securitization via biometric legibility, however, is neither an innocent nor neutral maneuver. This is made clear by scholars who point out that biometrics fail more often when analyzing marginalized people, such as people of color or those with disabilities (Amir & Kotef, 2017; Currah & Mulqueen, 2011; Magnet, 2011; Magnet & Rodgers, 2012; Murray, 2007). In fact, the inherent problems with even the simplest biometrics, such as the sex classification listed on government-issued ID, become apparent when transgender people are forced to navigate them (Currah & Mulqueen, 2011). When biometrics fail they result in certain bodies being made illegible, and therefore have the potential to push minorities and othered bodies further into the margins of society. Meanwhile, many suggest that biometrics tend to work best on the stereotypical young, white, blue-eyed male (Browne, 2015; Magdaleno, 2014; Magnet, 2011). Or as Magnet describes, they are designed for "a Goldilocks subject who is 'jussstright'" (Magnet, 2011, p. 31).

One reason for this preference of the 'Goldilocks subject', and a potential problem that many biometric technologies face is their implementation of machine learning, which relies on training data that may be either inadequate or misrepresentative of the population. For instance, Google's image labeling technology gained notoriety after it classified some of its users as "Gorillas" (Zhang, 2015). The users were African American, and the racist classification was made because of how the system 'learned' from its training data, which presumably contained racist content scraped from the web. This is a separate concern from the potential for prejudices to be programmed into the technology by developers themselves, although that is also relevant here. Nevertheless, that Google's system

made such an error simply based on its users' faces illustrates what effects similarly mis-trained biometric systems could have.

If this problem were to be solved in the future, concerns over biometrics' impact on marginalized bodies would remain. Because second generation biometrics will be used to recognize stress in the security context (Zetter, 2011), it is likely that those who already face discrimination will display a higher stress response when being questioned by security. For instance, a Muslim individual may legitimately fear racial profiling by security agents, and therefore display a higher level of stress as they pass through a security checkpoint, causing them to be singled out for further interrogation. Such a systematic bias could also impact those with mental illnesses, such as anxiety disorder, which may result in outlying (and therefore suspicious) data in a wide variety of situations (Mordini & Ashton, 2012).

Of course, security officers already look for behavioural cues that indicate nervousness or stress. However, the intensifying effects of second generation biometrics increase the efficacy of this practice, while the extending effects expand its reach. Moreover, because the system takes on an appearance of calculated objectivity, and therefore seems devoid of any room for human subjectivity, the 'truth value' of the practice may be exaggerated. As Lucas Introna notes, calculative practices "have a certain moral authority because they are taken to impose objectivity and neutrality in a complex domain" (Introna, 2015, p. 39). In other words, there exists a potentially dangerous disconnect between our perception of these technologies as objective and the real subjectivities that are almost always attendant to them.

Decades ago Mark Poster identified a similar disconnect when discussing the slim similarities between digital profiles and living, breathing humans (Poster, 1996). He referred to the proliferation of digital financial profiles as "skeletal selves" and correctly commented that none of us would recognize ourselves in these profiles. Biometric surveillance, of course, makes mockery of those distant concerns with its much more extensive profiling. However, the same arguments are relevant. These profiles and assumptions, made based on biometric surveillance, can never capture or fully represent a human being. And the more different someone is from the person who designed the algorithm and the people used to train it, the more likely someone will be classified as 'abnormal'. As argued above, finding fault in the algorithms is not a long term solution as the counter argument will always be that the technology can be improved. However, as Cathy O'Neil argues in *Weapons of Math Destruction* (2016), the algorithm can do a lot of damage before the technology is changed.

FAST'S supposed innocent objectivity as a technology that is "gender, culture and age-neutral" is clearly problematic (U.S. Department of Homeland Security, 2014). As a collection of entirely second generation biometric technologies that operate over space, we argue that FAST foreshadows how future

geosurveillance may be both intensified and extended to facilitate the utmost legibility of securitized subjects. Crucially, this shift will not have even-handed effects on all individuals, but rather will affect already marginalized bodies disproportionately.

Conclusion

In this article, we explored FAST as a collection of second generation biometric technologies that provide useful insight into both DHS priorities and their plans for future surveillance technologies. We argue that the spatial nature of second generation biometrics, as well as the fact that they operate on the body itself rather than some other carried technology, unlock the potential for geosurveillance to be greatly amplified in the near future. More specifically, this amplification of geosurveillance consists of an intensification due to the increased legibility of subjects, as well as an extension due to the technology's ability to analyze several individuals simultaneously over space.

Critically, we claim that this amplification of geosurveillance is most problematic due to its effects on already marginalized bodies. Indeed, while our use of Minority Report in our title and introduction is a nod to both the film that features biometric technologies as well as the concept of a minority report as a dissenting opinion, it is also a reference to the fact that minorities, in the broadest sense of the term, are more likely to be negatively impacted by biometrics. Unfortunately, these problems are only exacerbated by biometrics' veil of objective science (Introna, 2015).

Our contribution in this article is a lucid investigation into what we are collectively beginning to understand about the forms of surveillance that are looming on the technological horizon. This article contextualizes these developments technically, spatially, and topologically to better understand what makes these new technologies so powerful. It then analyzes them theoretically to inform on their detrimental social consequences. With these consequences in mind, we call for more geographical research and scholarly engagement with biometrics, as well as geosurveillance more broadly. At present, second generation biometrics are notably absent from the geographical literature, and future research should work to fill this gap. This article represents but one step towards this objective.

References

ABC News. (2008, September 18). Anxiety-detecting machines could spot terrorists. Retrieved November 23, 2016, from http://abcnews.go.com/Technology/story?id=5837147&page=1

Amir, M., & Kotef, H. (2017). In-secure identities: On the securitization of abnormality. *Environment and Planning D: Society and Space*, 0263775817744780. https://doi.org/10.1177/0263775817744780

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. *Political Geography*, *25*(3), 336–351. https://doi.org/10.1016/j.polgeo.2006.02.001

Amoore, L. (2009). Algorithmic War: Everyday Geographies of the War on Terror. *Antipode*, *41*(1), 49–69. https://doi.org/10.1111/j.1467-8330.2008.00655.x

Amoore, L. (2014). Security and the incalculable. *Security Dialogue*, *45*(5), 423–439. https://doi.org/10.1177/0967010614539719

Amoore, L., & Hall, A. (2009). Taking People Apart: Digitised Dissection and the Body at the Border. *Environment and Planning D: Society and Space*, *27*(3), 444–464. https://doi.org/10.1068/d1208

Amoore, L., Marmura, S., & Salter, M. B. B. (2008). Smart Borders and Mobilities: Spaces, Zones, Enclosures. *Surveillance & Society*, *5*(2). Retrieved from https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3429

Angeles, B. C. E. in L. (2008, September 23). New airport screening "could read minds." Retrieved from http://www.telegraph.co.uk/news/worldnews/northamerica/usa/3069960/New-airport-screening-could-read-minds.html

AutoEmotive. (n.d.). AutoEmotive. Retrieved November 24, 2016, from http://autoemotive.media.mit.edu/

Barrie, A. (2008, September 23). Homeland Security Detects Terrorist Threats by Reading Your Mind [Text.Article]. Retrieved November 23, 2016, from http://www.foxnews.com/story/2008/09/23/homeland-security-detects-terrorist-threats-by-reading-your-mind.html

Bian, L. (2009). Spatial Data Models. In R. Kitchin & N. Thrift (Eds.), *International Encyclopedia of Human Geography* (pp. 337–344). Oxford: Elsevier. https://doi.org/10.1016/B978-008044910-4.00417-X

Bosch, T., & Canfield, D. (2012, April 18). Why Homeland Security's Pre-Crime Prevention Technology Is a Terrible Idea. *Slate*. Retrieved from http://www.slate.com/blogs/future_tense/2012/04/18/future_attribute_screening_technology_homeland_security_s_minority_report_program_.html

Browne, S. (2015). *Dark Matters: On the Surveillance of Blackness*. Duke University Press. https://doi.org/10.1215/9780822375302

Castro, F. M., Marin-Jimenez, M. J., Guil, N., & de la Blanca, N. P. (2016). Automatic learning of gait signatures for people identification. *ArXiv:1603.01006 [Cs]*. Retrieved from http://arxiv.org/abs/1603.01006

Conner-Simons, A. (2016). Detecting emotions with wireless signals. Retrieved November 24, 2016, from https://news.mit.edu/2016/detecting-emotions-with-wireless-signals-0920

Currah, P., & Mulqueen, T. (2011). Securitizing Gender: Identity, Biometrics, and Transgender Bodies at the Airport. *Social Research*, *78*(2), 557–582. Retrieved from http://www.jstor.org.proxy.lib.sfu.ca/stable/23347190

Furnas, A. (2012, April 17). Homeland Security's "Pre-Crime" Screening Will Never Work. *The Atlantic*. Retrieved from http://www.theatlantic.com/technology/archive/2012/04/homeland-securitys-pre-crime-screening-will-never-work/255971/

Ghilardi, G., & Keller, F. (2012). Epistemological Foundation of Biometrics. In E. Mordini & D. Tzovaras (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context* (pp. 23–47). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_2

Häkli, J. (2007). Biometric identities. *Progress in Human Geography*, *31*(2), 139–141. https://doi.org/10.1177/0309132507075358

Hall, R. (2007). Of Ziploc Bags and Black Holes: The Aesthetics of Transparency in the War on Terror. *The Communication Review*, *10*(4), 319–346. https://doi.org/10.1080/10714420701715381

Harvey, A. (2017). CV Dazzle: Camouflage from Face Detection. Retrieved May 28, 2018, from https://cvdazzle.com/

Hill, K. (2015). You're Being Secretly Tracked With Facial Recognition, Even in Church. Retrieved November 24, 2016, from http://fusion.net/story/154199/facial-recognition-no-rules/

Horizon. (2016). CCTV software identifies people by their walk. Retrieved November 23, 2016, from http://horizon-magazine.eu/article/cctv-software-identifies-people-their-walk_en.html

Introna, L. D. (2015). Algorithms, Governance, and Governmentality: On Governing Academic Writing. *Science, Technology & Human Values*, *41*(1), 0162243915587360-. https://doi.org/10.1177/0162243915587360

Kravets, D. (2016, June 18). Smile, you're in the FBI face-recognition database. Retrieved November 24, 2016, from http://arstechnica.com/tech-policy/2016/06/smile-youre-in-the-fbi-face-recognition-database/

Loftus, J. (2011). DHS Begins Testing Controversial Pre-Crime FAST System (On the Willing). Retrieved November 22, 2016, from http://gizmodo.com/5847937/dhs-begins-testing-controversial-pre-crime-fast-system-on-the-willing

Lyon, D. (2010). Surveillance, Power and Everyday Life. In P. Kalantzis-Cope & K. Gherab-Martín (Eds.), *Emerging Digital Spaces in Contemporary Society* (pp. 1–37). Palgrave Macmillan UK. https://doi.org/10.1057/9780230299047_18

Magdaleno, J. (2014, February 4). Is Facial Recognition Technology Racist? Retrieved November 12, 2017, from https://creators.vice.com/en_us/article/53wp3k/is-facial-recognition-technology-racist

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

Magnet, S., & Rodgers, T. (2012). Stripping for the State. *Feminist Media Studies*, *12*(1), 101–118. https://doi.org/10.1080/14680777.2011.558352

Markoff, J. (2002, November 9). Threats and Responses: Intelligence; Pentagon Plans a Computer System That Would Peek at Personal Data of Americans. *The New York Times*. Retrieved from http://www.nytimes.com/2002/11/09/us/threats-responses-intelligence-pentagon-plans-computer-system-that-would-peek.html

Martin, L. L. (2010). Bombs, bodies, and biopolitics: securitizing the subject at the airport security checkpoint. *Social & Cultural Geography*, *11*(1), 17–34. https://doi.org/10.1080/14649360903414585

Milgrom-Levin, T., Teufel, H., Cohen, J., Jensen, D., Landesberg, M., Cate, F. H., … Wright, R. Department of Homeland Security Meeting: "Implementing Privacy Protections in Government Data Mining (2008). Retrieved from https://www.dhs.gov/xlibrary/assets/privacy/privacy_datamining_July24_2008_minutes.pdf

Mordini, E., & Ashton, H. (2012). The Transparent Body: Medical Information, Physical Privacy and Respect for Body Integrity. In E. Mordini & D. Tzovaras (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context* (pp. 257–283). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_12

Mordini, E., Tzovaras, D., & Ashton, H. (2012). Introduction. In E. Mordini & D. Tzovaras (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context* (pp. 1–19). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_1

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

Nguyen, N. (2015). Chokepoint: Regulating US student mobility through biometrics. *Political Geography*, *46*, 1–10. https://doi.org/10.1016/j.polgeo.2014.09.004

Nishiyama, H. (2015). Towards a Global Genealogy of Biopolitics: Race, Colonialism, and Biometrics beyond Europe. *Environment and Planning D: Society and Space*, *33*(2), 331–346. https://doi.org/10.1068/d19912

O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Retrieved August 28, 2017, from https://www.amazon.com/Weapons-Math-Destruction-Increases-Inequality/dp/0553418815

Pero, R., & Smith, H. (2014). In the "Service" of Migrants: The Temporary Resident Biometrics Project and the Economization of Migrant Labor in Canada. *Annals of the Association of American Geographers*, *104*(2), 401–411. https://doi.org/10.1080/00045608.2013.875804

Poster, M. (1996). Databases as Discourse, or Electronic Interpellations. In D. Lyon & E. Zureik (Eds.), *Computers, Surveillance, and Privacy*. Retrieved from http://readinglists.warwick.ac.uk/items/767FD110-73BD-3041-5332-F36BA62ACB3D.html

PublicIntelligence. (2012). *Future Attribute Screening Technology (FAST) Promotional Video*. Retrieved from https://www.youtube.com/watch?v=48FuWeF4m7U

Pugliese, J. (2012). *Biometrics: Bodies, Technologies, Biopolitics* (Reprint edition). London: Routledge.

Pulliam-Moore, C. (2015). Download Music Festival Comes Under Fire for Scanning People's Faces, Tracking Their Spending Habits. Retrieved November 24, 2016, from http://fusion.net/story/152495/download-music-festival-comes-under-fire-for-scanning-peoples-faces-tracking-their-spending-habits/

Sutrop, M., & Laas-Mikko, K. (2012). From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics. *Review of Policy Research*, *29*(1), 21–36. https://doi.org/10.1111/j.1541-1338.2011.00536.x

Swanlund, D., & Schuurman, N. (2018). Resisting geosurveillance: A survey of tactics and strategies for spatial privacy. *Progress in Human Geography*, 0309132518772661. https://doi.org/10.1177/0309132518772661

University of Waterloo. (2015, October 16). What is Topology? Retrieved December 15, 2017, from https://uwaterloo.ca/pure-mathematics/about-pure-math/what-is-pure-math/what-is-topology

U.S. Department of Homeland Security. (2007). *Future Attribute Screening Technology Mobile Module*. Presented at the S&T Stakeholders Conference. Retrieved from https://info.publicintelligence.net/DHS-FAST.pdf

U.S. Department of Homeland Security. (2008). *Privacy Impact Assessment for the Future Attribute Screening Technology (FAST) Project*. Retrieved from https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf

U.S. Department of Homeland Security. (2014). Future Attribute Screening Technology. Retrieved November 22, 2016, from https://www.dhs.gov/publication/future-attribute-screening-technology

U.S. Department of Homeland Security. (2015). Electronic Privacy Information Center Freedom of Information Act Request Filed to the Department of Homeland Security. Retrieved from https://epic.org/foia/dhs/fast/14-10-14-DHS-FOIA-20150511-DHS-Production.pdf

Van Der Ploeg, I. (2012). Security in the Danger Zone: Normative Issues of Next Generation Biometrics. In E. Mordini & D. Tzovaras (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context* (pp. 287–303). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_13

Vélez, A. (2012). Insecure Identities: The Approval of a Biometric ID Card in Mexico. *Surveillance & Society*, *10*(1), 42–50. Retrieved from http://proxy.lib.sfu.ca/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=i3h&AN=87532861&site=ehost-live

Weinberger, S. (2011). Terrorist "pre-crime" detector field tested in United States. *Nature News*. https://doi.org/10.1038/news.2011.323

Zetter, K. (2011). DHS Launches "Minority Report" Pre-Crime Detection Program. Retrieved November 23, 2017, from https://www.wired.com/2011/10/pre-crime-detection/

Zhang, M. (2015). Google Photos Tags Two African-Americans As Gorillas Through Facial Recognition Software. Retrieved August 15, 2017, from http://www.forbes.com/sites/mzhang/2015/07/01/google-photos-tags-two-african-americans-as-gorillas-through-facial-recognition-software/