Olympian Surveillance: Sports Stadiums and the Normalization of Biometric Monitoring

BRETT HUTCHINS
MARK ANDREJEVIC[1]
Monash University, Australia

Sports stadiums are a prime site for the deployment and development of facial recognition technology. They are being used to envision and model a spectator experience governed by the operation of automated surveillance and sensor-based monitoring systems, which promise greater security and enhanced consumption opportunities. This article draws on the planned but postponed rollout of NEC's NeoFace identification system for the Tokyo Olympics to examine broader trends in the deployment of biometric monitoring systems. Drawing on existing and planned uses of these systems, we focus on the sports stadium as a site for considering how biometric surveillance is introduced, implemented, and normalized. The themes of convergence, preemption, and spatiality are central to the messages presented in the industry's promotional materials, framing facial recognition technology as an essential component of the contemporary media-stadium. The immense popularity of mega-events and the pleasures of live sports erode the contestability of this framing, drawing attention away from the biases, inaccuracies, privacy concerns, and inequalities perpetuated by highly invasive systems that exercise social control in and beyond the stadium.

Keywords: automation, consumption, COVID-19, surveillance, health, pandemic, facial recognition, pattern recognition, policing, preemption, securitization, smart cameras

Seeing Machines and States of Exception

The extensive preparations required to stage sports mega-events demonstrate the growing affinities among mass spectator events, high-tech capital, pervasive monitoring, and securitization. The lead-in to the 2020 Summer Games in Tokyo (currently rescheduled for 2021) continued this pattern, mobilizing the spectacle of high-tech surveillance for international audiences and serving as a launching pad for the Olympic

Brett Hutchins: brett.hutchins@monash.edu
Mark Andrejevcic: mark.andrejevic@monash.edu
Date submitted: 2020-08-27

[1] The research presented in this article was supported by Australian Research Council funding awarded to Hutchins (FT130100506) and Andrejevic (DP200100189; CE200100005). Thank you to Ben Glasson and the anonymous reviewers for their helpful feedback in the development of this article.

debut of a facial recognition system developed by tech companies NEC and Intel. The anticipatory media coverage, always in search of an interesting angle, foregrounded Japan's embrace of high-profile "demonstration projects" that, as Boyle and Haggerty (2012) put it, "perform security capabilities" to a wide audience, while also serving as an opportunity for global technology corporations to market their wares (p. 250). These demonstration projects currently focus on drones and facial recognition technology—both dual-use systems that mark the convergence of surveillance, entertainment, and marketing. Drones can provide novel viewing angles of the event *and* scan crowds. Similarly, facial recognition systems identify and track spectators for the purposes of both security and profit. Much of the coverage of preparations for the Tokyo Olympics focuses on the Japanese multinational technology company NEC—a global leader in the implementation of facial recognition technology—and its deployment of the NeoFace system for automated facial recognition. NeoFace is part of a suite of biometric identification technologies dubbed "Bio-Idiom," which NEC (2018a) claims create "a whole new value in biometrics" (para. 2). The company announced plans to team up with flagship Olympic sponsor Intel to provide ID verification for an estimated 300,000 credentialed attendees for the Tokyo Olympics, including ticket holders, athletes, coaches, medical staff, and members of the media. Everyone registered to attend the Games, should they take place in 2021, will need to provide a government-issued ID photo to access Olympic facilities, including all stadiums and venues.

Drawing on the buildup to the Tokyo Olympics, this article analyzes the role of the sports stadium as a defining space in the deployment of facial recognition technology. The planning for the 2020 Olympiad provides a blueprint for the convergent uses of facial recognition technology for security and commerce. The COVID-19 pandemic may have delayed the rollout of NEC's "state of the art" monitoring technology, but it also provides a new set of imperatives for biometric monitoring that the company has been quick to embrace. NEC is already combining its facial recognition capability with systems for remote symptom tracking, social distance monitoring, and contact tracing to address pandemic concerns. In this respect, NEC and the surveillance technology sector are constructing the infrastructure for a "new normal," in which health securitization is incorporated into systems for public safety and marketing.

Major stadiums and arenas provide useful testing grounds for facial recognition technology and the biometric monitoring systems associated with it (such as surface body temperature sensors). They are settings in which tens of thousands of people are all looking in a predictable, centralized direction, and are associated with widely publicized in-stadium security concerns ranging from brawling and hooliganism to terrorism. As evental spaces for the spectacularization of speed and performance-based athletic competition, stadiums already function as what critical sports theorist Marc Perelman (2012) refers to as "seeing machines": architecturally designed visualization technologies that actively control the visual order and movement of spectators through the organization of physical space, stands, seating, in-venue screens, cameras, and sensors (p. 83). Featuring extensive communications, camera, and media networks, these "high-output image mills" dominate the sensory experience of "serially wired" spectators and, in so doing, make the stadium itself an element of the spectacle (Perelman, 2012, pp. 48, 81). The promotion and branding of stadiums as iconic destinations, or "cathedrals of sport," for fans and tourists solidify this positioning (e.g., former Olympic stadiums such as the Bird's Nest National Stadium in Beijing, Wembley Stadium in London, and the Melbourne Cricket Ground; Dyreson, 2013, p. 1). They thus partake of the double logic of the original plan for the Panopticon: both as observatory and spectacle (Bentham, 1995; Frank & Steets, 2010). Read culturally, stadiums are exceptional structures and historic symbols that are framed as requiring—and publicizing—extraordinary measures and opportunities for both security and commerce under the cover of spectator safety, convenience, and enjoyment. Facial recognition technology represents a problematic but logical extension of this framing.

The stadium serves as an "exceptional" space, in the sense that it models forms of surveillance that generate strong opposition in other realms of social life, and therefore as a means of habituating people to monitoring systems that will likely migrate into those realms. The huge financial outlay on surveillance technology for major sports events such as the Olympics and the FIFA World Cup doubles as justification for its continuing application. This security legacy has a record of delivering increasingly invasive citizen monitoring and policing mechanisms with the passage of each mega-event. The resulting surveillance technologies and systems, policing and security company operations, government policies and legislation, and urban redevelopments, alter and privatize public space and differentially impact poorer communities (Boykoff, 2014; Giulianotti & Klauser, 2010).

Examples of this phenomenon in the realm of surveillance technology and security systems are plentiful, with the Games serving as a large-scale "test-bed for new technologies" (Horne & Whannel, 2012, p. 87). For instance, the 2008 Beijing Olympics saw attendees purchase tickets with trackable Radio Frequency Identification tags (RFID), as well as the installation of a US$6 billion CCTV system in the city that increased the number of cameras surveilling public space to over 300,000 (Boykoff, 2014). In response to the astronomical costs of security technology for the 2010 World Cup, South Africa's police minister said, "These investments are not only meant for the event but will continue to assist the police in their crime-fighting initiatives long after the Soccer World Cup is over" (Mthethwa, 2010, para. 8). With a security budget estimated to be over £1 billion, the 2012 London Olympics saw the development of a lightweight aerial drone by the defense, security, and aerospace conglomerate BAE Systems. According to police, the GA22 drone had "considerable potential in the policing of major events, whether they be protests or the Olympics" (as cited in Boykoff, 2014, p. 90). In keeping with these developments, one commentator described the legacy of recent Olympic Games as the consolidation of a "cyber-surveillance" (Silverman, 2016, para. 1) state:

> In Athens, for example, the security legacy consists of a massive surveillance camera network. In Rio de Janeiro, many of the surveillance tools will remain and be used by different security institutions. The many cameras installed in the city will also remain and be used for the ordinary policing of Rio. (Silverman, 2016, para. 27)

The installation of NEC's NeoFace system in all Olympic venues in Tokyo represents the latest chapter in this ongoing story, habituating citizens to a highly invasive biometric mode of surveillance that operates throughout public space and everyday life:

> Olympic security officials have teamed up with Japanese tech giant NEC to deliver facial recognition technology to all Olympic venues for the first time in the history of the Games. . . . NEC biometric technologies including face, iris, fingerprint, palm print, and voice detection will also be available for identity authentication and other scenarios. . . . These technologies will be turned on Tokyo residents after the Games, allowing for more state control and the expansion of data mining operations. (Boykoff & Gaffney, 2020, p. 12)

Particularly since the events of 9/11, technological implementation coupled with media publicity acts as a form of security pedagogy, highlighting the perceived need for increasingly powerful surveillance technology. As Boyle and Haggerty (2011) argue, the Games normalize security practices, "that might otherwise be seen as intrusive" (p. 5).

The recent history of mega-events suggests that the security exception has become the new norm, with the spectacle, rituals, and pleasures of sport serving as both cover and justification for increasingly comprehensive forms of monitoring and tracking that service profit and security. This pattern emphasizes the importance of investigating how and why the stadium comes to serve as a space of exception for the implementation of surveillance technology. We begin by exploring the history of the sports stadium as a site of cultural meaning, securitization, and consumption. Drawing on coverage of the deployment of these systems worldwide and the marketing and publicity materials circulated by NEC and other facial recognition technology companies, we examine the logics of automated surveillance—that is, the stories told and sold in the publicity materials of technology companies about the promises, opportunities, and experiences made possible by facial recognition systems. Some of these promises come true, others remain in progress, and many (thankfully) are never realized. Nonetheless, these materials and trade literature more generally are valuable resources in uncovering the guiding imperatives and logics that shape the development and implementation of technology. Wilken (2014), for instance, observes that trade sources reveal key narratives and other discursive strategies used to shape technological platforms and services. In the case of facial recognition technology, these materials discursively transform the physical infrastructure of biometric surveillance systems into compelling stories and appealing justifications for their existence and use, and perform an active role in shaping these technologies alongside patents and the work of engineers and programmers (Delfanti & Frey, 2020; Mosco, 2014). The logics of convergence, preemption, and spatiality emerge from the coverage of existing systems and the projected development and deployment of future systems envisioned in stadium plans and industry materials. Facial recognition technology is framed as both a reducer of risk (of violence) and a maximizer of commercial opportunity (sales and profits); its representation oscillates between a technology of individuation and one of massification (both the ability to single out individuals and to observe emergent patterns), and it envisions the reconfiguration of physical space by securing circulation, identifying, sorting, and screening.

The stadium serves as a site of least resistance for the implementation of powerful surveillance technology because of its role in advancing top-flight sport as a site for lucrative middle- and upper-class consumption. There has been pushback against the expansion of surveillance and monitoring at both stadium events and major sporting venues, but it is eclipsed by responses to the implementation of facial recognition technology in other shared spaces, such as downtown areas, shopping precincts, and transport facilities. A mega-event like the Olympics is characterized by high-risk and immense opportunity, both of which serve as warrants for demonstrating the benefits of exceptional forms of monitoring. During these events, the stadium also serves as a site of entertainment and nation branding. If the spectacle is not secured, any failure runs the risk of becoming a spectacular indictment of the competence of the host city and country.

The Stadium: From Physical to Digital Enclosure

Sports stadiums and arenas are built structures that have accrued escalating levels of cultural, economic, and political significance over the past 150 years. Sitting within this history is the enclosure of the stadium and the creeping regulation, partitioning, and sorting of people within its confines. This process began in the 19th century with the erection of fences and walls that separated sporting grounds from their surrounding communities and land. This separation occurred in conjunction with the standardization of rules, codes of conduct, and playing conditions, including field, court, and track dimensions, that helped to determine seating and standing arrangements, and the design of stadiums (Bale, 1993; Guttmann, 1978/2004). Proceeding alongside a widespread process of enclosure that undermined the existence of the commons in favor of private property rights, physical enclosure enabled entry fees to be charged at the gate and fostered the promotion of sport by an emerging class of sport administrators and entertainment entrepreneurs (Holt, 1989; Vamplew, 1985). The construction of stands and the growing segmentation of spaces within the stadium served to differentiate ticket prices and provided superior lines of sight for wealthier spectators, members of the press, and, eventually, broadcasters. These developments also reflect and stimulate assorted forms of crowd behavior, including barracking, cheering, and singing, and on occasion verbal and physical conflict related to the stratified class-based geography of sporting arenas (Jamison, 1996).

The twin imperatives of securitization and consumption came to progressively govern life in the stadium from the middle years of the 20th century (Giulianotti, 2011). Policing and surveillance of the stadium create the conditions needed for the reliable and expansive commodification of the spectator experience from the moment of entry through to exit—for example, a multiplying number of ticket categories and upgrade options, premium seating, memberships, concessions, merchandise, fan zones, in-seat services, corporate boxes, bars and VIP lounges, gambling services, stadium and in-seat screens, and even swimming pools with prime views of the arena (Zinganel, 2010).

The impetus for securitized consumption is underpinned by both the maintenance of social order and cultural attachment to sport. A determination to limit unruly behavior and physical violence by fans is apparent across almost all continents. Football hooliganism in the UK and Europe in particular triggers unsettling flashpoints from the 1960s on. Terrorist incidents at the 1972 Montreal and 1996 Atlanta Olympic Games publicize attacks on athlete and spectator safety to international television audiences, helping to justify security measures that might otherwise be considered heavy-handed or invasive (Roche, 2017). The cultural dimensions of sports fandom and rituals further act to legitimatize a securitized mode of stadium governance. Tied to the sports, teams, and athletes competing on the playing arena, the historical and symbolic dimensions of stadiums generate topophilic responses among the supporter communities who spend seasons and years in attendance—that is, fond memories, shared stories, strong emotional associations, and sensory pleasures (Bale, 1993). These responses, in turn, are sold back to spectators via a place-based affective commercialism that melds spectacle, collective effervescence, and consumer convenience.

A process of digital enclosure defines the most recent stage in the development of major stadiums: maximizing capital and data accumulation through high-tech innovation (Andrejevic, 2007; Couldry & Mejias, 2019). The physical structure of the contemporary “media-stadium” (Perelman, 2012, p. 85) doubles as a sophisticated communications and technology infrastructure that features an array of wireless, broadband, mobile, screen, and sensor technologies and networks (including cellular networks, WiFi, Distributed Antenna Systems, under seat small cells, beacons, near-field communications, multicast video streaming, digital screens, and security cameras; Hutchins, 2016; Palvarini & Tosi, 2013; Yang & Cole, 2020). Pivoting around the live event, this infrastructure is focused on the transmission of screen-based content and advertising in conjunction with the tracking of smartphones, mobile apps, mobile tickets, identity cards, wearable media devices, and RFID chips/bands, including those used and worn by spectators, athletes, and stadium staff. Social life and commercial activity within the stadium are subject to ceaseless surveillance and datafication, which track and algorithmically analyze the movement and location of people, the mediated social interactions of spectators, commercial transactions, and facility use. A range of multinational technology firms such as Cisco and Hewlett Packard (through its wireless networking subsidiary Aruba Networks) supply the networking hardware and software that make such monitoring and datafication possible. Installed in iconic venues such as New York's Yankee Stadium and the Sydney Cricket Ground, the marketing of the "Connected Stadium" stresses the desirability of securitized consumption:

> The Cisco Connected Stadium is a highly scalable, secure network designed specifically for sports and entertainment venues to bring together all forms of access, communications, entertainment and operations onto a single innovative platform. It also provides the platform needed to transform stadium safety and security . . . [it] unifies incident management to improve threat detection, assessment and response times. ("Cisco Connected Stadium," 2020, para. 1)

Mega-events are ideal settings to showcase these systems by virtue of their demonstrable scale and global exposure. For instance, the 2008 Beijing Olympics saw the development of new 3G mobile technical standards in China, and the 2018 Winter Olympics in South Korea saw the first large-scale examples of 5G network applications displayed to the world (Hutchins, 2019). In the latter case, this included using "Internet of Things solutions" to ensure the "smarter and smoother" operation of venues (Interdigital, 2016, p. 6). The introduction of facial recognition technologies in Tokyo perpetuates the narrative of technological innovation in the organization and experience of mega-events (Roche, 2000), but conspicuously fails to acknowledge the privacy, accuracy, and political economic implications of surveillance systems.

Facial Recognition and the Stadium: An Overview

In the United States, the 2001 Super Bowl in Tampa provided the inspiration for the first widespread implementation of facial recognition technology in an urban space. Persuaded by a police officer who was part of the plainclothes unit patrolling Tampa's Raymond James Stadium during a covert trial of the technology at the nation's premiere sporting spectacle, Tampa City Council approved a one-year trial (later extended to two years) of the FaceIt technology provided by the biometric company Visionics (Gates, 2011, pp. 75–76). This was despite the fact that the Super Bowl trial did not yield a single arrest, although it did generate 19 possible matches of faces with outstanding warrants from a pool of 71,000 attendees (Rogers, 2016). The officer who later convinced the city to test the technology in Tampa's Ybor City entertainment district acknowledged the limitations of the system at Super Bowl XXXV: "We thought we were ready to use it, but getting through the crowd and the architecture of the stadium proved overwhelming" (Chokshi, 2019, para. 7). In response to public concerns about the migration of the surveillance technology from the Super Bowl to general police use in Ybor City, one city council member observed, "It's a public safety tool, no different than having a cop walking around with a mug shot" (Canedy, 2001, para. 5). Despite its apparently awesome technological capacity, the Tampa experiment was ultimately deemed ineffective and discontinued after two years. As a spokesman for the Tampa Police said, "We never identified, were alerted to, or caught any criminal. . . . It didn't work" ("Tampa Drops," 2003, para. 2).

That damning verdict was delivered almost two decades ago. Developers of facial recognition systems claim their technologies have become much more effective at scale in the interim. One company, for example, promotes its products with the claim that whereas an average human can only remember and identify up to 1,500 faces, automated systems can scan 1.4 million facial images per second (FaceFirst, 2020). However, concerns about both accuracy and bias remain. Though overall accuracy statistics are difficult to obtain given the range of companies and systems in use, a report by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) found large improvements in accuracy in recent years. In 2018, most algorithms outperformed those from five years earlier, with NIST reporting very low average failure rates (with 0.2% of searches failing to match the correct image; Grother, Ngan, & Hanaoka, 2018, p. 2). This sounds extraordinarily accurate, but it is worth noting that the test matched "good quality portrait photos" to images in a stored database—a very different proposition from capturing images of faces in a crowd and then matching them to a stored database in real time (Grother et al., 2018, p. 2). In live trials of one-to-many matching, the accuracy rate drops precipitously. For example, a 2019 study of the London Metropolitan Police Force's facial recognition system found a high level of misidentification—more than 80%—leading the researchers to conclude that use of the technology should be discontinued (Brewster, 2019).

The NIST study also found high levels of bias with respect to race and gender in the accuracy of facial recognition algorithms. Even when doing one-to-one matching, there was a recurring tendency to falsely identify

> African-American and Asian faces between 10 to 100 times more than Caucasian ones . . . and African-American females were more likely to be misidentified in so-called one-to-many matching, which compares a particular photo to many others in a database. ("Facial Recognition Fails," 2019, para. 9)

Despite these limitations, the push to develop and implement facial recognition technology remains strong, as demonstrated by the highly publicized use of these systems for a growing range of purposes across law enforcement, commerce, and the workplace.

In keeping with the initial test in Tampa, sports stadiums remain a primary site for the deployment and marketing of facial recognition technology. NEC has trialed and operated its systems throughout South America, Asia, and the UK. It first trialed its stadium system in late 2015 at the Atanasio Girardot Stadium in Medellín, Colombia, in response to concerns about hooliganism and fighting in the 40,000-seat stadium (NEC, 2016). The system allowed security to match images captured on 170 high-resolution cameras throughout the stadium with a database of known offenders. It also used AI to "automatically detect unusual or suspect behavior in real time, and to quickly send notification to stadium staff in order to help resolve any potential issues" (NEC, 2016, para. 4). These so-called smart camera systems create new information for the database, feeding an "efficiency cycle" whereby "hundreds of people are analyzed by the monitoring system all the time and when a disturbing or violent situation is identified, the cameras capture the faces of the involved individuals, increasing safety and also feeding the 'blacklist' database" (NEC, 2017, p. 2).

This combination of identification and preemption is an emerging theme in the promotion of facial recognition systems, which promise not just to identify individual faces but also patterns of behavior and interactions: inaugurating a physiognomy of the stadium itself. In 2018, NEC installed a facial recognition system in Jakarta's Gelora Bung Karno Stadium; in addition to matching faces with police databases, it could be used to "detect suspicious objects and intrusions into restricted areas" (Nott, 2019, p. 72). Other stadiums using NEC technology include the Arena da Baixada in Brazil, facilities for the annual Universiade multisports event in Taipei, and stadiums in Uruguay, China, and Chile. In the United Kingdom, NEC's facial recognition systems have been used by police at Cardiff City Stadium, drawing public protests from football fans who donned masks and sang, "We are Cardiff City, you can't see our eyes" (Wightwick, 2020, para. 3).

Other technology providers have found Australasia a receptive market for facial recognition technology in stadiums, including at the 2018 Gold Coast Commonwealth Games, Westpac Stadium in Wellington, the Sydney Cricket Ground, Optus Stadium in Perth, and arenas operated by Stadiums Queensland (SQ). Citing "security reasons," SQ representatives initially refused to reveal which of its facilities were using facial recognition technology and offered only the long-standing warning that CCTV cameras were in use for security purposes (Bavas, 2019, para. 19). This covert implementation is in sharp contrast to conditions imposed by Europe's General Data Protection Rules (GDPR). In Denmark, for instance, security staff for the football club Brondby IF deploy the technology in accordance with the requirements of the GDPR. This involves notifying those entering the stadium about the system, deleting watch list photos at the end of the day, cross-checking images to avoid false positives, and insulating the system from the Internet. These measures have not, however, prevented well-founded criticism by digital rights advocates about the invasiveness and inaccuracies of facial recognition systems (Overgaard, 2019).

Dromology in the Stadium

Differing approaches to the use of facial recognition technology reflect contrasts in cultural and regulatory regimes, which place varying emphases on security, access, and convenience. Thus, the technology enacts a familiar split in the deployment of surveillance systems more generally: the promise of access, customization, and convenience for some groups and, in stark contrast, detention, punishment, and exclusion for others. In both cases, the salient features are scope and speed. The stadium is a symbolically suggestive space for the deployment of the technology, exemplifying what critical urbanist Paul Virilio (1997) describes as the logics of the "dromosphere" (p. 22)—the imperative of the race.

Virilio coined the term "dromology" (from *dromos*, the Greek word for a race track) to describe the study of speed in political and technological contexts: "The history of the world is not only about the political economy of riches—that is, wealth, money, capital, but also about the political economy of speed. If time is money, as they say, then speed is power" (Armitage, 2001, p. 26). The stadium is not just a setting for the spectacle of speed and power on the field (and the video screens that blanket the stadium), but also for the rapid sorting, identification, and processing of spectators in accordance with economic and securitized stratification. At the heart of these developments is the velocity of automated recognition: the capability to recognize "tens of thousands in a nanosecond" (Nott, 2019, para. 11) and to discern scenarios of risk and opportunity as they arise in real time. The links among speed, competition, and technology position the sports stadium as a setting to test and perfect techniques of social control, as Giulianotti (2005) observes in his reading of Virilio:

> The instantaneous digital mediation of sports symbolizes the high-tech potency of the white-dominated West's military-industrial complexes. . . . Strategically, the surveillance and social control of sports spectators using advanced gadgetry, allow the military industrial complex to test its latest techniques in case of more overt political resistance. . . . Thus Virilio promotes our general understanding of how time-space compression connects to technological exercises of power. (p. 177; see also Redhead, 2007)

With an eye to what constitutes "the win," the following sections draw on the case study of NEC's role in the Tokyo Olympics to explore three defining elements of the promise of facial recognition technology: preemption, convergence, and ubiquity.

Securitization as Preemption

The promotional literature for NEC's stadium facial recognition system slips smoothly from individual identification to pattern recognition. If the rapid identification of individuals facilitates social sorting, pattern recognition enables the identification of troublesome or threatening behavior (or, on the other hand, potential marketing opportunities). Automated scanning ensures that people on a designated watch list can be identified and removed before causing trouble. But this limits the field of action to known bad actors. To address the security gaps pried open by the element of surprise, NEC (2018b) claims its cameras have the ability to identify *potentially* threatening or disruptive activity: "It can detect such behavior among a crowd of people using the latest in video analytics and artificial intelligence" (p. 7). In an echo of recent developments in so-called predictive policing, another major player in the stadium surveillance market, FaceFirst (2020), claims that its "real time analytics help you stop crimes before they start" (p. 2).

Making cameras "smart" marks the shift from deterrence to preemption (Andrejevic, 2019). To the extent that CCTV has a deterrent effect, this is predicated on the disciplining assumption that subjects alter their behavior in response to the spectacle of surveillance. This is the classic formulation of panoptic power according to Michel Foucault (2012): that surveillance relies on the internalization by monitored subjects of the behavioral norms enforced by authorities. The automated system described by NEC, however, does not rely solely on subjects internalizing the monitoring gaze; it also discerns patterns of suspicious behavior to enable authorities to intervene in real time, as the behavior takes shape. In other words, the promise of automation captures what Virilio (1994) describes as "the technological processes of foresight and anticipation" (p. 6).

The appeal of digital "clairvoyance" emerges against the background of the post-9/11 formulation of the terrorist threat, which is a recurring frame in the deployment of stadium surveillance. An NEC (2018b) white paper on facial recognition in stadiums notes the short interval between the Tampa Super Bowl trial in January 2001 and the subsequent 9/11 terror strike on New York: "Security has since been a foremost concern in not just stadiums, but all public infrastructures" (p. 6). Following on from the 2015 Paris terror attacks that commenced at Stade de France as the national football team played Germany, the NEC (2018b) white paper invokes security concerns triggered by a 2017 suicide bombing at an Ariana Grande concert in the Manchester Arena: "Undeniably, stadiums and large event venues have become areas where security against such attacks has been beefed up in recent years" (p. 6). As Bennett and Haggerty (2012) observe,

> In the aftermath of 9/11 there has been an enormous growth in the security industrial complex which has targeted mega-events as a lucrative opportunity to sell advanced security products. Hence, the drivers are often not what is necessary in light of the objective risk—something that is hard to determine—but what is the latest and greatest. (p. 6)

This observation is consistent with a stunning 800% jump in the security budget for the 2004 Athens Olympic Games compared with Sydney in 2000, as well as the International Olympic Committee (IOC) taking out an insurance policy against the risk of cancellation due to international terrorism for the first time during the same time period (Sugden, 2012).

The goal of discerning potential threats (and opportunities) in their moment of emergence underwrites the imperative of comprehensive and continuous monitoring. As Ben Anderson (2011) observes in his discussion of technologies of counterinsurgency, the framing of the terrorist threat "as a potential distributed everywhere and conditioned by everything and anything" results in the imperative of surveillance that extends "throughout life without limit" (p. 224). This logic can be generalized to encompass routine security concerns. As the NEC (2018b) report notes, the threat of terror attacks

> is just one of the many challenges facing stadium owners and large event organizers today. When it comes to security, there are more mundane everyday problems that are *just as vexing*. For example, hooligans and gangs who congregate at stadiums to create trouble and engage in anti-social behavior. (p. 7, emphasis added)

This is a significant slippage (from the threat of terrorist attack to that of antisocial behavior) that serves to legitimate the general deployment of exceptional security measures, habituating sport fans to an increasingly comprehensive monitoring regime.

The related strategies of exclusion and preemption rely on two different types of information processing. The former entails the creation of a database of known potential threats: an ID-based system that facilitates the social sorting of stadium entrants into those who will be allowed access and those to be denied. Preemption, by contrast, relies on machine learning to discern *patterns* of potential threat without the need for positive identification and can generate new data on undesirables to be fed back into the ID-based system. In the case of Stadiums Queensland, however, one of the original responses to public concern about the undisclosed use of smart camera technology was to claim the cameras were used only "to identify patterns and anomalies in crowd behavior [such as abandoned bags or long queues]" (Bavas, 2019, para. 17). Such claims are impossible to verify in the absence of greater transparency.

"Facial Loyalty"

The deployment of automated facial recognition exhibits a familiar hallmark of digital convergence: the oscillation between risk and opportunity. Biometric surveillance, we are promised, can be used to minimize threat *and* maximize convenience and profit. The promotional literature on the use of such technology in stadiums moves seamlessly between these two functions, based in part on the framing of foregone economic opportunity as a form of financial risk. As the NEC (2018b) white paper on stadium use of facial recognition states, "By recognizing who is turning up, face recognition also opens up the opportunity to provide a superior experience to VIPs. Event sponsors or media representatives, for example, can be pre-registered and allowed in more easily" (p. 17). This sentiment is echoed in the marketing materials of the California-based company FaceFirst (2020): "Event management isn't just about keeping out the wrong fans. It's also about taking care of your VIPs. Identify premium season ticket holders as they enter, and boost retention by offering a range of VIP services" (p. 4).

Taking a cue from data driven social sorting online, automated biometric systems promise to customize services and marketing on a mass scale. As NEC's website promises, "With facial recognition and a unified biometric key, a frictionless and personalized fan experience can increase loyalty and spending" (NEC, 2020b, para. 6). The site outlines a suite of potential benefits associated with biometric identification and sorting, including accelerated access and transactions, customized greetings on special occasions (birthdays, anniversaries, etc.), and tiered service (automatic access to VIP lounges and other designated spaces). Once the face serves as a machine-readable form of ID, it can also allow "fans to 'pay with their face'" and receive *Minority-Report*-style customized solicitations: "Intelligent customized displays can make suggestions in the concession or souvenir area dependent on previous fan activity" (NEC, 2020b, para. 10). NEC has coined the term "Facial Loyalty" to describe "self-ordering kiosks" that "can also make recommendations based on past food orders for faster decision making" (NEC, 2020b, para. 10).

The formula is a familiar one: the promise of "recognition" in the form of customized goods and services in exchange for willing inscription into a system for comprehensive and continuous monitoring. The result is increased social sorting—the ongoing process of consumer stratification, from tiered to individualized forms of marketing and service. On the one hand, the "banopticon" (Bigo, 2008, p. 20) screens for suspected troublemakers to exclude, while on the other, facial recognition provides enhanced opportunities for target marketing, personalized advertising, and market stratification. Predictably ignoring the problems of platform capitalism (Srnicek, 2017), the global professional services firm Deloitte (2020) peddles the "transformative potential" (p. 7) of the stadium as a technological and commercial "platform" built to extract data and "unlock new revenue streams" (p. 11):

> While we mean "platform" to refer to the entirety of the stadium business model, at its core is a technology ecosystem, the collection of hardware, software and tools that allow people to access and build on top of the stadium's core infrastructure and systems. (p. 9)

Thanks to AI-enhanced forms of pattern recognition and the new categories of data that can be captured via smart camera systems, the stadium becomes a site for data aggregation and intensified marketization. The promise of customization comes full circle, moving from mass customized commerce to targeted, individualized, and customized securitization. Rather than a "one-size-fits-all" model, "you can provide your security team with personalized directives specific to each suspected individual in order to keep fans and employees safe from harm" (FaceFirst, 2020, p. 3).

Dromo-Logics of Space and Flow

The imperatives of speed and efficiency manifest themselves not only in the affordances of the technology, which outstrips human vision and recall, but also in the rearrangement of the space of the stadium and the flow of people through it. The trade literature repeatedly emphasizes the role of the technology in facilitating entry for fans and in creating tiered services for VIPs and big spenders. Just as smart cars promise to decompress our highways, smart cameras offer to dispel stadium congestion: the long lines at entrances, concession stands, ticket booths, and restrooms (Yang & Cole, 2020). Although lines may draw attention to particular opportunities, they add friction to consumption of both the spectacle and the commodities that underwrite it:

> When an individual has to stand in line to enter the venue, purchase concessions or merchandise, they become frustrated while missing out on the event they came to see. With advanced recognition systems, a fan's face is the unified biometric key to unlocking the door to a more positive experience. (NEC, 2020b, para. 9)

The experience may be more positive for some than others, with privileged categories of fans provided expedited access. The "blacklists" associated with the security function are complemented by the creation of "whitelists" of preferred customers on the marketing side (NEC, 2018b, p. 17). The terminology here is particularly unfortunate, given the recurring evidence of racial bias in facial recognition systems.

For the Tokyo Olympics, NEC envisions a system in which all accredited individuals, ranging from ticket holders to athletes, supply a headshot used to match the images caught by smart cameras. This system is designed to take the place of slower and less accurate forms of ID matching, helping to facilitate the efficient flow of people throughout the event space. The automation of recognition on a mass scale relies on the proliferation and circulation of surveillance devices throughout the stadium—not just at checkpoints, but wherever threat or opportunity might emerge. The advantage of using stadiums for this purpose is that existing closed-circuit camera systems can be upgraded to incorporate "smart" technology. Nonetheless, the multiple uses of facial recognition technology require more comprehensive coverage than existing systems provide—and in some cases, more appropriate angles, since the overhead view from surveillance cameras differs from the face-on perspective characteristic of reference photos fed into the database.

Thus, NEC is partnering with two of Japan's largest security companies to augment existing camera infrastructures for the Tokyo Olympics. The cameras themselves become mobile to cover the event space as thoroughly as possible. One company (Secom) will "equip guards with smartphones that will be clipped to their shirts, turning them into 'walking cameras'" (Ryall, 2018, para. 11). The other (Alsok) is helping "reduce the workload of human guards" with a fleet of drones that can hover over the stadium for up to eight hours without a break ("Tokyo Transforming," 2018, para. 8). Some reports claim the drones will be weaponized with lasers or projectiles to shoot down other, unauthorized, drones entering the event airspace, potentially staging an additional spectacle above the sporting action (Ryall, 2018).

The corollary of "friction-free" management of movement and interaction in the event space of the stadium is flexible, distributed, and ubiquitous monitoring. More surveillance, suggestively, underwrites the promise of greater freedom of movement—for approved individuals. As NEC (2017) puts it, "Thanks to the use of the facial identification used at the admission and grandstands, we can have a situational control, also with no need of barriers between the audience and the stage where the show develops" (p. 2). Rigid physical barriers give way to digitally monitored ones, accompanied by the rapid deployment of security forces and marketing appeals. This is the model of technological control engineered for the spectacular space of the stadium that provides a testing ground for a reconfigured relationship between surveillance and sociality.

Conclusion: Securitized Consumption Meets Viral Threat

The facial recognition technology showcase prepared for the 2020 Olympics has been postponed in response to the COVID-19 pandemic, which nonetheless opens up a related market for ubiquitous biometric monitoring and tracking. NEC, predictably, has jumped on the bandwagon, developing infrared monitoring systems and facial recognition to trace crowd symptoms and track social distancing—tools it is pioneering in its own offices (Burt, 2020). The challenge posed by the circulation of people under pandemic conditions is not just to facilitate and accelerate movement, but to simultaneously minimize the forms of social contact that enable viral spread. The emerging goal is transactional "touchlessness," combined with automated monitoring of personal contacts. The ability to use automated technology to monitor individuals in a crowd is framed as an alternative to the economic threat of curtailing circulation altogether.

According to one report, the pandemic has boosted sales of security drones, which are "essentially acting as a platform for various cameras for facial recognition and crowd control" ("COVID-19 Accelerates," 2020, para. 5). The pandemic may well serve as an accelerant for the broader deployment of crowd monitoring and control technologies beyond the walls of the stadium. In Australia, for example, NEC's corporate communications manager predicted that the pandemic would "fast track" plans to use facial recognition for touchless access points to services such as mass transit. He claims the technology can provide the same benefits for commuters as stadium-goers—with the added hygienic benefits of touch-free access:

> Notwithstanding the obvious health benefits of thousands of commuters not having to physically touch a card reader each time they pass through an entry or exit point, just think of the improvements in speed of people movement and safety at crowded train stations and ferry and bus terminals. (White, 2020, para. 8)

In the United States, NEC has merged facial recognition technology with thermal imaging to provide a Hawaiian airport with automated symptom tracking capability. The goal is to identify travelers who may be running a fever and remove them from circulation, thus limiting viral spread. The thermal image system scans crowds at checkpoints to identify individuals who may be running a fever and shares an image of these individuals with security employees who roam the airport. As NEC's (2020a) press release states:

> Without the use of facial recognition technology, an employee would need to be next to each camera at all times to pull a person aside as they walk by the camera, creating bottlenecks and further exposing employees to travelers and, thus, possible COVID-19 infection. (para. 12)

The obvious next step is to equip the employees with portable face and temperature-scanning devices so they can become "walking sensors," like the Secom employees ready to be deployed at the Tokyo Olympic Games.

The current postponement of the Olympics does not defer the generalized diffusion of the technology it is scheduled to preview. Rather, the extended "moment" of exception called into being by the global pandemic is serving as a warrant for new forms of high-speed individual recognition on a mass scale. The delay of the Games adds an additional layer to the securitized consumption imperative: that of public health and hygiene. The example of the stadium provides a template for the widespread implementation of mass-customized monitoring, foreshadowing the shape that this implementation might take in all three contexts: security, commerce, and public health. Extrapolating from the example of the Tokyo Games, biometric sensors might not simply enable detection of existing risks (such as feverish individuals), but also potentially harmful patterns of interaction, profiles of high-risk individuals (based on behavior or other demographic traits), and even economic opportunities—such as, to imagine a dystopian example, charging a premium for access to spaces that include only individuals with a low risk of infection.

Automated biometric technology anticipates what might be described as the mass customization of population management, merging what Foucault (2003, 2007) describes as disciplinary and biopolitical forms of power. The former focuses on individual bodies and the latter on overall statistical outcomes (morbidity and mortality rates, for example), meaning that the two levels of governance rely on different monitoring strategies. Discipline requires individual identification and direct action on bodies, whereas biopolitics relies on the description of overall patterns and environmental level response (Foucault, 2003). Mass identification "at-a-distance" reconfigures these distinctions. If the faces of all individuals in a crowd can be identified in real time, action on the population and the individual can take place in a coordinated and simultaneous fashion. This combination, in turn, drives the development of techniques for customized response at the mass level: physical environments that selectively enable or thwart the circulation of specified individuals, or that impose regimens of behavior on them—sorting out those who are required to wear masks, for instance, or disciplining those who are found to be in violation of social distancing restrictions.

The stadium serves as a testing ground for these hybrid strategies and the proliferation of monitoring systems that normalize the enclosure and segmentation of social space, movement, and interactions. The history of stadium surveillance suggests the deployment of such technologies is likely to be less seamless than the trade literature promises, but the plans for the Tokyo Games, combined with existing forms of stadium surveillance, reveal the priorities that shape the coming generation of biometric surveillance. At a time when the stadiums themselves are emptied out because of a communicable virus, they simultaneously provide a model for the governance of circulation that threatens to characterize our new “normal”—one in which shared space is structured, along the lines of the stadium, as a seeing and sorting machine.

References

Anderson, B. (2011). Facing the future enemy: US counterinsurgency doctrine and the pre-insurgent. *Theory, Culture & Society*, *28*(7/8), 216–240. doi:10.1177/0263276411423039

Andrejevic, M. (2007). Surveillance in the digital enclosure. *The Communication Review*, *10*(4), 295–317. doi:10.1080/10714420701715365

Andrejevic, M. (2019). Automating surveillance. *Surveillance & Society, 17*(1/2), 7–13. doi:10.24908/ss.v17i1/2.12930

Armitage, J. (Ed.). (2001). *Virilio live: Selected interviews*. London, UK: SAGE Publications.

Bale, J. (1993). *Sport, space and the city*. London, UK: Routledge.

Bavas, J. (2019, June 5). Facial recognition quietly switched on at Queensland stadiums, sparking privacy concerns. *ABC News*. Retrieved from https://www.abc.net.au/news/2019-06-05/facial-recognition-quietly-switched-on-at-queensland-stadiums/11178334

Bennett, C. J., & Haggerty, K. (2012). Security games: Surveillance and control at mega-events. In C. J. Bennett & K. Haggerty (Eds.), *Security games: Surveillance and control at mega-events* (pp. 1–19). London, UK: Routledge.

Bentham, J. (1995). *The panopticon writings.* London, UK: Verso.

Bigo, D. (2008). Globalized (in) security: The field and the ban-opticon. In D. Bigo & A. Tsoukala (Eds.), *Terror, insecurity and liberty: Illiberal practices of liberal regimes after 9/11* (pp. 20–58). London, UK: Routledge.

Boykoff, J. (2014). *Celebration capitalism and the Olympic Games.* New York, NY: Routledge.

Boykoff, J., & Gaffney, C. (2020). The Tokyo 2020 Games and the end of Olympic history. *Capitalism Nature Socialism, 31*(2), 1–19. doi:10.1080/10455752.2020.1738053

Boyle, P., & Haggerty, K. (2011). *Privacy games: The Vancouver Olympics, privacy and surveillance: A report to the Office of the Privacy Commissioner of Canada under the contributions program*. Alberta, Canada: University of Alberta, Department of Sociology.

Boyle, P., & Haggerty, K. (2012). Planning for the worst: Risk, uncertainty and the Olympic Games. *British Journal of Sociology*, *63*(2), 241–59. doi:10.1111/j.1468-4446.2012.01408.x

Brewster, T. (2019, July 4). London police facial recognition "fails 80% of the time and must stop now." *Forbes*. Retrieved from https://www.forbes.com/sites/thomasbrewster/2019/07/04/london-police-facial-recognition-fails-80-of-the-time-and-must-stop-now/#8e2d36ebf950

Burt, C. (2020, July 13). *Real-time facial biometrics for COVID-19 response piloted at NEC headquarters and launched by Herta*. Retrieved from https://www.biometricupdate.com/202007/real-time-facial-biometrics-for-covid-19-response-piloted-at-nec-headquarters-and-launched-by-herta

Canedy, D. (2001, July 4). Tampa scans the faces in its crowds for criminals. *The New York Times.* Retrieved from https://www.nytimes.com/2001/07/04/us/tampa-scans-the-faces-in-its-crowds-for-criminals.html

Chokshi, N. (2019, May 15). Facial recognition's many controversies, from stadium surveillance to racist software. *The New York Times*. Retrieved from https://www.nytimes.com/2019/05/15/business/facial-recognition-software-controversy.html

Cisco connected stadium. (2020). Retrieved from https://www.cisco.com/c/en/us/solutions/industries/sports-entertainment/connected-stadium.html

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, *20*(4), 336–349. doi:10.1177/1527476418796632

Delfanti, A., & Frey, B. (2020). Humanly extended automation or the future of work seen through Amazon patents. *Science, Technology, & Human Values*, 1–28. doi:10.1177/0162243920943665

Deloitte. (2020). *The stadium as a platform: A new model for integrating venue technology into sports business.* Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consumer-business/us-cb-the-stadium-as-a-platform-final.pdf

Dyreson, M. (2013). Prologue—Cathedrals of sport: Mapping new territories. In M. Dyreson & R. Trumpbour (Eds.), *The rise of stadiums in the modern United States: Cathedrals of sport* (pp. 1–7). Abingdon, UK: Routledge.

COVID-19 accelerates the adoption of civil drone shipments, nearly doubling 2020 pre-pandemic forecast. (2020*,* July 3). *ENP Newswire*. Retrieved from https://www.eenewseurope.com/news/civil-drone-adoption-accelerates-wake-covid-19

FaceFirst. (2020). *The five minute guide to face recognition for event security.* Retrieved from https://www.facefirst.com/blog/5-minute-guide-for-retail

Facial recognition fails on race, government study says. (2019, December 20). *BBC News.* Retrieved from https://www.bbc.com/news/technology-50865437

Foucault, M. (2003). *"Society must be defended": Lectures at the Collège de France, 1975–1976*. London, UK: Allen Lane.

Foucault, M. (2007). *Security, territory, population: Lectures at the Collège de France, 1977–78*. Basingstoke, UK: Palgrave Macmillan.

Foucault, M. (2012). *Discipline and punish: The birth of the prison*. New York, NY: Vintage.

Frank, S., & Steets, S. (2010). The stadium: Lens and refuge. In S. Frank & S. Streets (Eds.), *Stadium worlds: Football, space and the built environment* (pp. 278–294)*.* Abingdon, UK: Routledge.

Gates, K. A. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance* (Vol. 2). New York: New York University Press.

Giulianotti, R. (2005). *Sport: A critical sociology.* Cambridge, UK: Polity.

Giulianotti, R. (2011). Sports mega events, urban football carnivals and securitised commodification: The case of the English Premier League. *Urban Studies, 48*(15), 3293–3310. doi:10.1177/0042098011422395

Giulianotti, R., & Klauser, F. (2010). Security governance and sport mega-events: Toward an interdisciplinary research agenda. *Journal of Sport and Social Issues*, *34*(1), 49–61. doi:10.1177/0193723509354042

Grother, P., Ngan, M., & Hanaoka, K. (2018). *Ongoing face recognition vendor test (FRVT), Part 2: Identification*. Washington, DC: National Institute of Standards and Technology.

Guttmann, A. (2004). *From ritual to record: The nature of modern sports.* New York, NY: Columbia University Press. (Original work published 1978)

Holt, R. (1989). *Sport and the British: A modern history*. Oxford, UK: Clarendon.

Horne, J., & Whannel, G. (2012). *Understanding the Olympics.* Abingdon, UK: Routledge.

Hutchins, B. (2016). "We don't need no stinking smartphones!" Live stadium sports events, mediatization and the non-use of mobile media. *Media, Culture & Society*, *38*(3), 420–436. doi:10.1177/0163443716635862

Hutchins, B. (2019). Mobile media sport: The case for building a mobile media and communications research agenda. *Communication & Sport*, *7*(4), 466–487. doi:10.1177/2167479518788833

Interdigital. (2016). *White paper: How will the Olympics shape 5G?* London, UK: Mobile World Live.

Jamison, B. (1996). The Sandgate Handicap riot: Sport, popular culture and working class protest. *Sporting Traditions*, *12*(2), 17–48.

Mosco, V. (2014). *To the cloud: Big data in a turbulent world*. Boulder, CO: Paradigm.

Mthethwa, N. (2010, January 24). How SA will secure the soccer World Cup. *PoliticsWeb*. Retrieved from https://www.politicsweb.co.za/opinion/how-sa-will-secure-the-soccer-world-cup--mthethwa

NEC. (2016, October 12). *NEC contributes to football stadium safety in Colombia* [Press release]. Retrieved from https://www.nec.com/en/press/201610/global_20161012_03.html

NEC. (2017). *Integrated surveillance and security system for stadium* [Press release]. Retrieved from https://sg.nec.com/en_SG/pdf/brochures/PublicSafety/Atanasio_Girardot_Stadium-Medellin.pdf

NEC. (2018a). *Bio-IDiom—NEC's biometric authentication brand*. Retrieved from https://www.nec.com/en/global/techrep/journal/g18/n02/180203.html

NEC. (2018b). *Finding a face in a crowded arena*. Retrieved from https://in.nec.com/en_IN/en/global/solutions/safety/resourcecenter/pdf/crowded_arena.pdf

NEC. (2020a, July 17). *NEC-led team to provide Hawaii's airports with passenger screening technology* [Press release]. Retrieved from https://www.nec.com/en/press/202007/global_20200717_02.html

NEC. (2020b). *With stadium facial recognition, the fan experience is #1.* Retrieved from https://nectoday.com/tag/unified-biometric-key

Nott, G. (2019, June 6). *NEC face recognition tech to screen athletes at Tokyo 2020*. Retrieved from https://www2.computerworld.com.au/article/662573/nec-face-recognition-tech-screen-athletes-tokyo-2020

Overgaard, S. (2019, October 21). A soccer team in Denmark is using facial recognition to stop unruly fans. *National Public Radio*. Retrieved from https://www.npr.org/2019/10/21/770280447/a-soccer-team-in-denmark-is-using-facial-recognition-to-stop-unruly-fans

Palvarini, P., & Tosi, S. (2013). Stadiums as studios: How the media shape space in the new Juventus Stadium. *First Monday*, *18*(11). Retrieved from https://firstmonday.org/ojs/index.php/fm/article/view/4959/3791

Perelman, M. (2012). *Barbaric sport: A global plague*. London, UK: Verso.

Redhead, S. (2007). "Those absent from the stadium are always right": Accelerated culture, sport media, and theory at the speed of light. *Journal of Sport and Social Issues*, *31*(3), 226–241. doi:10.1177/0193723507301051

Roche, M. (2017). *Mega-events and social change: Spectacle, legacy and public culture.* Manchester, UK: Manchester University Press.

Roche, M. (2000). *Mega-events and modernity: Olympics and expos in the growth of global culture.* London, UK: Routledge.

Rogers, K. (2016, February 8). *That time the Super Bowl secretly used facial recognition software on fans*. Retrieved from https://www.vice.com/en_us/article/kb78de/that-time-the-super-bowl-secretly-used-facial-recognition-software-on-fans

Ryall, J. (2018, September 6). Games changer: Technology that will innovate the Olympics in 2020. *Japan Today*. Retrieved from https://japantoday.com/category/tech/games-changer-technology-that-will-innovate-the-olympics-in-2020

Silverman, R. (2016, September 15). *The Rio Olympics' legacy is a cyber-surveillance state*. Retrieved from https://www.vocativ.com/352054/the-rio-olympics-legacy-is-a-cyber-surveillance-state/index.html

Srnicek, N. (2017). *Platform capitalism*. Cambridge, UK: Polity.

Sugden, J. (2012). "Watched by the Games: Surveillance and security at the Games." In J. Sugden & A. Tomlinson (Eds.), *Watching the Olympics: Politics, power and representation* (pp. 228–241). Abingdon, UK: Routledge.

Tampa drops face-recognition system. (2003, August 21). Retrieved from https://www.cnet.com/news/tampa-drops-face-recognition-system

Tokyo transforming to boost productivity, diversity. (2018, July 30). *Financial Tribune*. Retrieved from https://financialtribune.com/articles/world-economy/90790/tokyo-transforming-to-boost-productivity-diversity

Vamplew, W. (1985). *Pay up and play the game: Professional sport in Britain, 1875–1914.* Cambridge, UK: Cambridge University Press.

Virilio, P. (1994). *The vision machine*. Bloomington: Indiana University Press.

Virilio, P. (1997). *Open sky*. London, UK: Verso.

White, R. (2020, March 25). Is facial recognition an option as we look for coronavirus answers? [Blog post]. Retrieved from https://www.nec.com.au/insights/blog/facial-recognition-option-we-look-coronavirus-answers

Wightwick, A. (2020, January 12). Protest against police using facial recognition technology at the South Wales Derby. *Wales Online*. Retrieved from https://www.walesonline.co.uk/news/wales-news/protest-against-police-using-facial-17554862

Wilken, R. (2014). Places nearby: Facebook as a location-based social media platform. *New Media & Society, 16*(7), 1087–1103. doi:10.1177/1461444814543997

Yang, C., & Cole, C. L. (2020). Smart stadium as a laboratory of innovation: Technology, sport, and datafied normalization of the fans. *Communication & Sport*, 1–16. doi:10.1177/2167479520943579

Zinganel, M. (2010). The stadium as cash machine. In S. Frank & S. Steets (Eds.), *Stadium worlds: Football, space and the built environment* (pp. 77–97). Abingdon, UK: Routledge.