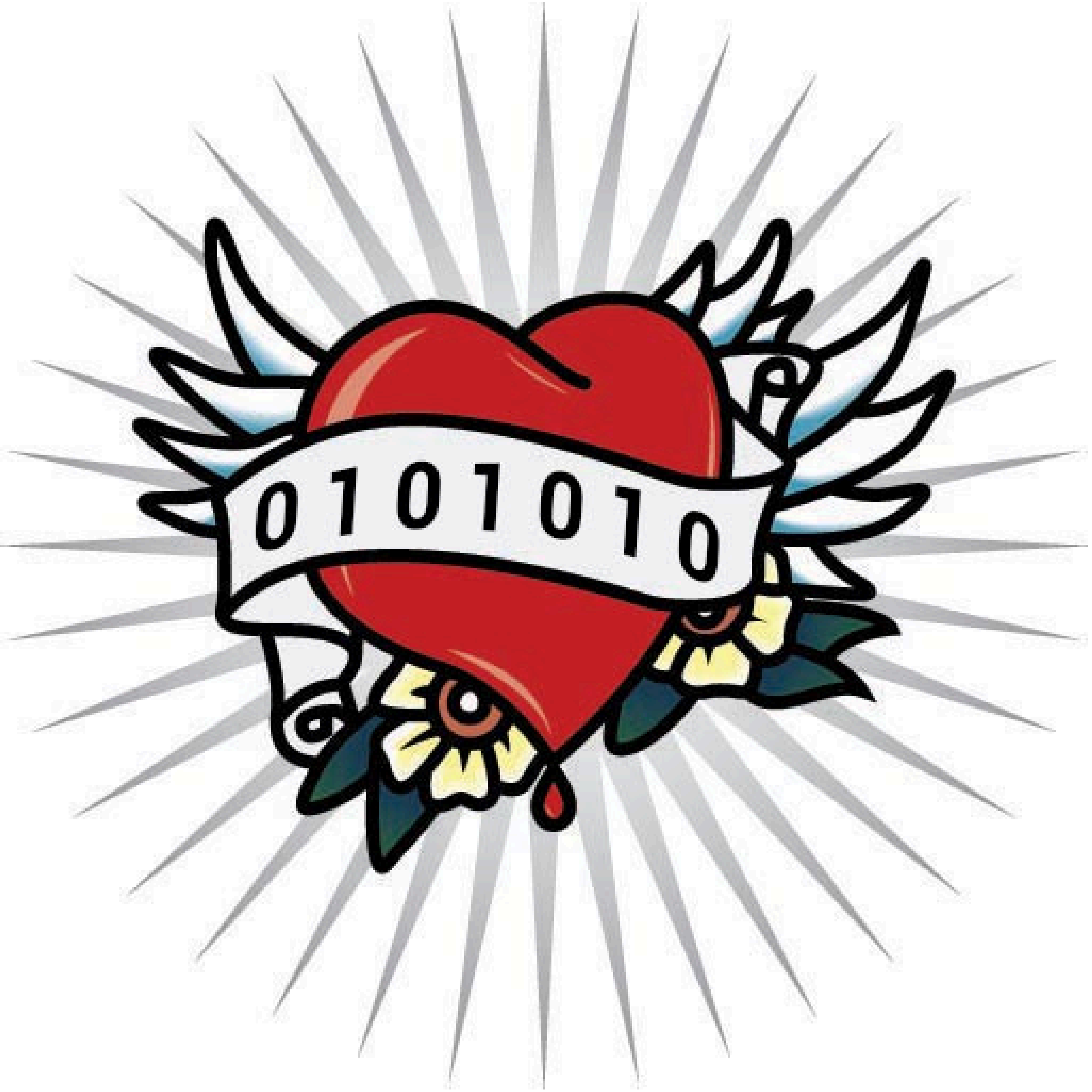
Anti Facial Recognition Make Up Workshop



Why?

- Surveillance and control: States and private companies use facial recognition to comprehensively document and control individuals.

- Loss of informational self-determination: Automatic identification processes encroach on privacy and personal rights.

- Discrimination and bias: Facial recognition systems show systematic prejudice, especially against marginalized groups.

- Economic use: Personal data is traded as a commodity in the context of “surveillance capitalism”.

- Identity attributions through algorithms: Bodies are dynamically categorized by training data and software, often without the consent of those affected.

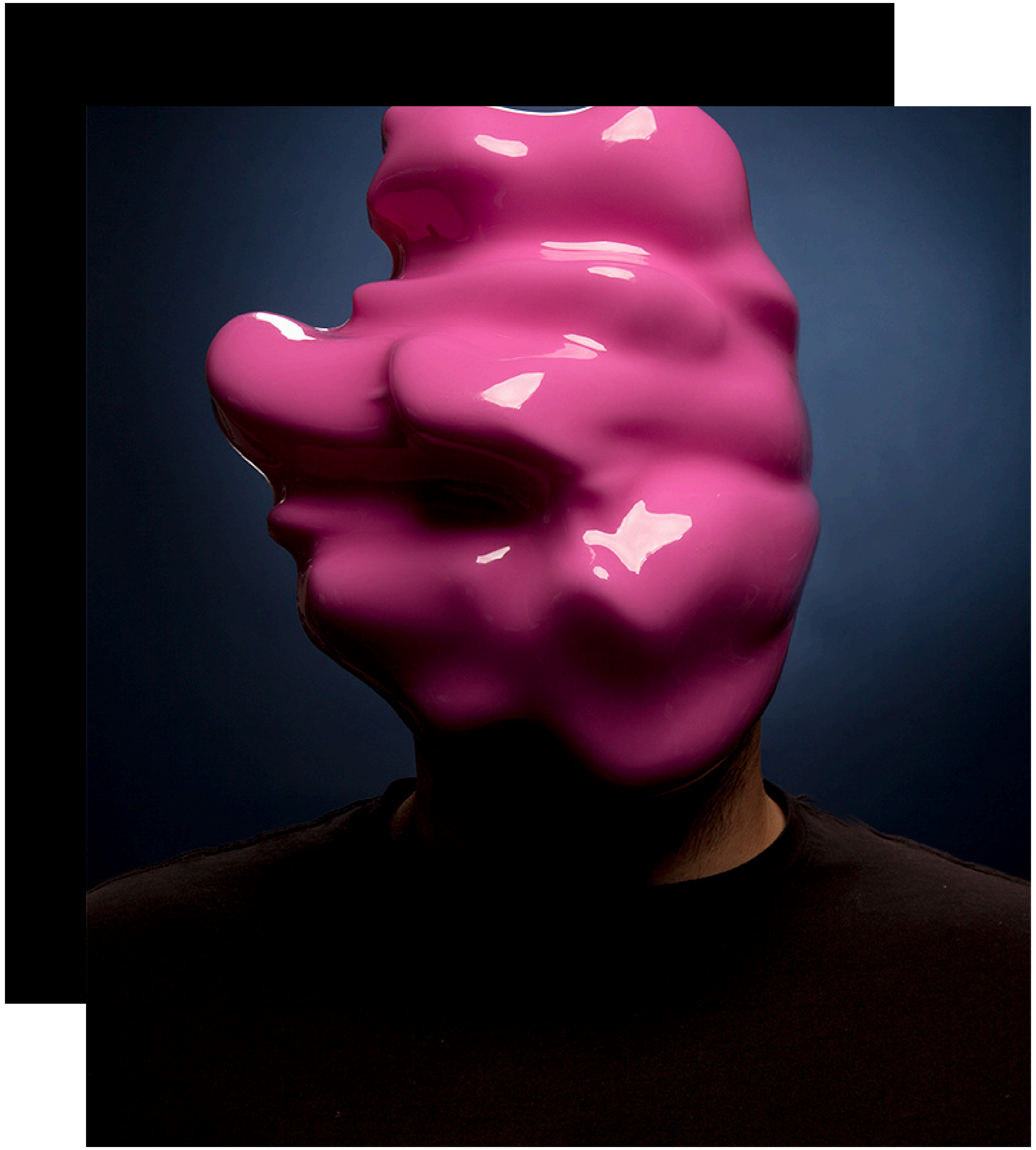
Interesting Projects

https://reclaimyourface.eu/

- German project: https://gesichtserkennung-stoppen.de/
- This is the project page for organising against facial recognition (on EU-level and German level). Lots of good information on the current state of affairs, and organising petitions against further breaches.

https://urban-privacy.com/pages/faception/

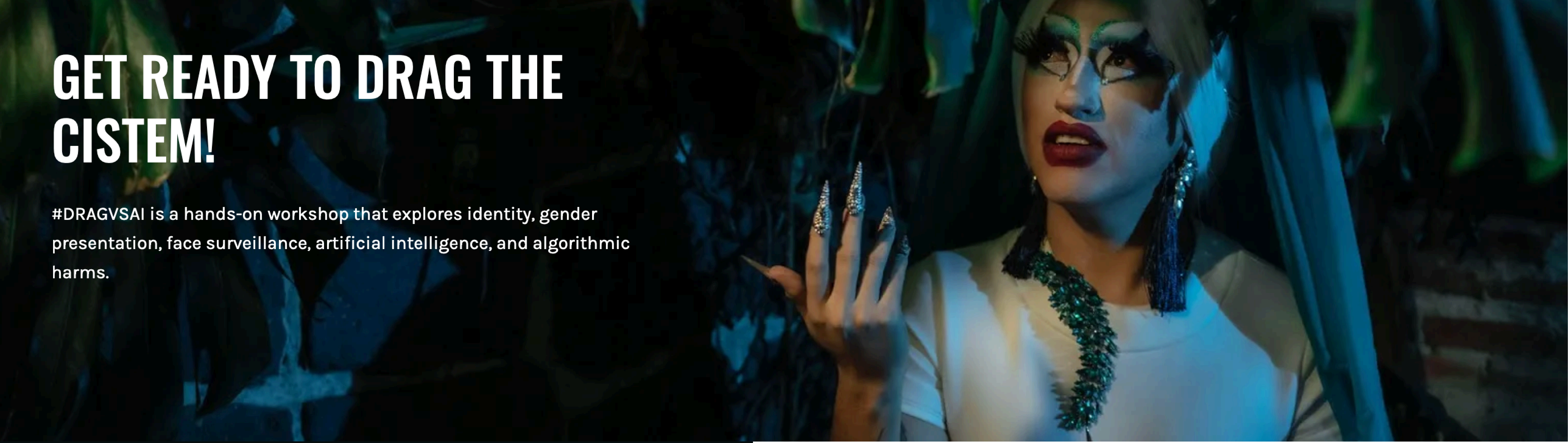
Fashion label that develops fashion against surveillance. e.g. a hoodie that includes irregular patterns to disrupt facial recognition



Facial Weaponization Suite

Zach Blas

Facial Weaponization Suite protests against biometric facial recognition–and the inequalities these technologies propagate–by making “collective masks” in workshops that are modeled from the aggregated facial data of participants, resulting in amorphous masks that cannot be detected as human faces by biometric facial recognition technologies. The masks are used for public interventions and performances. These masks intersect with social movements’ use of masking as an opaque tool of collective transformation that refuses dominant forms of political representation.



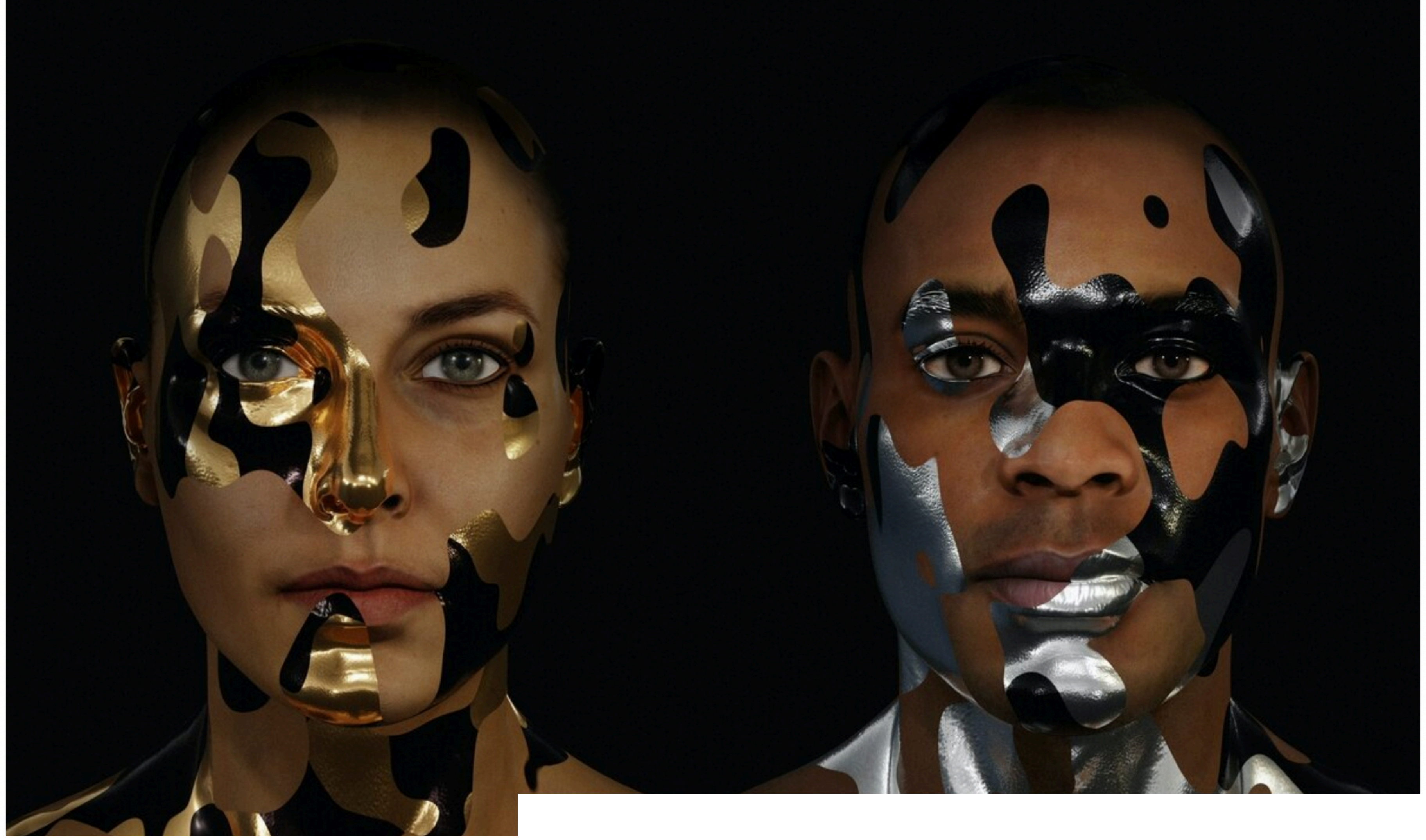
GET READY TO DRAG THE CISTEM!

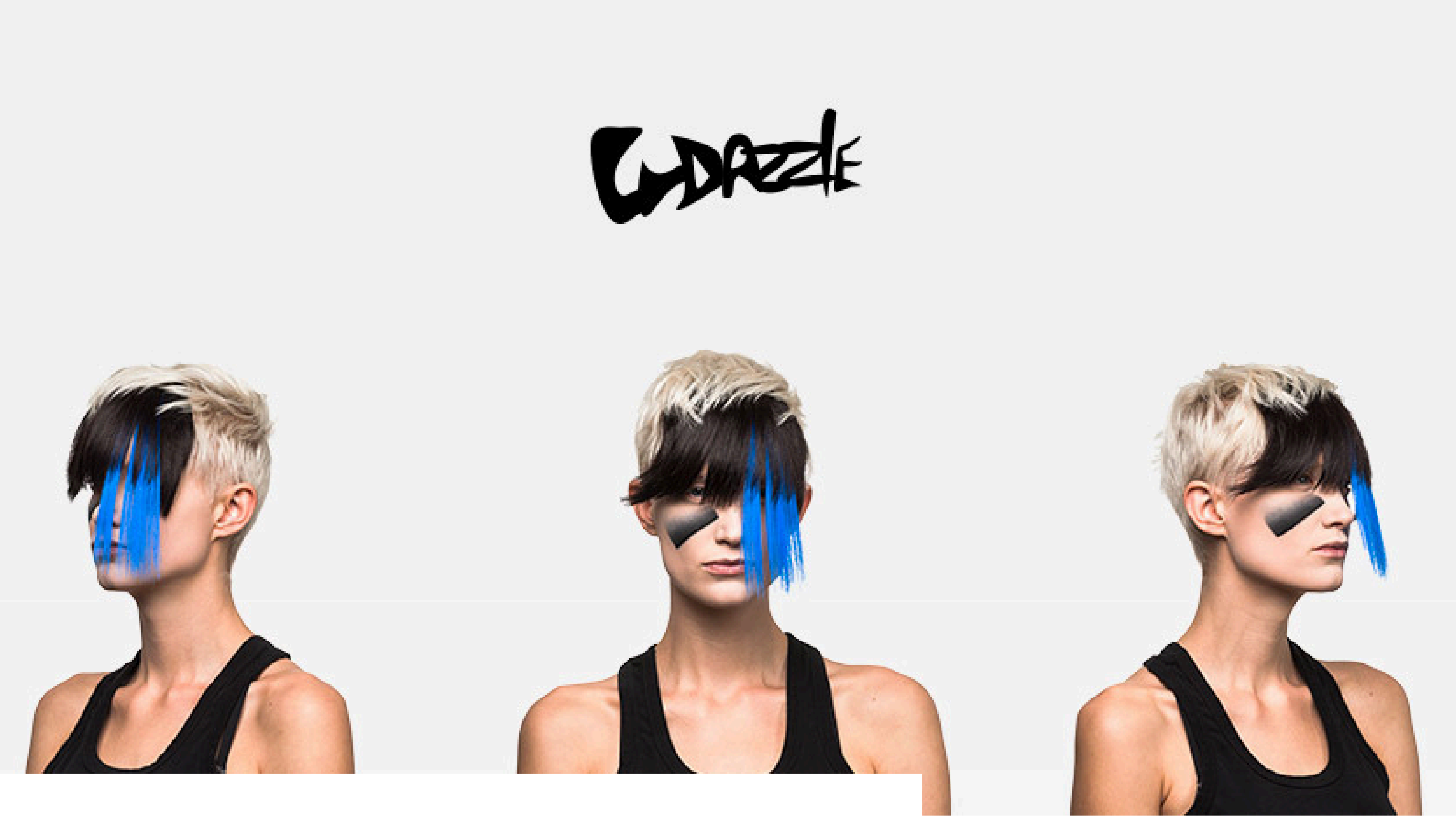
#DRAGVSAI is a hands-on workshop that explores identity, gender presentation, face surveillance, artificial intelligence, and algorithmic harms.

Drag vs AI Workshop

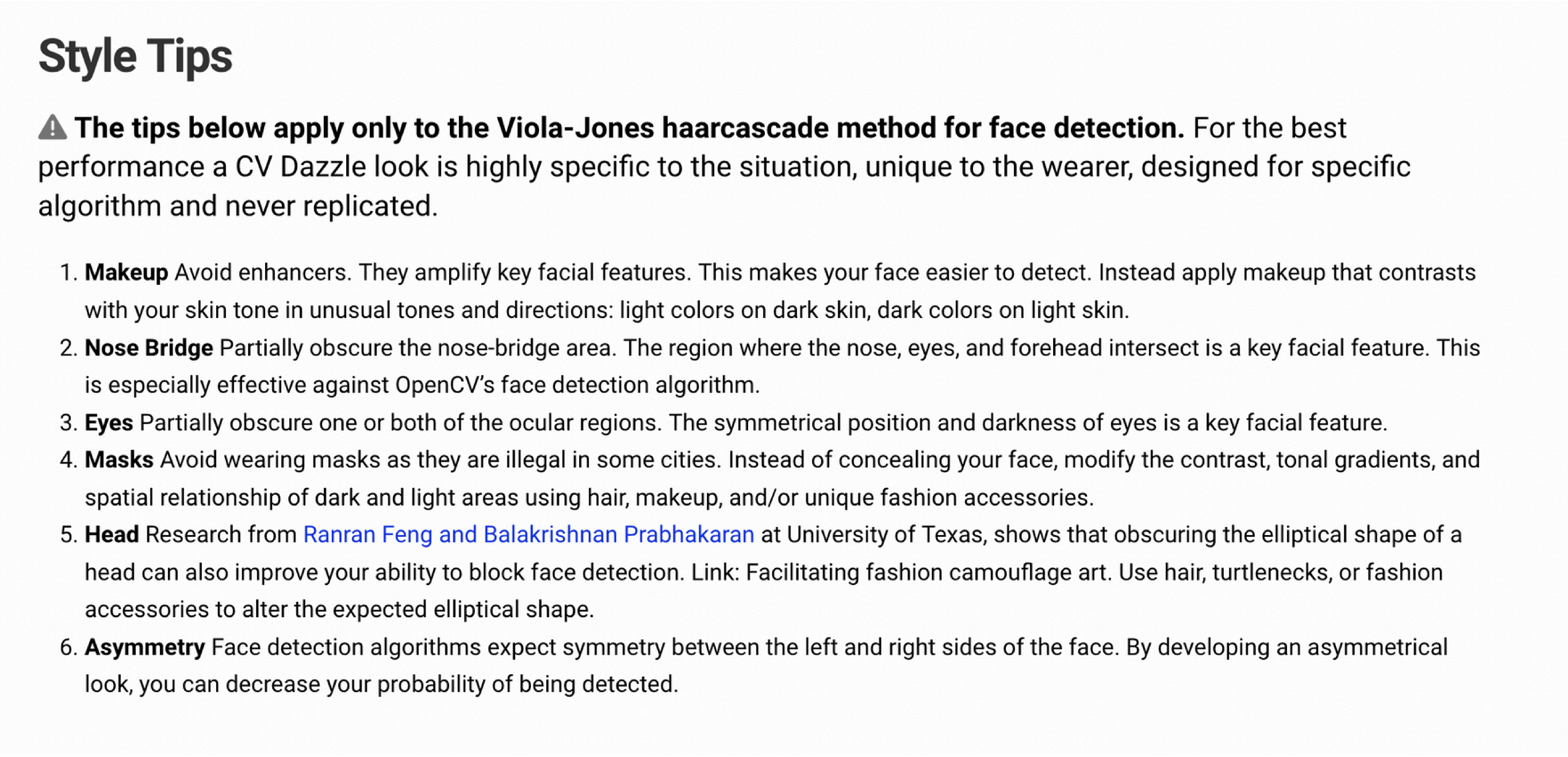
THE ALGORITHMIC JUSTICE LEAGUE

The Algorithmic Justice League is powered by an interdisciplinary and international team of activists, artists, researchers, and technologists. Founded by Dr. Joy Buolamwini, our collective is united by a commitment to challenging bias in artificial intelligence and advocating for ethical, accountable technology. We blend rigorous research with creative expression to illuminate the hidden impacts of AI systems on society.





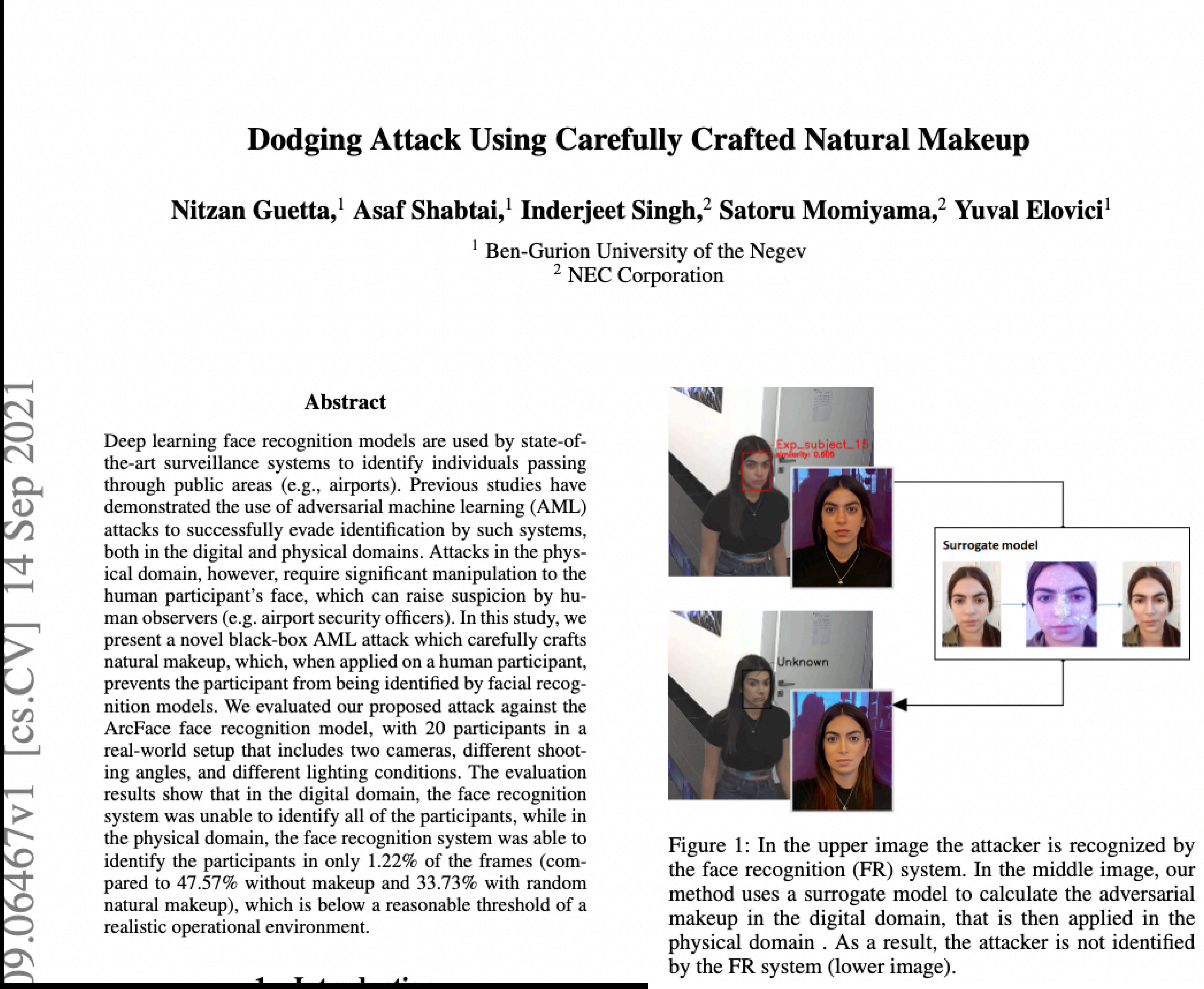
Adam Harvey: CV Dazzle



Style Tips

⚠ **The tips below apply only to the Viola-Jones haarcascade method for face detection.** For the best performance a CV Dazzle look is highly specific to the situation, unique to the wearer, designed for specific algorithm and never replicated.

1. **Makeup** Avoid enhancers. They amplify key facial features. This makes your face easier to detect. Instead apply makeup that contrasts with your skin tone in unusual tones and directions: light colors on dark skin, dark colors on light skin.
2. **Nose Bridge** Partially obscure the nose-bridge area. The region where the nose, eyes, and forehead intersect is a key facial feature. This is especially effective against OpenCV's face detection algorithm.
3. **Eyes** Partially obscure one or both of the ocular regions. The symmetrical position and darkness of eyes is a key facial feature.
4. **Masks** Avoid wearing masks as they are illegal in some cities. Instead of concealing your face, modify the contrast, tonal gradients, and spatial relationship of dark and light areas using hair, makeup, and/or unique fashion accessories.
5. **Head** Research from Ranran Feng and Balakrishnan Prabhakaran at University of Texas, shows that obscuring the elliptical shape of a head can also improve your ability to block face detection. Link: Facilitating fashion camouflage art. Use hair, turtlenecks, or fashion accessories to alter the expected elliptical shape.
6. **Asymmetry** Face detection algorithms expect symmetry between the left and right sides of the face. By developing an asymmetrical look, you can decrease your probability of being detected.



Dodging Attack Using Carefully Crafted Natural Makeup

Nitzan Guetta,[1] Asaf Shabtai,[1] Inderjeet Singh,[2] Satoru Momiyama,[2] Yuval Elovici[1]

[1] Ben-Gurion University of the Negev
[2] NEC Corporation

Abstract

Deep learning face recognition models are used by state-of-the-art surveillance systems to identify individuals passing through public areas (e.g., airports). Previous studies have demonstrated the use of adversarial machine learning (AML) attacks to successfully evade identification by such systems, both in the digital and physical domains. Attacks in the physical domain, however, require significant manipulation to the human participant's face, which can raise suspicion by human observers (e.g. airport security officers). In this study, we present a novel black-box AML attack which carefully crafts natural makeup, which, when applied on a human participant, prevents the participant from being identified by facial recognition models. We evaluated our proposed attack against the ArcFace face recognition model, with 20 participants in a real-world setup that includes two cameras, different shooting angles, and different lighting conditions. The evaluation results show that in the digital domain, the face recognition system was unable to identify all of the participants, while in the physical domain, the face recognition system was able to identify the participants in only 1.22% of the frames (compared to 47.57% without makeup and 33.73% with random natural makeup), which is below a reasonable threshold of a realistic operational environment.

1. Introduction

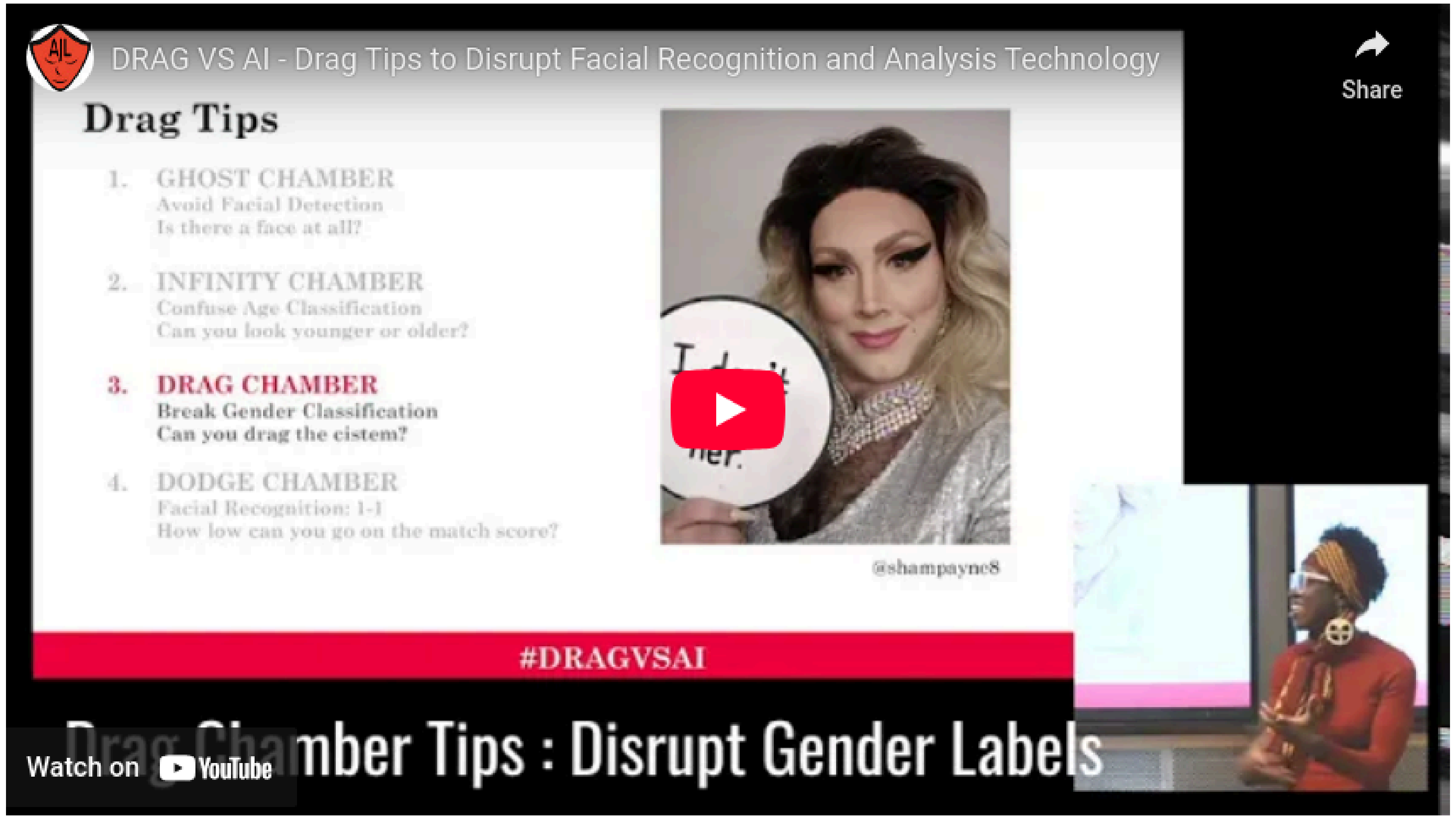
Figure 1: In the upper image the attacker is recognized by the face recognition (FR) system. In the middle image, our method uses a surrogate model to calculate the adversarial makeup in the digital domain, that is then applied in the physical domain . As a result, the attacker is not identified by the FR system (lower image).

“Natural” looking make-up

Non-makeup strategies

- Medical Masks, hoodies, sunglasses, ski glasses, costume masks, hats and more... may all serve as devices to avoid automated detection in different situations
- Consider: is it safe / sensible in your situation to potentially attract attention from humans with unique makeup, while evading machine automated detection?
- A note on Vermummungsverbot in Germany

Tutorials



DRAG VS AI - Drag Tips to Disrupt Facial Recognition and Analysis Technology

Drag Tips

1. GHOST CHAMBER
   Avoid Facial Detection
   Is there a face at all?
2. INFINITY CHAMBER
   Confuse Age Classification
   Can you look younger or older?
3. DRAG CHAMBER
   Break Gender Classification
   Can you drag the cistem?
4. DODGE CHAMBER
   Facial Recognition: 1-1
   How low can you go on the match score?

@shampayne8

#DRAGVSAI

Drag Chamber Tips : Disrupt Gender Labels