THE UNIVERSITY OF CHICAGO

Open-Source Surveillance- Do You Own Your Face?

By

Kiara D. Kiene

May 2024

A paper submitted in partial fulfillment of the requirements for the Master of Arts degree in the

Master of Arts Program in the Social Sciences

Preceptor: Marshall Kramer

Introduction

"…The PimEyes face search tool worked. David was able to upload screenshots of women whose pornography he had watched and get photos of them from elsewhere on the web, a trail that sometimes led him to their legal names. From there, he could know where they lived and find them in the real world, a scary possibility if he had the desire to hurt or assault them. But that was not the appeal for him. Unmasking them was all he sought to do.

"You find them on Facebook and see their personal pictures or whatever and it makes it more exciting," David said. "It's like the secret identity of Batman or Superman. You're not supposed to know who this person is, they didn't want you to know, and somehow you found out." (Hill, 2023a)

Questions regarding privacy have gained incredible urgency, especially in light of the vast amount of data that can be used to identify individuals and ascertain their lives, preferences, and behaviors which have effectively "...summoned the digital into our everyday lives" (Zuboff, 2019: 18). Data in all of its forms has become the primary axis for profitability in digital spaces and some of the types of data that could exert truly profound impacts on individual lives include data with knowledge that directly impilcates and involves the body (Grauer, 2023) and legal question about the nature of data and the bounds of its ownership have gained additional weight (Leonard, 2020). Facial recognition technologies are an example of this and there has been a great deal of discussion as to the threat this technology as used by governments and large corporations poses to privacy and freedom (*The fight to stop face recognition technology,* 2023). However, a new application and potential for the technology has begun to take shape: the creation and use of facial recognition tools and applications potentially accessible to all with

knowledge of its existence and/or the means financial or social to do so. The most important of these tools is at present the paid facial recognition service and search engine PimEyes. And while it is operated by and on the basis of the individual as opposed to by powerful institutions on the level of populations, its potential for profound social and personal impacts cannot be ignored.

A Brief History of Facial Recognition Technology

The incredible changes that have defined the 20th and 21st centuries have facilitated an immense variety of imperatives, needs and perspectives on the roles and interests of governments, cooperations, and citizens. Among the greatest of these were the co-occurring (though occasionally conflicting aims) circulation of goods, but also of people and ideas aided by technologies such as the telegraph, telephone, railway, highway, and the consequent aim of regulating, rendering understandable, tracing, and using this information to guide subsequent governmental or administrative action. Foucault cites this focus in circulation as a central part of the development of market liberalism (Foucault 48-49). It is of little surprise then that many observers have noted that these shifts led to the formation of drives to account for the movement of individuals and populations. Kelly A. Gates cites John Torpey who argues that there was a subsequent logic to "monopolize the legitimate means of movement" (Gates, 2011: 33). These simple facts combined with the power of the human face in almost all human interaction (and its accompanying perceived irrevocable, biological, and unique tie to one specific person) created a problem and an interest in "reembodying disembodied identities" (Ibid, 32).

Facial recognition technologies as they are understood now began their development in the mid-1960s. This was facilitated by a cooperation between computer scientists, namely Woodrow Wilson Bledsoe, his colleagues, their company Panoramic Inc. and the investment of numerous US government agencies interested in the technology for the purposes of surveillance and national security (Andrejevic and Selwyn, 2022: 5). There were myriad deficiencies in these early attempts, but the most meaningful was a limited diversity of faces, often deliberately (Andrejevic and Selwyn, 2022: 7-8). And, the issue of datasets itself is one that has posed continual challenges to the projects of computer vision more broadly. After this, the development of these technologies waxed and waned. However, in the aftermath of the September 11 terror attacks, the accompanying reconceptualization around the importance of privacy led to an increased interest in curating and creating datasets for the purposes of national security (Woodward, 2001).

A few short years later, these imperatives received yet another critical supplement: the large quantity of images of just about everything, but in particular, the abundance of human faces on search engines and social media platforms, anticipated with creations of large comprehensive datasets like ImageNet, which was critical to aiding in the development of deep learning for computer vision projects (Levy, 2023). It is central to my argument that these datasets and the application of AI as ways to work with them have had implications beyond the goal of simply recognizing faces or verifying identities. In fact, it will later be argued that this democratization of these technologies may prove the impetus for twin and co-constitutive reconfigurations of the human body. One is where representation is more easily able to be tied to the body and is therefore increasingly inseparable from the body itself. This is representation as body. The other is where the same monetary imperatives that animated the development and proliferation of these

technologies articulate with the stakes these technologies have generated in a novel way. This is where there are interests in creating a sort of copyright of the human body, enabling for the legal and financial enforcement of the protection of images of the body and face. This is the body as copyright.

A critical intervention in these implications and reformations are the number of democratized and easily accessible facial recognition services for both their ostensibly approved and more outwardly malicious purposes, the most well-known and controversial one being PimEyes. PimEyes operates essentially like a search engine for faces and advertises itself as concerned with aspects of protections against fraud and misuse of images and is available to ordinary citizens, or at least those who can pay the subscription fee (this aspect is notably complicated with the service's use in practice). A user can protect themselves through a variety of means using the service such as removing their face from the results, and critically for this analysis, the ability to use copyright claims.

Another noteworthy aspect of PimEyes' advertisement worthy of note is how it singles out another technology deeply enabled by a glut of facial data and the importance of digital images For instance, simulated media colloquially known in their malicious incarnations as deepfakes (Meikle, 2023: 2) are reliant on datasets like facial recognition and have been enabled by them and both also intersect on some of the same principles such as liveness detection (*Passive liveness detection*…; Myers, 2023). Both of these technologies have as importance to their use concerns such as whether what is being observed is actually a living human face (presence of blood flow) as well as the recognition of the object class "human face". That the specter of their existence is a primary fear justifying the use of PimEyes, both by the company itself and those using it and the gender dynamics have a great degree of overlap (to say nothing

of the potential for democratized facial recognition could aid in acquiring the data necessary to make a deepfake) means that understanding democratized facial recognition is also dependent on understanding deepfakes as both a related technology and major animating force to their use. Because of this fact, these simulated media will be mentioned throughout as important co-producers of these concerns around the face.

It is important to note that deepfakes were enabled by an advancement in deep learning; the generative adversarial network (GAN). This is essentially two neural networks, which are machine learning programs modeled after the structure of the brain that can emulate its functionality (IBM, 2024), competing against each other. One creates the fake and the other attempts to detect it. The first network then readjusts its fake and the process ultimately ends when the detector can no longer detect that the product is indeed inauthentic (Goodfellow et al: 2014). There are instances where the principles of simulated media production have been integrated into facial recognition systems. For example, GANs are used to project what an individual may look like at an older age or with a different expression, so that the individual in question may be better identified either through visual or technological means (Pupala et al, 2021; Tang, 2021). What is being dealt with at this juncture could be considered the totality of technologies of the face.

Currently, facial recognition technologies are present well beyond their initial scope of use by governments or corporations, and are now seen as the mundane actions of everyday life with regard to personal security such as unlocking a phone or even one's house (Dennon, 2021). Posting images of oneself for any number of purposes is entirely ordinary and mundane. Simulated media in addition to its pernicious effects (Jankowicz, 2021) is now an increasing part of the entertainment industry (Velasquez, 2023). And it is now being used to accommodate for

the increasing difficulty in generating facial datasets from willing participants, with examples such as the use of Nvidia's StyleGAN for facial recognition datasets and training (Sevastopolsky et al, 2023).

Methods

The fact that concerns regarding the image, control over it raises questions about what representations of the body actually are and specifically. PimEyes raises several fundamental questions that this paper cannot even begin to totally answer but are nevertheless worthy of consideration. How and why has this technological democratization occurred and been facilitated by certain companies. Surveillance capitalism itself possessed many questions about this but how are questions of ownership and privacy further upended when the tools of surveillance capitalism are now usable for ordinary citizens on each other. This is especially in light of the contradictory imperatives (collaborative construction, data extraction and brokering, privacy, fair-use, copyright, etc.) have shaped current conditions of this kind?

To attempt to shed some light on (but not fully answer these questions), I will pull upon the theories and insights of important scholars such as Kelly A. Gates, N. Katherine Hayles, Paul Virilio, Shoshana Zuboff, Luke Stark, and Katherine Levy. I will also conduct digital ethnography on the uses of democratized facial recognition on two specific online communities, though the conversation is not wholly confined to these sites and conversations from other communities will be examined.

Ethnographically, the spaces online dedicated to this task are considerably diffuse, with multiple potential uses in internet sleuthing (may include identifying suspects of crimes, missing persons, and/or unidentified decedents). Other uses include doxxing using the internet to make

public identifying and personal information for the purpose of harm to that individual (Nguyen, 2023), and the completely opposing end of identity protection. However, the prevailing trend was that the primary focus of these technologies and their use was focused on ascertaining or protecting the identities of women, often who had been involved in some type of digital sex work. Even in instances where this was not the case, there was nonetheless a prevailing trend of preoccupation with sexuality and sexual predation.

Additionally, the dynamics of vigilantism and use of this technology will be examined, but this too will in another instance intersect with the recurring concerns of sexual violation and protection from it, as well as how this may intersect with monetization, which itself was much of the primary engine for creating these lucrative and powerful datasets in the first place and continue to drive development and use.

PimEyes can be described as a democratized facial recognition service and search engine. Its stated mission is to protect the privacy of its users through "Using the latest technologies, artificial intelligence and machine learning, we help you find your pictures on the Internet and defend yourself from scammers, identity thieves, or people who use your image illegally." (*PimEyes- Select Your Plan*). On the front page of the site their purpose is described as a search going "through the Internet to find pictures containing given faces. PimEyes uses face recognition search technologies to perform a reverse image search." Additionally, the tool is stated as being "available for everyone. It is a great tool to audit copyright infringement" (*Face Recognition search engine…*). PimEyes provides tiered subscription: Open Plus, PROtect/Premium, and Advance ($29.99, $79.98, and $299.99 respectively) (ibid). There are also options to utilize the service once for $14.99 (ibid).

With the higher tiers, there is a possibility to be continually updated on instances of your image as the algorithms detect you and starting with the PROtect tier, the service provides the ability to make requests for DMCA (Digital Millennium Copyright Act) and GDPR (General Data Protection Regulation) protections on the user's behalf (ibid), further exemplifying the importance of the protection and control of one's digital image and likeness. To this end, the service also provides an opt-out feature, removing a user's image from the search results. Importantly, the opt-out feature does not remove instances of a face from sites, only from its search results (ibid), which belies an understanding of the fact that the service is used both by those who aim to protect their own privacy and those who wish to know the identity of an individual.

Participatory creation of surveillance and its subsequent Democratization

In discussions regarding digital media and surveillance, the focus has shifted from one concerned primarily with governance. As the history charted above indicates, the degree of fine-grained specificity and knowledge of the most minute and intimate details of an individual's life, down to their appearance, was possible only with the advent of social media and the ways in which search engines such as Google surveil and monitor users. Indeed, in her work *The Age of Surveillance Capitalism*: *The Fight for a Human Future at the New Frontier of Power*, Shoshana Zuboff charts the history and development of surveillance capital through Google extensively. She states that within Google specifically and amidst the struggle for purpose and profitability that beset Google when the dotcom bubble burst, the purpose and scope of the company was reimagined. She states that "Larry Page is credited with a very different and more profound answer to the question 'What is Google'... 'If we did have a category, it would be personal information... Storage is cheap. Cameras are cheap. People will generate enormous amounts of

data... Everything you've ever seen or heard or experienced will become searchable. Your whole life will be searchable" (Zuboff, 2019: 98).

The focus on images is of particular importance in this discussion. Because of the vast corpus of data emblematic of creations like Google or Facebook, a consequence was making use of this glut of image data to improve computer vision projects more broadly, and facial recognition projects more specifically. Many of these datasets are derived from image searches and social media, such as the Flickr Faces HQ Dataset. For their own part Facebook participated in an early experiment in giving access to facial recognition to ordinary citizens but also in the process collecting yet more data on users. In 2010, Facebook introduced a feature wherein users in uploaded photos could be tagged and automatically recognized. This was done with the logic of convenience (O'Brien and Ortutay, 2021), which is also a common justification for surveillance (Stark and Levy, 2018: 1211; Gates, 2011: 132; Zuboff, 2019: 91). Facebook has eliminated this feature after the subsequent controversy (Pesenti, 2021), keeping with the reaction of other large companies like IBM that same year (O'Brien and Ortutay, 2021).

While the analysis of Zuboff has a great deal of utility, certain trends complicate the perception of this phenomena being confined to institutional hierarchies, and to that end, Stark and Levy formulate the concept of the "surveillant consumer." As certain tools such as home security systems, tracking systems for food delivery and more, ordinary citizens now, in many ways, have access to tools of surveillance. Stark and Levy state that "...we highlight the emergence and development of a new phenomenon: the discursive positioning of individuals not only as surveilled persons within digitally mediated systems of consumption- but also, simultaneously, as surveillors themselves' ' (Stark and Levy, 2018: 1203). In this way PimEyes

(at least for the aspects of the use of their service that they find acceptable to advertise) transform users into surveillors of themselves.

It is important to note that these tools may be of comparatively rudimentary power to what governments and corporations have and that Stark and Levy are emphatic that the "democratization" of power often does little more than re-affirm existing inequalities of power wherein (Ibid, 1203). They further argue that "surveillance has become a normalized mode of interpersonal relation mediated by digital systems, as the technical affordances of such systems make such relations more and more 'focused, systematic, and routine'" (Ibid, 1203).

In the emphasis on digital systems, it is clear that these datasets and corpuses of facial data were only possible with the knowing and unknowing, and the willing and unwilling, cooperation of ordinary citizens in their generation. Stark and Levy cite the observation of Ritzer and Jurgenson as "putting consumers to work" (Ibid, 1204). Furthermore, the four of them all discuss Zwick's concept of the "co-creation" afforded by these new systems as potentially liberating but also as harmful as the data gained from consumer activity may be used to achieve anti-democratic aims (Ibid, 1205). Clearview AI, a pre-eminent firm specializing in facial recognition technologies for police forces, governments and corporations, collected their datasets in large part, from images scrapped from the internet (Gross, 2023).

Stark and Levy structure their analysis as encompassing two roles of this emergent surveillant consumer, the consumer as observer and as manager. The former revolves around a logic and drive of protection, though it is notably one surrounding a user's dependents, namely children and elderly or otherwise incapable family members (Stark and Levy, 2018: 1206). For the consumer as manager, there are already programs and products aimed not at the large

corporations that may have accelerated the development of this technology, but also for small, more intimate businesses. For example, the company Luxand, offers a variety of plans for their FaceSDK and Face API for small businesses, education, and the hospitality industry. Specifically highlighted are uses for tracking classroom attendance, authentication for company computers and building security, age verification, and the prevention of fraud ("Lightning fast, accurate, and stable face recognition API"). There are also seemingly more mundane uses for photo-editing or mobile apps designed primarily to "play" with the appearance of a face with filters (*Face recognition for developers*). Technologies of the face need not be purely confined to the predominantly political uses once primarily imagined for them, And, while much of the use focused upon in this paper will focus on the sexualized aspects of this technology, the fact that these technologies have filtered down opens their use up to any number of things with any number of implications, should prompt some serious consideration and concern.

To fully understand how this operates with at least certain parts of the imperatives with the democratization of facial recognition technologies, synthesis with another idea on how technologies fit into, and shape social relations is also necessary, particularly surrounding responsibility and security. Gates discusses this trend in some detail in her chapter "Inventing the Security Conscious, Tech-Savvy Citizen." It is also interesting to note that she discusses this primarily in terms of two events in 2008, those being Lenovo's release of Veri-face equipped business laptops, and the company Betaface releasing the MyFaceID search engine (Gates, 2011: 125). Gates describes two recurring imperatives that drive this. The most important for understanding the logics behind the use and the development of applications such as PimEyes is the interest in maintaining the security of a user's devices and information. The other imperative is that of indexing the glut of images that mark the digital age (Ibid, 126-7), which for this new

age of democratized (though perhaps not democratic) media and image creation and access, likely and especially feeds into the first imperative.

Indeed, among the main selling points of PimEyes is in protecting against both general misuse and theft of a user's images, but also against the non-consensual creation of synthetic media using an individual's likeness. The development team states "Now, if you want to find your images through the web and check if somebody used our images for deepfake, the perfect tool for that, will be PimEyes. You can upload your image, and it will find your photos that are appearing on the internet. The way facial recognition search PimEyes works is that it crawls the public Internet, finds photos of faces, and then creates 'face fingerprints' by indexing their parameters. Unlike regular reverse image search engines, such as Google Images, it only focuses on the face in a picture..." (P Team).

A user that is subscribed can ask for updates to see if any new images of the same (presumably their own face) have been detected as a way to stay on top of any pertinent developments and maintain an ownership over their biometric data. In this way, the Tech Savvy citizen is able to use technology to keep up with the dromological (the increasing imperative of speed that marks modern society that also generates evermore dangerous unforeseen consequences) nature of modern digital media. Though there are concerns that must be raised about certain aspects of digital media, including how simulated media may justify increasing use of these recognition technologies, which were only possible with the impossibly large dataset of the internet and social media.

PimEyes has faced a myriad of pressures and journalistic criticism in the past few years regarding how their application is used and what data is allowed. One such instance came in

October of 2023 in response to a *New York Times* article criticizing potential harms to children (Vasani, 2023). Specifically, the revolves around how those images can be used to stalk children for the purposes of harassment, stalking or the generation of simulated child sexual abuse material. The company has consequently banned searches of children from its algorithms (Hill, 2023b), though with the caveat that the algorithm may have difficulty detecting teenagers and is still a work in progress. Additionally, the company was also forced to no longer rely on data scraping social media (Ibid). These stakes around the body are only just beginning to be articulated and certain boundaries established and concerns around power and vulnerable populations will be key focuses for Sites #1 and #2.

Another safeguard that has been put in place is that PimEyes says that any pictures uploaded are stored temporarily for a period of 48 hours and promptly deleted. It is important to note that in certain spaces in the ethnographic work that supports this paper (though not the primary ones), I have encountered a great number of complaints regarding the increased efficacy of the program starting in 2021, quite potentially as a result of this concerted media pressure and the consequent responses from the company and interests in finding alternatives.

These technologies and their uses lead to an additional critical question which this paper aims to aid in charting: what have been the different consequences of the advent of the image-based information economy that marks digital spaces as they are now? And how has it led to technologies of both recognition and subversion? Lastly, what impact does this have on how we understand the digital world in relation to the material world and, in particular, how bodies have been reconfigured and reimagined? The question of bodies is likely to be critical in light of the fact that the reach of PimEyes regarding the body is so profound that it may be changing how the body can even be conceptualized in digital contexts as representations of the body and by

extension the body itself become sites of heated and impactful conflict with little precedent for understanding and considering this new reality and its implications.

Dromology, The Original Accident, The Body

The current media landscape is exceptionally unique throughout history, in large part because of the extent and scope of its participatory potential. Furthermore, there have been drives on the part of the sorts of companies focused on in Zuboff's analysis that have effectively made the internet you experience tailor made to your interests, or the "internet of me" (Hodkin, 2015). According to Andre Spicer writing for the World Economic Forum, the "internet of me" is expanding further into devices and tools that integrate an individual's body into the experience (Spicer, 2015). Moreover, our interactions have changed in the participatory power that we now have to create and upload our own media.

Many scholars have anticipated the possibility of the mass medias that have made services like PimEyes possible in the first place. For instance, Yaron Ezrahi, in arguing for the present period as being one marked by the emergent category of "outformations," which while not replacing information (such as news media), are marked by democratized participation (Jasanoff, 2005: 260) that focus on subjective experience of aesthetic and emotional realms (Ibid, 258). These outformations may include the selfies, videos, and other individualized content of human faces that have aided in forming a potentially infinite facial recognition dataset and corpus and have animated facial recognitions technologies proliferation and democratization. Moreover, outformations possess a marked emphasis and are arguably reliant both on the central importance of images to their construction (Ibid, 258) and the ability of ordinary citizens to create them and participate in their dissemination (Ibid, 260). This is further emphasized by the

simple fact that technologies to both produce high fidelity digital images and to edit and change them as it suits an individual have never been more accessible. Social media has now become for many a critical center of socialization where the images of faces are omnipresent and methods to commune and meet with others, mark important life events, and display their own identities as they understand them.

Similarly, Vilem Flüsser presciently anticipates certain trends in media, though perhaps not some of the deeper implications of them. In discussing what he calls technical images and the creation of utopias, he understands the two trends. One being characterized by being controlled by authoritarian and undemocratic "image receivers and image administrators" (Flüsser, 1989: 4). In that instance, he is likely referring to institutions able to exercise incredible power over the lives of both individuals and populations such as governments or corporations. The other possibility is characterized as leading to a more democratic and, in his opinion, more positive "...telematic society of image producers and image collectors" (Ibid 4). While these previous arguments presented in this section all point to a trend of accessibility and democratization in these technologies, it is once again important to note that these trends are not therefore, necessarily democratic.

Paul Virilio posits that the defining characteristic of modern society is speed (Virilio, 2007: 1), referring to this complex as the Dromosphere. The speed of the circulation of all things, but most crucially of information poses according to Virilio the danger of the original (and then consequently the integral) accident which is further engendered by the fact this this speed in media, images, sound and so on are no longer bound any specific geographic boundaries (Ibid, 38). Additionally, there is the argument that the passage of time itself leads to accidents, or that, quoting Aristotle, all accidents are "the accident in time" (Ibid, 91). This, combined with the fact

that technologies developed faster than even their developers can fully comprehend or appreciate, further displays the risk of the drive to do things with yet more speed and that the more time that passes, the likelier misuse or highly consequential use is to come to fruition. Central to this paper is the fact that technologies designed to supposedly capture reality fully (in this case, technologies designed to recognize the human face), those that can fill in what is incomplete about reality, and those designed to transpose faces rendering a reality that never happened (simulated media technologies), all had their development contingent on the creation of the unfathomably large dataset curated in large part by citizens of relatively ordinary means who enabled the creation of these tools, facial recognition in particular.

Virilio's idea of the Dromosphere/Dromology leads critically to his concept of the original accident, the accident inherent in any invention. He states that accidents, or all the ways in which an invention can go wrong, are co-produced with and by the invention itself, stating that "To invent the sailing ship or steamer is to invent the shipwreck. To invent the train is to invent the rail accident or derailment. To invent the family automobile is to produce the pile-up on the highway" (Virilio, 2007: 10). This idea is of particular interest and, I would argue, is possible to expand upon further. Perhaps also with the invention of currency, there has also been the invention of counterfeiting, or for the purpose of this paper, the deepfake. It is then argued as a consequence that this can be combated with democratized facial recognition like PimEyes, though PimEyes of course prompts its own unknown consequences.

It could be argued that, if he discusses the accident in time and in space, the accident that is the center of this paper is the accident of scope in both senses of the word. It is the accident in scope in the sense that it is now in the digital space, unencumbered by traditional questions of time in space, occurring in a seemingly infinite parallel world that nevertheless has material

impacts on the world and people's lives, while being truly accessible to all. It is also the accident in scope in the sense that it importantly deals with vision, images, and being seen and the potential consequences of aspects of life one wished to be hidden being seen, potentially by all and this itself has ramifications for how the body is to be understood and whether or not images of the body are entirely separate from the materiality of the body itself.

N. Katerine Hayles hints at this tension when she discusses the posthuman body and how it can be conceptualized when the posthuman body is described, centrally, as a type of prosthesis, an integration of human reality and powerful and intelligent machines and also as generating "no essential differences or absolute demarcations between bodily existence and computer simulation, cybernetic mechanism and biological organism, robot teleology and human goals" (Hayles, 1999: 3). Another particularly important insight of Hayles, and one that is of critical significance when discussing visual technologies, is in how she charts the evolution from ownership to access (Ibid, 39) and further argues that this shift also generates a shift, blurring, or dissolution between preconceived divisions of the private and the public, where the private is predominantly an aspect of ownership, and is not about the physicality of a space or person on the internet but about data (Ibid, 40). Hayles notes that materiality and virtuality are themselves not separate, but rather are co-constituting elements, where acting as if one has more precedence than the other is a misguided and potentially deleterious error.

BodyRight, Body Drift, and Gendered Impacts

Throughout fieldwork on numerous sites, it became clear to me that quite often that much of the use of PimEyes centered around identifying the faces of women. This is of notable interest when it is contextualized with the simple fact that facial recognition (and AI more broadly)

possesses a notable negative bias against those who are not cisgendered white men (Hardesty, 2018). It has also been well observed that despite the fears of how simulated media could be used to disastrous political impact, the technology is overwhelmingly used to generate simulated adult content by superimposing the face of one woman onto the body of an adult film actress in video. In fact, it could be argued that certain "nudifier apps" have their data biased in terms of operating with female bodies as certain apps are incapable of generating a speculative male body. Instead, putting a clothed male body and face through the algorithm will result in the male faces being rendered as part of a female body (used here to refer to a body possessing breasts and a vulva) (Cole, 2019).

This noted bias is particularly amplified in deepfakes, where Sensity AI noted in a 2019 report that of the detectable instances of deepfakes, 96% were of non-consensual pornography and 99% featured women (Hodge, 2023). The uses of TOF thus outlined have been ones that have, in contrast to practically every other AI application, focus much of their use and data collection on women. In a collection of essays surrounding the work of Judith Butler, N. Katherine Hayles and Donna Haraway describes the concept of Body Drift, which Kroker argues is emblematic of a technologically induced posthuman condition, stating that it is no longer possible to have a singular conception of the body, that we all now inhabit a variety of bodies and that subsequently this has created the phenomenon of Body Drift (Kroker, 2012: 2).These listed bodies may include aspects of social performance, sexuality, gender, labor, and the technological mediations of these and more categories. Important for this analysis is speed, instantaneity, and traceability can make asserting any control over these bodies a challenging proposition.

All of the members in the Site #1 presented images of women, often in various stages of undress and who based on the suggestiveness of the images appeared to be engaged in the sex industry in some way. However, other instances in my fieldwork showed images of women that appeared to be typical selfies likely taken from social media, and one post even contained two images of a woman who appeared to be shopping in a supermarket, with the poster asking “Help me find her name” and “I need help finding her name”

In this community, members ask for help identifying specific people from pictures. These posts generally have few or no comments underneath them and there appears to be the tacit understanding that the posts are available to solicit interest from those with premium PimEyes accounts, but that any information thus gleaned from a search will be communicated via private message. This trend could also be observed in numerous other spaces and forums where there was interest in using it. For example, multiple posts in various communities had individuals offering their premium PimEyes account for those that felt the need, with specifications that it was for protection and “safety”. Posts such as this were replete with requests for communication through direct messaging

This privacy may be in keeping with the general (and important aim) of maintaining personal security on internet spaces, but can ultimately obscure the reason for a user’s interest. Certain users may have a vested interest in ensuring the presence of a photo of an individual cannot be traced back to them. That is: if the target of their interest (or someone who has taken an image and presented that image as being themselves) has a PimEyes account, they can find an instance of these images being posted as requests for identification. This could be exemplified in the competing aims of much of the posts of Sites #1 and #2. The former seemingly populated predominantly by men wanting to identify women who often appeared to be cam models or

otherwise engaged in the creation of adult content. The latter states its mission as having its mission being created and managed by cam models with the purpose of fighting the misuse, or theft of the images they have produced.

While theories of cybernetic prosthesis are clearly important to understanding this reconfigured relationship between the signifier and the signified, Feminist film theory has long observed the interaction between the camera and sexualization. In Laura Mulvey's landmark *Visual Pleasure and Narrative Cinema*, the term scopophilia is used to describe the pleasure (often erotic) derived from seeing, particularly that which is often private, intimate, or otherwise hidden (Mulvey, 1975: 806). While much of the content sought out and created with these technologies of the face is distinct from Mulvey's focus in that Mulvey is focusing on vision and scope within studio created film with deliberate cinematography, one critical commonality stands out. Mulvey describes that in film narratives, the male protagonists (and while she separates the two in her analysis, I would argue to an extent the camera itself) act as surrogates for the presumably male viewer. The culmination of the end of the narrative of a film is that the male protagonist (and by extension the viewer) can, in a way, possess her erotically (Ibid, 811).

Juxtaposed with Hayles' insights into a transition between the ownership of information towards the access of it that marks the digital world. If there are to be numerous technologies that individual's interface with every day that are tied inexorably to their own bodies as well as depicting their bodies, to what extent is the signifier of the body no longer a part of the body? Because facial recognition technologies can be used in the words of Gates, to once again "reembody disembodied identities" and simulated media can transpose aspects of a body with the goal of making that fantasy indistinguishable from reality. To what extent can a body or a picture of that body be separated into discrete categories of material or virtual, given the

profound impacts on the lives of people that this can cause and furthermore, to what extent any individual be said to actually own their bodies?

This analysis is particularly meaningful when the fact that for certain users of PimEyes, it is not enough to have this sexualized content under an internet pseudonym, there is a direct desire to possesses knowledge (and in a way, ownership) of both the image and the name (Hill, 2023a). Perhaps in Hayle's understanding this may be a way to own both the signified and the signifier. These questions surrounding ownership take on a particular importance. The SAG-WGA strikes over the summer of 2023 further exemplify this, where the scanning of extras on Disney's Wanda-Vision led to fears about extras being replaced by AI generated simulacra, amounting essentially to a sort of biometric theft, where their images could be used in perpetuity (Allyn, 2023).

This potential reality has not been generated without resistance. Even before these powerful technological tools were widely available, questions about the alarming permanence of data online led to protests in Spain over "the right to be forgotten" for the protection of dignity and identity in 2011 (Zuboff, 58). More currently, the United Nations Population Fund has created the advocacy group BodyRight, which describes its mission as "a new copyright for the human body" (*Bodyright - own your body online*). BodyRight also recognizes the importance of their mission particularly for Women and Girls as well as other groups like members of Racial/Ethnic Minorities and members of the LGBTQ community who are also continually failed and victimized by these technologies (Ibid). Individuals can upload images of themselves with a stylized b over their bodies to copyright that image, and BodyRight argues that this is both as protection and to urge both Big Tech companies and smaller ones to "take the abuse of human bodies at least as seriously as copyright infringements" (Ibid), potentially anticipating a need to

make this a legal and social reality. BodyRight's mission is mostly done in response to the creation of non-consensual sexualized images and videos or deepfakes (ibid). This is a revealing and deliberate decision that further indicates trends concerning ownership and right over images that are very much entrenched in conceptions of financial and legal protections like copyright

The Body as Copyright

Questions of copyright have been perennial issues in the digital landscape, perhaps in large part because certain conflicts and contradictions are exhibiting themselves in terms of both the lucrative nature of data as well as the ways in which digital technologies can, for better or worse, foster cooperation and collaboration. While these technologies have in large part been created by certain powerful interests and entities such as governments and corporations, their use has often filtered down to ordinary citizens, though admittedly not with the scope and power available to either.

Aspects of digital culture such as open-source can refer broadly to decentralized technologies that utilize collaborative creation and efforts in their development. With technologies such as PimEyes, these democratized logics and imperatives have begun to intersect with those of personal privacy, protection, and security. While the aforementioned ideas of open source software, which enables anyone to participate in its development and alter its code (*What is open source?*), the concept of fair use which affords the use of copyrighted material under certain controlled circumstances (*What is fair use?),* and the Creative Commons , which itself offers licenses for copyright and has its mission as a critical facet of a "global movement built on a belief in the power of open access to knowledge and creativity" (*The Creative Commons*). These aspects of digital communications technologies that celebrate collaboration and

decentralized creation have articulated with neoliberal extractive imperatives in both complementary and contradictory ways.

Aspects of the fair-use of protected content has long been a source of tension with imperatives of copyright and the protection of intellectual property. Data and its distribution have been a driving force of the growth in tech companies and has facilitated the development of what Shoshana Zuboff calls “surveillance capitalism.” This use of extraction of data has included photographs, audio, names, various accounts, passwords, location data, online dating, sexual activity, purchases, and many other kinds of identifying data (Zuboff, 2019: 143). The extraction of data and its use is all centered around exactly who any individual user is and what that entails, that this has expanded into the body itself is consistent with this greater trend.

Furthermore, other aspects of the business model of PimEyes exemplifies additional trends that Zuboff marks as emblematic of surveillance capitalism. Critically, the idea of Software as a Service (SaaS) and more specifically Surveillance as a Service (SVaaS) (Zuboff, 2019: 171). While Zuboff analyzes this primarily in the sense that many online services for their use companies collect the behavioral data of their users to profit from that data in various means (ibid, 172), this shift exemplifies a turn these democratized logics generate: the ability of potentially anyone to be data brokers of some kind and for certain communities the dire stakes (financially, personally, or bodily) that this may introduce. Now, protection of one’s past, present, future, and identity is a service.

That the PROtect tier of PimEyes provides the capability to provide DMCA requests further hints at an additional way in which the body can become the focus on concerns of copyright. The DMCA was part of a series of amendments to US code Title 17, passed in 1998

(US Copyright Office.b). Later, in 2020, provisions were added including the creation of a Copyright claims board that would assist smaller creators "…resolve copyright disputes of a relatively low economic value" (US Copyright Office.a). The GDPR is the European Union equivalent, concerned mainly with protecting the data of EU citizens and companies as well as enforcing the "right to be forgotten" (Staff Editor, 2022). AI and Machine learning applications and technologies are themselves subject to concerns about copyright in ownership because they are created with pre-existing data created by humans (Italie, 2022). That these technologies have become further de-centralized and democratized, it may be argued that the same rights over likeness had (in theory) by celebrities should necessarily also be democratized. While several proposals exist (Blackburn…, 2023; Rosenberg, 2023), little has been done to truly achieve this potential necessity. The likeness is clearly still difficult to think of in these terms. It is worth noting that the aforementioned BodyRight has a stated mission to create a new copyright for the human body", signified by a stylized b on an image as a supposed sign of protest and a way to get companies to "take the abuse of human bodies at least as seriously as copyright infringements" (*Bodyright - own your body online*) and this is mainly done in response to the creation of non-consensual sexualized images and videos or deepfakes (ibid).

In this current democratized incarnation, these technologies are being promoted and advertised by companies like PimEyes as a way to protect one's image and likeness, even using the tools of copyright. Concerns of this kind are not entirely new. Indeed, these concerns have long existed for celebrities and their estates to the point where there exist companies that partially serve the purpose of controlling the image and likenesses of celebrities as intellectual property. Concerns with simulated media using the likenesses of both living and deceased celebrities have notably been subjects of incredible controversy (Associated Press, 2024;

Edwards, 2023; Pasquini, 2019). This is important in light of companies such as Authentic Brands Group which owns the likenesses of Elvis Presly, Muhammad Ali, and Marilyn Monroe as intellectual property (Authentic Brands Group), though now even living celebrities are increasingly pursuing this end whether to enforce their own rights to control their likeness against non-consensual use, or as "liberatory" (Coffee, 2023). Much like the democratization of the surveillance technologies used by powerful institutions, the visibility and instant accessibility of the bodies of all in ways that once only existed for celebrities has further democratized an ability or imperative to "brand" and protect a body through financially based mechanisms like copyright.

While the social media that enables and facilitates the perceived need for services like PimEyes has come out of a kind of neo-liberal self-fashioning and protection, these new trends can be understood through a synthesis of two ideas related to technologies of surveillance and identification. Much of the interest in these technologies has been to "re-embody disembodied identities" (Gates, 2011: 32) after the increased mobility of the 20th century. However, in these growing democratized incarnations, Kelly A. Gates notes the construction of the "Security Conscious, Tech-Savvy Citizen", an individual able to understand and keep up with technologies, utilize them so as to secure their own "empowerment" and take an active role in the protection of their own security (ibid, 126). The goal to be adept at the use and adoption of new technologies is of critical importance due to the constantly shifting circumstances of post-modernity defined by instantaneity and no temporal or geographic bounds to communications technologies (Virilio, 2008: 39). This is itself, part of a larger neoliberal trend, that of responsibilization.

Wendy Brown, in *Undoing the Demos*, describes responsibilities as a way to account for neoliberal imperatives and their erosion of certain protections once provided by government programs and initiatives, in its place is a regime where individual actors are tasked with cultivating, fashioning, and protecting themselves as individual subjects (Brown, 2015:84), in this instance through novel technologies. What makes this unique is that as certain extractive technologies are now within the reach of ordinary citizens, the increased presence of these technologies, while advertised as a new tool to achieve this, is ultimately also a driver of opposing ends regarding this logic of protection. There are also contradictions in the imperatives of both the wide circulation of data to enable profit and the walling off of certain information for the purposes of both being able to secure the profits described from the information and to protect one's present or current livelihood, a dilemma not lost on those who feel that the use of this technology is both necessary and dangerous. It is of further concern that while the aspects of PimEyes anticipate to some extent the importance of viewing a body and its representations as copyright, no substantive projections yet exist that would actually be automatic or available to all. Protection of this kind is rendered solely the duty of an individual

These stakes around bodies including the instantaneity of being able to trace bodies and identities and the use of financially mediated and based protections of these mean that new conceptualizations are needed. I argue in part that these trends imply two unique (but deeply interrelated) reconfigurations of the human body. The first is that because images and representations of the human body are easily traceable to the person they represent, they can be argued to be a part of the body. And now that the body is no longer specifically bound by the traditionally conceptualized material borders of the "body proper", these aspects are occupying a new materiality no less impactful on individual lives. The second reconfiguration has worked in

tandem with the financial drives that enabled these issues in the first place leading to a conceptualization of the body as copyright amidst the contradictory articulations of extractive logics and decentralized production and digital communities. The issues that arise from these changes are further exacerbated by a lack of meaningful institutional recognition of them that is allowing potential harms to go unmitigated and unaddressed. The phenomenon of body drift and the instantaneous (dromological) reach and development of these technologies has created a situation where these technologies implications extend far beyond their designed scope. The primary peril of speed to Virilio is that any tool or technique created is necessarily always ahead of its creators (Virilio, 2007: 10). And there is no way for any tool or technique and its full implications and ramifications to be understood when they are created, especially when they can be used by everyone in ways inventors may not necessarily account for or anticipate. While these tools may be advertised as ways to protect one's privacy or one's self from adversarial actors, the use of these technologies has since expanded far past these "common-sense" and understandable uses.

The Body Contested: Democratized Facial Recognition as a Shield and a Weapon

Both of the places ethnographic analysis took place were different forums, henceforth referred to as Site #1 and Site #2. Both of these communities utilize these democratized facial recognition technologies, but to diametrically opposed ends. The mission of Site #2 is focused on combating explicit images of the users from being disseminated without compensation or their consent and by extension to protect themselves and their image from any number of potential negative consequences this may entail such as the leaked material having lifelong consequences that may harm their reputations and financial well-being. Multiple users expressed concerns about having to essentially live a "double life" and expressed fears that the ambitions and

realities of their professional lives were simply incompatible with webcam modeling or "camming." Camming is the creation of sexual content live and in front of a web camera as a form of sex work (Richtel, 2013). Also prominent were fears of what exposure could mean, including the potential and reality of losing one's family as a result of willingly divulging this information or having it non-consensually leaked.

Others expressed fears about sextortion or impacts on their reputations more broadly. Each of these fears highlights this comprehensive totality of the implications of being so easily traceable. Numerous attributes of this experience were relevant to the discussions in the community: questions, advice, requests for help and responses to them, emotional support, and thanks. While most of the users were women as far as could be ascertained, there was a sizable contingent of men, many of them gay, active on this forum. Additionally, certain sites that stole content were noted by members to be specifically for gay male cam models, and these were noted as particularly problematic, further highlighting the differential impact of the accessibility of bodies that virtual spaces and technologies have engendered. It is clear that the impacts of and digital re-fashioning of the body does not affect everyone equally, targeting the bodies of those already disempowered and stigmatized (women, members of the LGBTQ community, and sex workers). This is further exemplified by the fact that this community and numerous others like it exist solely because of how little support there is for sex workers at all, regardless of the legality (internet sex work is generally legal) or type of their work, meaning they must resort to a patchwork of various tools and protections that makes Site #2, and others like it, indispensable communities

By contrast, the no longer existing Site #1 was remarkable in how incredibly similar to the point of being formulaic every post was. Overwhelmingly posts were titled variations of "her

please” or “her name pls." These posts seldom received more than a few replies that were usually a prompting for the original poster to DM the replier, and presumably requests and sharing the results would take place via direct message. Obviously, these interactions were inaccessible to anyone other than the two users. Other responses would be additional requests for assistance. At other intervals, the replier would upload a full link to the PimEyes search results which could be partially accessed by anyone who had the link, which revealed a large sum of images of the specific woman (or women that resembled her).

I followed these links when they appeared and some pictures could be accessed through full access to the results of any individual search were locked behind a one-time fee of $14.99. With the exception of one, all of the images were of women. That the forum was so small, with a membership of 274 users while observation and archiving was occurring is worth considering given that it uniquely is concerned with this technology. Other communities throughout digital space would have mention of or aid in use of the technology for the same purpose as Site #1, and while there was a potential for this service to have incredible utility for issues general application in Open-Source intelligence initiative and for a sort of democratized sleuthing focused on identifying criminal suspects, missing persons, or unidentified decedents, instances of these technologies being used for the latter end in particular were surprisingly sparse and no other communities observed were so invested and facilitating the use of PimEyes or similar technologies, at most having brief discussions about use of these technologies or just answering inquiries as to what PimEyes even was.

This and the relatively hidden nature of some of the exchanges may complicate generalizable knowledge. But the fact that these images were overwhelmingly of women and more importantly, overwhelmingly of women who appeared to be in sexualized contexts, is

worthy of further attention, especially when considering certain gender biases already present in the development and implementation of AI technologies concerning the human face. For instance, facial recognition technologies have historically been noted to be less efficacious on the faces of individuals who are not white or male (Lohr, 2018). However, the creation of deepfakes, which is in part a phenomenon PimEyes claims to be interested in assisting subscribers in combating, is noted to overwhelmingly (98%!) take the form of sexualized images of women (Hurst, 2023).

Furthermore, the use of generative AI in particular, is noted to have a distinct bias, with men utilizing the technologies up to twice as much as women (Koetsier, 2023). Many of the images were of women who appeared to be engaged in independently produced and distributed cam modeling (arguably some of the user base of Site #1 may be some of the very same pirates that are the adversaries of the user base of Site#2). This is not to say that all of the images were of this particular kind. One post was regarding an image of someone claimed to be the poster's girlfriend, which the original poster used to make a request to use another poster's premium account to trace the provenance of the image. This image had the appearance of a fairly innocuous selfie. Requests regarding girlfriends were observed to occur multiple times and in multiple different spaces (beyond the two sites discussed here) when the subject of PimEyes and help in finding and tracing images came up. Though it is very notable, that in the many satellite sites that were not primary loci but also informed this research, specifically in the context of reddit where users could be active in multiple areas that this may at least in some instances be less than honest, as a look into user histories may reveal participation in various explicit communities.

Another image entered in the request was significant in that it seemed to have been an unambiguously innocent selfie, depicting a woman wearing a sweater in what appeared to be a public park. It is unclear exactly what the origin of this image is but there is a decent possibility it was taken from the pre-existing social media of whoever this woman was. Another instance was a post containing two pictures of the same woman in what appeared to be a supermarket as she perused the store with a shopping cart. The first image presented (and presumably also the first taken) showed her from behind and seemed to focus on her tight and revealing clothing. The second picture presented shows her face and the user who took the image shows that he was able to get her attention in some way and perhaps spoke to her for a period. The resulting image offers a rather clear picture of the woman's face and it is unclear how aware she was that she was being photographed. Nonetheless, the image appears candid. This post is titled "Help me find her name", once again displaying this preoccupation with finding the true identity of a stranger that was omnipresent in this community.

As an aside, the fact that the only image that was not of a woman was of a linked post (not by the original poster) concerning allegedly haunted antique furniture. While this strange deviation may seem as if it bears little relevance to the greater conversation, it still manages to speak to certain themes regarding digital technology, specifically in their elimination of both time and space. In their history of Facial Recognition technologies and in describing PimEyes, Mark Andrejevic and Neil Selwyn note the potential of these technologies and their growing democratization and decentralization to reveal certain horrifying truths, stating "uploading a photo of one's own face could lead to all manner of images that you are likely to have forgotten, presumed lost, or hoped to be lost" (Andrejevic and Selwyn, 2022: 71). In the terminology of

Mitchell, images of the past "re-present" (Mitchell, 2010: 9) events, resurrecting the past with potentially far-reaching consequences.

In this instance individuals who could not have imagined the advent of facial recognition technology of any kind are now subject to its use and within its domain. Facial recognition technology as a whole has even begun to expand into the speculative, that yet to be or which could be. Whether it is attempting to speculate of the likelihood of an individual to commit crime (BBC, 2020) or default on loan payments (*What your face*…, 2019), or to use simulated images to train facial recognition datasets (images created from pre-existing images) (Schmidhuber et al, 2020), or using a DNA phenotype to be a part of a facial recognition dataset (Mehrotra, 2024), these technologies have become uniquely total in scope, including even people who either no longer exist or never even existed in the first place. The issue of creating facial recognition datasets served as a perennial and inhibiting problem for the governments and corporations working on them. Yet now with the advent of social media and an image-based information economy that embraces de-centralized production and collaboration, these datasets and technologies can be constructed and built like was never before possible (Levy, 2023). Any image of any face uploaded is potentially a part of this complex.

The most important contrast between these two sites of analysis is the simple fact that the implicit understanding on Site #1 that none of the images and none of the requests were of the original poster and it was unambiguous that much of the interest was in people unknown to the poster and the purpose was to ascertain and render legible their identity for any number of purposes. These purposes were never explicitly voiced, but based on the nature of the majority of the images present, it is not difficult to guess what some of the motivation may be. While some showed a degree of candidness or appeared to be selfies taken from social media, the majority of

the images appeared to show the subjects in various states of undress, being taken with what appeared to be web cameras based on the angling and visual fidelity and clearly somewhat sexually charged. Ultimately, Site #1 was deleted between late December of 2023 to January 2024, potentially as a consequence of reporting or other action. Certain new trends may aid in contextualizing this. Recently, many sites and now some countries, have recognized the threat of and even banned the creation and distribution of certain malicious simulated medias (or deepfakes) and with the advent of a new law in the United Kingdom it has actually become a criminal offense punishable by "unlimited fine" (Cooney, 2024), Still this addressed only one aspect of the issue as this law is bounded by the borders of the UK, but the reach of these technologies is unambiguously global. Given many of the similar gendered implications and additional dangers of being able to trace a specific individual with great ease, a potential crackdown on these uses of facial recognition technologies akin to the one that occurred for deepfakes is certainly a possibility. This is especially given the particular controversy PimEyes as a service has engendered, with much of the media coverage describing the service as "dangerous" or "disturbing" and able to facilitate stalking, doxxing or vigilantism (Harwell, 2021; Allyn, 2023; Vallance, 2022). The service was also criticized for its potential to facilitate the exploitation of children by revealing potentially images of child sexual abuse (Hvistendahl, 2022), which the organization has responded to by only recently (as of October 2023) blocking reverse image searches of children (Hill, 2023).

Another community that has made use of the technology mostly for the broad umbrella of applications related to "open-source intelligence", has chosen to effectively end hosting requests and discussion for the use of PimEyes due to the potential for unethical use as well as the sheer volume of discussion and requests regarding it. Those in support of the decision noticed that the

requests they had observed the same trend which is the focus of much of this paper: that these inquiries were overwhelmingly focused on identifying women and that this was likely not a bid to assist a girlfriend or other acquaintance but instead done for unethical purposes and that potentially any discussion of the service should be summarily banned While Site #1 is gone, the demand for similar communities is not and certain communities serve much the same role though they are notably less tied to the use of facial recognition technology specifically and there are likely other similarly focused sites and communities that are likely to be created in the future.

The second site of focus is a general forum created and maintained by a user-base made out of cam-models, those otherwise involved in the production of adult content online, and certain volunteers knowledgeable about legal applications to enforce this imperative of protection. That this specific non-consensual misuse is framed as theft is meaningful. Much of the concerns surround the dissemination of images found on other platforms without the consent or compensation to the creators. For members of this community, PimEyes is but one of a great number of tools used to track, identify and enforce the protection of their images. Here users commiserate, share advice and even share access to PimEyes account, much the same as in Site #1 but for clearly opposing reasons, perhaps these same adversaries were the members of Site #1.

That this communal sharing seemed ubiquitous in multiple contexts with sometimes diametrically opposed interests is worthy of note. In other cases, an individual's involvement with the community would begin with whatever they found on a PimEyes search which they may have done simply for the sake of curiosity. Often for them to seek out the community in the first place, the scope and scale of the results derived from the search could be deeply shocking. Those who had not used PimEyes yet but had suspected the presence of instances of piracy would be

assisted by certain users that subsequently accepted direct message requests to help facilitate a user's ability to use the service and (especially for the premium tier) to receive updates of new occurrences of their images and whether or not it is appearing in a context that was not agreed to. These initial posts often described feelings of shock, fear, and regret but more established community members would often reassure that there were many useful avenues, often giving advice and prompting these new members to collect the links to facilitate future action and to use the opt-out feature of PimEyes so that they may not be found in this way by bad actors. Because of its existence as a tool, it should be noted that "opt-out" features of this kind have not been without criticism. Zuboff notes that the tech companies that created surveillance capitalism recognize conceptions of consent as deleterious to their business models even arguing this very point in legal proceedings (Zuboff, 2019: 170-171). Furthermore, it is noted that these policies are generally pursued after a degree of public controversy (ibid, 168) and further responsibilizing subjects into attaining knowledge of this feature and going through this process (ibid, 293) when it was impossible for them to consent to participating in this process to begin with.

Afterwards, a PimEyes search would not be the end of this process, and the users of Site #2 ultimately viewed PimEyes as one of many tools in facilitating the protection of their content (much unlike Site #1, where the process began and ended with one query and its subsequent answer: "what is her name," a PimEyes search would only facilitate the need for additional intervention and tools. Site #1 was a tool in the form of an internet community whereas Site #2 is a community that offers a myriad of tools and supports for its user base, both practical and affective. It should be noted that PimEyes was not the only tool used to trace instances of images being reuploaded and used without an individual's consent. Other services such as Yandex's

reverse image search (Yandex, n.d.) and FaceCheckID (Sentient Labs, n.d.) exist, but PimEyes is by far the most well-known and used.

After a PimEyes search that turns back results, the subsequent focus would be on removing the images from the sites altogether through a variety of means. One avenue would be to go to any of these sites and directly make requests to their domains. This however is contingent on the individuals who ran the site actually being amenable or sympathetic to these requests. These issues would be documented and users would ask for further advice on what to do if sites were uncooperative and those with more experience with those sites may reveal their own experiences. In one instance, a member detailed one specific site as particularly cruel, even outright refusing to remove explicit images of even minors and mocking these pleas on the forums.

Another potential tool in the arsenal of members, there were many discussions of DMCA firms and services (all paid) that would specifically aid in removing stolen content from sites that performed this. However, a recurring theme was simply that not all sites were responsive to requests for removals. At multiple intervals users would describe certain sites failing to respond to requests stating their interest in archiving materials as well as the stance that they would refuse to delete anything uploaded for any reason. Additionally, these DMCA firms also gained suspicion for their perceived exploitative pricing and lack of efficacy. This was to the point that in several instances, it was clear that experienced members would never recommend the use of commercial DMCA firms, implying that there were unnecessary, scams or that the tools needed to achieve removal were already available by being a member of this community and that these firms were effectively no more capable. Nonetheless, the drive to purchase these surfaces (sometimes multiple times) marks the users of Site #2 as surveillant consumers, needing to

continually purchase and learn of different services and tools to achieve any degree of protection which is similarly depending on their cultivation into being “security conscious tech-savvy citizens” (Gates, 2011: 125). Which while conceptualized securing empowerment, nonetheless burdens them with total individual responsibility of images with potentially infinite reach

Even if a DMCA request had gone through there were instances of the content simply reappearing at a later date. Users often credited this to particularly prolific individuals who ran many of these adversarial sites (often there would be just a few individuals listed and these names would continually re-occur, being semi-regular topics of discussion. A three-year-old post mentions an individual named. Interestingly, older posts (2+ years old), were generally not reticent to “name and shame” such individuals deemed particularly prolific and problematic.

DMCA requests are noted to be time consuming, FaceCheckID even advertises as a virtue the speed with which the removal request can occur as being preferable to the not untraceable, expensive and inconvenient process of securing a DMCA request, (again it is notable that the removal of these images occurs only within the context of the service’s search engine, it does not in any way remove instances of these images from the broader internet because it is simply not possible to do so. To accomplish that, measures like a DMCA request, the involvement of a lawyer or the charity of those operating a site where content is being non-consensually uploaded are the only means of actual removal. That this ability to opt-out of the search results both for PimEyes and FaceCheckID is present belies a certain understanding of these potentials for both protection, (of one’s image, identity, well-being, and family) and the possibility of violating the integrity and protection of these categories.

An interesting note and another tie to the existence of deepfakes is found in a particularly noteworthy conversation. While these services may be highly efficacious tools, it is not lost on users that PimEyes and other similar services pose their own dangers and some expressed worries about AI image technologies more broadly. It was not uncommon for certain images to stubbornly remain and that there is a risk of always being found with tools like PimEyes even if the goal of using it is to prevent this very outcome. In this discussion there was a potential silver lining. That this rise of image-based technologies offered another useful tool: the ability to say that any image of oneself is inauthentic

These technologies both possess within them the abilities to enact harm. But this articulation between the supposedly competing ends of facial recognition and deepfakes: ascertaining reality (who someone is) and subverting it (making someone appear to do something they didn't), seems to pose even more questions as to their specific harms on specific peoples. While the existence of deepfakes can be used to aid someone in disavowing images of themselves as fake, this very same artificiality is a major source of fear for those who have not been involved in the world of camming. To them, it is likely that this simulated appearance of something that bever actually happened is not potentially helpful, but actively harmful and terrifying.

In Site #2, discussions about opting out of PimEyes were common. Generally, the consensus was that it worked fairly well (for some users within a few hours or within the day. For their part PimEyes states that images will be removed from search results within a period of 48 hours. For others, it was efficacious though they did note that in their cases and others it may take a couple of requests to see results. Other sites such as the aforementioned FaceCheckID and the still rather small Camgirlfinder were also recommended as services with which to utilize their

respective opt-out features. In only one instance were there concerns of needing to continually resend opt-out requests because content would once again be in the search results with some regularity (roughly every few months). Community members were not unaware of the double-edged nature of these tools, using them both to find instances of their images being misused, while also keeping in mind the potential issue of these services facilitating and exacerbating that very same use.

Another significant trend that has been observed is related to the presence of potentially bad-faith actors finding the community and entering discussion. At certain intervals when a DMCA request was successfully enacted and an adversarial site deleted, many of the members of the community would celebrate, while others would find and enter into the space leasing to somewhat heated arguments would ensue. There would be debates as to if any created material was truly protected by copyright and thus its creator able to enforce ownership over their being uploaded. These debates could become incredibly heated and reveal some of the emotional stakes around this the proliferation and non-consensual use of images of oneself, one user stating that it was tangible to a kind of virtual "rape." And this further ties to the overall fears that this forum and numerous other discussions of PimEyes both in other forums and in journalistic media express: that democratized facial recognition introduces further challenges in hiding aspects of their life that could bleed into and ruin others. Hayles also notes these very same tensions, as exemplified by her conception of "embodied virtualities" (Hayles, 1999: 48-49). Specifically, Hayles notes also emphatically states that because of the blurring of boundaries concerning data and the person it represents, or how the person represents themselves to the data, all critically returns back to the materiality of the body.

That images can impact the totality of their lives means that it is impossible to "hide." Where once anonymity could once (at least ostensibly) be secured by changing one's name or using names to keep aspects of one's life separate, these technologies map identity, being, and life specifically to the body and means that once diffuse representations of the body are able to in some way metastasize and reach every aspect of a person's life with profound psychological, personal, professional, and emotional consequences. While Kroker argues that we each inhabit multiple bodies due to the reality of body drift that marks postmodern/posthuman life (Kroker, 2012: 2), what gives makes these technologies meaningful is that these many bodies and lives (in the case of the members of Site #2, their real lives and their constituent aspects, the totality of their digital lives, and their lives in digital sex work) are all traceable in unprecedented ways. They are no longer representations; they are now the all body and this is what makes their potential consequences so dire. The question now becomes what this advent means and what must be done now that this course has been taken. That there is an attempted enforcement of protection with tools such as DMCA requests hints at one likely direction this new reality may bring about, the body itself as being a kind of copyright.

On other occasions where outsiders would enter the community it would also be clear that certain comments were bad faith or facetious responses to user's request for help with removing images such as "what kinds of pictures?" There would also be the notably ambiguous and somewhat suspicious posts attempting to solicit the ability to use a PimEyes account out of concern for a "girlfriend." On occasion when substantial events occurred (potentially the removal of content, the sites hosting it, or new laws that may be helpful), the celebratory air could become beset by outside users entering into arguments with members. In debates with male members, outsiders may mock their masculinity or sexuality ("white-knights," "simps")

and otherwise make violently charged comments and comments directed towards female members were particularly revealing in terms of the critical trends analyzed in this paper. These interlopers would disparage them as “bitches” who deserved having their content leaked because they supposedly already made money, and that any leaking was their fault stating simply that if they didn’t want content to be disseminated, they shouldn’t have posted it in the first place. This notion of choice further exemplifies trends towards responsibilization. Any lost career opportunities, profits from the content, or even social capital are solely the fault of any anyone for posting these kinds of photos, though the use of the word “leaked” seems to imply an understanding of the material being non-consensually uploaded in the first place, nor does it seem to question that while this work may have profit, it is also heavily socially stigmatized.

While PimEyes is a useful tool for some members of this community, and none of the people observed to use it seem unaware of its potential implications, it cannot uncritically be viewed as apart from this trend. PimEyes is an entirely individualized “solution” to this issue that puts the onus of resolving any potential harm purely on individuals who are already in many ways vulnerable and in positions of precarity. It depends on them having the money, knowledge, access, or ability to use it and renders itself a paid service being just another aspect of the capitalistic logics that have guided data collection and use, forcing private citizens to pay to find and access images they themselves produced. Some members noted that they were participating in this work to be financially independent and aid them in gaining the security to pursue other careers, but these technologies can also utterly destroy these plans.

This framing of choice is an interesting one, particularly in how it links with debates about whether or not any material made is able to be copyrighted. There would be debates regarding whether or not producers actually owned the content they produced and were not

copyright holders. This implicates the use of DMCA requests as a tool and therefore should be unable to use DMCA requests to get content removed. For many sites the terms of service agreements state that one's created and uploaded content was entirely their property and that the host site did not own it, in effect making an individual a copyright holder, though this discussion possessed many tensions between this fact and the collaborative trend and tendency towards virality of the internet. Obviously, the legal structures around these questions are not currently well-formed or explicated and it is generally recognized that in almost every way, the development of these technologies has far outpaced the laws supposedly built with the purpose of their regulation (Wadhwa, 2020; Kang and Satariano, 2023). In this way, it is clear that digital communications are decidedly driven by increased acceleration (as are the many avenues of monetization that these technologies generate) whereas systems of legal regulation possess an inbuilt conservatism and resistance to rapid change (Mueller, 2022). The DMCA, for example, is an amendment of US copyright law. But as these issues regarding likeness become increasingly relevant to growing numbers of people, the decentralization and democratization of these technologies may necessitate the democratization of these ideas of likeness as an intellectual property.

In his book *Digital Barbarism*, Mark Helprin addresses these concerns regarding the conflicts of copyright and open-source digital trends with a polemical and, what he claims as a Jeffersonian angle (Helprin, 2008: 101) in regards to the individual right to property. Helprin states that groups such as Creative Commons and by extension open-source imperatives themselves seek to "cut away at intellectual property rights until they disappear" (ibid: xiii). Throughout the text he dubs this sharing of content "digital barbarism" and proposes extended copyright as a potential antidote to this perceived scourge (ibid, 30). For many on Site #2 it is

likely that as soon as an image is a part of the internet, it can almost instantly be copied and widely disseminated across the world with an immediacy that clearly proves difficult to combat. That any laws regarding this issue necessarily operate in a wide patchwork with numerous different standards and that the technology is moving so quickly results not only in the dissolution of boundaries of time and space, but also of the public and private and of the digital and material. That data produced and gathered from digital spaces is so lucrative for Tech companies and even private citizens either protecting their images or non-consensually using them, this displays the continued power of the image. Helprin for all his polemical vitriol, presciently notes that a point may be being reached where these questions of law can or are no longer able to be viewed as "the exclusive province of lawyers" (Helprin, 2008: 123). These technologies generated by collaborative efforts seem to articulate with this understanding and Zuboff also notes that to some extent that while surveillance capitalism was enabled by capitalist markets and logics, it departs from some of its precepts in some truly fundamental ways. Among them, its totalizing interest in using every aspect of human life as profitable data as one that realizes a sort of collectivist control that nonetheless denies human rights and democracy (Zuboff, 2019: 504-505) even though new markets have democratized certain aspects of its functioning. It is therefore difficult to understand who or what owns any data or anything in digital spaces and this fact has in large part supported the nascent though still undeveloped conception of the body as copyright.

Sedition Hunters, Sleuthing & Vigilantism

While the previously presented case studies have focused on the competing aims of revealing and protecting identities in regards to PimEyes specifically, there are other uses and concerns regarding the use of these technologies in facilitating vigilantism of various kinds.

Indeed, there have been concerns over the use of the technology in the wake of the January 6, 2021, U.S. Capitol insurrection. This has led to the formation of a small but active collective of volunteers terming themselves "sedition hunters" who utilize Open-Source Intelligence tools and practices to ascertain the identities of Insurrection participants (*Sedition hunters)*.

This group has even generated a freely available database collated from hundreds or thousands of videos of the insurrection from various social media platforms. The link https://capitolmap.com/ can lead to either this facial recognition dataset and the ability to enter an image in it as a way to verify if this individual in question was present, or to a very detailed video map that contextualizes videos with their locations all throughout the capitol and the surrounding DC area. (*Facial recognition tool for the capitol storm; US Capitol Attack Video Map)* These specific tools were of course both developed in concert with government resources and members of the Sedition Hunters community that are self-proclaimed "facial recognition experts"

While earlier in the paper, I argued that these democratized tools, while having potentially profound implications on individual lives do not possess the scope and scale of the tools available to and built by corporations and governments, it is worth noting that U.S. intelligence agencies such as the FBI have collaborated with and relied on tips from sedition hunters, in large part because of the sheer volume of images, video, and data (Harris, 2023; Tenorio, 2023). Indeed, this issue of separation is further complicated by instances such as the finding by Anna Kuznetsova (not to be confused with the Duma deputy chair of the same name). In 2020, she was working with a digital activist group investigating the Russian government's use of facial recognition technology as well as other concerns surrounding surveillance. After seeing a public advertisement promising access to Moscow's comprehensive and extensive facial

recognition infrastructure (Bacchi, 2020). This transaction, with which she used her own face, was able to return a relatively short period of two days a number of images (seventy-two, to be precise) tracing her movements over the past month throughout the city (ibid). It was able to situate her specifically in both time and space, once again "re-embodying disembodied identities" (Gates, 2011: 32). Naturally, while collaboration is open-source, the particulars of this process were not able to be ethnographically observed because they must be somewhat clandestine by necessity, now involving concerns of national intelligence.

There are other applications of these technologies for general sleuthing. Still, it is worth considering that while there would be clear utility in using these technologies for finding missing persons or identifying unidentified decedents and suspects of crimes, the hypothetical utility and actualized use of services like PimEyes for these purposes exhibits a gap. For instance, while searches on one specific internet sleuthing community turned out 25 pages of content for the search phrase "facial recognition", these posts were almost invariably regarding police use of the technology, mostly whether or not it was used, if it could be used, or if other factors were complicating its use, such as facial injury.

The search phrase PimEyes turned back only 7 results, 3 of which were part of the same large thread regarding the 2022 Moscow, Idaho college murders. A search on another community created to help identify unidentified decedents, yielded only one result simply asking exactly what PimEyes was. This may be something of an aside, but this post in particular has a great deal of discussion regarding the fact that many of the search results seemed to link to adult sites, with one member wondering if this skewing of the results was due to the sheer amount of adult content available or if it was because of knowledge of and deliberate attempts to focus on

his kinds of content because on the parts of services like PimEyes because of the visceral fear, anxiety and urgency this content and its consequences often engenders.

Still, PimEyes is far from the only service of this type. Aside from PimEyes and the previously discussed facial recognition database and application created by sedition hunters, services such as Yandex and Facecheck.ID are also widely available. In regards to Yandex, it is noted by the investigative journalist and open-source intelligence collective Bellingcat as being something of a combination of facial recognition and reverse image search applications, stating "While Google and Bing may just look for other photographs showing a person with similar clothes and general facial features, Yandex will search for those matches, and also other photographs of a facial match," (Toller, 2019). Though this is with the caveat that Yandex is a Russian company (in fact the largest Russian tech company) and there are concerns about the potential security implications of that (ibid).

FaceCheckID is more similar to PimEyes in a variety of ways. FaceCheckID also includes a feature for opting out of appearing in search results (here it is called a removal request) even down to uploading a picture from an individual's photo ID with identifying information obscured (Sentient Labs. a). Interestingly, the company has an angle different to PimEyes, while much of PimEyes advertising focuses on the protection of an individual's identity, FaceCheckID's sensibility, mission and advertising is decidedly more pugilistic. They describe themselves as a "investigative service", and state "As society became soft on crime, criminals repeat their behavior without fear of any consequences. There's a good chance you too will come across someone with a criminal history. FaceCheckID's facial search engine allows you to check anyone's internet footprint using a picture. A quick search may reveal a person's shady history." (Sentient Labs. c)

Additionally, the service also states “We reserve the right not to remove photos of child sex offenders, convicted rapists, and other violent criminals who could pose physical harm to innocent people” (Sentient Labs. a). This is just another instance of the omnipresent trend that has been observed with these services and those who use them; there is a decided preoccupation with concerns sexual violation whether the technologies are utilized as an aegis against victimization or misuse or a weapon in them. This is perhaps unsurprising. If the body is being remade in this new way (or at least through novel and unprecedented means), then it makes sense to a degree that the primary stake around the body and its integrity has to do with concerns of sexuality, specifically as it relates to those who are incredibly vulnerable, whose bodies have been misunderstood, policed and hated.

Whereas FaceCheckID has a legalistic focus and advertises itself more so as providing an avenue for necessary vigilantism in the wake of “softness on crime” and is focused on other people who may be dangerous or dishonest (Sentient Labs. B), PimEyes is much more in line with concerns about neoliberal self-cultivation and the protection of that self. This combined with PimEyes considerably more far-reaching press coverage has made PimEyes considerably more well-known and popular.

Search results for other such applications such as Yandex, and Facecheck.ID turned back even less, with the former mostly being used as a conventional search engine and the latter returning only one post which also discussed using PimEyes for one case. The searches for PimEyes generally had singular posts discussing their use. In one regarding the 2016 disappearance of an ex-girlfriend of a minor celebrity, where a PimEyes search of her face revealed previous involvement in the adult film industry. One member of the board, brought this up in the post to see if the information could help but was also unsure of its relevance to the

investigation. Once again, despite the myriad potential uses, the specter of concerns regarding sexuality, and sexual violation is nonetheless omnipresent. This is perhaps unsurprising. If the body is being remade in this new way (or at least through novel and unprecedented means), then it makes sense to a degree that the primary stake around the body and its integrity has to do with concerns of sexuality, specifically as it relates to those who are incredibly vulnerable, whose bodies have been misunderstood, policed and hated. Even images themselves or the act of taking and collecting them has been recognized as highly affectively driven, viewed as exemplifying some kind of power over the subject. In discussing the nature of body drift, Kroker similarly notes that contrary to views that digital space disappears the body, technologies of this kind actually bring salience that the image machine is itself "haunted" by bodies of the disempowered and abused (Kroker,2012: 1) and that these bodies are nonetheless made material and lay bare many kinds of injustice and "precarity" (ibid, 63)

Indeed, many scholars such as the previously discussed Laura Mulvey and WJT Mitchell discuss the image, particularly of a person (and perhaps even more so the center of affect and identity: their face), discuss the image and the act of looking as being invested with a sort of psychic and erotic power, which Mulvey describes as Scopophilia and Mitchell describes as the image being imbued with the power of the fetish. While these images could represent icons in that they are, Mitchell proposes a new framework that would situate the images of focus in Site #1 and Site #2 as fetishes, due to their private, sexual, and intimate aspects to their form and use (Mitchell, 2011: 76). These are also viewed as subject to interests of control, power, and obsession (ibid, 121), which may feel like, and even become to a degree control over the person represented. In On Photography, Susan Sontag notes that photographs are both magical and can have erotic components complicated and urged by distance (Sontag, 1977: 16), whether this

difference is a question of time, place, or even reality themselves becoming “emblems of desire” and ways to “possess the past” (ibid, 175). That PimEyes provides such comprehensive and potentially total search results for one image exemplifies a kind of collection that exemplifies the extent of power to ascertain potentially every aspect of an individual’s life, regardless of how hidden it may be and any differences in distance or time. The past can be possessed but as Site #2 indicates it can also profoundly impact the future. Clearly, Flüsser’s utopian democratic ideal of a society of image producers and collectors (Flüsser, 2011: 4), has been beset by issues of already existing social bias, recreating instead of subverting them.

There is an interesting way, in which these concerns of sexuality, sexual violation and vigilantism intersect. One individual (henceforth referred to as “James” has gained a sizable following and much of his content revolves around finding and catching predatory men on various chat rooms or otherwise pranking them. Each of these videos begins with a description of the use of Facial Recognition and how it has been used to catch predators by him on multiple occasions. He does this by posing as an underaged girl named “Jessica” (usually between the ages of 13-15-years-old), and begins to speak with male users, often middle-aged men. If the conversation begins to take an inappropriately sexual turn which is generally prompted by the middle-aged man initiating sexually suggestive conversation with “Jessica” that promptly escalates to ever more explicit and disturbing content. The conversation proceeds and eventually an exchange of selfies occurs.

It should be noted that it is not entirely clear what image he uses to pose as this underaged girl as both the images of this girl and these men have the faces blurred at least on YouTube. And though he advertises uncensored content on a specialized platform, it is unclear to what extent this context is uncensored. He then describes putting this newly procured selfie as

being processed by a facial recognition service, though he does not describe if he is using PimEyes, Facecheck.ID (the most in line with his mission), or some other service. He then proceeds to find all of their social media and other personal/identifying but publicly available information such as friends and family on social media, employment, and more. At that point the conversation is likely escalating to become increasingly explicit with the man sending nude photographs and describing masturbating and beginning to detail things he wishes to do in graphic detail. When the search is complete and all of the personal information is found "Jessica"/ "James" may pivot suspensefully pivot sending a message revealing the truth, opening by showing that he knows their true identity including associates and that if this individual can either start a voice call to explain themselves or can ignore it and have this conversation and its contents provided to employers, friends, family, and local authorities

This formula remains consistent. It is then that a voice call may proceed and "James" will open with a rhetorical question as to why a call is occurring in the first place. "James" will then often try to catch these men in lies, which are generally taken as evidence that this is part of a pattern and that there is no true remorse for the contents of the text chat. Often the man in question may beg for "James" not to go through with this throughout this conversation which invariably ends with "James" proceeding to send this information to the authorities and the man's friends and family. On occasion these chats may begin on discords designed exclusively for teenagers, further exemplifying predatory intent. In a few instances these individuals may threaten suicide if this information is forwarded and while "James" may call authorities to ascertain the safety of these individuals, in at least one confirmed instance this all culminated in a completed suicide at some point after this contact. At this point "James" confirms this on video and states that there will be no further updates on this case as a result of this suicide and that he

considers this a regrettable outcome for this individual's family and closes with a picture of a message from this man's sister stating that any further contact with the family on the part of "James" will lead to legal escalation and that they should be able to recover from the trauma of this event in peace. Bordering this presented text message in the video was a request from Thomas to respect this wish and not try to find them

This instance further shows the material reach of facial recognition even though their democratized and digital form lacks power scope compared to that of these technologies as used by governments. These incriminating images are no longer separate from reality (if ever they were, that fiction can no longer be maintained), and the power of re-presenting these events has lasting impacts that may make decisions regarding people's employment, reputations, freedoms, and lives that are now further democratized in the sense that now governments or corporations are not the only agents with this profound power. While there is little doubt that the individuals in these series are undoubtedly criminal and quite likely dangerous to children, this democratization of power and its implications needs to be fully appreciated and understood. This potentially represents a critical juncture in terms of questions of privacy, legality and the role of ordinary citizens within these systems of frameworks.

What is also interesting about the format of "James's" videos is their reach. These compilations can have views numbering in the tens or hundreds of thousands. Many of the comments are full of those thanking "James" for catching predators in this way, many stating that they themselves were victims of child sexual abuse and that they wish someone cared enough to prevent what happened to them like "James" has done. That "James" is able to nearly instantly ascertain who these people are (including much of their publicly available personal information and where they are, he can use local authorities regardless of the geographical

distance between him and these men to enact consequences on their body (police questioning, arrest, etc.). This can be done to prevent violence (whether via digital space or in physical reality) from being performed on the bodies of children. This is an extraordinarily tangible power enabled by only one photograph of one individual person's face. Once again, these photos enable interventions directly on the level of the body, further bringing into question whether or not representations and bodies can be viewed as separable or discreet any longer. Presciently Virilio, anticipating the potential of technologies that transcend space and time to obtain "hyper-realism" that began with law enforcement and general surveillance, where technological means of ascertaining reality are overruling and usurping the role once afforded to the eyewitness and in instances such as "the telepresence of witnesses... poses the whole question of habeas corpus all over again" (Virilio, 1999:44). To this question, the "where" in this current point in time, appears to be everywhere and nowhere and any time past or present, but also able to be once more contextualized to an exacting degree in specific time and place. While images have often been viewed as material throughout history, the extent of the capability is entirely unlike anything that has been available to ordinary citizens

This instantaneous reach is worthy of great attention. It is unlikely that any of the conversations in these videos exceed an hour. And once these men's facial information is secured, "James" is able to both nearly instantly ascertain their identity, lives, location, and then to take prompt action. Virilio in discussing speed notes that it has effectively brought about the "...end of geography" as facilitated by the scale, scope and immediacy of digital communications technologies (Virilio, 2007: 39). The wide reaching complex of the wide corpus of digital images that enabled the creation of these technologies has essentially fully integrated the world, and the global reach of these tools attests to the ability of anyone, regardless of distance, finding

discovering the identity of an individual, regardless of when these images in question were taken with the real potential to have this information/image and its discovery to manifest as lasting and irrevocable consequence on the lives of individuals. It is through this total integration and distortion and overturning of these boundaries in favor of instantaneity and spacelessness, that the original accident has the potential to become the integral accident, no longer bounded by a single region or technology and a cascading complex of dysfunction and calamity (Ibid, 46). He further contends that if powerful tools with the ability to affect comprehensive harm are within the hands of the "socially excluded, the argument for deterrence evaporates" (Ibid, 78) and that this has the subsequent potential for even greater calamity. Any of the boundaries they may have once existed, no longer do, and to predict the consequent outcome is potentially even beyond imagination.

While in some ways, the videos of "James" are presented as entertainment with eye-catching animated graphics, this community seems to view this as both an important public service and a way to prevent other children from being abused like they were. However, there were other elements of "James's" work, he even goes as far as to state that this is what he does is to some degree, a part of his income, that are clearly more so focused on concerns of entertainment and the monetization of this use of technology. He could do this work (admittedly with no or minimal compensation) and use it to inform the appropriate authorities, but is instead making a deliberate choice to make this content available and consumable.to the point where other videos may similarly focus on predators but instead of identifying them are concerned with making them unwittingly humiliate themselves. Interestingly in at least one instance the faces of one of these individuals in unobscured, notable given the fact that his audience is now aware of technologies that can identify specific people from one image

The fact that this content is publicly available (albeit in supposedly censored form), prompts questions about what exactly the goal of this content is. A public service? A way to expose these specific individuals (why are their identities mostly obscured then)? Entertainment? Catharsis? Vigilantism? Some combination of these factors or something else entirely? That this content is apparently monetized, further links the economic components of development and use in a novel way for this democratized use. In a way, the technologies of surveillance capitalism and their democratization has rendered the use of these technologies more than just a tool for protection and identification but that it can be a site of emotional catharsis and even entertainment, further indicating a normalization and entrenchment of this technology. Thus, facial data corpus that has enabled this technological democratization was enabled in large part by entertainment such as Ezrahi's outformations and now the use of these derived technologies is once more a site of entertainment. It must be noted that despite the reach of these videos and their highly charged content, the channel does not appear to have violated any policies and still exists as of April of 2024 with a semi-regular upload schedule.

Conclusion

These potentialities are critical. These reconfigurations of the human body and its meaning (as either inseparable from its representations or as something that must be legally and financially protected and possessed) are both co-constitutive of each other and are critically animated by the trend of technological democratization. Questions around the body have only been intensified in this regard, as what and where the body is questioned by the immediacy, reach, scope and material impacts of these technologies.

Ultimately, each case presented here centers on secrets surrounding identity, and those who wish for them to no longer be so and aim to use these technologies to reveal and re-embody (potentially even to very specifically place in the case of the sedition hunters) the truth of a person and their actions. More immediately, that these tools are so readily available and that their focus is so often on information with the potential to impact life, reputation and freedom displays clearly that digital technologies while often viewed as possessing an immateriality can no longer be conceptualized as so, and this is especially true for technologies of the face which center upon the affective center of human activity and the primary marker of human self and identity. More than simply being semitic icons, these representations both seem to have a tendency to bid their own repetition replication and spread as Mitchell would understand it, and they also can point to exactly who an individual is, their past, their location, and every other imaginable aspect of their being that is also present digitally.

While these tools may have been created to assist, what they appear to have done is created a self-perpetuating loop of concern with images and their protection. While it is difficult to know precisely if the materiality of facial recognition's impacts (and that of other technologies of the face) will be resolved by serious legislation, the creation of an actual bodily copyright, the (quite unlikely at this juncture) banning of these technologies in their totality or merely their democratized incarnations, or any other means. It is worthy of great attention that Tech companies of all sizes and persuasions have been able to extract information because of no formal system of data ownership and that this ability has now become widely available. Any shift in ideas of ownership and control of data of all kinds what have the potential to fundamentally remake how and what tech companies and ordinary citizens are allowed to extract, and resistance would be likely to any proposal for substantive change

What is clear is that notions of individual responsibility are clearly no longer enough to simply treat this issue like it is purely a matter of individual choice, responsibility and protection that also serves as a lucrative industry for companies like PimEyes. The full scope of this problem can no longer be considered simply that "workers with AI skills will replace workers without them" (*Ai won't replace humans...* 2023). Or, in this instance, that everyone must use these technologies to protect themselves when they are capable of being a weapon just as easily as an aegis. Any solution must necessarily be as concerned with implications and potentialities as with current realities. This may not be able to be undone but how we view the body/face, technologies surrounding them and digital technologies requires far more deep consideration and care, because these tools have already exacted once unthinkable consequences.

References

Ai won't replace humans - but humans with AI will replace humans without AI. Harvard Business Review. (2023, August 4). https://hbr.org/2023/08/ai-wont-replace-humans-but-humans-with-ai-will-replace-humans-without-ai

Allyn, B(a). (2023, August 2). *Movie extras worry they'll be replaced by Ai. Hollywood is already doing body scans*. NPR. https://www.npr.org/2023/08/02/1190605685/movie-extras-worry-theyll-be-replaced-by-ai-hollywood-is-already-doing-body-scan

Allyn, B(b). (2023, October 11). *"too dangerous": Why even google was afraid to release this technology*. NPR. https://www.npr.org/2023/10/11/1204822946/facial-recognition-search-engine-ai-pim-eyes-google

Allyn, B. (2023, August 3). *Movie extras worry they'll be replaced by Ai. Hollywood is already doing body scans*. LAist. https://laist.com/news/arts-and-entertainment/movie-extras-worry-theyll-be-replaced-by-ai-hollywood-is-already-doing-body-scans

Andrejevic, M., & Selwyn, N. (2022). *Facial recognition*. Polity Press.

Andrejevic, M., & Selwyn, N. (2022). *Facial recognition*. Polity.

Associated Press. (2024, January 26). *George Carlin's estate sues over ai-generated standup comedy special*. The Guardian. https://www.theguardian.com/technology/2024/jan/26/george-carlin-lawsuit-ai-standup-comedy-special

Authentic Brands Group. (n.d.). *Brands*. https://corporate.authentic.com/brands

Bacchi, U. (2020, November 9). Face for sale: Leaks and lawsuits blight Russia facial recognition. https://www.reuters.com/article/idUSKBN27P10R/

BBC. (2020, June 24). *Facial recognition to "predict criminals" sparks row over Ai Bias*. BBC News. https://www.bbc.com/news/technology-53165286

Bodyright - own your body online: Bodily integrity: UNFPA. United Nations Population Fund. (n.d.). https://www.unfpa.org/bodyright

Bodyright - own your body online: Bodily integrity: UNFPA. United Nations Population Fund. (n.d.). https://www.unfpa.org/bodyright

Coffee, P. (2023, June 18). Celebrities use AI to take control of their own images. https://www.wsj.com/articles/ai-deepfakes-celebrity-marketing-brands-81381aa6

Cole, S. (2019, June 26). *Deepnude: The horrifying app Undressing women*. Deepnude: The Horrifying App Undressing Women. https://www.vice.com/en/article/kzm59x/deepnude-app-creates-fake-nudes-of-any-woman

Cooney, C. (2024, April 16). *Creating sexually explicit deepfakes to become a criminal offence*. BBC News. https://www.bbc.com/news/uk-68823042

Data Real-Lies. (2022, April 3). *Pimeyes is extorting victims of sexual abuse.* Medium. https://data-real-lies.medium.com/pimeyes-is-extorting-victims-of-sexual-abuse-8ceef45299a3

Dennon, A. (2021, September 8). *What you need to know about facial recognition home security cameras*. ZDNET. https://www.zdnet.com/home-and-office/smart-home/what-you-need-to-know-about-facial-recognition-home-security-cameras/

Edwards, B. (2023, October 3). *Deepfake celebrities begin shilling products on social media*. Ars Technica. https://arstechnica.com/information-technology/2023/10/tom-hanks-warns-of-ai-generated-doppelganger-in-instagram-plea/

Face recognition for developers. Luxand. (n.d.). https://www.luxand.com/

Face recognition search engine and reverse image search. PimEyes. (n.d.). https://pimeyes.com/en

Flüsser, V. (2011). *Into the universe of Technical Images*. University of Minnesota Press.

Foucault, M. (2014). Two: 18 January 1978. In *Security, territory, population lectures at the College de France, 1977-78* (pp. 29–49). essay, Palgrave Macmillan.

Gates, K. A. (2011). *Our biometric future: Facial recognition technology and the culture of Surveillance*. New York University Press.

Gates, K. A. (2011). *Our biometric future: Facial recognition technology and the culture of Surveillance*. New York University Press.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative adversarial nets. *Advances in neural information processing systems*, *27*

Grauer, Y. (2023, September 22). What big tech knows about your body. The Atlantic. https://www.theatlantic.com/technology/archive/2023/09/online-privacy-personal-health-data/675182/

Gross, T. (2023, September 28). *Exposing the secretive company at the forefront of facial recognition technology*. NPR. https://www.npr.org/2023/09/28/1202310781/exposing-the-secretive-company-at-the-forefront-of-facial-recognition-technology

Tenorio, R. (2023, October 28). *Sedition hunters: How ordinary Americans helped track down the Capitol Rioters*. The Guardian. https://www.theguardian.com/books/2023/oct/28/sedition-hunters-book-jan-6-rioters-fbi-trump

Hardesty, L. (2018, February 11). *Study finds gender and skin-type bias in commercial artificial-intelligence systems*. MIT News | Massachusetts Institute of Technology. https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

Harris, M. (2023, November 3). *How the sedition hunters won*. Slate Magazine. https://slate.com/news-and-politics/2023/11/jan-6-riot-arrests-online-sedition-hunters-fbi-sleuths.html

Harwell, D. (2021, May 14). *Pimeyes: A facial recognition website that can turn anyone into ...* The Washington Post. https://www.washingtonpost.com/technology/2021/05/14/pimeyes-facial-recognition-search-secrecy/

Hayles, N. K. (2010). *How we became posthuman: Virtual bodies in cybernetics, literature and Informatics*. University of Chicago Press.

Helprin, M. (2011). *Digital barbarism*. Harper Collins Publishers.

Hill, K. (2023a, September 20). *How a "Digital peeping Tom" unmasked porn actors*. Wired. https://www.wired.com/story/kashmir-hill-privacy-surveillance-facial-recognition/

Hill, K. (2023a, September 20). *How a "Digital peeping Tom" unmasked porn actors*. Wired. https://www.wired.com/story/kashmir-hill-privacy-surveillance-facial-recognition/

Hill, K. (2023b, October 23). *Face search engine PimEyes blocks searches of children's faces*. The New York Times. https://www.nytimes.com/2023/10/23/technology/pimeyes-blocks-searches-childrens-faces.html

Hill, K. (2023b, October 23). *Face search engine PimEyes blocks searches of children's faces*. The New York Times. https://www.nytimes.com/2023/10/23/technology/pimeyes-blocks-searches-childrens-faces.html

Hodge, R. (2023, November 22). *Ai deepfakes, women, and the liberating imagery of feminist sexual vengeance*. Salon. https://www.salon.com/2023/11/21/ai-deepfakes-women-and-the-liberating-imagery-of-feminist-vengeance/

Hodkin, S. (2015, August 7). *The internet of me: Creating a personalized web experience*. Wired. https://www.wired.com/insights/2014/11/the-internet-of-me/

Hurst, L. (2023, October 20). *How AI is driving an explosive rise in deepfake pornography*. EuroNews. https://www.euronews.com/next/2023/10/20/generative-ai-fueling-spread-of-deepfake-pornography-across-the-internet

Hvistendahl, M. (2022, July 16). *Facial recognition tool "PimEyes" could allegedly contribute to child exploitation; Incl. co. comments*. Business & Human Rights Resource Centre. https://www.business-humanrights.org/en/latest-news/facial-recognition-tool-pimeyes-allegedly-could-contribute-to-child-exploitation-incl-co-comments/

IBM. (2024, February 20). *What is a neural network?* https://www.ibm.com/topics/neural-networks

Italie, H. (2023, September 20). *John Grisham, George R.R. Martin and other authors sue openai for copyright infringement*. Los Angeles Times. https://www.latimes.com/world-

nation/story/2023-09-20/john-grisham-george-r-r-martin-and-other-authors-sue-openai-for-copyright-infringement

Jankowicz, N. (2021, March 25). *Opinion | the threat from deepfakes isn't hypothetical. women feel it every day.* The Washington Post. https://www.washingtonpost.com/opinions/2021/03/25/threat-deepfakes-isnt-hypothetical-women-feel-it-every-day/

Jasanoff, S., & Ezrahi, Y. (2006). Science and the political imagination in contemporary democracies. In *States of knowledge the co-production of Science and the social order* (pp. 254–273). essay, Routledge.

Koetsier, J. (2023, November 28). *Men 2x more likely to use generative AI than women: Report*. Forbes. https://www.forbes.com/sites/johnkoetsier/2023/11/27/men-2x-more-likely-to-use-generative-ai-than-women-report/?sh=4aa629204149

Kroker, A. (2012). *Body Drift: Butler, Hayles, Haraway*. University of Minnesota Press.

Leonard, P. (2020, January 17). *Beyond Data Privacy: Data "ownership" and regulation of data-driven business*. The American Bar Association. https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/winter/beyond-data-privacy-data-ownership-and-regulation-datadriven-business/

Levy, S. (2023, November 10). *Fei-Fei Li started an AI revolution by seeing like an algorithm*. Wired. https://www.wired.com/story/plaintext-fei-fei-li-ai-revolution-seeing-imagenet-algorithm/

Lightning fast, accurate, and stable face recognition API. Facial search | Free face recognition API | Luxand.Cloud. (n.d.). https://luxand.cloud/

Lohr, S. (2018, February 9). *Facial recognition is accurate, if you're a white guy*. The New York Times. https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

Los Angeles Times. (2021, November 2). *Facebook to shut down facial recognition system and delete data*. Los Angeles Times. https://www.latimes.com/world-nation/story/2021-11-02/facebook-to-shut-down-face-recognition-system-delete-data

Mehrotra, D. (2024, January 22). *Cops used DNA to predict a suspects face-and tried to run facial recognition on it*. Wired. https://www.wired.com/story/parabon-nanolabs-dna-face-models-police-facial-recognition/

Meikle, G. (2023). *Deepfakes*. Polity Press.

Mitchel, T. W. J. (2010). *What do pictures want?: The lives and loves of images*. University of Chicago Press.

Mueller, J. (2022, February 1). *We the people: Why changing the constitution isn't easy*. Medill News Service. https://dc.medill.northwestern.edu/blog/2022/02/01/we-the-people/

Mulvey, L. (1975). Visual Pleasure and Narrative Cinema. *Film: Psychology, Society, and Ideology*, 803–816.

Myers, T. (2023, November 2). *Liveness detection for face recognition: Evolution of biometrics*. Facia.ai. https://facia.ai/blog/how-face-liveness-detection-is-used-in-authentication-and-authorization/#:~:text=Face%20liveness%20detection%20is%20a%20verification%20mechanism%20that,a%20photograph%2C%20video%2C%20or%20even%20a%203D%20mask.

Nguyen, S. (2023, February 7). *What is doxxing and what can you do if you are doxxed?*. CNN. https://www.cnn.com/2023/02/07/world/what-is-doxxing-explainer-as-equals-intl-cmd/index.html

Pasquini, M. (2019, January 3). *Scarlett Johansson says it's "useless" to fight back against "Deepfake" porn that uses her face*. People Mag. https://people.com/movies/scarlett-johansson-useless-fight-back-porn-uses-her-face/

Passive liveness detection for face validation. try it free. Sensity. (2023, September 19). https://sensity.ai/passive-liveness-detection-try-it-free/

Facial recognition tool for the capitol storm. US Capitol Dome. https://capitolmap.com/faces

US Capitol Attack Video Map. https://thepatr10t.github.io/yall-Qaeda/map.html

Pesenti, J. (2021, November 3). *An update on our use of face recognition*. Meta. https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/

PimEyes- Select Your Plan. PimEyes. (n.d.). https://pimeyes.com/en/premium

Pupala, A., Mokal, S., Pandit, N., & Bharne, S. (2021). Identification of lost children using face aging with conditional gan. *ITM Web of Conferences*, *40*. https://doi.org/10.1051/itmconf/20214003005

Rauenzahn, B., Chung, J., & Kaufman, A. (2021, August 6). *Facing bias in facial recognition technology*. The Regulatory Review. https://www.theregreview.org/2021/03/20/saturday-seminar-facing-bias-in-facial-recognition-technology/

Richtel, M. (2013, September 22). *Intimacy on the web, with a crowd*. The New York Times. https://www.nytimes.com/2013/09/22/technology/intimacy-on-the-web-with-a-crowd.html

Roose, K. (2023, December 10). *This A.I. Subculture's motto: GO, GO, GO*. The New York Times. https://www.nytimes.com/2023/12/10/technology/ai-acceleration.html

Rosenberg, S. (2023, November 28). *Metaphysic CEO says you might want to own your digital likeness*. Axios. https://www.axios.com/2023/11/28/likeness-laws-metaphysic-ai-tom-graham

Schmidhuber, J., Blanz, V., Donahue, C., Goodfellow, I., He, Z., Karras, T., Kingma, D. P., Kortylewski, A., & Makhzani, A. (2020, November 27). *Generating photo-realistic training data to improve face recognition accuracy*. Neural Networks. https://www.sciencedirect.com/science/article/pii/S0893608020303932

Sedition hunters. Sedition Hunters. (n.d.). https://seditionhunters.org/

Sentient Labs. (n.d.). *Find people online by photo*. FaceCheck. https://facecheck.id/

Sevastopolsky, A., Malkov, Y., Durasov, N., Verdoliva, L., & Nießner, M. (2023, July 28). *How to boost face recognition with stylegan?*. arXiv.org. https://arxiv.org/abs/2210.10090

Spicer, A. (2015, January 20). *What is the "internet of me"?* World Economic Forum. https://www.weforum.org/agenda/2015/01/what-is-the-internet-of-me/

Staff Editor. (2022, August 25). *The impact of the GDPR*. NYU Journal of Intellectual Property & Entertainment Law. https://jipel.law.nyu.edu/the-impact-of-the-gdpr/

Stark, L., & Levy, K. (2018). The Surveillant Consumer. *Media, Culture & Society*, *40*(8), 1202–1220. https://doi.org/10.1177/0163443718781985

Tang, K. (2021, February 1). *An efficacious method for facial expression recognition: Gan Erased Facial Feature Network (GE2FN): Proceedings of the 2021 13th International Conference on Machine Learning and Computing*. ACM Other conferences. https://dl.acm.org/doi/10.1145/3457682.3457746

Tangalakis-Lippert, K. (2023, April 2). *Clearview ai scraped 30 billion images from Facebook and other social media sites and gave them to cops: It puts everyone into a "perpetual police line-up."* Business Insider. https://www.businessinsider.com/clearview-scraped-30-billion-images-facebook-police-facial-recogntion-database-2023-4?op=1

Team, P. (n.d.). *FAQ*. PimEyes. https://pimeyes.com/en/contact

Team, P: b. (2023, October 23). *How to remove your images from Pimeyes search results*. https://pimeyes.com/en/tutorials/how-to-remove-your-images-from-pimeyes-search-results

Team, PimEyes. (2023, April 24). *Navigating the world of Deepfakes*. https://pimeyes.com/en/blog/navigating-the-world-of-deepfakes-and-how-to-fight-them-with-a-face-search-engine

The Creative Commons Homepage. Creative Commons. (2023, November 16). https://creativecommons.org/

The fight to stop face recognition technology. American Civil Liberties Union. (2023, June 7). https://www.aclu.org/news/topic/stopping-face-recognition-surveillance

Toler, A. (2019, December 27). *Guide to using reverse image search for investigations*. bellingcat. https://www.bellingcat.com/resources/how-tos/2019/12/26/guide-to-using-reverse-image-search-for-investigations/

U.S. Copyright Office. (n.d.-a). *The Copyright Claims Board (CCB)*. Copyright Claims Board. https://www.ccb.gov/

U.S. Copyright Office. (n.d.-b). *The Digital Millennium Copyright Act*. The Digital Millennium Copyright Act | U.S. Copyright Office. https://www.copyright.gov/dmca/

Vallance, C. (2022, November 8). *Stalking fears over Pimeyes facial search engine*. BBC News. https://www.bbc.com/news/technology-63544169

Vasani, S. (2023, October 23). *Massive facial recognition search engine now blocks searches for children's faces*. The Verge. https://www.theverge.com/2023/10/23/23929271/pimeyes-facial-recognition-ai-children-privacy

Velasquez, S. J. (2023, July 20). *How ai is resurrecting dead actors*. BBC News. https://www.bbc.com/future/article/20230718-how-ai-is-bringing-film-stars-back-from-the-dead

Virilio, P. (1999). *The vision machine*. Indiana University Press.

Virilio, P. (2007). *The original accident*. Polity Press

What is fair use?. Copyright Alliance. (2023, May 17). https://copyrightalliance.org/faqs/what-is-fair-use/

What your face may tell lenders about whether you're creditworthy ... The Wall Street Journal. (2019, June 10). https://www.wsj.com/articles/what-your-face-may-tell-lenders-about-whether-youre-creditworthy-11560218700

What your face may tell lenders about whether you're creditworthy ... The Wall Street Journal. (2019, June 10). https://www.wsj.com/articles/what-your-face-may-tell-lenders-about-whether-youre-creditworthy-11560218700

Woodward, J. D. (n.d.). Biometrics: Facing up to terrorism. https://www.rand.org/content/dam/rand/www/external/congress/terrorism/phase1/biometrics.pdf

Yandex. (n.d.). https://yandex.com/images/

Zuboff, S. (2020). *The age of surveillance capitalism: The fight for a human future at the New Frontier of Power*. PublicAffairs.