Miguel Loor, Universidad San Francisco de Quito, professor of the College of Communication and Contemporary Arts COCOA. mloor@usfq.edu.ec.
Quito, Ecuador.
• M.A in Digital Media: Technology and Cultural Form – Goldsmiths University of London

Abstract

Facial recognition systems are increasingly embedded into everyday artifacts. This article examines how they operate based on preset patterns and algorithms, as well as their utility for corporate and state interests. Furthermore, this work sustains the critical argument of "No recognizable pattern", a photo series that envisages alternative digital identities, through 'cyborg imagery', in order to generate untraceable biometric templates to outwit surveillance methods that expand in the current technological environment.

Keywords: facial recognition, cyborg, digital art, surveillance, social media

Resumen

Los sistemas de reconocimiento facial son cada vez más insertados en artefactos cotidianos. Este artículo examina cómo operan a partir de patrones y algoritmos preestablecidos, así como también su utilidad para intereses corporativos y estatales. Adicionalmente, este trabajo sostiene el argumento crítico de "No recognizable pattern", una serie de fotografías que imagina identidades digitales alternativas, a través de retratos con referencias al cyborg, con el fin de generar plantillas biométricas irreconocibles, para burlar los mecanismos de vigilancia que se expanden en el ambiente tecnológico actual.

Palabras clave: reconocimiento facial, cyborg, arte digital, vigilancia, redes sociales

Fecha de envío: 10/02/2016 • Fecha de aceptación: 05/05/2016
email: posts@usfq.edu.ec • web: http://posts.usfq.edu.ec
post(s). Serie monográfica • agosto 2016 • Quito, Ecuador
Colegio de Comunicación y Artes Contemporáneas COCOA
Universidad San Francisco de Quito USFQ

Non recognizable pattern

> 'A stable identity is not a fixed and finished one. Faces are forever changing and forever being cut and sorted by habits of mind and sight that are hard to break. The question is not whether to classify, but who classifies, how, when and why?' (Kember, 2014, p.197)

Face recognition and biometric systems are becoming an everyday practice of the current technological environment. More and more, these systems are being embedded in common activities. These range from migratory controls and CCTV circuits, to web analytics, social media profiles, and online transactions. Nowadays, a 'smartphone' can be unlocked with our eyes (Temperton, 2015), a car camera system can prevent us from feeling road rage (Solon, 2014), and technology companies, such as Facebook, Google and Apple, are developing and merging face recognition applications alongside with their databases.

This raises many questions about the future development of these technologies. Moreover, the documents leaked by Edward Snowden in 2013 about the N.S.A. espionage practices, plus evidences that several governments now hire private companies to spy their citizens, exposed to the public opinion that this and other intelligence agencies intercept 'millions of images per day', plus information from 'emails, text messages, videoconferences', and social networks (Risen and Poitras, 2014). This confirms that we are entering a period where we could all be subject to mass surveillance, despite the economic, social and political differences between of our contexts. What could only be considered as a sci-fi literature theme is now a vigilance apparatus on the rise. Bentham's Panopticon discussed by Foucault (1980, p. 147) continues to expand as the architectural design of computer networks as technology becomes more affordable and popular.

At the same time it is common to observe the increasing popularity of social networks and applications such as Snapchat or Masquerade

(MSQRD) - recently acquired by Facebook, which entertain their users by offering them face swaps with celebrities and other people, as well as transfigurations with facial filters. This phenomenon reveals 'the increased integration of government and commercial surveillance' (Lyon, 2014, p.5) as part of our media landscape. However, it also exposes how these technologies act as a dispositif (Foucault, 1980, p. 194) upon the individuals, since they internalize them and auto-regulate their behavior acknowledging that are being observed. As a result, data-mining mechanisms and face recognition applications have been well received for those involved in business, but also in homeland and state security, especially in the aftermath of the 9/11 events, as many authors indicate (Gates, 2011; Kember, 2014; Lyon, 2014). Yet, it remains unproblematic and still dismisses debates about privacy and civil rights in the digital era.

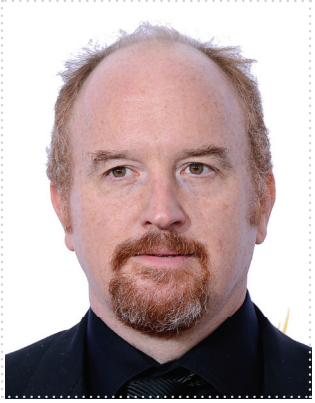
Thus, this essay analyses what lies behind facial recognition technologies, and their combination with intelligence and market research. In order to do this, it will offer an overview of their development, and some of the implications that arise due to the categorization of faces and identities. Then, it will offer various viewpoints about the role of algorithms in this process of classification, and data mining methods. From this perspective, it will draw on some key arguments of feminist science and technology studies to offer a critical response to this topic. More specifically, Haraway's cyborg to engage with technology as a tool for political intervention (Kember, 2014, p.197) Finally, these arguments will be linked to my photo series, and video, No recognizable pattern'. Through this art project I pretend to address these issues and pin out questions about how we could imagine our future identities as a subversive strategy towards this apparatus. In this sense, I will argue how we can become differently with media as an ethical practice, by drawing on Kember and Zylinska (2012), to think these portraits 'on the mutual constitution of self and other as and through the process of mediation' (p.129). As well as a political response towards these new technologies -beyond celebrating or demonizing them, that questions about the future of human rights.

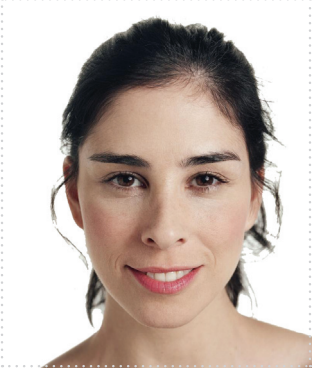
Understanding face recognition

Facial recognition technologies are still in continuous development. Computer scientists and scholars trace back the early forms of these systems to the 1960s. In her book, Our Biometric Future, Gates (2011, p.24) points out that this technology was developed as a public-private venture mainly shaped by military objectives. According to this author, it was essentially funded by the U.S Department of Defense and intelligence agencies 'in the struggle for Cold War technological superiority' (Gates, 2011, p.24). During the next decades, the computers that processed the visual information of this technology had several limitations to manage the amount of data. Consequently, the issue of developing artificial intelligence became central, since developers trained computers to learn how to discard information through trial and error algorithms (Gates, 2011, p.31). This is still the basis of the more up-to-date facial recognition technologies, as various researchers explain. In this context, the accuracy of these systems remains unsolved (Li and Jain, 2011).

However, these technologies are gradually becoming ubiquitous. For instance, they integrate many of the safety and migratory regulations in border controls. These facial recognition applications combine image analysis with fingerprints or other biometrics, and are now being incorporated into every international airport in the United States to prevent identity fraud (Noble, 2016) and certainly will be expanded into many other terminals in the near future. In addition, these systems are progressively embedded in workplaces and retail stores to control the employees' daily schedules or to reduce shoplifting (Roberts, 2015). But probably the most significant evidence of their ubiquity is Netatmo's Welcome, a smart home facial recognition camera that can notify you 'who is at home when you are not' (Wee Sile, 2015). In other words, a device that predictably invites us to wonder about Orwellian visions of our future.

Yet, most of the current face recognition applications are sensitive to unconstrained settings. These include lighting variations, facial expres-





Esteban Sargiotto
181.29.42.236
Rosario, Argentina

Metadata:
Sarah Silverman, Louie CK
Funniest Louis CK ComedyStore HD
Cha Cha Cha - La Droga en el Futbol (Fatigatti)

sions, occlusion and aging (Taigman et al, 2014). For this reason, as Kember (2014) exposes, 'the principal mechanism of machine learning is reductionism' (p.185). According to her, this implies generating standard feature templates, which are compared with a database. Finally, the process standardizes the face into a simplified representation known as a biometric template (Kember, 2014, p.187). In other words, the conventional course of face recognition aims to detect, align, represent, and classify (Taigman et al, 2014). Therefore, machines and networks are trained to categorize based on recognizable patterns. More specifically, 'Support Vector Machines', 'Principal Component Analysis' and 'Linear Discriminant Analysis' algorithms (Taigman et al, 2014), which 'discriminate between classes and types of faces' (Kember, 2014, p.191). Bowker and Star (2000) argue that 'standards, categories, technologies, and phenomenology are increasingly converging in large-scale classification systems' (p.47). Therefore, these systems become 'invisible, erased by their naturalization into the routines of life. Conflict and multiplicity are often buried beneath layers of obscure representation' (Bowker and Star, 2000, p.47).

In this sense, as Gates (2011, p.14) affirms, the digital image becomes an accurate, and definitive means of tying an identity to the body into the information networks. Thus, standardized faces emerge from these processes of pattern recognition. Furthermore, Kember (2014 p. 194) argues that after the events of 9/11, the stereotypical face of terror is always gendered and racialised. In addition she declares that,

> According to the manufacturers and promoters of face recognition systems, the complex sequence of technical operations and transformations performed on the face image does nothing to undermine the objectivity of the process. This is partly because the underlying principle of the system is photographic, and historically, the authority of photography derives not only from its strong claim to indexicality, but from its development and use in the very institutions in which it continues to be deployed (Kember, 2014, p.187).

This raises questions about who designs and configures these technologies, but also echoes the power of photography in past centuries for early criminologists, such as Lombroso, who on a similar way determined and anticipated potentially dangerous subjects based on their physiognomy.

Closing the gap between humans and machines (and business)

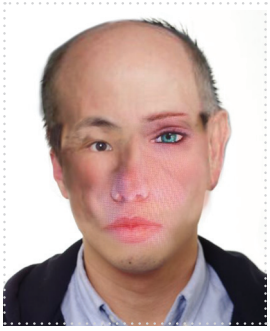
Hence, the main interest for facial recognition systems developers is to prove their precision, and inscribe them as a reliable mechanism for security, and on the other hand, business. For this reason, both authors note that computer scientists are not mainly concerned about designing ways of contrasting facial features based on racial and gender differences (Gates, 2011; Kember, 2014). On the contrary, as Kember (2014) points out, the key is to generate 'essentialised categories that guarantee system performance by ensuring that input (a recognizable face) is equivalent to output (a recognized face)' (p.186).

On a related basis, in 2014, Facebook's AI Research Department presented Deepface. This method claims to be 'at the brink of human level accuracy' (Taigman et al, 2014) since it reached a 97.35% of accuracy, according to its developers. In their published paper, Taigman et al explain how this process combines a 3D alignment of individual faces with the large 'labeled' database of their network. Or as they describe:

> The proposed face representation is learned from a large collection of photos from Facebook, referred to as the Social Face Classification (SFC) dataset. The representations are then applied to the Labeled Faces in the Wild database (LFW), which is the de facto benchmark dataset for face verification in unconstrained environments, and the YouTube Faces (YTF) dataset, which is modeled similarly to the LFW but focuses on video clips (Taigman et al, 2014).

In other terms, this is an application of the emergence of 'smart photography' (Kember, 2014, p.182). This sort of technology is based on the integration of face recognition systems with imaging, information and biotechnologies (Kember, 2014, p.182). Additionally, as Kember notes, is 'adaptive and able to learn' (p.182). In this sense, the company seems to be honoring its motto: "Move fast, with stable infrastructure" (Baer, 2014). This might explain how Facebook is increasingly building more sophisticated methods of surveillance and data mining.

As well, it reveals how technology corporations are ever more investing resources in these systems, in order to diversify the use of their image databases. In this sense, between 2015 and 2016, Internet giants Facebook and Snapchat acquired Masquerade (MSQRD) and Looksery, respectively. Both start-ups created face modification apps that allow their users to take selfies with filters based on celebrities, emojis, monstrous faces, and various other sorts of graphics layers. This significant transaction indicates the popularity of these applications, and the interest of these corporations to invest more and more in these facial recognition software. Therefore, the underlying question behind the expansion of these systems is where these face shots are being stored? Should we remain uncritical whenever we take a selfie and allow an application to access our camera, hence our private



Hujun He
82.22.19.59
Guangzhou, China

Metadata:
2421國光第一美尻 這身材真的太不科學了 國光幫幫忙
DARK SOULS (React: Gaming)
《萬萬沒想到第二季》 04 勇者的遊戲

photo archive? Therefore, should we be asked about whether we want to opt in/opt out in these surveillance practices? Or should we all be classified, inspected and instructed in the Panopticon? Logically this should be one of our main concerns for the future.

For this reason, facial recognition technologies are not only designed to be reliable mechanisms of surveillance to secure nation-states from 'the other', the 'enemy'. They are also tied to a process of neoliberalization, which has been intensified through the development of computer networks, as Gates (2011) claims:

> […] The transition to biometric identification must likewise be understood as a response to a set of conflicting demands of both the state and the business system to individualize and classify, to include and to exclude, to protect and to punish, to monitor and define patterns, and to otherwise govern populations in the face of their radical destabilization under the wrenching neoliberal reforms instituted in the United States and across the globe during the latter part of the twentieth and early twenty-first centuries (p.28).

Similarly, Lyon (2014, p.7) claims that algorithms are increasingly being used to target specific types of consumers. As he puts it,

> […] A key reason why those commercial and governmental criteria are so imbricated with Big Data is the strong affinity between the two, particularly in relation to surveillance. Big Data represents a confluence of commercial and governmental interests; its political economy resonates with neo-liberalism (Lyon, 2014, p.9).

Besides this integration of corporate and state powers, what is still most problematic about the identities and faces that are being classified 'is not whether to classify, but who classifies, how, when and why?' (Kember, 2014, p. 197). As aforesaid this appears as a revival of 19th century criminology and phrenology, moreover, if we recognize that there is still a significant gap between countries that develop these technologies and the ones that adopt them. Consequently, it is not unlikely to wonder if there could be an ethnic-bias in the algorithms that determine 'dangerous' face patterns. Therefore, it is inevitable to think if we are going to look suspicious in the future, and as a consequence –if it is possible, should we build an appearance that classifies us as law abiding citizens?

Prefiguring an alternative 'algorithmic identity'

By now, it should be no mystery that every time that a user enters a website, the browser deploys a set of tools that extract his/her personal information. Thus, through preset algorithms, Internet firms are using data mining techniques to anticipate his/her demands, as well as locating him/her on a particular segment of the market (McGarry et al, 2005, p.176). Then, it is now common for Internet users to be targeted by advertisements based on their browsing history. But also from registration forms, server logs, past online purchases, search patterns, cookies, according to a paper published by McGarry et al (2005, p.176). This vast amount of data is then embodied in what Cheney-Lippold (2011) calls 'algorithmic identity': an

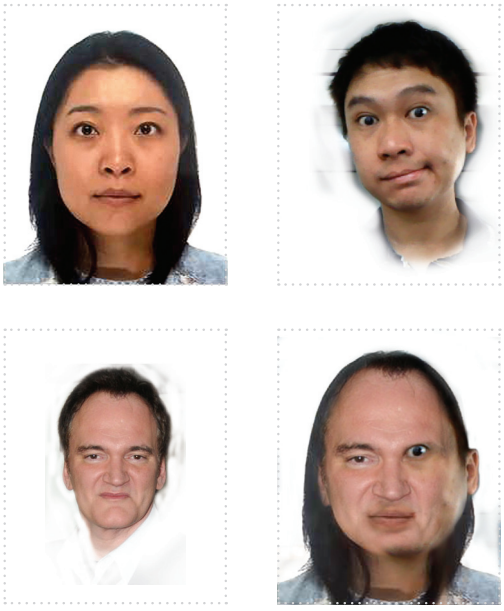
'identity formation that works through mathematical algorithms to infer categories of identity on otherwise anonymous beings' (p.165). This author goes further on to argue that the regulations of gender, class, and race in computer networks, are defined through a 'cybernetics of purchasing' and market research (Cheney-Lippold, 2011, p.171). Thus, the browser decides the gender, supposedly as an autonomous agent during this process of data mining.

Data mining, then, becomes a form of control over the subject, according to Cheney-Lippold (2011). By drawing on Foucault's biopolitics, the author declares that the algorithmic suggestions generated by computer networks, 'persuade users towards models of normalized behavior and identity' (Cheney-Lippold, 2011, p.168). From this perspective, he provides the following example:

> A new value like X = male can then be used to suggest sorting exercises, like targeted content and advertisements, based entirely on assumptions around that value. Yet code can also construct meaning. While it can name X as male, it can also develop what 'male' may come to be defined as online […] How a variable like X comes to be defined, then, is not the result of objective fact but is rather a technologically-mediated and culturally-situated consequence of statistics and computer science (Cheney-Lippold, 2011, p.167).

Hence, 'algorithmic identities' operate on a similar basis to facial recognition technologies, as Kember (2014) states in relation to how they profile customers and/or criminals:

> Contemporary face recognition makes the same moves whether the context is institutional or commercial, classifying and segregating individuals into groups and types depending on their appearance as an indicator of behavior, and evincing a form of biopolitical control that is perhaps more effective, or at least more insidious, for being at a distance (p.190).



Niw Wong
86.134.193.180
Bangkok, Thailand

Metadata:
Quentin Tarantino on
Chungking Express
Life as an Introvert
10 Funniest Shibu Inu videos

As I mentioned before, Facebook is diversifying its infrastructure by combining its own pattern recognition architecture with its large database. In such a way, pattern recognition systems are merging large amounts of user information with facial recognition technologies. Thus, computer networks have the potential to classify their users into totalizing categories that supposedly could prevent criminal activities. But on the other hand, they can track, locate, and anticipate their next action as consumers. This is an example of what Kember (2014) calls 'Ambient Intelligence systems': a set of technologies that 'normalize a culture in which the joint operation of marketing and surveillance is becoming dominant' (p. 184).

As many authors respond (Kember, 2014; Kember and Zylinska, 2012; Suchman, 2007) to this matter, this is an ethical issue, as well as an opportunity, to contest these forms of biopolitical power over subjects. We can find other accounts to critique these computer networks, rather than only addressing our concerns with the limited 'subject-object dualism that structures Western Philosophy' (Kember and Zylinska, 2012, p.125), and the idea that agency only rests on one of the sides. In particular, I agree with Kember's argument (2014, p.185) that feminist technoscience studies offer an effective account to contest the tensions within these technologies.

Haraway's cyborg, more specifically, still proves to be a powerful figure to intervene these systems, and address the questions that emerge (Kember, 2014, p.194). According to Haraway (1997) 'figures do not have to be representational and mimetic, but they do have to be tropic, that is, they cannot be literal and self-identical […]', instead, they 'must involve at least some kind of displacement that can trouble identifications and certainties' (p.11). Furthermore, it is a form of 'serious play' (Haraway in Kember, 2014, p.194), a useful 'trope' to refer about the hybridity of media technologies and humans. In this sense, we could act in response differently to our encounter with facial recognition systems, data mining methods, machine learning, algorithms, biometric templates, etc.

Similarly, by analyzing creative responses to these issues, Suchman (2007) makes a strong argument about the affordances of digital media and 'the ways that through them humans and machines can perform interesting new effects' (p.281). She goes further on to argue that,

> Not only do these experiments promise innovations in our thinking about machines, but they open up as well the equally exciting prospect of alternate conceptualizations of what it means to be human. The person figured here is not an autonomous, rational actor but an unfolding, shifting biography of culturally and materially specific experiences, relations, and possibilities inflected by each next encounter – including the most normative and familiar – in uniquely particular ways (Suchman, 2007, p.281).

Hence, a future possibility relies on exceeding reductionist debates about new technologies, such as technophiles versus technophobics, or hopes and fears from utopias and dystopias. We should then embrace the 'cyborg' as a powerful image to contest these state and corporate structures, and to blur the distinctions between humans and machines in order to deceive the apparatus that seeks to categorize us into specific patterns and behaviors.

Configuring 'No recognizable patterns'

'No recognizable pattern' is a response from digital media to facial recognition systems. At the same time, it reflects upon the convergence of these surveillance technologies with marketing web analytics, algorithms, and the uses of personal information gathered in databases. I refer to the concept of the 'algorithmic identity' (Cheney-Lippold, 2011) to imagine, in a parodic way, 'a serious play', how computer code and metadata would fill in the gaps that facial recognition technologies cannot detect. That is, a user's profile informed by his/her browsing history and cookies, added to the ID pictures that float around the web with a particular name and surname. Also, this project acknowledges our 'entanglement' with media technologies, in which 'ethics is figured as a process of becoming-with constitutive others' (Barad and Haraway in Kember, 2014, p.194). This project is a political statement towards surveillance and the right to anonymity, and at the same time it recognizes the importance of our 'co-constitution' with media technologies.

From this perspective, the portraits of 'No recognizable pattern' draw on the figure of the cyborg. Considering that Haraway (1991) explains,

> Cyborg imagery can suggest a way out of the maze of dualism in which we have explained our bodies and our tools to ourselves. This is a dream not of a common language, buy of a powerful infidel heteroglossia [...] It means both building and destroying machines, identities, categories, relationships, space stories [...] (p.181).

On a basic level, distorting faces is a way of prefiguring untraceable 'biometric templates', informed by algorithms such as PCA or LDA, or the latest addition to the field, known as "DeepFace". But also, these 'cyborg portraits' attempt to play and subvert fixed faces, and potential 'dangerous' identities, while they open up a dialogue between human and non-human agencies. Yet, more importantly, my objective is to make intelligible that 'the role of technology in this process of evolution is neither determining nor determined. Neither is this role merely instrumental or anthropological; rather, it is vital and relational' (Kember and Zylinska, 2012, p.203). We, as part of the process and not as a discrete entity separated from its devices.

In this process, I requested several people to submit personal ID photos. The participants of this project had to fill out a form with personal information, such as names, place and date of birth, etc. This was provided along with other data and metadata such as IP address, recommended content by their social media sites, such as videos, advertisements, websites, music, etc. Once the information was collected, I merged the original sent images with faces that appeared in the content that was algorithmically suggested by the social media sites of each user. In this manner, I imagined how the Facebook's DeepFace algorithm would have done it. My self-portrait 'Miguel Loor' (Fig.1), for instance, is a combination of my ID photo, with other image files linked to this name in Google. Additionally, my original picture has been merged with other faces based on recommended videos from YouTube, such as: "How to grow your hair longer and faster!" a suggestion that stands on the browsing history of my partner with whom I share an IP address. In the same way, the other portraits from this photo series are layered with Google Images search outcome, and, then combined with their specific metadata. These include video game characters, celebrities, and anonymous users, regardless their sex, age, and race. As a result, the faces are 'monstrous and illegitimate […] potent myths for resistance and recoupling (Haraway, 1991, p.154). Likewise, these 'new' ID photos are also humorous, ambiguous and genderless as a way of configuring untraceable patterns for any surveillance mechanism, such as CCTV circuits, biometric controls or built-in cameras.

Furthermore, this photo series is a starting point to delve further in the possibilities of becoming differently with media. Consequently, we could mediate a more unstable 'algorithmic identity' and perhaps open up the boundaries for the performativity that enacts social media profiles in Facebook, Twitter, Instagram, etc. As Kember and Zylinska (2012) assert, 'performativity is an empowering concept, politically and artistically, because it not only explains how norms take place but also shows that change and intervention are always possible (p.189). In this way, they appeal for 'a new paradigm' not only for 'doing media critique-as-media analysis but also for inventing media' (Kember and Zylinska, 2012, p.189). In other words, what if the participants of this project use these portraits as a new 'profile picture' in Linkedin, a professional networking site? Or how about if they mix up the recommendation algorithms in Facebook, which are based on their 'posts' and 'likes' activity? Or what if the project can work as a test to design social networks and apps to perform alternative identities with puzzling categories? From here, the project may extend to different creative paths, since several questions and possibilities are now open.

However, this project aims to be positioned in what Kember and Zylinska (2012) recognize as 'creative media'. The notion of 'creativity' here becomes a method to contest the neoliberal rationality inscribed by the industry. Therefore, as stated before, this series of portraits aims to go further, 'from the theater of mere form to an ethic political performance' (p.200).

In a similar way, other creative projects are offering this sort of affordances for digital media in response to facial recognition systems. In Your Face is Big Data, young artist Egor Tsvetkov from Russia photographed around 100 people in the subway. Later, he tracked them through FindFace a facial-recognition app that explores the enormous database of images in VK, the most popular social media site in Russia (Noyes, 2016) and then produced various diptychs of his photos and the results of both web applications. Likewise, artist Philipp Schmitt created Unseen Portraits, in which he inquires 'what face recognition algorithms consider to be a human face' (Schmitt, 2016). In such a way, through his installation that includes two computers, two screens and a webcam he distorts original ID photos

Signe Hede
92.24.109.72
Tønder, DK

Metadata:
Sharon Osbourne - Best Moments (Part1)
My Homemade 40W LASER SHOTGUN!!!!!
Of Monsters and Men- My Head is an Animal Full Album

through code until the face becomes unrecognizable for any machine. On the other hand, designer Adam Harvey proposes an 'anti-face', which through make-up and hair styling a facial recognition system would fail to identify (Burns, 2015).

Thus, these projects reflect upon privacy issues as well as the agency of computers when they process facial images and data, and as a result how they classify and categorize people. But more importantly they recognize the role of technology in envisaging alternative identities in a digital context. They are all 'cyborgian' statements to the surveillance state.

Conclusion

Throughout this article, I have argued how facial recognition technologies, and their link with marketing web analytics, are becoming an everyday practice of the media environment. In addition, I have pointed out how the increased development of these media technologies entails the ubiquity of several sets of algorithms, which may result problematic. As a response, the faces of "No recognizable pattern" dissent from the totalizing categories, and fixed identities, constituted by these surveillance practices. With the previous arguments, it is not illogical to believe that a lot of inequity and biases, such as race, gender and potentially class, inform the development of these new technologies. Yet, through the lens of feminist technoscience, and the figure of the cyborg, we can contest to technocapitalist structures of power, and envision from within our media technologies 'a difference that matters' (Kember and Zylinska, 2012, p.200).

Despite that facial recognition systems might seem as an improbable technology for certain social contexts, the debate is not about the development of these media devices. It is about positioning ourselves towards a future where we embrace these machines, and take advantage of the uncertainties that emerge from that encounter. Then we could set a political statement for the future and our rights in the digital era. post(s).

Miguel Loor
192.158.12.2
Guayaquil, Ecuador

Metadata:
How To Grow Your Hair In 1 Day 2015!
How To: My Quick and Easy Hairstyles | Zoella
2 Tone Mix

List of references

Baer, D.
(2014) Mark Zuckerberg Explains Why Facebook Doesn't 'Move Fast And Break Things' Anymore. Available at: http://www.businessinsider.com/mark-zuckerberg-on-facebooks-new-motto-2014-5?IR=T (Accessed: 10 August 2015).

Burns, J.
(2015) The Anti-Surveillance State: Clothes and Gadgets Block Face Recognition Technology, Confuse Drones and Make You (Digitally) Invisible. Available at: http://www.alternet.org/news-amp-politics/anti-surveillance-state-clothes-and-gadgets-block-face-recognition-technology (Accessed: 10 August 2016)

Cheney-Lippold, J.
(2011) 'A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control', Theory, Culture & Society, 28(6), pp. 164–181. doi: 10.1177/0263276411424420.

Foucault, Michel.
(1980) 'Truth and power', in C. Gordon (ed.), Power/ Knowledge. Brighton: Harvester.

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

Haraway, D. J.
(1991) Simians, Cyborgs, and Women: The Reinvention of Nature. New York: Routledge.

Haraway, D. J.
(1997) Modest Witness@Second Millenium. FemaleMan Meets OncoMouse: Feminism and Technoscience. London: Taylor & Francis.

Kember, S.
(2014) 'Face Recognition and the Emergence of Smart Photography', Journal of Visual Culture, 13(2), pp. 182–199. doi: 10.1177/1470412914541767.

Kember, S. and Zylinska, J.
(2012) Life after new media: mediation as a vital process. Cambridge, MA: MIT Press.

Li, S. Z. and Jain, A. K. (eds.)
(2011) Handbook of Face Recognition. 2nd edn. New York: Springer-Verlag New York.

Lyon, D.
(2014) 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique', Big Data & Society, 1(2). doi: 10.1177/2053951714541861.

McGarry, K., Martin, A. and Addison, D.
(2005) 'Data Mining and User Profiling for an E-Commerce System', in Classification and Clustering for Knowledge Discovery. Springer Science + Business Media, pp. 175–189.

Noble, A.
(2016) U.S. airports to roll out facial-recognition software to catch fake passports. Available at: http://www.washingtontimes.com/news/2016/jan/21/us-airports-roll-out-facial-recognition-software/ (Accessed: 05 July 2016)

Noyes, K.
(2016) Your face is big data:' The title of this photographer's experiment says it all. Available at: http://www.pcworld.com/article/3055305/analytics/your-face-is-big-data-the-title-of-this-photographers-experiment-says-it-all.html (Accesed: 05 July 2016)

Risen, J. and Poitras, L.
(2014) N.S.A. Collecting Millions of Faces From Web Images. Available at: http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html (Accessed: 20 August 2015)

Roberts, J.J
(2015) Walmart's Use of Sci-fi Tech To Spot Shoplifters Raises Privacy Questions. Available at: http://fortune.com/2015/11/09/walmart-facial-recognition/ (Accessed: 05 July 2016)

Schmitt, P.
(n.d.). Unseen Portraits - Philipp Schmitt. Available at: http://philippschmitt.com/projects/unseen-portraits (Accessed: 05 July 2016)

Solon, O.
(2014) Car camera system knows when you have road rage (Wired UK). Available at: http://www.wired.co.uk/news/archive/2014-03/18/in-car-emotion-detector (Accessed: 23 August 2015).

Star, S. L. and Bowker, G. C.
(2000) Sorting Things Out: Classification and Its Consequences (Inside Technology). Cambridge, MA: The MIT Press.

Suchman, L. A.
(2007) Human-Machine Reconfigurations: Plans and Situated Actions. 2nd edn. Cambridge: Cambridge University Press (Virtual Publishing).

Taigman, Y., Yang, M., Ranzato, M. and Wolf, L.
(2014) 'DeepFace: Closing the Gap to Human-Level Performance in Face Verification', 2014 IEEE Conference on Computer Vision and Pattern Recognition, . doi: 10.1109/cvpr.2014.220.

Temperton, J.
(2015) Eyes-on with Fujitsu's smartphone retina scanner (Wired UK). Available at: http://www.wired.co.uk/news/archive/2015-03/05/fujitsu-retina-scanner (Accessed: 15 August 2015).

Wee Sile, A.
(2015) French firm takes home security cameras to new level. Available at: http://www.cnbc.com/2015/10/08/netatmo-welcome-smart-home-security-camera-has-face-recognition-technology.html (Accessed: 05 July 2016)