Counter(media) Intelligence and Visioning: An Interview with Adam Harvey

by Adam Harvey and Patrick Brian Smith

What are the uses and misuses of computer vision and artificial intelligence? How can technologies that are indissolubly wedded to modalities of surveillance and capture be taken up subversively, made to speak back to the technics of state and corporate power? In this short interview piece, Adam Harvey—an artist and research scientist based in Berlin focused on computer vision, privacy, and surveillance—responds to these questions. He is a graduate of the Interactive Telecommunications Program at New York University (2010) and is the creator of the VFRAME.io computer vision project, the Exposing.ai dataset project, and the CV Dazzle computer vision camouflage concept.

I wanted to start by asking you how your research and artistic practice came to be focused on the theoretical and practical potentialities (and pitfalls) of computer vision and artificial intelligence. Did this emerge from a set of material developments in your artistic practice, or a broader conceptual and political interest?

My original interest in computer vision was motivated by previous experience as a photographer, and the harsh realization that photography was not only a form of art-making but also evidence-production. As image making technology grew more powerful and cheaper, photography became indistinguishable from surveillance and that pushed me further away from it. Around 2009, I realized that photos being posted online were laying the foundation for a future where the Internet would become a giant facial recognition database, which is clearly now a reality. Based on this projection, I reoriented my artistic practice and started exploring counter-surveillance projects

Within much of your work, there are interesting tensions around how we define artificial intelligence, or, often, how we dangerously *misdefine* and *misuse* the term. Here I'm also thinking of the volume *Fake AI* (edited by Frederike Kaltheuner, Meatspace Press, 2021), to which you contributed an article on face recognition technologies. I was wondering if you could speak a little about how you both understand and apply the term within your own work?

The joke is that everyone applies for Artificial Intelligence funding but then just uses it to make a web scraper. Actually, there isn't much difference. Most of what is considered to be AI is other peoples' data. In the same way that the "Cloud" metaphor abstracts and hides infrastructure, the term "AI" abstracts and hides the origins of information.

Among the largest and most popular datasets used in AI research projects are Common Crawl (for NLP), and ImageNet and COCO (for computer vision), which are all derived from user-generated content. In my research project Exposing.ai, I've highlighted how this becomes problematic when images are used for building face recognition technologies. For example, the MegaFace dataset used over 4.7M faces from photos uploaded to Flickr in order to build what was at the time the largest publicly available face recognition dataset. MegaFace is instrumental in advancing the capabilities of face recognition for law enforcement, defense contractors, and surveillance companies. Face recognition, as well as the term AI, can be better understood by considering the data sources because that's where the actual value is. Without data AI is useless.

In the chapter for Fake AI, titled "What is a Face?" you suggest there is a need to balance between "making room" for the development of artificial intelligence technologies in certain spheres but also a need to "blunt" them within others. I was wondering if you might be able to expand on this broad tension between the liberatory or activist potentialities of such technologies, and their longer historical interconnections with regimes of state/corporate surveillance and control?

Echoing the final lines of the essay, it is critical to deconstruct the vague and misleading language used to describe AI/ML/CV systems in order to prevent their misuse. For example, it would not be practical to outright ban "face recognition" if the same technology is also used to log into your phone. But it's not. And that's become hard to explain because the language around face recognition is too limited and narrow. The essay explains why this is more complicated than it seems. Even the term "face" is not yet well defined. I think deconstructing and recontextualizing the terms is a good starting point to imagine liberatory or activist applications. For example, face detection, often linked to surveillance applications, can also be used in reverse for redacting faces because face detection is not a surveillance algorithm, it's merely a specific class of object detection with many other applications to entertainment.

Within your recent video that explores your collaborative work with Mnemonic (a Berlin-based organization dedicated to documenting war crimes and human rights violations), you explain how you are developing "synthetic image training data to build object detection algorithms to locate munitions in large-scale video archives from conflict zones." Here, synthetic data helps locate material evidence. There is an interesting relationship between the synthetic and material here. I was wondering if you could speak about this interconnection a little bit more?

I've addressed this topic in an essay for the volume *Chimeras: Inventory of synthetic cognition* (edited by Ilan Manouach and Anna Engelhardt, Onassis Foundation, 2022), which is also available on my website. Hopefully this also provides a response to the question.