

Move over, Paris. Sartorial hacking is le dernier cri

August 18 2019, by Nancy Cohen



- License Plate** MJZ52X Florida
- Vehicle Color** Black
- Vehicle Orientation**
- License Plate** 8D6234 Nevada
- Vehicle Orientation**
- License Plate** 97Y7946 California
- Vehicle Type** Suv-Crossover
- Vehicle Orientation**

Not fashion chic; it is fashion cheek.

We have moved from a fashion era of Power Dressing to Sartorial Hacking.

Difficult to stop the pithy critiques but one must, to relay the anti-surveillance news.

Garments were revealed at the DefCon cybersecurity conference in Las Vegas earlier this month. The designer Kate Rose presented the collection of her Adversarial Fashion line of clothing. Its license-plate images are to confuse automated license plate readers by introducing "garbage data" into the reader systems.

Rose shared her upbeat view of hacking in *Vice*: "[Hacking](#) is fundamentally about democratizing and [demystifying](#) the systems and devices we all use, helping each other learn that we're smart enough to take apart and tinker with them, and reapply them to what you personally think is a good idea," she said.

Samantha Cole wrote about the Rose undertaking on Thursday in *Vice*. The clothes, covered with images of fake license plates, are designed for deceiving an ALPR, which stands for Automatic License Plate Reader.

The readers are seemingly everywhere. But, Cole wrote, "they're much more than speed trap cameras. ALPRs are privately-owned systems that capture everything resembling a license plate within their purview, collecting up to a thousand plates per minute."

On the website Adversarial Fashion, Rose explained that "The patterns on this page were generated by testing a series of modified license plate images with commercial ALPR APIs, working to generate aesthetic [fabric](#) patterns that read in to devices and services as if they were real plates."

What kinds of garments in her collection? You name it: crop tops, unisex t-shirts, [jackets](#), hoodies, dresses, skirts.

The designer developed and tested the repeating patterns on her fabrics to look as close to a real plate as possible, so that the system will save it as real, said *Vice*. A model's body hugging dress does not say Grateful Dead or Dior or Fendi or Ralph Lauren. It has words and numbers strings like YNM 270 and EYP-4735.

The Electronic Frontier Foundation had more: ALPRs are high-speed, computer-controlled camera systems, and data includes photographs of the vehicle and sometimes its driver and passengers. Information is uploaded to a central server. According to the EFF, "One vendor brags that its dataset includes more than 6.5 billion scans and grows at a [rate](#) of 120-million data points each month."

Most of this data is stored in databases "for extended periods of time—often as much as five years. The databases may be maintained by the [police departments](#), but often they are maintained by private companies," said the EFF.

Charlotte Jee in *MIT Technology Review*: The ALPRs have caused "consternation among privacy advocates, who say they enable a legally questionable form of mass [surveillance](#)."

Nonetheless, arguments in favor of ALPRs were included in the *Vice* article. "Without ALPR technology, law [enforcement](#) officers must collect license plates by hand. This creates practical limitations on the amount of data that can be collected and means officers must make choices about which vehicles they are going to track. ALPR technology removes those limitations and allows officers to track everyone, allowing for faster and broader collection of license plates with far reduced staffing requirements."

On the other hand, Rose could be sending a helpful wakeup call for those who issue verification systems. [Alex](#) Hern, *The Guardian*, reported

from Vegas on Wednesday: "Rose likens her work to that of other security researchers at DefCon. 'If a phone is discovered to have a vulnerability, we don't throw our phones away. This is like that, disclosing a vulnerability. I was shocked it was so easy, and I would call on people who think these systems are critical to find better ways to do that verification.'"

Surveillance-thwarting fashion has a history; Rose's line of reader-confusing images on clothes shares a history with other attempts.

"Though it's the first to target ALPRs, this isn't the first fashion project aimed at fighting back against surveillance," said Jee in *MIT Technology Review*. "[Researchers](#) have come up with adversarial images on clothing aimed at bamboozling AI, makeup that lets you hide your face from recognition systems, and even a hat that can trick systems into thinking you're Moby."

More information: adversarialfashion.com/

[adversarialfashion.com/pages/d ... privacy-presentation](https://adversarialfashion.com/pages/d...-privacy-presentation)

© 2019 Science X Network

Citation: Move over, Paris. Sartorial hacking is le dernier cri (2019, August 18) retrieved 20 September 2024 from

<https://techxplore.com/news/2019-08-paris-sartorial-hacking-le-dernier.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.