Expression as Resistance, Resistance as Expression:

The Role of Art & Artists in Furthering Anti-Subordination Goals Under Surveillance Regimes

By Jessica Shand

Overview

§1 Introduction

In the decades since the September 11 attacks and the passage of the Patriot Act, state-sanctioned surveillance has transformed dramatically from individual searches warranted by probable cause to suspicionless mass data collection programs. Pushback has seen limited success in state and federal legislatures, and with few exceptions, private-sector technology companies remain unwilling to self-regulate. But as public awareness of government surveillance has risen in the wake of the so-called Snowden effect—and as surveillance itself has become more pervasive, amid COVID-19[1] and the unilateral rise in protest movements[2] across the globe—the public has begun to adopt countersurveillance measures once considered niche. Among these measures is what Torin Monahan describes as "a curious [...] panoply of artistic projects—and products—for concealing oneself from ambient surveillance in public spaces."[3] Think: fractal face paint that obscures the region

[1] Antónia do Carmo Barriga et al., "The COVID-19 Pandemic: Yet Another Catalyst for Governmental Mass Surveillance?," *Social Sciences & Humanities Open* vol. 2, no. 1, December 2020, https://www.sciencedirect.com/science/article/pii/S2590291120300851.

[2] Adam Taylor, "Why Is the World Protesting so Much? A New Study Claims to Have Some Answers," *The Washington Post*, November 4, 2021, https://www.washingtonpost.com/world/2021/11/04/protests-global-study/.

[3] Torin Monahan, "The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance," *Communication and Critical/Cultural Studies* 12, no. 2, February 2015, https://doi.org/10.1080/14791420.2015.1006646.

around the eyes. Hats with embedded infrared LEDs that blind CCTV cameras. Full-body, metalliferous coats that block all incoming and outgoing signals.

In this paper, we ask: what can art and artists experimenting with adversarial designs contribute to anti-surveillance movements, and in particular, to notions of privacy in public? First, we establish a basic technical understanding of facial recognition systems to provide context for the designs presented in this paper, which are tailored to exploit specific features of these systems. We then examine both how aestheticized forms of resistance fail to challenge the disproportionate impacts of automated facial recognition technologies by law enforcement agencies, and the strategic fallacies of implementing adversarial designs in the first place. In light of this, we argue that aestheticized forms of resistance ought not to be examined uncritically. We consider a performative theory of privacy to suggest that these kinds of artistic interventions may further anti-subordination goals insofar as they highlight the expressive dimension of functional, quotidian demands for privacy in public. To conclude, we offer recommendations for future research in expressive resistance to state surveillance—reaching beyond physical space, and toward cyberspace.

§2 A Primer on Automated Facial Recognition

Wearable adversarial designs first appeared primarily as niche academic projects and art installations before gaining public traction vis-à-vis the protest movements of the 2010s and beyond. (*See Figure 1*). The factors that may have contributed to this trend are numerous. For one, as increased awareness of federal monitoring programs has led to a decline of public trust in governments worldwide, partaking in protest against those very programs has also meant dressing for anonymity and safety, even in democratic

Figure 1. *Left:* Computer Vision (CV) Dazzle, an anti-surveillance tactic created by artist Adam Harvey, attempts to fool algorithms for face detection by developing an asymmetrical look that partially obscures the eyes and contrasts with the subject's skin tone in unusual tones and directions. *Right*: Founders of the Dazzle Club don asymmetric makeup while protesting the Metropolitan police's use of live facial recognition on the streets of London. (Photos: Cha Hyun Seok & Cocoa Laney).

societies.[4] And there is no doubt that widespread mask-wearing to reduce the spread of COVID-19 has made people more amenable to—and expecting of—the possibility for privacy in public. But the technology is only getting better, and nowadays, facial recognition systems can identify individuals with relatively little data. Amid reports of heightened police surveillance during the Black Lives Matter protests of 2020, the NYPD's use of facial recognition software to track down 28-year-old protestor Derrick Ingram—then send dozens of officers to his home without a warrant, some equipped with riot gear—stands out as a particularly insidious example of how advances in technology continue to enable the disparate policing and prosecution of racial justice activists, and Black activists in particular, by law enforcement.[5]

To contextualize, understand, and critique artistic contributions to adversarial machine learning, we must first take a step back and ask: what are the technologies these interventions seek to fool, and how do they function? What weaknesses do adversarial designs seek to exploit, and under what circumstances? In this section, we provide a basic overview of automated facial recognition algorithms and how they are deployed by corporations and governments alike.

At the most fundamental level, face *detection* refers to the processing of digital images to locate the presence of human faces, if any. Facial recognition extends this process to establish *to whom* a given face belongs. This typically involves gathering a set of values meant to summarize the differentiating features of the face—called a *faceprint*—and then using a face-matching algorithm to compare that set of values against up to n other such sets in a database.

Facial recognition algorithms that compare a faceprint to a specified template, which we call *1:1 matching* or *verification*, have become a standard security feature in various commercial products and government programs. In 2017, Apple released its Face ID software on the iPhone X, which uses facial biometrics to verify a user's identity when attempting to unlock the device or authorize payments. Under the social distancing mandates of the COVID-19 pandemic, facial recognition technology became a contactless authentication solution for everything from online banking to telemedicine. And in late 2021, Delta Air Lines launched a digital identity program for pre-approved flyers, who

[4] Jay Rosen, "The Snowden effect: definition and examples," *PressThink*, July 5, 2013, https://pressthink.org/2013/07/the-snowden-effect-definition-and-examples/.

[5] "Struggle for Power: The Ongoing Persecution of Black Movement by the U.S. Government," M4BL, September 1, 2021, https://m4bl.org/struggle-for-power/.

can now opt in to using facial recognition for everything from obtaining baggage tags to going through security and even boarding domestic flights.[6]

While these implementations give us a sense of how verification algorithms can and have made our lives easier and more secure, the technology is not without its darker sides. In 2020, the Australian government's trial of a system that sent random check-in requests to travelers upon arrival in the country—collecting location data and 'selfies' to ensure their compliance with pandemic quarantine requirements—sparked warnings of surveillance overreach from privacy advocates worldwide.[7] Of course, there is an argument to be made that in a public health crisis, some sacrifice of individual privacy may be necessary for the collective good. And if facial images are collected consensually and confidentially with equal outcomes across demographics, this technology might be defended as a means of keeping people safe.

However, *1:n matching* algorithms that compare a faceprint to thousands or even millions of others—that is, facial *identification* systems—have been a primary cause for concern because in practice, unlike the aforementioned software for COVID-19 containment in Australia, they may be more likely to be deployed without the knowledge or consent of subjects. In July 2020, *Reuters* reported that drugstore chain Rite-Aid had quietly added facial recognition systems to more than 200 stores across the U.S., primarily in non-white and low-income neighborhoods. The cameras captured shoppers' facial images to identify those who had previously been suspected of criminal activity of any kind, then directly alert security personnel, who could ask a customer to leave on those grounds.[8] And as of 2016, more than 117 million American adults had profiles in law enforcement face recognition networks.[9] These networks have been cited in at least three wrongful arrests, including that of Robert Williams, a Black man who was handcuffed and put into a police car in front of his two young daughters after being misidentified as a shoplifting suspect by facial recognition software deployed by Detroit police.[10]

---

[6] Elaine Glusac, "Your Face Is, or Will Be, Your Boarding Pass," *The New York Times*, December 7, 2021, https://www.nytimes.com/2021/12/07/travel/biometrics-airports-security.html.

[7] Mia Sato, "The Pandemic Is Testing the Limits of Face Recognition," *MIT Technology Review*, September 30, 2021, https://www.technologyreview.com/2021/09/28/1036279/pandemic-unemployment-government-face-recognition/.

[8] "Rite Aid Deployed Facial Recognition System in Hundreds of U.S. Stores," *Reuters*, July 28, 2020, https://www.reuters.com/investigates/special-report/usa-riteaid-software/.

[9] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Line-Up: Unregulated Police Face Recognition in America," October 18, 2016, https://www.perpetuallineup.org/.

[10] Drew Harwell, "Wrongfully Arrested Man Sues Detroit Police over False Facial Recognition Match," *Washington Post,* April 13, 2021, https://www-washingtonpost-com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/ology/2021/04/13/facial-recognition-false-arrest-lawsuit/.

To be clear, the underlying technology for verification and identification is often similar, if not the same. As the Electronic Frontier Foundation (EFF) points out, "any face recognition system used for 'tracking,' 'clustering,' or 'verification' of an unknown person can easily be used for 'identification' as well."[11] But in a 1:n system, the sheer number of comparisons made amplifies the statistical likelihood of misidentification. And the deployment of this technology on non-cooperative subjects—that is, subjects who are unaware they are being surveilled in this way—only exacerbates the issue, because while most identification algorithms perform well on appropriately lit and well-positioned facial images, they tend to produce large numbers of false positives "in the wild."[12] Ultimately, the use of facial identification aggravates the power imbalance between ordinary people and both law enforcement and private corporations—who can use the technology to monitor, predict, and control behavior. As such, "even if it was accurate and unbiased, widespread deployment of facial identification [...] is incompatible with a free society."[13]

§3 Adversarial Designs as Functional Fashion & Forms of Play

Anti-surveillance camouflage designed to exploit specific features of surveillance systems first arose within universities and niche circles of artists both as a functional means of "hiding in plain sight" and as a playful form of protest.[14] On the one hand, by confusing computer vision algorithms with everything from avant-garde minimalism to information overload, these designs may render the wearer invisible to machines. On the other hand, they may likely draw *more* attention—at least human, and often also media, attention—to the wearer, who need not become "reclusive under the withering gaze" of surveillance technology.[15] As such, especially in spaces of confrontation, designs of this sort may at their best help appeal to "a symbolic overturning of hierarchy much like medieval carnival," both provoking law enforcement in a non-threatening manner while

---

[11] Bennett Cyphers, Adam Schwartz, and Nathan Sheard, "Face Recognition Isn't Just Face Identification and Verification: It's Also Photo Clustering, Race Analysis, Real-Time Tracking, and More," Electronic Frontier Foundation, October 15, 2021, https://www.eff.org/deeplinks/2021/10/face-recognition-isnt-just-face-identification-and-verification.

[12] Seth Lazar, Claire Benn, and Mario Günther, "Large-Scale Facial Recognition Is Incompatible with a Free Society," *The Conversation*, July 10, 2020, https://theconversation.com/large-scale-facial-recognition-is-incompatible-with-a-free-society-126282.

[13] Bennett Cyphers, Adam Schwartz, and Nathan Sheard, "Face Recognition Isn't Just Verification and Identification."

[14] Torin Monahan, "The Right to Hide," 160.

[15] Ibid.

offering opportunities for solidarity building.[16] In this section, we showcase several examples of adversarial designs tailored to state-of-the-art facial recognition technologies, before elaborating further on the extent to which such designs may fail to challenge the violent and discriminatory logic of surveillance.

Ewa Nowak's Incognito

In 2018, Polish designer Ewa Nowak tested a project called *Incognito*, a wearable mask of sorts that is contoured to the individual's face, against Facebook's DeepFace algorithm. (*See Figure 2*). A deep convolutional neural network trained on upwards of four million photographs uploaded by some four thousand Facebook users, DeepFace is one of the most sophisticated facial recognition algorithms known to date. Studies of the algorithm on Labeled Faces in the Wild (LFW) datasets suggest it reaches to upwards of a 97.25% accuracy rate on facial identification tasks. (By comparison, human beings have shown an accuracy rate around only .28% higher on the same tasks).[17] Nonetheless, Nowak claims that *Incognito* can be used to successfully thwart DeepFace, stating that "the form almost entirely resulted from the function of this object," while not compromising its aesthetic appeal and simplicity.[18]

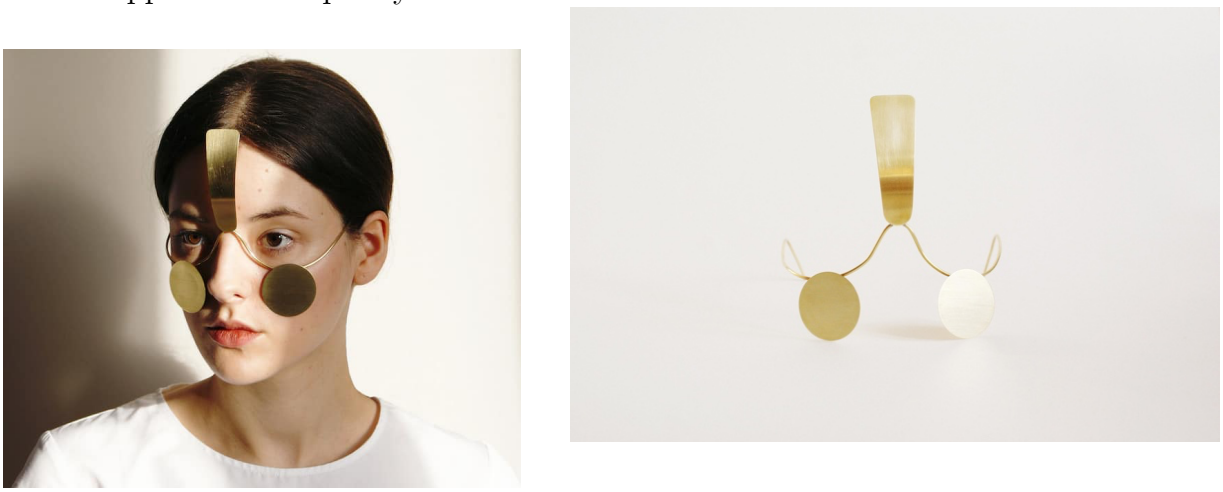

Figure 2: Ewa Nowak designed *Incognito* to fool Facebook's DeepFace algorithm. (Photo: Ewa Nowak).

[16] Jeffrey S. Juris, "Performing Networks at Direct-Action Protests," in *Networking Futures the Movements against Corporate Globalization* (Durham, NC: Duke University Press, 2008).
[17] "Facebook's Deepface Shows Serious Facial Recognition Skills," *CBS News* (CBS Interactive, March 19, 2014), https://www.cbsnews.com/news/facebooks-deepface-shows-serious-facial-recognition-skills/.
[18] Natashah Hitti , "Ewa Nowak's Anti-AI Mask Protects Wearers from Mass Surveillance," *Dezeen*, July 30, 2019, https://www.dezeen.com/2019/07/30/ewa-nowak-anti-ai-mask-protects-wearers-from-mass-surveillance/.

Described by the designer as a kind of "face jewelry," *Incognito* consists of three minimalist brass plates, one between the eyebrows stretching toward the hairline, and two on the cheekbones, all connected by a wire that tucks behind the ears like eyeglasses. Not unlike the CV Dazzle tactic, the shape, size, and positioning of the elements is meant to obscure key facial features, such as the region where the nose, eyes, and forehead intersect. The polished metallic plates also reflect light and may therefore blind CCTV cameras installed in public spaces. The project won Nowak the Mazda Design Award at the Łódz Design Festival and is now available for sale online—at a hefty £15,000.

Jing Cai-Liu's Wearable Face Projector

On an entirely different end of the design spectrum, consider the wearable face projector designed in 2017 by University of Arts Utrecht student Jing Cai-Liu. (*See Figure 3*). Shown alongside a set of fictional anonymity products by students under the name "Group Anonymous" at Milan Design Week, the gear consists of a projector attached to a headband, which projects a stream of different faces onto the subject's face.[19] The brightness of the projection, shakiness of the flashing stream of images, and continuous shifting between faces is meant to confuse computer vision algorithms that expect a steady facial image.

Figure 3: Wearable headgear designed by Jing Cai Liu would project a stream of different faces onto the subject's face. (Photo: Jing Cai Liu).

In contrast with Nowak's relatively minimalist design, Cai-Liu's stands out as an especially futuristic intervention. But not futuristic enough to avoid fooling people,

[19] Cory Doctorow, "Design Fiction, Politicized: The Wearable Face Projector," *Boing Boing*, October 17, 2019, https://boingboing.net/2019/10/17/jing-cai-liu.html.

apparently. When videos demonstrating how the wearable face projector might function were falsely attributed to pro-democracy protestors in Hong Kong, going viral on social media as the region instituted an emergency mask ban at rallies, the designer clarified to the Associated Press that "it was made to be a thought-provoking art piece," not a functional—or "political"—object.[20]

Textured Eyeglasses for Dodging and Impersonation

Unlike either of the designs by Nowak or Cai-Liu, a recent creation by researchers at Carnegie Mellon University and the University of North Carolina at Chapel Hill not only has the capability to *dodge* surveillance systems—that is, to cause the face to be misidentified as some other arbitrary face, if not go entirely undetected by the machine—but also to *impersonate* specific other faces. The team claims that "in addition to malicious purposes," such adversarial attacks "could also be used by benign individuals to protect their privacy against excessive surveillance."[21]

With inconspicuousness and physical realizability as its underlying design principles, the team's adversarial object of choice is a pair of textured eyeglasses that manipulate the physical state, as opposed to the digitized representation of this state, of the attacker. (*See Figure 4*). Assuming that the attacker cannot "poison" the system by

Figure 4: Examples of successful dodging and impersonation attacks by a team of researchers using textured eyeglasses. The images on the bottom of the second through fourth columns indicate the corresponding impersonation targets. (*Figure: Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition, Mahmood Sharif et al*).

[20] Ibid.

[21] Mahmood Sharif et al., "Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition," *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, October 1, 2016, https://dl.acm.org/doi/10.1145/2976749.2978392.

altering training data or injecting mislabeled data, the researchers focused on producing perturbations that can cause the input to be misclassified.[22] This involved initializing the color of the object to a solid yellow, then iteratively updating pixels through the design process while altering the texture of the glasses to obfuscate the three-dimensional 'shape' of the data passed into the neural network.

The team tested its design against a deep neural network developed by Parkhi et al., which surpassed even DeepFace to outperform humans on the LFW challenge, as well as several other facial recognition algorithms.[23] Nonetheless, all impersonation attempts succeeded, with successful dodging occurring between 80% and 100% of attempts, depending on the attacker.

§4 Where Anti-Surveillance Camouflage Gets It Wrong

The adversarial designs presented in the previous section may offer both—though perhaps not simultaneously—the ability to render oneself invisible to machines, and the ability to engage in symbolic forms of resistance as a form of solidarity and non-violent protest. In this section, we follow Monahan's logic of "resisting the impulse to celebrate [them] as progressive or innovative."[24] Instead, we critique these interventions from both philosophical and technical angles. We invoke a history of disparate surveillance against marginalized groups, specifically racial minorities, and question the extent to which these designs have the capacity to transform systems of oppression, especially given their hyper-individualized nature. We then argue that, even if it were possible to separate the adversarial technology from the social, political, and historical context into which it is embedded, its implications may be fraught even from a purely technical lens.

First and foremost, anti-surveillance camouflage may "enact a play of individual avoidance" that neglects the way in which surveillance systems, while virtually ubiquitous in the 21st century, inflict disproportionate suffering on marginalized communities.[25] As Simone Browne has pointed out, the disparate surveillance of Black people in the United States dates back at least to the so-called lantern laws of the 18th century, which required that "Black, mixed-race and Indigenous enslaved people carry candle lanterns with them

---

[22] Ibid., 1530.

[23] Omkar M Parkhi, Andrea Vedaldi, and Andrew Zisserman, "Deep Face Recognition," *Proceedings of the British Machine Vision Conference (BMVC) 2015*, September 2015, http://www.bmva.org/bmvc/2015/papers/paper041/index.html.

[24] Monahan, "The Right to Hide," 161.

[25] Ibid., 162.

if they walked about the city after sunset" without the company of a white person.[26] Lanterns as such were a means of exposing enslaved peoples to view at all times, not only serving to create and maintain racial boundaries, but to provide justification for further surveillance and subjugation based on racial categories. But racialized surveillance is not a relic of the past. Its evolution can be charted through the Jim Crow era, to the COINTELPRO program of the 1960s, and to the contemporary use of floodlights to "illuminate areas where people of color live and congregate."[27] In the face of this long history of marginalizing and discriminatory surveillance, these aestheticized forms of resistance may "reproduce discourses of universalism that elide difference [...] identifying vital areas of concern, but addressing them in ways that may fetishize, trivialize, and normalize larger structural conditions of inequality and danger."[28] And as Garfield Benjamin writes, "protecting privacy as a process of individual self-defense also fails in the collective implications of information leakage or exploitation such as the similarities in genetic information of family members, the relational information of one's contacts or communication metadata, or the normalizing effects of data *en masse* as a tool for discrimination."[29]

Implicit in this problematization is the issue of how governments demarcate between public and private space, then use this delineation to justify surveillance of marginalized peoples. Of course, in the age of the Internet, "keeping one's activities and information completely secret (and thus entitled to a right to privacy under the traditional 'secrecy paradigm')" is essentially impossible, regardless of one's status in relation to minority groups.[30] But as Scott Skinner-Thompson points out, marginalized communities that are "more likely to live in conditions where their information is exposed to others and [...] to be subject to and targeted for government surveillance in the first instance" have long known, and disparately feel the impacts of, the conceptualization of public space as a domain in which there is no reasonable expectation of privacy.[31]

Over the past century—and corresponding to this protectionist and property-based view of privacy—the ability to preserve one's privacy has been commodified, and

---

[26] Claudia Garcia-Rojas, "The Surveillance of Blackness: From the Trans-Atlantic Slave Trade to Contemporary Surveillance Technologies," *Truthout*, March 3, 2016, https://truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police/.
[27] Scott Skinner-Thompson, *Privacy at the Margins*, Cambridge: Cambridge University Press, 2021.
[28] Torin Monahan, "The Right to Hide," 162.
[29] Garfield Benjamin, "From Protecting to Performing Privacy," *Journal of Sociotechnical Critique*, May 2020, https://digitalcommons.odu.edu/sociotechnicalcritique/vol1/iss1/1/.
[30] Scott Skinner-Thompson, *Privacy at the Margins*, 8.
[31] Ibid, 8-9.

accordingly aestheticized forms of resistance in part offer "consumer-oriented adaptations to undesired surveillance."[32] Khiara Bridges puts this simply: "wealth [has become] the condition of possibility for privacy."[33] As a protectionist notion of privacy is always subject to further encroachment, it is for the sake of all in society that we should "oppose the framing of privacy as a commodity (for the wealthy) that emerges from defining privacy as property."[34]

Equally as ironic as it should be unsurprising, major technology corporations including Amazon and IBM—both of which have directly contributed to the militarization of domestic surveillance[35]—have profited from the rising consumer demand for anti-surveillance clothing and equipment. A simple search on Amazon yields thousands of products that purport to defend against facial recognition technologies, ranging from "invisibility hoodies" to deepfake masks. These products, to be sure, are made by third-party sellers—but third-party seller fees and commissions constitute Amazon's second-highest revenue stream, generating more than 80 billion USD in revenue in 2020.[36] As for IBM, the company collaborated with several universities during the COVID-19 pandemic to design T-shirts that evade detection by YOLOv2 and Faster R-CNN at rates of 63% and 52%, respectively.[37] The T-shirts, however, were never sold commercially; rather, they were designed and tested to help spot and fix weaknesses[38] in surveillance systems—in turn strengthening the grip of those systems.

Even on a purely technical level, the basic logic and functionality of aestheticized resistance is not without its fallacies. First, in assuming that attackers have knowledge of the *internals* of a system on a 'white-box' basis—that is, the system's basic architecture and parameters—these designs are inaccessible to the majority of people who lack specialized technical training. Not only that: they belie a reality in which we are rarely privy to the specificities of the surveillance systems deployed against us. And second,

---

[32] Torin Monahan, "The Right to Hide," 171.
[33] Khiara M. Bridges, *The Poverty of Privacy Rights*, Stanford, CA: Stanford Law Books, 2017.
[34] Garfield Benjamin, "From Protecting to Performing Privacy."
[35] Karen Hao, "The two-year fight to stop Amazon from selling facial recognition to the police," *MIT Technology Review*, June 12, 2020, https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/.
[36] "Global net revenue of Amazon from 2014 to 2020, by product group (in billion U.S. dollars)," February 3, 2021, https://www.statista.com/statistics/672747/amazons-consolidated-net-revenue-by-segment/.
[37] Kaidi Xu et al., "Adversarial T-Shirt: Evading Person Detectors in a Physical World," July 7, 2020, https://arxiv.org/pdf/1910.11099.pdf.
[38] Alex Lee, "This Ugly T-Shirt Makes You Invisible to Facial Recognition Tech," *WIRED UK*, May 11, 2020, https://www.wired.co.uk/article/facial-recognition-t-shirt-block.

adversarial designs may ultimately only serve to improve surveillance systems, which are likely to be programmed and re-programmed to overcome perturbations. In the wake of COVID-19, Japanese company NEC, whose NeoFace Live Facial Recognition application is used by the Met Police in the UK, accepted the challenge to develop new technology that could identify people wearing face masks. A spokesperson for the company told *Reuters* that the technology had been introduced as "needs grew even more, due to the coronavirus situation."[39] The new system's identification of people wearing face coverings takes less than one second, with an accuracy rate of more than 99.9%. If not for the widespread adoption of masking—and its doubling as not only a tool for public health, but also for privacy in public—it is possible that this technology may never have been developed.

§5 The Unharnessed Potential of a Performative Framework for Privacy

For all their philosophical failures and technological fallacies, is there any role at all for these aesthetic interventions—or the artists behind them—in the anti-surveillance and anti-subordination movements of contemporary society? Previously, we briefly alluded to their potential to create solidarity as conspicuous and symbolic forms of expression, which may be helpful in overcoming collective action problems in spaces of confrontation. Going beyond that, here we argue that they may point toward the need—and help pave the way for—a wholly new framework for privacy in public. As the role of the artist is a public-facing one by nature, artists may be able to support anti-subordination efforts insofar as they continue to redirect attention toward everyday forms of preserving privacy that have been, and continue to be, criminalized by law enforcement and broader society alike.

As John McGrath has explained, "while art and theatre work responding to surveillance society can help us exist productively in this world, it is still the banal experience of day-to-day footage and data that defines our encounter with surveillance."[40] And relatedly, everyday attempts to maintain privacy in public are ultimately what define a community's relationship with law enforcement, which—in the case of marginalized groups—may likely criminalize these efforts, using them as a basis for further surveillance and subjugation. Xenophobic proposals to ban the public wearing of burqas by Muslim

[39] "Facial Recognition Identifies People Wearing Masks," *BBC News* (BBC, January 7, 2021), https://www.bbc.com/news/technology-55573802.

[40] John McGrath, *Loving Big Brother: Surveillance Culture and Performance Space* (Florence: Taylor and Francis, 2004).

women, a religious practice that also helps to preserve privacy in public, have been passed into law in France, Belgium, Denmark, Austria, and Bulgaria.[41] And in the highly publicized murder trial of George Zimmerman, who shot and killed innocent 17-year-old Trayvon Martin in his own neighborhood, the defense counsel perversely framed the victim's hoodie as a symbol of aggression, begetting suspicion and even a need for self-defense.[42] It is impossible to reckon with such an argument, however, without considering the lens of race. Since its use by predominantly Black graffiti artists in the '70s, the hoodie has been understood—by Black communities, in particular—as both a functional means of maintaining anonymity while being expressive in and of itself.[43] The hoodie's expressive dimension only grew as Black activists organized massive "Million Hoodie Marches" to demand justice for Trayvon, and for the countless other Black men criminalized by a systemically racist criminal justice system.[44] (*See Figure 5*).

Figure 5: Protestors donned hoodies as a symbol of resistance against a racist criminal justice system in 2012, in the wake of the fatal shooting of Trayvon Martin. (Photo: Adrees Latif, *Reuters*).

Following this line of reasoning, Scott Skinner-Thompson has written extensively on how "attempts to preserve a degree of privacy or anonymity in public [...] are frequently a form of performative and expressive opposition to an ever-expanding surveillance society

[41] "Switzerland Bans Burqa, Here's List of Nations That Have Made Face Coverings in Public an Offense," *News18*, March 8, 2021, https://www.news18.com/news/buzz/switzerland-bans-burqa-heres-list-of-nations-that-have-made-face-coverings-in-public-an-offense-3510107.html.

[42] Colleen Curry, "Smithsonian Eyes Trayvon Martin Hoodie for Museum Exhibit," *ABC News*, August 1, 2013, https://abcnews.go.com/US/smithsonian-eyes-trayvon-martin-hoodie-museum-exhibit/story?id=19836962.

[43] Scott Skinner-Thompson, *Privacy at the Margins*, 66-67.

[44] "A Million Hoodies March," *Reuters*, March 22, 2012.

and [...] may be protected as symbolic, expressive conduct under the First Amendment."[45] As such, "...once conceptualized as acts of performative, expressive resistance, attempts to maintain privacy in public against government surveillance may fare better under the First Amendment's protections for expressive conduct than under traditional Fourth Amendment privacy protections, which have been severely hamstrung by doctrines such as the third-party doctrine."[46] And the implications go beyond the doctrinal, toward the discursive. Through the lens of expression, privacy moves away from the defensive and toward the assertive. In this sense, a theory of performative privacy also "has the potential to subvert the perceived reality that a surveilled individual 'is the object of information, never communication,'" in the words of critical theorist bell hooks.[47]

§6 Recommendations for Future Research

As cyberspace, not physical space, is arguably the emerging frontier for technologically mediated oppression, future research might benefit from considering online performativity as a form of expressive privacy. Moreover, considering that the European Union employs a very different paradigm for privacy protections than the U.S.—a framework that premised on protections *by* the government, *from* corporate surveillance—it would be valuable to investigate how adversarial strategies might differ in this context. Finally, considering the disproportionate effects of surveillance on marginalized groups in society, the central charge issued by Audre Lorde in her essay "The Transformation of Silence into Language and Action" remains urgent as ever. "Where the words of [these marginalized communities] are crying to be heard," Lorde writes, "we must each of us recognize our responsibility to seek those words out, to read them and share them and examine them in their pertinence to our lives."[48] In all its potential directions, future research ought in any case to commit fiercely to elevating the voices of those most vulnerable to privacy infringements, for whom privacy is most essential for the whole circle of human activities—from basic survival, to cultural expression, to the many intersections therein.

---

[45] Scott Skinner-Thompson, *Privacy at the Margins*, 45.
[46] Ibid., 95.
[47] Ibid., 45-46.
[48] Audre Lorde and Mahogany L. Browne, *Sister Outsider* (New York: Penguin Books, 2020).

§7 References

Barriga, Antónia do Carmo, Ana Filipa Martins, Maria João Simões, and Délcio Faustino. "The COVID-19 Pandemic: Yet Another Catalyst for Governmental Mass Surveillance?" Social Sciences & Humanities Open. Elsevier, December 4, 2020. https://www.sciencedirect.com/science/article/pii/S2590291120300851.

Benjamin, Garfield. "From Protecting to Performing Privacy." ODU Digital Commons. Journal of Sociotechnical Critique, May 2020. https://digitalcommons.odu.edu/sociotechnicalcritique/vol1/iss1/1/.

Bennett Cyphers, Adam Schwartz. "Face Recognition Isn't Just Face Identification and Verification: It's Also Photo Clustering, Race Analysis, Real-Time Tracking, and More." Electronic Frontier Foundation, October 15, 2021. https://www.eff.org/deeplinks/2021/10/face-recognition-isnt-just-face-identification-and-verification.

Bridges, Khiara M. *The Poverty of Privacy Rights*. Stanford, CA: Stanford Law Books, 2017.

Curry, Colleen. "Smithsonian Eyes Trayvon Martin Hoodie for Museum Exhibit." ABC News. ABC News Network, August 1, 2013. https://abcnews.go.com/US/smithsonian-eyes-trayvon-martin-hoodie-museum-exhibit/story?id=19836962.

Doctorow, Cory. "Design Fiction, Politicized: The Wearable Face Projector." Boing Boing, October 17, 2019. https://boingboing.net/2019/10/17/jing-cai-liu.html.

"Facebook's Deepface Shows Serious Facial Recognition Skills." CBS News. CBS Interactive, March 19, 2014. https://www.cbsnews.com/news/facebooks-deepface-shows-serious-facial-recognition-skills/.

"Facial Recognition Identifies People Wearing Masks." BBC News. BBC, January 7, 2021. https://www.bbc.com/news/technology-55573802.

Garcia-Rojas, Claudia. "The Surveillance of Blackness: From the Trans-Atlantic Slave Trade to Contemporary Surveillance Technologies." Truthout, March 3, 2016. https://truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police/.

Garvie, Clare, Alvaro Bedoya, and Jonathan Frankle. "The Perpetual Line-Up: Unregulated Police Face Recognition in America." Perpetual Line Up. Accessed December 9, 2021. https://www.perpetuallineup.org/.

Glusac, Elaine. "Your Face Is, or Will Be, Your Boarding Pass." *The New York Times*. The New York Times, December 7, 2021. https://www.nytimes.com/2021/12/07/travel/biometrics-airports-security.html.

Harwell, Drew. "Wrongfully Arrested Man Sues Detroit Police over False Facial Recognition Match." *Washington Post.* https://www-washingtonpost-com.ezp-prod1.hul.harvard.edu/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/ology/2021/04/13/facial-recognition-false-arrest-lawsuit/.

Hitti, Natashah. "Ewa Nowak's Anti-AI Mask Protects Wearers from Mass Surveillance." Dezeen, July 30, 2019. https://www.dezeen.com/2019/07/30/ewa-nowak-anti-ai-mask-protects-wearers-from-mass-surveillance/.

Juris, Jeffrey S. "Performing Networks at Direct-Action Protests." Essay. In *Networking Futures the Movements against Corporate Globalization*. Durham, NC: Duke University Press, 2008.

Lee, Alex. "This Ugly T-Shirt Makes You Invisible to Facial Recognition Tech." WIRED UK. WIRED UK, May 11, 2020. https://www.wired.co.uk/article/facial-recognition-t-shirt-block.

Lorde, Audre, and Mahogany L. Browne. *Sister Outsider*. New York: Penguin Books, 2020.

McGrath, John. *Loving Big Brother: Surveillance Culture and Performance Space*. Florence: Taylor and Francis, 2004.

"A Million Hoodies March." Reuters. Thomson Reuters, March 22, 2012. https://www.reuters.com/news/picture/a-million-hoodies-march-idUSRTR2ZQ6L.

Monahan, Torin. "The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance." *Communication and Critical/Cultural Studies* 12, no. 2 (2015): 159–78. https://doi.org/10.1080/14791420.2015.1006646.

Parkhi, Omkar M, Andrea Vedaldi, and Andrew Zisserman. "Deep Face Recognition." Proceedings of the British Machine Vision Conference (BMVC) 2015, September 2015. http://www.bmva.org/bmvc/2015/papers/paper041/index.html.

Reports, Special. "Rite Aid Deployed Facial Recognition System in Hundreds of U.S. Stores." Reuters. Thomson Reuters, July 28, 2020. https://www.reuters.com/investigates/special-report/usa-riteaid-software/.

Sato, Mia. "The Pandemic Is Testing the Limits of Face Recognition." MIT Technology Review. MIT Technology Review, September 30, 2021. https://www.technologyreview.com/2021/09/28/1036279/pandemic-unemployment-government-face-recognition/.

Seth Lazar, Claire Benn, and Mario Günther. "Large-Scale Facial Recognition Is Incompatible with a Free Society." The Conversation, July 10, 2020. https://theconversation.com/large-scale-facial-recognition-is-incompatible-with-a-free-society-126282.

Sharif, Mahmood, Sruti Bhagavatula, Lujo Bauer, and Michael K. Reiter. "Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, October 1, 2016. https://dl.acm.org/doi/10.1145/2976749.2978392.

Skinner-Thompson, Scott. *Privacy at the Margins*. Cambridge: Cambridge University Press, 2021.

"Switzerland Bans Burqa, Here's List of Nations That Have Made Face Coverings in Public an Offense." *News18*, March 8, 2021. https://www.news18.com/news/buzz/switzerland-bans-burqa-heres-list-of-nations-that-have-made-face-coverings-in-public-an-offense-3510107.html.

"Struggle for Power: The Ongoing Persecution of Black Movement by the U.S. Government." M4BL, September 1, 2021. https://m4bl.org/struggle-for-power/.

Taylor, Adam. "Why Is the World Protesting so Much? A New Study Claims to Have Some Answers." *The Washington Post*. WP Company, November 4, 2021. https://www.washingtonpost.com/world/2021/11/04/protests-global-study/.

Xu, Kaidi, Gaoyuan Zhang, Sijia Liu, Quanfu Fan, Mengshu Sun, Hongge Chen, Pin-Yu Chen, Yanzhi Wang, and Xue Lin. "Adversarial T-Shirt: Evading Person Detectors in a Physical World," July 7, 2020. https://arxiv.org/pdf/1910.11099.pdf.