Routledge
Taylor & Francis Group

International Journal of Performance Arts and Digital Media

ISSN: 1479-4713 (Print) 2040-0934 (Online) Journal homepage: http://www.tandfonline.com/loi/rpdm20

URME Surveillance: performing privilege in the face of automation

Leonardo Selvaggio

To cite this article: Leonardo Selvaggio (2015) URME Surveillance: performing privilege in the face of automation, International Journal of Performance Arts and Digital Media, 11:2, 165-184, DOI: 10.1080/14794713.2015.1086138

To link to this article: http://dx.doi.org/10.1080/14794713.2015.1086138

International Journal of Performance Arts and Digital Media, 2015
Vol. 11, No. 2, 165–184, http://dx.doi.org/10.1080/14794713.2015.1086138

URME Surveillance: performing privilege in the face of automation

Leonardo Selvaggio*

Independent Artist, Chicago, IL, USA

URME Surveillance transforms my identity into a defense technology for the public's protection against facial recognition software. My work encourages the public to substitute their identity with my own by wearing a 3D printed prosthetic mask made in my likeness. This paper begins by examining the impetus that led me to creating this work, including the development of my artistic practice while living in Chicago, a city with a highly networked surveillance system. I then discuss the work of Adam Harvey and Zac Blas as two contemporary artists working with identity recognition technologies and their works' relationship to my own. Finally, I examine how *URME Surveillance* engages both the destabilization of White male privilege and public performance as a strategy to address systems of oppression inherent in surveillance and other structures of patriarchal power. While this paper assumes that the reader has a fundamental understanding of facial recognition technologies, it also asserts that the proliferation of such automated systems is alarming.

Keywords: identity; facial recognition; privilege; performance; prejudice; prosthetic; race; surveillance; subversion

I imagine a future where everyone wears my face, literally. Take a moment to consider this future. As you walk down the street to the subway, you pass by me over and over and over again. The sliding doors of the train open to a swarm of Leos. Some are tall lean elegant Leos while others are short, chubby, athletic, skinny compact or obese. All of them wear my face. A few are visibly female, while some of the others are male. The majority are more difficult to identify as either. As you get on, your eye catches the reflective plastic window of the door. My face stares back at you. You almost forgot that you put it on this morning. The train churns down the tracks and you realize that you have not really thought much about it, what people really look like. After all, you look at Leos all day, every day. You get off at your stop and head for the exit. As you walk up the stairs to street-level you catch a glimpse of an old rusted box with a camera lens on it hanging from the wall. You have to remind yourself that it is called a surveillance camera, not that you know why you should bother remembering what they are called. They have not been used in years.

In 2014, I launched *URME Surveillance*, an artistic intervention that protects the public from facial recognition surveillance systems by allowing them to substitute their face with my own by wearing a photo-realistic 3D printed prosthetic of my face. When

*Email: leo.selvaggio@gmail.com

a user dons the prosthetic, cameras equipped with facial recognition are likely to identify the wearer as myself, thus attributing all of their actions in surveilled public space to the identity known as 'Leo Selvaggio'. In this way, the wearers of the prosthetic safeguard their identities by convincingly performing my own in surveilled areas.

In addition to protecting the wearer, *URME Surveillance* also subverts and confounds large systems of surveillance through the creation of disinformation, primarily through asserting the presence of my identity to surveillance systems in areas of public space that my physical body does not in fact inhabit. For example, if multiple users were to wear my face and each become a 'Leo' in different areas of the same city at the same time, facial recognition systems would have conflicting locative information: the identity 'Leo Selvaggio' would be inhabiting more than one space at a time. Consequently, as the bodies of each individual wearer are different, there may also be inconsistent data gathered about my height, weight and gender. If one wearer is tall, athletic and female, while another wearer is short, rotund and male, then the collected data would reflect that 'Leo Selvaggio' is tall, short, athletic, rotund, female and male. Taken to its farthest conclusion the massive generation of contradictory data, as it relates to my identity in facial recognition databases, by users of *URME Surveillance* challenges and subverts facial recognition technology by questioning its efficacy to identify a body in space accurately. This subversion becomes all the more relevant as surveillance practices traditionally conducted by human beings are increasingly being turned over to automated systems under the false supposition that such systems are accurate and free of bias and prejudice which we will see is not in fact the case.

Before I discuss facial recognition systems in more detail, it would help the reader to have some context to my artistic practice, which informs both the goals and strategies used in *URME Surveillance*. As an artist, my practice revolves around creative research. I investigate and form hypotheses that I then experiment with, both in terms of concept and material, in the studio. The questions that arise from my investigations iteratively build upon each other to produce a focused and rigorous body of work, which never seems to be 'complete' and often inspire other lines of inquiry. As such, the research that eventually developed into *URME Surveillance* began in early 2012. At the time I was working with themes of identity, gender and the valued body when I was first introduced to the Open Source Movement in software.

According to the Open Source Initiative, 'Open source software is software that can be freely used, changed, and shared (in modified or unmodified form) by anyone. Open source software is made by many people' (Opensource.org, n.d.). In other words, open-source culture rejects the model that software needs to be designed in a capitalist corporate structure. Rather, it advocates for software to be both developed through community, in which each programmer adds to the contributions of the last programmer, and democratically distributed to others to use and modify outside of a profit structure. I began wondering what the intersection of open-source methodology and identity might look like. Several weeks later YouAreMe.net was born.

YouAreMe.net is an interactive web-based project in which my digital identity is offered freely for others to use as material any way they saw fit. The website provides several contexts for visitors to experiment with: control of my avatar in Second Life, images of my nude body to download and manipulate, an email account to write to others as me, 3D models of my body to integrate into video games, opportunities to author my biographical information, and logins and passwords for my social media

accounts such as Facebook and Twitter. For example, a visitor could log in to my Facebook account, interact with my friends, make new friends for me, or even potentially destroy my online relationships by posting messages as me. Like open source, which begins with a 'kernel' or base program that is then developed by others, YouAreMe.net began to ask who exactly could 'Leo Selvaggio' be if that identity were a matter of public discourse.

YouAreMe.net provided me with a critical outcome. Identity as it stands in our current technological state is highly unstable and susceptible to external influence. Susceptibility is not particularly new to identity. For example, gossip has always had a strong effect on how individual identity is perceived by others. However, the rate of proliferation and size of influence of something like gossip is exponentially increased online because its distribution and audience are often global. As such, individual authorship over one's identity is threatened by a model of digitally distributed authorship, one in which online identity is formed just as much by others as it is the individual. In our increasingly digitally networked society, identity can and should be thought of 'data' that can be developed, manipulated and edited. Social media has done for our identities what email and text messaging has done for our personal communication: it has provided individual with the curatorial opportunity to revise expressions and presentations of one's identity at the expense of immediacy, giving each of us greater control of how we are perceived by others as well as an unimaginable flexibility with our digital identity in comparison to just a decade or before. We can edit our Facebook posts to be funnier, apply filters to our Instagram selfies to be more attractive, decide what information to share with whom, etc. However identity can also be hacked or, as in the case of YouAreMe.net, outsourced, leaving individual identity pliable and permeable to both internal and external sources.

Over the next year and half I continued to develop these ideas around identity's malleability by extending my materials, audience and contexts. For example, in URME Mirror, I created and interactive digital installation in which a participant can see their face digitally replaced by my own on a monitor using a live webcam. As their movements in space are captured by the webcam, the software I designed tracks their face and in real time places a stable image of my face over theirs, resulting in, what I conceptualized at the time, as a hybrid identity. I questioned whose identity, if any, was being appropriated? Was the participant now Leo Selvaggio or vice versa? Could I assert that if the participant was female or danced with my face on theirs, that I could now be female and know how to dance when I could not beforehand?

Though up to this point there were certainly questions arising in my work about the supposed boundary between private and public space, information and its connection to identity, it was not until I worked on IMU: Google Street Portraits that I began to consider surveillance as it pertains to the performance of identity. IMU: Google Street Portraits is a video work that came about by accident. I was given the opportunity to produce a public work in an empty downtown Chicago retail window. It was raining on the day that I had decided to do an informal site visit. Not wanting to get wet, I decided to take an online Google walk to the location using Google Maps' street view feature. As I 'walked' there, the blurred faceless portraits of pedestrians created by Google's face recognition software haunted me. On their website Google explains:

> We have developed cutting-edge face and license plate blurring technology that is applied to all Street View images. This means that if one of our images contains an identifiable face (for example that of a passer-by on the sidewalk) or an identifiable license plate, our technology will automatically blur it out, meaning that the individual or the vehicle cannot be identified. (Google.com, n.d.)

Created in an attempt to mediate our right to privacy within its mapping technology, I began to question the success of Google's facial recognition algorithm. If this process occurs in post-production, where are the original image files with recognizable faces housed? Are they being used in ways we do not know? Is automation really an acceptable mediation of a surveillance practice in public space that happens to occur on a global scale?

Thus the video work became a composite of my several Google walks to the site juxtaposed with the faceless portraits I found along with way. In addition, I made my own portraits in which I digitally superimposed my face over the blank visages. Though similar in strategy, to URME Mirror, this work is conceptually very different. While URME Mirror played with hybridization and malleability of identity, IMU: Google Street Portraits began to hypothesize that identity could be used as a defense technology within the context of mass surveillance. My research then led me to investigate facial recognition, surveillance systems employing it and strategies artists have developed around it.

Facial recognition software has been one of the most developed surveillance technologies of the last 10 years and is now as pervasive a practice as the use cellular phones. In fact, facial recognition is now a key component of most smart phones, with Android and iPhones each have their own versions of Face Unlock, a system that will keep your phone locked unless the camera can recognize your face. As anthropologist Mark Mcguire states,

> Face recognition is at the vanguard of biometrics research and development for several reasons. Firstly, it rests upon the history of photography and is thus acceptable to the public whilst offering existing archives of face images. Secondly, despite problems arising from contexts where veiling is common, it is regarded as non-intrusive and contact-less. And, finally, cutting edge systems hold out the promise of allowing for security authentication and identification without stopping people moving. (Mcguire 2012, 600)

As Mcguire suggests, there is what amounts to an arms race to apply facial recognition to as many contexts as possible, specifically as it applies to mass surveillance systems. Furthermore MarketsandMarkets marketing firm reports that,

> It is expected that 21% of the global smart cities and smart buildings will embed face recognition technology in surveillance systems and access control systems by 2018 … Collaboration with major system integrators for implementation of large scale security solutions in these smart city or building projects will act as an ideal growth strategy for the facial recognition vendors in the long run. (Marketsandmarkets.com, n.d.)

One such city that has implemented a large-scale surveillance system is Chicago. The 25,000 federated security cameras that make up Chicago's surveillance program known as Virtual Shield (VS) also make Chicago the most widely surveilled city in the USA. What makes Chicago all the more frightening a case study for surveillance is that it is also the national leader in fiber optic networks. This means that the images

VS can collect from 'blue-light' cameras, cameras in public school, traffic cams, and those on buses and trains, can be easily transmitted throughout the city of Chicago through the vast network of fiber optic cables. In the case of VS, all surveillance images are aggregated to one centralized hub housed in the 911 Emergency Response Center. (Shah 2014)

Because the database of images is stored in single location, it becomes much easier to process all those images through VS's facial recognition system. According to The-Verge, an online news source, this enabled the Chicago Police Department to claim its first arrest and conviction using facial recognition to identify Pierre D. Martin for a crime in 2013, even though the validity of such a claim has come into question (facial recognition was not formally mentioned in the trial, nor was it mentioned in any CPD records) (Stroud 2014). As the Electronic Privacy Information Center, or EPIC, warns us about another large surveillance system, the FBI's 'Next Generation Identification' system,

> using a CCTV system linked to facial recognition, the police will be able to routinely identify individuals walking down a city street. If a particular individual is proximate to another person who is an actual suspect in an investigation, then that individual may also be added to the investigative database. This could be done routinely and automatically across a wide range of public activity all across the country. (EPIC 2013)

The implementation of such a system not only infringes on rights to privacy in America, but it also threatens the personal security and stability of our individual identities. As EPIC explains,

> Improper collection, storage, and use of this information [data collected through indiscriminate mass surveillance] can result in identity theft, inaccurate identifications, and infringement on constitutional rights. An individual's ability to control access to his or her identity, including determining when to reveal it, is an essential aspect of personal security and privacy that biometric identifiers [like facial recognition] erode. (EPIC 2013)

These systems, which are primarily forms of automated data collection, threaten the well-being of the American citizen. The inclusion of facial recognition in surveillance practices has had a profound effect on the way artists engage with and resist surveillance. Though there are various examples of our relationship to surveillance and identity in art dating back several decades, such as Bruce Nauman's *Video Corridor* (1970), several contemporary artists have shifted their strategies to include the face as a sight for intervention. Two such artists are Zach Blas and Adam Harvey, both of whom have been integral to the formation of my own work on the subject.

In 2013, Adam Harvey created *CV Dazzle*, a method that uses makeup to confound facial recognition software. As he put it,

> CV Dazzle uses avant-garde hairstyling and makeup designs to break apart the continuity of a face Since facial-recognition algorithms rely on the identification and spatial relationship of key facial features, like symmetry and tonal contours, one can block detection by creating an 'anti-face'. (Harvey 2013)

As Harvey points out, facial recognition works based on feature detection, such as analyzing the distance between each eye, or the size of a person's chin. Harvey is able

Figure 1. Monica Mclure is demonstrating the makeup techniques found in Adam Harvey's CV Dazzle. *Monica McClure*. Photography by Emily Raw.

to successfully change how these features appear to a camera by using makeup to alter the appearance of those features to the point that most surveillance systems cannot even detect a face let alone identify it. *CV Dazzle's* strength lies in its simplicity and in being fairly democratic as most Americans have access to some form of cosmetic makeup. It also favors individuals who enjoy extreme aesthetics and are comfortable presenting themselves in public space in ways that garner attention (Figure 1).

Harvey's work has enjoyed considerable attention and has been emulated and practiced by several groups. One of the most successful groups in adopting this aesthetic form of resistance is the 'Anti-Surveillance Feminist Poet Hair & Makeup Party' (ASFPH&MP). ASFPH&MP was created by Stephanie Young, a poet based in California, to adapt Harvey's techniques in order to disrupt the machine gaze of surveillance systems as well as the male gaze of the female form in public space. When discussing her motivations for creating such a group she stated,

> I wanted to be in alliance. Wanted more agency. To hide, to go hard, to be ugly. To ask who gets protected. Who pays. I wanted to be with young women in bustiers, middle aged women in onesies, old women in ruffles, women in peplum and big bauble necklaces, in hospitality sweaters, in disposable latex, poly, or vinyl gloves, in high-waisted shorts, in shapewear … . Your worst nightmare. (Young 2014)

Figure 2. *Natalie Eilbert*. Photography by Emily Raw.

In addition to privacy concerns, Harvey has created a system that can be adopted and appropriated by others to address other issues that stem from surveillance such as the Feminist discourse demonstrated by the ASFPH&MP (Figures 2 and 3).

Similarly, Zach Blas has been working on his *Facial Weaponization Suites* since 2011. His project consists of a series of prosthetic masks made from distorted 3D models of amalgamated faces. For example, his 'Fag Face' suite is a prosthetic comprised 3D scans of several queer men's faces that were collected through a series of community-based workshops. As with all his *Suites*, the face of each participant is scanned and then turned into 3D models. Afterwards, all the models are meshed together and distorted using 3D modeling software and then fabricated into a wearable mask. Because of the distorted features of these masks, when worn, they successfully hide faces from biometric scans and other forms of facial recognition (Figures 4 and 5).

When discussing the *Suites* Blas has said 'I wanted that process of collectivization to produce some kind of excess. When you first see those masks, there's something incredibly "othering" about them that you can't really parse' (Hiscott 2014). By engaging communities of 'others', Blas has been able to bring issues like border security and institutional racism to the foreground with his work. For example, in his work *Militancy*, *Vulnerability*, *Obfuscation*, Blas creates a Black *Suite* mask, made in a similar way to 'Fag Face', that 'explores a tripartite conception of blackness, divided between biometric racism (the inability of biometric technologies to detect

Figure 3. *Clara Lipfert, Natalie Eilbert, Emily Brandt, Marina Weiss, Carina Finn, Becca Klaver, Jennifer Tamayo*. Photography by Emily Raw.

Figure 4. *Facial Weaponization Suite: Fag Face Mask*. 20 October 2012, Los Angeles, CA. Photograph by Christopher O'Leary.

Figure 5. *Facial Weaponization Suite: Fag Face Scanning Station*. Reclaim: pride with the ONE Archives and RECAPS Magazine. Christopher Street West Pride Festival. West Hollywood, CA, 8 June 2013. Photograph by David Evans Frantz.

dark skin), the favoring of black in militant aesthetics, and black as that which informatically obfuscates' (Hiscott 2014). These black *Suites* are then used in protest lines in which 'the mask becomes this force of collectivization. It's hiding the individual face so this other, collective demand emerges' (Hiscott 2014) (Figure 6).

While having considerably different aesthetics and systems of distribution, these two projects fundamentally share the same strategy: protect the individual by hiding or occluding their face from security cameras. This idea of 'hiding' is in fact the

Figure 6. *Facial Weaponization Suite: Militancy, Vulnerability, Obfuscation*. Tableau vivant. San Diego, CA, 7 June 2013. Photograph by Tanner Cook.

most prevalent strategy both in and out of the art community offered to the public. The majority of YouTube videos on the subject of anti-surveillance include how-to videos involving the use of ski masks, hoodies and the hat/sunglasses combo. Unfortunately, these strategies of hiding often draw suspicion from onlookers as they are often associated with criminality and can have deadly repercussions. One recent example is the tragic case of Trayvon Martin, a Black teen whose death was blamed on his concealing his identity with a hoodie, rather than being the victim of a murder with serious racial undertones. In the case of Harvey and Blas, each of their projects have considerably extreme aesthetics which as forms of cultural expression that make them successful as bold, overt and public visual statements of resistance. However these aesthetics, by their very nature, will likely draw more attention to the user than would be useful for a practical anti-surveillance intervention. As Stephanie Young states, 'the [CV Dazzle] techniques make you more noticeable. Makeup otherwise used to highlight facial features instead disrupts symmetry and obscures those same features' (Young 2014). She goes on to add, 'It's not like you can just pull it [CV Dazzle] off and blend back into the crowd' (Young 2014).

In contrast to the important, yet overt public visual assertions made by Harvey and Blas, when considering how I might add to this ecology of art concerned with facial recognition, my goals became to rethink this prevailing strategy of 'hiding' through an artistic intervention that focused on subverting facial detection while retaining real-world functionality. Though Harvey and Blas' work is well suited for those willing to assert themselves in public space without fear of repercussion, I aimed to produce something others could use without drawing unwanted attention to themselves.

Thus when considering both Harvey and Blas' work, along with the majority of information provided to the public as jumping off points for my own work, I came to two conclusions. The first was that I needed to create a new strategy if I wanted results that did not immediately associate the wearer as suspicious or criminal. Simply continuing to hide a face with new aesthetics would not suffice. The second conclusion was that in addition to facial recognition systems, I had to consider the role of the general public as agents of surveillance as well. I required a strategy that would protect the user from being identified by cameras in the way that Harvey and Blas work does, but, aesthetically speaking, would also pass inconspicuously in a crowd of people.

These two conclusions led me to the strategy that would launch *URME Surveillance*: rather than hide a face, substitute it. Show the camera and the public a face, but not the actual user's face. Having already opened up my identity for others to use in YouAreMe.net, using my own face was a natural choice. Though I considered creating a fictional face, I decided that this would defeat the long-term purpose of my strategy. With facial recognition systems having the potential to access not only our public records but also searchable information on social media, it would only be a matter of time until the face was found to be a fraud. The most likely scenario would be that anyone using that face after a certain amount of time would be tagged as suspicious or perhaps even criminal. There was also the ethical concern that the face I created may inadvertently resemble an actual person who would be affected by a kind of identity fraud. Thus my face was easily accessible, attached to real-world data, and ethically speaking, was the only identity I was willing to put at risk (Figure 7).

Figure 7. *URME Surveillance*, 2014, courtesy of the artist Leo Selvaggio.

URME Surveillance primarily consists of two anti-surveillance devices, each using my face as its primary material: the URME Surveillance Identity Prosthetic, and the URME Paper Mask. The prosthetic came first conceptually, and based on my self-imposed criterion of functionality is the more successful of the two. The prosthetic is a photo-realistic, hard resin, 3D printed rendering of my face made by my partners at ThatsMyFace.com, a company with a proprietary technology that enables them to first create a 3D model of a person's face from a single image, and then print that face as a wearable mask (Figures 8 and 9).

Unlike other options like latex prosthetics, the photo realism does not come from air brushing over the prosthetic, but rather the color is injected directly into the material, like an ink-jet print. This results in the inside of the prosthetic, or the side of that touches the wearer's face, having all the photo-realistic features found on the outside, creating the illusion that one is putting on another person's skin when wearing the device. While the prosthetic has boundaries, such as the top of the brow, side of the face and the under part of the chin, that are detectable to the human eye upon inspection, normal expected elements such as hair, a scarf or a hat, dramatically increase its ability to pass undetected in a crowd of people. In addition, because most surveillance cameras operate at a significantly lower resolution than the human eye, the prosthetic blends seamlessly to all but HD cameras. This is important because up until now we have ignored the human element in surveillance systems such as a security officer. While interventions like those in Blas and Harvey's work thwart facial recognition by obscuring facial features, they offer little to prevent a human from tracking the user from camera to camera, a task easily accomplished on a network such as Chicago's VS. The nature of their aesthetics – pink blob and futuristic warrior paint – as with the majority of other strategies mentioned, make it easy for a human to spot, even on low-resolution cameras (Figure 10).

The URME prosthetic turns the weaknesses of these cameras into strengths. As mentioned above, the lower the resolution of the camera the higher a chance the prosthetic will pass undetected to a human watching a monitor because the edges appear to blend into the rest of the face, whereas in higher resolution systems those edges may be more visible to the human eye due to the larger amount of visual information available. Thus there is a direct correlation between low-image-resolution cameras, of which most surveillance systems use, and the prosthetic's ability to 'pass' as a real face on a set of surveillance monitors. In this way, the security officer or other human element will continue to track the prosthetic with conviction, believing that they are actually seeing the identity presented to them on camera, 'Leo Selvaggio' (Figures 11 and 12).

Figure 8. *URME Surveillance*, 2014, courtesy of the artist Leo Selvaggio.

Furthermore, as *URME*'s strategy is not to hide but rather substitute, it is simultaneously important that the camera recognize an identifiable face. The prosthetic is designed with all the same features that trigger facial recognition. In other words, the prosthetic works on two levels as a kind of recognition/misrecognition duality. The camera recognizes a face while the human does not recognize the face as a prosthetic. In this way, the URME Surveillance Identity Prosthetic falsifies the documentation created by surveillance convincingly. In doing so, *URME Surveillance* subverts networked systems as well as questions their efficacy by fooling these systems into attributing the wearer's actions as my own.

Proof of this has already occurred on a rather large surveillance system known as Facebook photo-tagging. Mark Zuckerberg, Facebook's CEO has invested in a multi-million dollar recognition program known as 'Deep-Face' which can identify a face

Figure 9. *URME Surveillance*, 2014, courtesy of the artist Leo Selvaggio.

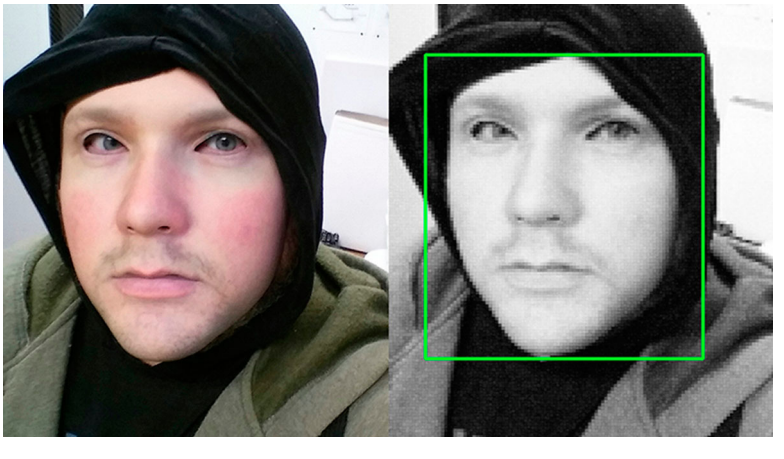

Figure 10. *URME Surveillance*, 2014, courtesy of the artist Leo Selvaggio.

Figure 11. *URME Surveillance*, 2014, courtesy of the artist Leo Selvaggio.

regardless of the angle the image is taken from with 97.2% accuracy: the equivalent accuracy of a human being (Grandoni 2014). While several of the images on Facebook are not convincing to the human eye due to the extremely high-resolution photographs, the system still successfully and automatically tags all new images of the prosthetic and its users as me. Furthermore, because Zuckerberg's system was built for automation not requiring a human security element, uploading images of others as me via the prosthetic on Facebook is a successful test of the prosthetic's ability to confound facial recognition systems in general.

That being said, as with all projects, the URME prosthetic is not free of problems. The first and most obvious concern is the rigidity of the resin. Its lack of flexibility does not allow for the emulation of facial expression the way some high-end latex

Figure 12. *URME Surveillance*, 2014, courtesy of the artist Leo Selvaggio.

prosthetics do. This is further compounded by its muffling of the human voice due again to the fact that the mouth does not move. Any direct interaction with a human, will lead to immediate detection of the prosthetic which limits the contexts in which the prosthetic is viable.

The rigidity also presents another problem. Because the prosthetic is a 3D rendering of my face, it has its own unique set of contours and variables, such as the depth of my eye-sockets, or width of my chin. It is actually quite specific and not everyone is genetically compatible with it. For example, it has been known to cause injury in some by digging into the eyes of the wearer whose eyes protrude farther than own. Yet on others, it fits flawlessly. While the addition of scarves and hats can help to obscure the hard edges of the prosthetic, their use in certain climates would draw suspicion. Alatex prosthetic would correct several of these physical limitations; however, the need for the prosthetic to be as democratic as possible outweighed the advantages latex would provide. The average price of a custom, Hollywood-grade latex mask is anywhere from 8 to 1200 dollars each. The *URME Surveillance* Identity Prosthetic can be purchased directly from Thats-MyFace.com for 200 dollars. Because it is considerably less expensive than the alternatives to make, it has the potential to be more widely used. However, when compared to the availability of makeup in Harvey's work, the Prosthetic is still a device for economically privileged users, only available to those with a certain amount of disposable income (Figure 13).

This fact led me to the creation of a second URME device in the form of an economical paper mask. The URME Paper Mask takes the form of a DIY kit that I have manufactured. By having the buyer make the mask, the initial costs go down significantly. They are also light and very inexpensive to ship. Furthermore because they are flat they are extremely portable. The total cost spent to make each kit, which includes the price of ink, cardstock paper, mask fastners and bubble mailer, comes out to a little

Figure 13. *URME Surveillance*, 2014, courtesy of the artist Leo Selvaggio.

under $1.00, which is also the price it will sell for. All URME devices are sold at cost to maximize their potential use by the general public.

However, like the prosthetic, the mask suffers from several problems as well. First, though it will identify the wearer as me via facial recognition, it is not passable to human eye. It is flat which means that it does not contour to the shape of the face. Because cameras capture two-dimensional images, the paper masks are slightly more passable at certain angles but a human would easily detect the mask. In order to acknowledge this flaw, I shifted the proposed purpose of the masks into a device used by those who may want a low level of protection but are comfortable asserting themselves in public space, such as the activists and protesters in Blas and Harvey's work. When sold in packages of 12 or 24, the paper masks have been rebranded as Community Development Hacktivist Kits. Rather than try and pass inconspicuously, the goal of these kits are to make a strong unified statement about the group's right to assert itself in public space. The kits also are quite apt at producing a sense of spectacle. Photographed for the first time in downtown Chicago, the small group of 10 volunteers wearing these masks drew crowds, stares and camera photos. People were interested by this strange phenomenon taking place on the street: a cluster of pedestrians all wearing the same face. The general interest of the people I talked to while photographing this spectacle led me to produce other work in public such as conducting workshops and guided walks with the paper masks. The paper mask shifted the original goals of *URME Surveillance* to include promoting civic engagement and empowering people in public spaces (Figures 14 and 15).

Thus far, with both the prosthetic and the mask, I have only discussed some of the physical problems surrounding *URME Surveillance* when considering my original criteria of function. While developing this project, it became clear that there were several sociological and ethical concerns that need to be examined as well. Foremost among

Figure 14. *URME Surveillance*, 2014, courtesy of the artist Leo Selvaggio.

these is that the *URME Surveillance* is asking others to present themselves in public as a white man within the context of a surveillance culture. This of course brings about questions of race, gender expression and nationalism, to name a few. What does it mean to ask a Latin immigrant male to present as a Caucasian man, or a Black woman to do the same? What would it mean to any transgender individual to become me; to perform as me? In addition to these questions about identity, there are also questions about the historical use of surveillance as a component of institutional racism in the form of pervasive profiling, disproportionate incarceration of non-white citizens and suppression of political expression in public spaces. In his essay 'Black Men in Public Space', journalist Brent Staples describes his experiences of being profiled as a criminal throughout most of his life. He describes exactly how this profiling circumscribed his behavior in public space:

> Over the years, I learned to smother the rage I felt at so often being taken for a criminal. Not to do so would surely have led to madness. I now take precautions to make myself less threatening. I move about with care, particularly late in the evening. I give a wide berth to nervous people on subway platforms during the wee hours, particularly when I have exchanged business clothes for jeans. If I happen to be entering a building behind some people who appear skittish, I may walk by, letting them clear the lobby before I return, so as not to seem to be following them. (Staples 1986)

It is uncertain how this history of prejudicial surveillance practices will integrate into the conversion from human-powered surveillance to automated digital systems we are currently witnessing. Though many may assume that automated systems like facial recognition are not subject to the concerns of racial profiling due to technological impartiality, this is not the case. As Zach Blas states, 'These technologies are being developed by humans, so there are sociopolitical biases being programmed into these technical architectures' (Hiscott 2014). Facial recognition is only a tool developed and used by other human beings who can be prejudiced. As such we should be wary of any

Figure 15. *URME Surveillance*, 2014, courtesy of the artist Leo Selvaggio.

and all systems of automation that are implemented without rigorous public discourse around the affects of such implementation. My work, which is only a small part of the ecology of artists, activists and academics concerned with surveillance, is tasked with producing such a discourse.

Though it is beyond the scope of this paper to properly survey the entanglement of racial and gender politics within surveillance practice, the most important conversation that *URME Surveillance* can contribute to, even more than the right to privacy, is discussion of white male privilege in public space. *URME Surveillance* asserts the utopian ideal that everyone could and should benefit from the same privilege that white men do, which is to simply be valued for being themselves despite their behavior.

The *URME Surveillance* Prosthetic, if undetected, allows for an individual to temporarily experience and consequently perform white male privilege in public space, while at the same time drawing attention to the very nature of privilege as a component of a patriarchal power structure that excludes the majority of Americans. It is not the goal of *URME Surveillance* to transform everyone into White men, and as an artist I reject that notion of milky homogenization. However, by engaging the idea that white male privilege could somehow be shared and distributed to others, then as a metaphor, *URME Surveillance* has the potential to become a platform to examine questions of race, class, nationality, gender, sexual orientation and expression and other factors that circumscribe our freedoms in public space. As Maguire mentions, 'Biometrics also allow for a critical engagement with "race" and racialization, especially as new forms of racism are enabled by biometric security, but also because the history of biometrics shows an inherent mutability in the notion of "race"' (Mcguire 2012, 604). As *URME Surveillance* develops, I hope to engage with and learn from communities on how surveillance is tied to their experience of systemic oppression like racism.

URME Surveillance as a whole is yet incomplete. As technology becomes more accessible and commercially viable, many of the physical concerns of the project will be addressed. The projects conceptual concerns must also continue to be addressed. While I have described several reasons for why the project started with my face, the next iteration of the work will have facial prosthetics that ideally represent every race, gender expression, age and sexual orientation. I have already had several volunteers wanting to 'donate' their faces to *URME Surveillance*. However the ethical concerns which prevented me from using others' faces originally will not allow me to accept said donations until I am able to understand the legal ramifications for the donors and hopefully provide them with some form legal protection. Still, harkening back to texts like Donna Haraway's 'Cyborg Manifesto' in which she describes a future free of gender binaries and other markers, I look forward to a day when we are all trying on each other's faces and identities (Haraway 1991). I imagine a world where there is a one-to-one ratio, with everyone having access to any prosthetic they want to wear that day, including their own. How do we resist surveillance? I am not completely certain, but I know it has to start with an 'us'. It is my hope that by beginning with 'me', we can find our way toward a collective power that champions our undeniable human right to self-actualize and express the wonders of our identities.

Disclosure statement

No potential conflict of interest was reported by the author.

ORCID

Leonardo Selvaggio http://orcid.org/0000-0002-6085-3318

Notes on contributor

Leonardo Selvaggio is a Chicago based interdisciplinary artist whose work examines the intersection of identity and technology. He has shown work internationally in France and Canada; domestically in New York, Chicago, Florida, and New Mexico. He has been awarded an Albert P. Weisman grant for his work, URME Surveillance and a DCASE IAP Professional Grant to

present supporting research. That artistic intervention invites users to wear a photo-realistic prosthetic of his face as protection from pervasive facial recognition surveillance systems. In 2015, URME has been selected for the Art Souterrain festival in Montreal, the ISEA conference in Vancouver, and the Saint-Etienne Design Biennial in France to name a few. URME Surveillance was also adapted for television in an episode of CSI: Cyber titled "Selfie 2.0". Selvaggio's arts practice has been featured in notable publications: Hyperallergic, Techcrunch, The Washington Post, CNET, The Verge, and The Creator's Project. He holds a BFA from Rutgers University and an MFA from Columbia College's Interdisciplinary Arts program.

References

Epic.org. 2013. "Spotlight on Surveillance." *EPIC – Spotlight on Surveillance*, December 1. Accessed May 13, 2015. https://epic.org/privacy/surveillance/spotlight/ngi.html.

Google.com. n.d. "Privacy and Security – About – Google Maps." *About Google Maps*. Accessed May 3, 2015. http://www.google.com/maps/about/behind-the-scenes/streetview/privacy/.

Grandoni, Dino. 2014. "Facebook's New 'DeepFace' Program is Just as Creepy as it Sounds." *The Huffington Post*, March 18. http://www.huffingtonpost.com/2014/03/18/facebook-deepface-facial-recognition_n_4985925.html.

Haraway, Donna J. 1991. "A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century." *Simians, Cyborgs, and Women*. 141–181, 243–248. Print.

Harvey, Adam. 2013. "Face to Anti-Face." *The New York Times*, December 13. Accessed May 7, 2015. http://www.nytimes.com/interactive/2013/12/14/opinion/sunday/20121215_ANTIFACE_OPART.html?_r=0.

Hiscott, Rebecca. 2014. "'Fag Face' Mask Protests Sex Discrimination in Facial-Scanning Tech." *Mashable*, May 7. Accessed May 7, 2015. http://mashable.com/2014/03/07/biometrics-facial-scan-mask/.

Maguire, Mark. 2012. "Biopower, Racialization and New Security Technology." *Social Identities* 18 (5): 593–607.

Marketsandmarkets.com. n.d. "Emerging Trend in the Facial Recognition Market." *Facial Recognition Market*. Accessed May 3, 2015. http://www.marketsandmarkets.com/ResearchInsight/facial-recognition-market.asp.

Opensource.org. n.d. "Welcome to the Open Source Initiative." Accessed May 13, 2015. http://opensource.org/.

Shah, Rajiv. 2014. "Surveillance in Chicago: Growing, but for What Purpose?" *The Selected Works of Rajiv Shah*. http://works.bepress.com/rajiv_shah/5.

Staples, Brent. 1986. "Black Men and Public Space." Accessed via http://www.phil.washington.edu/ (originally published in *Harpers* Magazine). December 1986. Accessed May 7, 2015. http://www.phil.washington.edu/sites/default/files/uploads/Black Men in Public Space Article.pdf.

Stroud, Matt. 2014. "Did Chicago's Facial Recognition System Catch its First Crook?" *The Verge*. August 8. Accessed May 3, 2015. http://www.theverge.com/2014/8/8/5982727/face-wreck-how-advanced-tech-comes-up-short-for-police.

Young, Stephanie. 2014. "Some Notes on the Anti-Surveillance Feminist Poet Hair & Makeup Party." *Dusie*. Accessed May 3, 2015. http://antirecognition.tumblr.com/post/78775543535/probably-the-abject-materials-are-too-strong-too?soc_src=mail&soc_trk=ma#notes.