ISEA2015
Proceedings of the 21st International Symposium on Electronic Art
ISSN: 2451-8611
ISBN: 978-1-910172-00-1

URME Surveillance: Analyzing Viral Face-crime

Leonardo Selvaggio

Chicago, IL, USA
Leo.Selvaggio@gmail.com

Abstract

This self-reflective art paper examines my position within the ecology of surveillance art focused around facial recognition. *URME Surveillance*, transforms my identity into a defense technology for the public's protection against facial recognition software. This project encourages the public to substitute their identity for my own by wearing a 3d printed prosthetic mask made in my likeness.

This paper will begin by examining our relationship to surveillance and identity by discussing the surveillance system in Chicago as a case study. I will then discuss the work of Adam Harvey and Zac Blas as two contemporary artists working with identity recognition technologies. I will then use their work as a jumping off point for my own, discussing the strategies that lead me to *URME Surveillance* including an overview of its successes and failures.

Keywords

Surveillance, Subversion, Identity, Performance, Facial-Recognition, Data, Power structure, Prejudice, Prosthetic

It was terribly dangerous to let your thoughts wander when you were in any public place or within range of a telescreen. The smallest thing could give you away… In any case to wear an improper expression on your face was itself a punishable offense. There was even a word for it in Newspeak: facecrime [1] *-George Orwell, 1984*

Considering the quote above, I am struck by the Newspeak word, "facecrime". Its implication is disturbing: that the part of the body most indicative of an individual could perpetrate a crime. This link between face, or identity, and crime is not as unfamiliar as Orwell's futuristic novel would have us believe. One example in the United states of this is the notion of Shopping while Black. The United States has a myriad of these examples: post 9-11 profiling of Arab Americans, immigration practices on the Mexican border, Japanese internment camps in World War II, etc. While these examples may be construed as racial rather than facial, the genetics that make up race have a circumscriptive determination on our facial features as well, such as eye shape and color, cheek bone height, nose width, lip size, etc. Perhaps we should translate "facecrime" into a relatively new English term from our own technological era: facial recognition.

Facial recognition software has been one of the most developed surveillance technologies of the last 10 years and it is an arms race to apply facial recognition to as many contexts as possible. For example Mark Zuckerberg, creator of Facebook, has invested in a multi-million dollar recognition program known as "Deep-Face" which can identify a face regardless of the angle the image is taken from with 97.2% accuracy: the equivalent accuracy of a human being [2]. This investment reflects Zuckerberg's interest in improving the photo tagging experience on Facebook.

The embedding of facial recognition within social media is indicative of another shift within the last 10 years: the digitization of accessible personal information, which I would argue is the most prevalent form of identity formation and expression today. In the sci-fi television show Caprica, a grieving father attempts to resurrect his daughter by downloading all the public information about her into a robot body. His rationale is that all her preferences, experiences, memories, and accomplishments in one way or another have been archived online through photos, videos, posts, articles, etc, and that these are the relevant components of who his daughter was. Research scientists working at the intersection of social media and marketing share this idea. In a 2013 study from Cambridge University, a group of researchers developed a method of constructing an identity profile of a person based solely on what someone "likes" on Facebook. They claimed that with access to this information, it was possible to accurately determine a person's gender, age, race, religion, sexual orientation, political stance, socio-economic class, whether they are an only child or not, and consumer behavior to name a few [3].

Facebook, and other social media platforms use this information to sell marketing profiles about its users to advertisers based on our perceived identity. This external creation of identity through interpreted data collected by others, along with the global reach and ubiquitous nature of social media, threatens each of our own authorships over our individual identities. When this data is combined with facial recognition surveillance systems the potential to tag this data to a physical body in the world arises. Most importantly, what will happen when this "data" is used to profile potential criminal behavior: facecrime.

Enter real world surveillance systems, such as Chicago's own "Virtual Shield". Known as the most widely surveilled city in the nation, Virtual Shield houses over

25,000 federated cameras, including blue-light cameras, cameras in public school, traffic cams, and those on busses and trains. What makes Chicago frighteningly special is that it is also the national leader in fiber-optic systems, meaning that all 25,000 government cameras are networked together, moving thousands of surveillance images into one centralized hub [4]. Housed in the 911 Emergency Response Center, Virtual Shield also has some of the most sophisticated facial recognition software anywhere in the country, and with each camera having a known corresponding physical location, Virtual Shield has the potential to track an individual's movements throughout Chicago, using their face as the trigger.

The inclusion of facial recognition in surveillance practices has had a profound effect on the way artists engage with the subject of surveillance. Though there are examples in art concerning our relationship to surveillance and identity 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 Adam Harvey and Zach Blas, 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. 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 to successfully change how these features appear by using makeup to alter the image the camera system sees to the point that most surveillance systems can't even detect a face let alone identify it. Harvey's work has enjoyed considerable attention and has been emulated and practiced by several groups such as the "Anti-Surveillance Feminist Poet Hair & Make Up Party," a Tumblr blog that catalogues women using makeup as a subversion tactic [5].

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. Arguable the most famous of these *Suites* is "FagFace" which is a model comprised of several queer men's faces. These faces, as with all of his *Suites*, are collected through a series of community-based workshops. The faces are scanned and then turned into 3d models. Afterwards, 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 the wearer's face from biometric scans and other forms of facial recognition.

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 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 and tend to be associated with criminality, which 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 a form of cultural expression 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 is useful for a practical anti-surveillance intervention.

As a result, when considering how I might add to the ecology of art concerned with facial recognition, my goals became to address this prevailing strategy of "hiding" through an artistic intervention that underlined real world function with an emphasis on subversion and avoiding detection by surveillance as opposed to the important, yet overt, public visual statments made by Harvey and Blas. I aimed to produce something others could potentially 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, 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 pass inconspicuously in a crowd of people as well.

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, an interactive web project that provided open access to various aspects of my cyber identity to visitors, 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 with the most likely scenario being 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, it was the only identity I was willing to put at risk.

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 the criteria used in analyzing Blas and Harvey's work, 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.

Unlike other options such as latex prosthetics, the photo realism doesn't 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, normally 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, such as a security officer, in surveillance systems. Though both Blas and Harvey's work thwart facial recognition, 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 Virtual Shield. The conspicuous nature of their aesthetics- pink blob, and futuristic warrior paint- as with the majority of other strategies discusse, make it easy for a human to spot on a monitor, even on low-resolution cameras.

The URME prosthetic turns the weaknesses of these low resolution cameras into one of the project's strengths. As mentioned above, the lower the resolution of the camera the higher the chance the prosthetic has to pass undetected to a human watching a monitor because the edges appear to blend seamlessly into the rest of the face. In contrast, on 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, 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, a security officer or other human element will continue to track the prosthetic with conviction, believing that they are in fact seeing the person presented to them on camera, "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 was designed with all the same features that trigger facial recognition and so cameras detect it immediately as a face. 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, thus subverting a system into attributing the user's actions as my own

Proof of this has already occurred on a rather large surveillance system known as Facebook photo-tagging. As previously mentioned, Facebook has invested in some of the most sophisticated facial recognition software anywhere in private sector. 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.

However, as with all projects, the 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 prosthetics do. This is further compounded by its muffling of the human voice due again to the fact that the mouth does not move. Thus, 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. As such, 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. I have had successful and unsuccessful fittings on members of various races, ethnicities, and both genders. That being said, differences in skin pigmentation can present a problem. While the addition of scarves and gloves can help, their use in certain climates would draw suspicion. A atex 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 eight to twelve hundred dollars each. The URME Surveillance Identity Prosthetic can be purchased directly from ThatsMyFace.com for two-hundred dollars. Because it is considerably less expensive than the alternatives to make, it has the potential to be more widely used. When compared to the availability of makeup in Harvey's work however, the prosthetic is still an economically privileged device, only available to those with a certain amount of disposable income.

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 under a $1.00, which is also the price it will sell for. All URME devices are sold at cost to maximize potential use by the 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. 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 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 cameras. People were interested by this strange phenomena taking place on the street: a cluster of pedestrians all wearing the same face. The 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 utility of the paper mask has shifted the original goals of URME Surveillance to include civic engagement in public spaces.

While developing this project, it became clear that there were also several sociological and ethical concerns that needed to be examined. Foremost amongst 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? In addition to these questions of 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 the suppression of cultural and political expression in public spaces.

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 themselves and valued for it despite their behavior, criminal or otherwise.

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. 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.

Surveillance is a system based on fear that offers us the illusion of safety by sacrificing freedom. The source of this fear comes from the very questions stated above. That fear has lead us to build an architecture of prejudice that acts against the democratic ideals of the United States. This power structure prejudices women, prejudices minorities, and prejudices the lower class and old age. It fears Arab Americans post 9-11 and Mexican immigrants at the border the same way we once feared the Japanese we interned. Surveillance in a product of an American culture that fears Black people who shop and only finds safety in Whiteness. Want to be invisible to surveillance? Be a White man in a suite. No prosthetic needed. What is at stake is nothing short of our freedom to express and explore the very nature of our individual identities. The *URME Surveillance Identity Prosthetic* may never allow the user to be who they really are in public space, but neither does the current state of Surveillance. We are fundamentally changed when we are watched. We perform prescribed acceptable versions of ourselves rather than simply be. So be me instead. URME.

References

1. Orwell, George. *1984*. New York: Signet Classic, 1950.

2. Grandoni, Dino. "Facebook's New 'DeepFace' Program Is Just As Creepy As It Sounds." The Huffington Post. March 18, 2014. Accessed March 22, 2014. http://www.huffingtonpost.com/2014/03/18/facebook-deepface-facial-recognition_n_4985925.html.

3. Kosinsk, Michal, David Stillwell, and Thore Graepel. "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior." *Proceeding of the National Academy of Science in the United States* (2013): 1-4. *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*. 11 Mar. 2013. Web. 04 May 2013.

4. Rajiv Shah. 2014. "Surveillance in Chicago: Growing, but for what purpose?" The SelectedWorks of Rajiv ShahAvailable at: http://works.bepress.com/rajiv_shah/5

5. "ANTI-SURVEILLANCE FEMINIST POET HAIR&MAKEUP PARTY." ANTI-SURVEILLANCE FEMINIST POET HAIR&MAKEUP PARTY. Accessed March 23, 2014. http://antirecognition.tumblr.com