Lotte Houwing

Reclaim your Face and the Streets

Why Facial Recognition, and Other Biometric Surveillance Technology in Public Spaces, Should be Banned

Public spaces play a crucial role in democratic societies. They are sometimes called a sanctuary for our fundamental rights. With the deployment of biometric surveillance technology you can be identified, analysed, tracked, manipulated and controlled throughout your day. It is easy to see how this deployment is incompatible with a free society in which we can exercise our fundamental rights. However, in this article I will take some more space to elaborate on the problems of biometric surveillance, and why the use of this technology in public spaces should be effectively and legally banned.

Biometric surveillance reduces people to walking barcodes. It leaves no space for an opt-out, but enables the connection between persons in physical space with that of profiles in existing, searchable databases. Belonging to the family of surveillance technologies that make use of profiling, it aims to sort people. Neither these profiles, the algorithms nor the technology are neutral and they exacerbate systemic inequalities in our society. These are not just technological deficiencies that are solvable with more diverse datasets to train the algorithms. Making the technology working equally well ON everybody does not mean it works equally well FOR everybody. The deployment of the technology is inherently untargeted, making it a means of mass surveillance. The law is clear about that: Biometric mass surveillance is illegitimate. However, two parties might benefit from a slow and steady introduction of the technology: governments hungry for control and industry seeking product-market-fits. And in practice we see the use of biometric surveillance popping up like mushrooms in autumn. To protect our streets, our freedoms and our societies, we need a more explicit and effectively enforced ban on biometric surveillance technology in publicly accessible spaces.

Public Space: The Street is Where it Happens

When we talk about a free democracy it is important to realise that parliament is not the (only) space where politics happen and society is formed. Publicly accessible spaces play a fundamental role in facilitating debate among the people who together form a society. It are the places where individuals encounter each other in a more random fashion than in the private sphere and therefore have to relate to each other's differences and have a public debate about how to live together.

Moreover, public space is the physical stage for protest and political interventions. An analogue example of the effect that altering public space

has on the potential for protesting is seen in the urban planning of Paris by Georges-Eugène Haussmann. His broad boulevards made it much more easy for the French army to control and repress popular uprisings.[1]

A more technological example can be found in Hong Kong where AI surveillance in public space can severely impact the freedoms that underlie the right to protest and form a threat to the safety of protesters. Protesters fight back by finding ways to block or demolish the invasive technology, like laser pointers against cameras or simply tearning down poles with facial recognition cameras on them.[2] But fighting back gets harder when you have to fight technology that is turning your own face into a weapon that will be used against you.[3] We see that this kind of surveillance in public space is used to target protesters against the establishment, but we also see that it prevents people from going to protests in the first place.

Surveillance technologies in public spaces are also introduced from other, less obvious, angles like smart cities. The idea of monitoring and measuring everything to make experiences as seamless as possible introduces all kinds of data-driven surveillance technologies that rearticulate the experience and function of public spaces. From a place of (relative) anonymity, all kinds of smart devices make the urban public spaces into places of data capture which before was reserved for research laboratories and high-surveillance institutions like prisons, hospitals or mental institutions.[4] It is of the utmost importance that from the smart city perspective, we should also be very critical of the introduction of surveillance technology into our public spaces. Too often in these debates, the value of privacy and public space are stripped of their political meaning and reduced to respectively data protection and an open space where the public aspect is translated into 'up for grabs' of your personal information. When we look at publicly accessible spaces as

1 Cf. Willsher, Kim: Story of Cities #12 : Hausmann rips up Paris—and divides France to this day. In: The Guardian of March 31, 2016, https://www.theguardian.com/cities/2016/mar/31/story-cities-12-paris-baron-haussmann-france-urban-planner-napoleon (March 5, 2021).

2 Cf. Reason TV: Hong Kong protestors combat the surveillance state. In: Youtube of 4 October 2019, https://www.youtube.com/watch?v=VXog6t4kNyc (January 13, 2021).

3 Cf. Mozur, Paul: In Hong Kong protests, faces become weapons. In: The New York Times of July 26, 2019, https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html (December 8, 2020).

4 Cf. Galic, Maša: Surveillance, privacy and public space in the Stratumseind Living Lab: the smart city debate, beyond data. In: Ars Aequi (2019), July/August, p. 1.

spaces where public debate takes place, where the plurality of people and their lifestyles is facilitated and where democratic rights are exercised. And we look at privacy as more than the protection of our personal data but also as a fundamental right, a fundamental social value, a necessary condition for the safe use of other fundamental rights such as our freedom of speech, freedom of religion and the protection of our autonomy. We realise that we cannot let our guard down regarding the protection of privacy in public spaces when we value a free society.

Maša Galič and Marc Schuilenburg examine the current debate on smart cities by looking at three contemporary perspectives on "the right to the city" a concept which is coined by Henri Lefebvre. This concept consists of several aspects that are important in understanding the political aspects and role of public spaces in a city. Lefebvre argues that "struggles for the city are vital to any emancipatory politics of space".[5] In this context, a few qualities of the city and public space come to the fore: The centrality of public spaces in a city facilitates surprise, meeting and difference. It is the space where (near-) strangers have social encounters that enable a community. The right to difference entails the creation of an inclusive city composed of different lifestyles as opposed to forces of abstraction and homogenization of space, produced by a bureaucratic capitalist system.[6] And appropriation, the idea that the public space in a city should be shaped according to the inhabitants needs.

In their paper Galič and Schuilenburg describe how the roll out of smart cities often happens from a perspective of Morozov's 'solutionism', a way of thinking that "presumes rather than investigates the problems that it is trying to solve, reaching for the answer before the questions have been fully asked".[7] Investing in smart technology is seen as the best way to avoid and solve all kinds of problems, when it comes to 'smart' surveillance technology, this mostly comes down to fighting crime, protecting property, creating a seamless experience and maintaining public order in a very narrow sense. Galič and Schuilenburg identify, as others before them, public safety and security as key drivers for the implementation of smart technologies. There is a strong focus on the elimination of disorder and conflict and smart technolo-

5 Galič, Maša; Schuilenburg, Marc: Reclaiming the Smart City: Toward a New Right to the City. In: Juan Carlos Augusto, Handbook of Smart Cities (2020), p. 5.

6 Cf. Galič; Schuilenburg 2020.

7 Morozov, Evgeny: To save everything, click Here, New York 2013, p. 6.

gies promise better protection against these dangers by taking a more proactive approach, based on and coupled with a trend of datafication.[8]

An example of this can be found in the Dutch city of Eindhoven. The local government wanted to 'revitalise' this street with mostly bars. To do that, a Living Lab was started to measure, analyse and influence the behaviour of its visitors. Several kinds of sensors in the street and monitoring of social media together give an impression of the atmosphere. The collected data onsists of among others the amount of beer that is sold, the amount of people that are present, the weather, the volume of the sound and data from wifi-tracking. The aim of the project is to no longer react to every small incident after a norm is breached, but to change the environment to manage the relationship between the incident and the crowd. Central to this project is a business-model of undisturbed consumption: More beer, less unrest.[9] Here you see that the technology that is deployed in this space is mostly serving the goal of efficiency in maintaining public order and the commercial interests of the bar owners, by placing everybody in the space under surveillance. Whether you are living there, just passing by, working in a bar, having a date or celebrating a birthday.

To limit the scope of the discussion within this paper, I will focus specifically on biometric surveillance technologies in public space. I made this choice because work on the topic feels urgent. Wee see facial recognition popping up significantly in Europe, infiltrating our public spaces and the discussion on the topic is lively. We do not have the luxury to make this mistake. Therefore we, a coalition of more than 40 (digital) human rights organisations throughout Europe, started the campaign Reclaim Your Face. In the campaign we call for a ban on all biometric surveillance technologies in publicly accessible spaces. I will now explain why we need to stop this.

8 Cf. Galič; Schuilenburg 2020, p. 4.

9 Cf. Houwing, Lotte: Experimentele Manipulatie: Burger steeds vaker onwetend proefdier. In: Bits of Freedom of June 5, 2019, https://www.bitsoffreedom.nl/2019/06/05/experimentele-manipulatie-burger-steeds-vaker-onwetend-proefdier/ (December 2, 2021).

From Bio to Metrics: A Fundamental Reduction

Ok, so let's first take a step back. What are we talking about when we are talking about biometric surveillance technologies? In the General Data Protection Regulation (GDPR), biometric data is defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic [fingerprint] data".[10] This means that the European law recognises two categories of information as biometric data: The first one pertains to bodily characteristics like facial features, DNA or fingerprints. The second one pertains to behavioural characteristics like handwriting or gait. To both categories applies the logic of the word biometric: The specific technical processing requires and performs a reduction from a biological characteristic of a natural person to something that a computer can digest; metrics.

The next step in the development of facial recognition technology, technologies that perform emotion recognition, are normally also included in biometrics. These technologies might not be focussing on the unique identification of a natural person, but they do analyse behavioural characteristics of our bodies in a specific technical process with personal data as a result. What they also do is cause the same reduction. Motions of the muscles in our face and our facial expressions are made machine-readable and linked to emotional states by algorithms, based on a presumption of universality.[11] This is the reduction in full glory: even our emotions get quantified.

David Lyon, director of the Surveillance Studies Center at Queens University, has provided a definition of surveillance: "Any focused attention to personal details for the purposes of influence, management, or control."[12] Biometric data can be used to identify people, but it can also be used to categorise people, and sort them. An example is facial recognition software that

10 Article 4 sub 14 GDPR.

11 Cf. Schwartz, Oscar: Don't look now, why you should be worried about machines reading your emotions. In: The Guardian of March 6, 2019, https://www.theguardian.com/technology/2019/mar/06/facial-recognition-software-emotional-science (March 5, 2021).

12 Lyon, David: Surveillance Power and Everyday Life. In: Oxford Handbook of Information and Communication Technologies (2007) January, p. 1.

is used in China to recognize Uighur minorities.[13] But we should not just point our finger at China, EU Horizon 2020 projects include for example a virtual agent using emotional recognition systems at its borders to judge the truthfulness of travelers.[14]

To put it all together: Biometric surveillance technologies are technologies that make use of our unique and highly personal, biometric data in order to automatically influence, manage, or control us. It reduces us as human beings to walking barcodes allowing different regimes to apply according to automatically ascribed values and decisions.

Shaping Behavior and Shaping Society: To Shape or to be Shaped?

This fundamental reduction brings along some effects. One is strongly normative. Since measurable things have averages and enable data about what is most common, it delivers an account of what seems to be normal, and thus also what is perceived as divergent, which is easily viewed as suspicious. Especially when the technology that is deployed is there to mostly serve goals of public order and safety. Examples of this are 'smart' cameras at airports or train stations that detect suspicious behaviour when people pursue abnormal walking patterns or forget their luggage. We should never forget that we shape technology, but that thereafter, technology is shaping us. When we design cameras to detect divergent behaviour, it might trigger some alert when we start behave in a manner that diverges from the expectations and predictions that are coded in the technology, for example when we start dancing in the streets. Are we

13 Cf. Harwell, Drew; Dou, Eva: Huawei tested AI software that could recognize Uighur minorities and alert police, report says. In: The Washington Post of December 8, 2020, https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/ (December 8, 2020).

14 Cf. Gallagher, Ryan; Jona, Ludovica: We tested Europe's new lie detector for travelers and immediately triggered a false positive. In: The Intercept of July 26, 2019, https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/ (December 8, 2020).

OK with surveillance choreographing us?[15] Wouldn't that be a very dystopian image?

An other effect of this reduction is that uncertainties are being removed. A risk score of 0.7 leaves room for uncertainties. But when this score is attributed to an individual it is used to inform a decision: Either classify it as a high risk score, treat it as a 1 and apply a more strict regime to this individual, or do not do that, treat it as a 0 and let the person pass. To get to an outcome, all the uncertainties in the process of getting there have to be removed.[16] This subtracts nuance and grey tones as well as accountability from reality, leaving black and white action perspectives.

By taking the road of datafication and surveillance we demand citizens to be continually transparent. By taking a proactive approach in preventing crimes or anticipating on behaviour that the machine might interpret as suspicious, the tables of fundamental principles of the rule of law are turned. Citizens have to consistently provide insight and justification about themselves and their actions as opposed to the situation that their actions should give reason to a reasonable suspicion that needs to precede off the legitimize any form of control. By legitimizing control in advance and outsourcing the judgment of what behaviour is a reason for suspicion, we limit the scope of what might be acceptable behaviour, chilling our political freedoms and sense of social experiment, risking our Lefebvrian right to the city.

There is no Opt-Out

The biggest fallacy of surveillance in publicly accessibel spaces is that it can legitimately be based on consent. This is not possible because consent needs to be informed and freely given. Informed means that it must be clear to the person whose information is processed what he/she/they is consenting to. So it must be claur what kind of surveillance is being deployed, what data is processed, by whom, under what conditions etc. Freely given means that it must be possible for the person to say no, without having negative consequences of this refusal. This situation simply does not correspond with the practicallities of surveillance in publicly accessible spaces. In general, there is

15 Cf. Doringer, Bogomir: When you feel pain, keep on dancing. In: TQW of June 24, 2020, https://tqw.at/when-you-feel-pain-keep-on-dancing-doringer/ (January 13, 2021).

16 Cf. Rasch, Miriam: Ethiek in tijden van dataïsme, Amsterdam 2020, p. 120.

a lack of transparency when it comes to the deployment of surveillance. And it is also not realistic to think that people will read informative signs before entering spaces they need to be going throughout their daily lifes. Above that, there is no option for refusal, you cannot opt-out.

There are two distinct ways in which the deployment of biometric surveillance technologies in publicly accessible spaces leave people no choice to opt-out. Although public space might not be well-defined in law, and the limits of which spaces are public and which aren't, are not agreed upon, there is consensus about the fact that public space is a place where people wanting to take part in society have no ability to opt out from entering. So deployment in public space requires people to accept their bodies being scanned to take part in society.

In addition to the impossibility to opt-out from public space, it is impossible to opt-out from your body, and difficult to prevent your body from being surveilled once the technology is being deployed on the streets. The extremely personal nature of your biometric data means that it cannot be changed or left at home in a drawer. On top of that, it is fairly easy to gather biometric information covertly and distantly. This allows others to identify and follow people through public space without their knowledge.[17]

The demand for transparency on the side of people and the disability to opt-out from your body as a unique identifier are shown in the battle about facial datapoints. Several countries have laws that forbid to cover your face when in public space. The coronavirus created an exception to this, requiring people to wear facemasks and thus also covering data points that are used in identification. However, the protection this exception had to offer was only a matter of time, since researchers already scraped images of masked up faces from social media, creating specific datasets to train face recognition on masked faces.[18]

17 Cf. Houwing, Lotte: Stop the Creep of Biometric Surveillance Technology. In: European Data Protection Law Review (2020), nr. 2, p. 174.

18 Cf. Ng, Alfred: Your face mask selfies could be training the next facial recognition tool. In: Cnet of May 19, 2020, https://www.cnet.com/news/your-face-mask-selfies-could-be-training-the-next-facial-recognition-tool/ (March 5, 2021).

Transformation of Existing Surveillance Infrastructure

Before the deployment of biometric surveillance technology in publicly accessible spaces it was already hard to move around the city without being spied upon. Most people living in cities are used to being surveilled by CCTV systems when going about their daily lives. Still, it makes a difference whether this is a 'normal' camera, or one equipped with biometric data analysis functions, because it is shifting the focus from the "what" to the "who". Where CCTV systems capture stories of what is happening in a certain place, biometric surveillance technologies are adding the dimension of identification, making it about tracing people and their personal behaviour, and expanding the scope of information that can be extracted from and linked to the images.

Using our physical characteristics as unique identifiers brings along another aspect of transformation of existing surveillance infrastructure: It enables a connection between our physical appearance and information about us in existing, searchable databases. This may sound abstract, so a few examples:

Churchix is facial recognition software that is used to measure attendance.[19] It makes it possible for church leaders (or for that sake, everybody) to automatically track which members of a religious community are attending a mass and which are not, based on the feed of the security camera near the entrance.[20]

The app FindFace makes it possible to search for people on VK, the biggest social network of Russia. The photographer Egor Tsvetkov tried it out in his project "Your face is Big Data" with random people in the subway, and he was able to link 70% of the young people he encountered to their online presence.[21] They might not even have noticed.[22]

Last but not last, your personal identity is linked to several kinds of government registration systems, like a social security number, or a police file. Once surveillance systems in the streets are able to uniquely identi-

19 https://churchix.com/ (December 8, 2020).

20 de Zwart, Hans: 'Geen gezicht'—De Big Brother Awards speech van Hans de Zwart. In: Bits of Freedom of 15 November 2016, https://www.bitsoffreedom.nl/2016/11/15/geen-gezicht-de-big-brother-awards-speech-van-hans-de-zwart/ (December 8, 2020).

21 Cf. Tsvetkov, Egor: Your Face is Big Data. In: Cargo Collective, https://cargocollective.com/egortsvetkov/Your-Face-Is-Big-Data (December 8, 2020).

22 Cf. de Zwart 2020.

fy passersby, people in crowds are like walking barcodes connected to their whole cabinet of files. The chilling effect this creates is something Haussmann could only dream about.

To show how easy it is to use this potential, and thus how easy deployment of it gets out of control, Bits of Freedom took it to the test and made the first steps to build the ultimate stalker tool.[23] On the website www.webcam.nl/amsterdam you can follow several livestreams of what is happening throughout the city of Amsterdam. We went to the Dam to get our face on camera. We downloaded the livestream as well as a free trial of Amazon's Rekognition to see whether the facial recognition software was able to correctly identify us out of the feed, and succeeded. This shows that it is possible for every slightly tech savvy person to build a tool that enables you to follow a specific person ((ex-)partner? Child? Employee?) around and to maybe even add notifications if they get in a certain area, without spending any money or having to get up from their couch.

Another transformation that takes place is that this extra functionality can go into hiding. 'Plain' cameras (can) look the same as for example facial recognition cameras. So while this extra functionality makes you a lot more transparent, you are left in the dark about the kind of surveillance that is performed.

Surveillance Sorts People

As I described above, surveillance can be defined as "any focused attention to personal details for the purposes of influence, management, or control".[24] Social sorting is "a way to establish identities, but also to assign risks and value(s) to people". Biometric surveillance technology is focussing on unique personal details to identify people, and based on the information that is linked to them certain rules apply. Social sorting is what's happening when you are buying a washing machine online, and based on your location you get a different price. But this is also what's happening when you are stopped more often for a police control because you are a non-white person.

23 Cf. Hooyman, Paula: Amazons Rekognition shows its true colors. In: Bits of Freedom of December 12, 2019, https://www.bitsoffreedom.nl/2019/12/12/amazons-rekognition-shows-its-true-colors/ (December 8, 2020).

24 Lyon, David: Surveillance Power and Everyday Life. In: Oxford Handbook of Information and Communication Technologies (2007) January, p. 1.

In the Netherlands there is a very well-known game, called "Wie is het?" (Who is it?). The point of the game is that you have to ask questions to single out the person that the other player has in their mind. You do this by categorising people, based on characteristics of their physical appearance. For example: Does this person wear any kind of hat? If yes, all others go down. It is the analogue gamification model of social sorting based on physical appearance.

A real life example where values and risks are automatically assigned to people, based on an analysis of their face is iBorderCtrl.[25] IBorderCtrl uses a virtual agent to have conversations with migrants at the EU border and serves as an automated lie-detector. While you answer questions at customs like "What is your name?" and "What is the reason of your visit?" the system analyses the movements of the smallest muscles in your face, assigning you a reliability score on which depends whether you should be subject to further checks or not.

Bias in the Technology

Before I get into this point I want to make a remark: Biases are very problematic, but too often they are presented as the main problem with invasive surveillance technology, like facial recognition. I want to emphasize that in my perspective, these technologies will also be problematic if they would not contain biases. With that of out of the way, what are we talking about when we talk about bias in technology? One of the problems with these systems is that they are built with data. Data that is subjective and established in colonial and patriarchal structures.[26] While to many people automated decision making has a hint of objectivity as compared with human made decisions

25 Cf. https://cordis.europa.eu/project/id/700626, last updated on 22 October 2020 (December 8, 2020).

26 See for more: Crawford, Kate: The Atles of AI: The Real Worlds of Artificial Intelligence, Yale University Press 2021; D'Ignazio, Catherine; Klein, Lauren F: Data-Feminism, MIT Press 2020; Digital Freedom Fund: The Decolonising Data Panel. In: YouTube, https://www.youtube.com/watch?v=WRobUCm13m4 ; Fubara-Manuel, Irene: Biometric Capture: Disrupting the Digital Codification of Black Migrants in the UK. In: African Diaspora of April 2, 2020, S. 117–141; Van Dijck, José: Datafication, dataïsm and dataveillance: Big Data between scientific paradigm and ideology. In: Surveillance & Society 2014 12(2), S. 197–208; Gitelman, Lisa: Raw data is an oxymoron, MIT Press: 2013.

but it is the other way around. The bias is in the data that is used to train the algorithms and in the decisions made by humans in the design of the algorithms. The bias might be hidden by the promise of neutrality that goes out from the technology, but in fact, it has the power to unjustly discriminate at a much larger scale than biased individuals.[27] This means that the categories, profiles, algorithms etc all entail, reproduce and exacerbate this bias. When we use these tools to surveil people, which effectively means to sort people, the systemic inequality is reinforced to say the least. We could also say it in more simple words: Biometric surveillance technologies like facial recognition are racist and sexist.

Some examples: Since corona made us all work and study from home, it hurts me to see the messages of frustrated black students and students of color who are having a hard time dealing with proctoring software failing to deliver a fair and valuable contribution to a functioning education system in this new situation in several ways. One of the most painful ones being that it shuts them out from entering their online exams because the facial recognition gives an error of "poor lighting".[28] One student that is also software researcher looked into Proctorio, one of the most used proctoring softwares. His research has shown that the software uses a facial detection model that is failing to detect black faces more than 50% of the time.[29]

This racism also plays a part in algorithms used to prioritise images and deciding who gets a digital stage and who doesn't, based on the characteristics in the picture. People with Twitter might be familiar with this experiment on the cropping algorithm of the social media platform.[30] The main goal of the algorithm is to make people click on links and let them stay on the platform. Therefore it prioritises the parts of content that it expects you to prefer. Resulting in that it gives the stage to the people on stage.

Then there is a great research from Joy Buolamwini called Gender Shades[31], where she shows how much better European and American facial

27 Cf. Benjamin, Ruha: Assessing risk, automating racism. In: Science (2019) vol. 366 issue 6464, p. 421–422.

28 Khan, Alivardi on Twitter on September 11, 2020, https://twitter.com/uhreeb/status/1304451031066083331

29 Cf. Feathers, Todd: Proctorio is using racist algorithms to detect faces. In: Vice of 8 April 2021 (May 11, 2021).

30 Cf. Arcieri, Tony on Twitter on September 20, 2020, https://twitter.com/bascule/status/1307440596668182528

31 Cf. Buolamwini, Joy: 2018, http://gendershades.org/

recognition systems are in recognising white males compared to the recognition of women of color, and thus how the chances of being false flagged are unequally spread over society, along the lines of privilege.

Database Scandals and Unethical Revenu Models

In the discussion about automated surveillance, this is sometimes portrayed as just a matter of technological deficiencies, and thus easily solvable. In that perspective, the solution lies in training these systems with bigger, more diverse datasets. And if the goal is to let the technology work equally well on everybody, and we look at technology as something that exists in a vacuum, it might be true. In taking this solution into the real world we live in today, it sketches a different scenario. Since technology does not exist in a vacuum, the problem of discriminatory effects is not just in the technology, but also in the deployment of it. We get to this later. First I want to pay some attention to the way in which the same problems reoccur in the so-called solution of attempts to de-bias this technology. We find that in database scandals and unethical revenu models.

A few examples, coming from the real world: To improve its Pixel 4 facial recognition technology, Google contractors targeted homeless people of color to collect more facial scans of people with darker skin. These people were offered a 5 dollar coupon in return for their face data, they were asked to play a "selfie-game", or tricked without knowing they were recorded.[32] Homeless people were specifically targeted because they were least likely to say anything to the media, and the most likely to be convinced by a small amount of money. There are too many stories to pay attention to them all in this article, but there are many examples of tech companies scraping our faces from the internet without permission and use them to fuel the development of their surveillance systems.[33]

32 Cf. Hollister, Sean: Google contractors reportedly targeted homeless people for Pixel 4 recognition. In: The Verge of October 2, 2019, https://www.theverge.com/2019/10/2/20896181/google-contractor-reportedly-targeted-homeless-people-for-pixel-4-facial-recognition (December 8, 2020).

33 Cf. Solon, Olivia: Facial recognition's 'dirty little secret': Millions of online photos scraped without consent. In: NBC News of March 19, 2019, https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921 (Dec 8, 2020); Murgua, Madhumita: Who's using your face? The

People even provide companies with their facial data in a more direct way. A quite well-known example is FaceApp, a free photo manipulation app that showed you what you would look like in 30 years after uploading a photo to their server. For a short time it was a very popular app, and many people gave their face to this company. And not just this company. In their privacy policy FaceApp stated that all data you gave them could be shared with other companies in their group, that could be expanded at any moment, and be used to develop their new technologies. So users of the app provided their data to a non-defined group of companies that can use it to develop their own technologies and services. It should not be surprising that when this data consists of faces, the services and technologies that are trained also include face surveillance systems. By wanting to have a look into the future, the future will be watching us.[34]

The largest scandal of the year might have been the now infamous company Clearview AI that scraped three billion images from the internet, put it in a database and sold it to law enforcement as a service that gives them easy access to personal information on people. It enabled police officers to walk on the streets, make pictures of people, upload it in the app and get to see public photos of that person with links to where these photos appeared on the internet. It is important that although this already happened so often that we keep seeing these as scandals and unethical revenu models, because the internet

ugly truth about facial recognition. In: the Financial Times of September 18, 2019, https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e (December 8, 2020); Roberts, Jeff John: The Business of your face: While you weren't looking, tech companies help themselves to your photos to power a facial recognition boom. Here's how. In: Fortune of March 27, 2019, https://fortune.com/longform/facial-recognition/ (Dec 8, 2020); Hill, Kashmir: How photo's of your kids are powering surveillance technology. In: The New York Times of 11 October 2019, https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html (Dec 8, 2020); Liao, Shannon: IBM didn't inform people when it used their Flickr photos for facial recognition training. In: the Verge of March 12, 2019, https://www.theverge.com/2019/3/12/18262646/ibm-didnt-inform-people-when-it-used-their-flickr-photos-for-facial-recognition-training (December 8, 2020) and there are many, many more.

34 Cf. Houwing, Lotte: FaceApp: Van kijken naar bekeken worden. In: Bits of Freedom of July 19, 2019, https://www.bitsoffreedom.nl/2019/07/19/faceapp-van-kijken-naar-bekeken-worden/ (December 8, 2020).

is not a face database for the development of mass surveillance technology.[35] And it should not be.

The Problem is Not Just Technological

The creation of those bigger, more diverse databases is not making the picture more beautiful. However, there is something more important going on. Focussing on the aspect of technological accuracy is leading the attention away from a more broad discussion and context of racialised surveillance. Solving the accuracy problem is just making sure that the technology is working equally well ON everybody, leaving the question whether it works equally well FOR everybody unaddressed. It might be that we are talking about technology that becomes more dangerous the better it works.

Even if the technology would be de-biased, it is highly likely that it will be disproportionately used against communities of color.[36] It would be used mostly for policing less serious crimes associated with poverty and against people in more vulnerable positions like protestors.[37] Since these problems are ingrained in larger society, fixing the discriminatory effects of biometric surveillance technology is not that simple. There is more work to be done.

35 Cf. Hill, Kashmir: The secretive company that might end privacy as we know it. In: The New York Times of January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (December 8, 2020).

36 Cf. Chowdhury, A: Unmasking Facial Recognition. an exploration of the racial bias implications of facial recognition surveillance in the United Kingdom. In: webrootsdemocracy.org: 2020.

37 Cf. Gellman, Barton; Adler-Bell, Sam: The Disparate Impact of Surveillance.In: The Century Foundation of December 21, 2017, https://tcf.org/content/report/disparate-impact-surveillance/?agreed=1 (December 8, 2020); Henly, Jon; Booth, Robert: Welfare surveillance system violate human rights, Dutch court rules. In: The Guardian of February 5, 2020, https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules (December 8, 2020).

Mass Surveillance

Often when surveillance technology is introduced, arguments are made that it will only be used to combat serious crimes, and deployed in a targeted manner. But this is impossible. To recognize this one person in the crowd, the technology has to scan every passerby, process their physical data and match it to the database. Especially when this is deployed in a publicly accessible space, the effect of the deployment of this technology is untargeted and amounts to mass-scale processing of very sensitive, biometric data.

The databases that entail the list of persons who the so-called targeted deployment of the technology is aiming for show a great drive to expand. In 2016, a study from Georgetown Law's Center on Privacy and Technology found that half of US adults were already recorded in police facial recognition databases.[38] In the Netherlands it is already 1 in every 12 adults.[39]

These large scale databases and untargeted effects of the deployment of surveillance technologies mean that fundamental principles of the rule of law are not being upheld. Where the rule of law requires reasonable suspicion before infringing capabilities can be deployed against citizens, untargeted mass surveillance technologies start with treating everybody as a suspect. We have to be very conscious that with the choices we make in which technology we are going to use, especially in public space, we are shaping our gaze into society and society itself. Therefore we should include in those processes the question: what kind of society do we want?

(Self)Regulation Won't Do

We do not need (self)regulation of biometric surveillance technology in publicly accessible spaces, we need to get rid of it.

Calling for a regulatory framework might imply to some that current legislation is ambiguous about the acceptability of biometric mass surveillance. We need to be very clear that assessing biometric surveillance in the

38 Cf. Garvie, Clare; Bedoya, Alvaro/Frankie, Jonathan: The Perpetual Line-Up: Unregulated police facerecognition in America. Georgetown Law Center on Privacy and Technology October 18, 2016, https://www.perpetuallineup.org/

39 Cf. Houwing, Lotte: We need to be bolder. In: Bits of Freedom of 30 January 2020, https://www.bitsoffreedom.nl/2020/01/30/we-need-to-be-bolder/ (December 8, 2020).

light of the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, and the principles set out in the General Data Protection Regulation, do not leave space for the deployment of these biometric surveillance technologies in publicly accessible spaces, since it requires mass-scale processing of biometric data.

Regulation implies a limited legitimization. My concern is that we will not be able to contain the use of biometric surveillance. History has taught us never to underestimate the power of function creep. There are several ways the use and effects of facial recognition surveillance might expand over time. First, the legal basis and/or the scope of the basis can be expanded. Limiting the use of such far-reaching technology to combating terrorism might sound limited, but the limitation and therefore protections are dependent on government classifications. Several examples around the world, including in the Netherlands, show that even non-violent citizen interests groups are classified as 'extremist' or 'terrorist' when more powers to surveil these groups are desired. A second example of how function creep will take place, is with regards to access to the data. Waiving the fraud-prevention-flag, and showing a complete distrust of citizens, government institutions are very keen to share access and combine databases. Why would databases filled with our biometric data be exempt from this data hunger?[40]

Several companies pleaded for a moratorium. However, more than anything else, what a moratorium will result in, is time. Time in which the technology will become normalized. Time in which industry will deploy its lobbyists. Time in which the companies at the forefront of product development, search for and find product-market-fit. Time in which civil society will again and again mobilize citizens until those citizens become fatigued and weary, and disbelieving that their voice makes a difference.

Then there are the tech companies themselves, taking part in the political discussion that have evolved about facial recognition. We already see this happening in communications from tech companies. The CEO of IBM wrote a letter to Congress to sunset their general purpose facial recognition.[41] And a little later Amazon followed with a one year moratorium on the use of the

40 Cf. Ibid.

41 Cf. Krishna, Arvind: A letter from our CEO on IBM.org: 2019, https://www.ibm.org/responsibility/2019/letter (December 8, 2020).

technology by law enforcement.[42] It is hard however, to see this as anything else than a PR stunt.

The EDRi-network wrote IBM a letter with a request for more information about their statement. It included questions like "Which contracts will be stopped as a result? Which contracts won't? How does IBM define general purpose? Has IBM engaged fundamental rights experts? Do these steps apply only to the US, or to IBM's global activities?" In the response the Chief Privacy Officer of the company only reiterated the general statement and gave some more information about initiatives on artificial intelligence and ethics IBM participated in. Not a single question that was asked, was answered.[43]

We're concerned, therefore, that the demand for a moratorium isn't bold enough. We believe existing regulation needs to be enforced, banning the deployment of facial recognition as a surveillance tool in public space.

Conclusion

The important notions that Lefebvre describes when it comes to the right to the city are all put under pressure by the deployment of biometric surveillance in publicly accessible spaces: Building a community and have our community events in freedom. The freedom to be ourselves and live our lives the way we want to and we believe it should be lived. Without having to abide to a norm that is an arbitrairy average, destilled out of big data and forced upon is by technology that makes assumptions of suspicion about every person, every body and every behaviour that deviates from this norm. And the ability to give shape to public space in a way that it facilitates the needs of the people that use it, instead of just the commercial interests of tech companies or the interests of people who are responsible for enforcing public order.

The introduction of biometric mass surveillance in publicly accessible spaces reduces lively public spaces to spaces where technology is monitoring,

42 Cf. Kari, Paul: Amazon to ban police use of facial recognition software for a year. In: The Guardian of 11 June 2020, https://www.theguardian.com/technology/2020/jun/10/amazon-rekognition-software-police-black-lives-matter (December 8, 2020).

43 Cf. European Digital Rights: IBM's facial recognition: the solution cannot be left to companies. In: https://www.edri.org of July 17, 2020, https://edri.org/our-work/ibm-facial-recognition-solution-cannot-be-left-to-companies/ (December 8, 2020).

analysing, judging and manipulating us and our behaviour. It reduces variety among people to different ways in which people deviate from norms, that can be quantified into risk scores based on which people can be sorted into different regimes at airports and border or ticketcontrols. It reduces people to walking barcodes that can be scanned while walking the streets, linking their physical appearances to information about them in existing and searchable databases. And if we don't pay attention, it reduces our minds and what we perceive as possible or acceptable ways to shape our future realities and approach each other and our differences with an open mind.

Current legislation does not leave space for the mass processing of biometric data, and thus not for biometric surveillance technology in public spaces. However, in practice we see it popping up like mushrooms in autumn. Often introduced as pilots, surveillance technology finds its way in, but once introduced these kinds of technology tend to stick around. Therefore, we need a clear statement from the EU and national legislators to protect our public spaces and democratic rights. Their task is clear: Ban biometric mass surveillance.

Preferably this would be layed down in a human-rights based piece of legislation, but there are opportunities for this in upcoming legal instruments as well, like the European legislation on AI. The Commission published their proposal the 21nd of April 2021 and included a very limited ban on real time biometric identification systems in publicly accessible spaces for law enforcement purposes.[44] By including this ban the European Commission shows she acknowledges the far-reaching infringements biometric surveillance in oublicly accessible spaces is making into our fundamental rights, and the risks it brings along for our free societies. However, by the way it is formulated at the moment it will not solve this: The ban is too narrow, the exceptions are too broad and there is too much unclarity that leaves room for misuse.[45]

44 Cf. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence.

45 Cf. Houwing, Lotte: Europees AI wetsvoorstel laat zien waarom wij vechten voor een verbod. In: Bits of Freedom of April 22, 2021, https://www.bitsoffreedom.nl/2021/04/22/europese-ai-wetgeving-laat-zien-waarom-wij-vechten-voor-een-verbod/ (May 11, 2021); Reclaim Your Face: European Commission's proposal for new AI Regulation shows exactly why we are fighting to ban BMS. In: Reclaim Your Face of April 21, 2021, https://reclaimyourface.eu/european-commission-proposal-new-ai-regulation-fighting-ban-biometric-mass-surveillance/ (May 11, 2021).

We don't need to regulate biometric surveillance technologies, we need to ban them. That's not just my position, but the position of many surveillance experts and (digital) human rights activists in civil society. Together with several digital rights organisations throughout Europe we gathered forces in the Reclaim Your Face campaign to make this ban a reality. We have launched a European Citizens' Initiative to call the European Commision to seize the chance it has to set a global example in upcoming AI legislation to protect our fundamental rights and public spaces against the harm that biometric mass surveilance can do. We need one million signatures of EU-citizens within a year, so we urge all of you to #ReclaimYourFace with us. Go check it out, and sign, at https://www.reclaimyourface.eu

This Citizens' Initiative is just one form of struggle against one form of algorithms limiting our freedoms. But there are many more and there is much more to be done. If you are now asking yourself the question: What else can I do (in the meantime)? Remember the title of this book. Here is some inspiration:

- Here you can find the ultimate stalker tool project we did with the public livestreams and Amazon's Rekognition: h*ttps://www.bitsoffreedom.nl/2019/12/12/amazons-rekognition-shows-its-true-colors/*
- Students from the Digital Society School developed a prototype mouthmask on which you can print an AI generated face, to trigger misidentification by facial recognition technology that is trained to recognize masked up faces: *http://projecthiveminds.com/ph/letsfaceit.php*
- They also made this analogue webcam filter that is 3p printable and provides you with privacy during your videocalls without letting your personal space be analyzed by algorithms: *http://projecthiveminds.com/ph/filteredreality.php*
- You can make your own LED throwies that stick to surveillance technology in public spaces to make them more visible and inform people about their presence. Here is a guide on how to make them: *https://www.instructables.com/LED-Throwies/*
- Several designers made fashion that protects you against surveillance. Some examples: *https://www.newyorker.com/magazine/2020/03/16/dressing-for-the-surveillance-age | https://www.theguardian.com/world/2019/aug/13/the-fashion-line-designed-to-trick-surveillance-cameras | https://mashable.com/article/anti-surveillance-masks/?-europe=true | https://yr.media/tech/guide-to-anti-surveillance-fashion/*

In this piece I elaborated on the risks and problems of biometric surveillance technologies. I also wrote about our European Citizens' Initiative as one way to address this. As shown by the examples there are much more strateies of disobedience possible. I hope this will inspire others to keep on fighting against algorithms where they are limiting our freedoms and imagination.

Literature

Benjamin, Ruha: Assessing risk, automating racism. In: Science (2019) vol. 366 issue 6464, S. 421–422.

Buolamwini, Joy: 2018, http://gendershades.org/

Chowdhury, A: Unmasking Facial Recognition. an exploration of the racial bias implications of facial recognition surveillance in the United Kingdom. In: Webrootsdemocracy.org 2020.

Doringer, Bogomir: When you feel pain, keep on dancing. In: TQW of 24 June 2020, https://tqw.at/when-you-feel-pain-keep-on-dancing-doringer/

European Digital Rights: IBM's facial recognition: the solution cannot be left to companies. In: https://www.edri.org of July 17, 2020, https://edri.org/our-work/ibm-facial-recognition-solution-cannot-be-left-to-companies/

Galic, Maša: Surveillance, privacy and public space in the Stratumseind Living Lab: the smart city debate, beyond data. In: Ars Aequi 2019, July/August.

Galič, Maša; Schuilenburg, Marc: Reclaiming the Smart City: Toward a New Right to the City. In: Juan Carlos Augusto, Handbook of Smart Cities 2020.

Gallagher, Ryan; Jona, Ludovica: We tested Europe's new lie detector for travelers and immediately triggered a false positive. In: The Intercept of July 26, 2019, https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/

Garvie, Clare; Bedoya, Alvaro/Frankie, Jonathan: The Perpetual Line-Up: Unregulated police facerecognition in America. Georgetown Law Center on Privacy and Technology October 18, 2016, https://www.perpetuallineup.org/

Gellman, Barton; Adler-Bell, Sam: The Disparate Impact of Surveillance. In The Century Foundation of December 21, 2017, https://tcf.org/content/report/disparate-impact-surveillance/?agreed=1

Harwell, Drew; Dou, Eva: Huawei tested AI software that could recognize Uighur minorities and alert police, report says. In: The Washington Post of December 8, 2020, https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/

Henly, Jon; Booth, Robert: Welfare surveillance system violate human rights, Dutch court rules. In: The Guardian of February 5, 2020, https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules

Hill, Kashmir: The secretive company that might end privacy as we know it. In: The New York Times of January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Hollister, Sean: Google contractors reportedly targeted homeless people for Pixel 4 recognition. In: The Verge of October 2, 2019, https://www.theverge.com/2019/10/2/20896181/google-contractor-reportedly-targeted-homeless-people-for-pixel-4-facial-recognition

Hooyman, Paula: Amazons Rekognition shows its true colors. In: Bits of Freedom of December 12, 2019, https://www.bitsoffreedom.nl/2019/12/12/amazons-rekognition-shows-its-true-colors/

Houwing, Lotte: Experimentele Manipulatie: Burger steeds vaker onwetend proefdier. In: Bits of Freedom of 5 June 2019, https://www.bitsoffreedom.nl/2019/06/05/experimentele-manipulatie-burger-steeds-vaker-onwetend-proefdier/

Houwing, Lotte: Europees AI wetsvoorstel laat zien waarom wij vechten voor een verbod. In: Bits of Freedom of April 22, 2021. https://www.bitsoffreedom.nl/2021/04/22/europese-ai-wetgeving-laat-zien-waarom-wij-vechten-voor-een-verbod/

Houwing, Lotte: FaceApp: Van kijken naar bekeken worden. In: Bits of Freedom of July 19, 2019, https://www.bitsoffreedom.nl/2019/07/19/faceapp-van-kijken-naar-bekeken-worden/

Houwing, Lotte: Stop the Creep of Biometric Surveillance Technology. In: European Data Protection Law Review (2020), nr. 2, S. 174.

Houwing, Lotte: We need to be bolder. In: Bits of Freedom of 30 January 2020, https://www.bitsoffreedom.nl/2020/01/30/we-need-to-be-bolder/

Kari, Paul: Amazon to ban police use of facial recognition software for a year. In: The Guardian of June 11, 2020, https://www.theguardian.com/technology/2020/jun/10/amazon-rekognition-software-police-black-lives-matter

Krishna, Arvind: A letter from our CEO. In IBM.org: 2019, https://www.ibm.org/responsibility/2019/letter

Lefebvre, Henri: Writings on cities. Cambridge 1996.

Lyon, David: Surveillance Power and Everyday Life. In: Oxford Handbook of Information and Communication Technologies, (2007).

Morozov, Evgeny: To save everything, click Here. New York 2013.

Mozur, Paul: In Hong Kong protests, faces become weapons. In: The New York Times of Juli 26, 2019, https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html

Ng, Alfred: Your face mask selfies could be training the next facial recognition tool. In: Cnet of May 19, 2020, https://www.cnet.com/news/your-face-mask-selfies-could-be-training-the-next-facial-recognition-tool/

Rasch, Miriam: Ethiek in tijden van dataïsme. Amsterdam 2020.

Reason TV: Hong Kong protestors combat the surveillance state. In: Youtube of October 4, 2019, https://www.youtube.com/watch?v=VXog6t4kNyc

Reclaim Your Face: European Commission's proposal for new AI Regulation shows exactly why we are fighting to ban BMS. In: Reclaim Your Face of April 21, 2021, https://reclaimyourface.eu/european-commission-proposal-new-ai-regulation-fighting-ban-biometric-mass-surveillance/

Schwartz, Oscar: Don't look now, why you should be worried about machines reading your emotions. In: The Guardian of March 6, 2019, https://www.theguardian.com/technology/2019/mar/06/facial-recognition-software-emotional-science

Tsvetkov, Egor: Your Face is Big Data. In: Cargo Collective, https://cargocollective.com/egortsvetkov/Your-Face-Is-Big-Data

Willsher, Kim: Story of Cities #12: Hausmann rips up Paris—and divides France to this day. In: The Guardian vom March 31, 2016, https://www.theguardian.com/cities/2016/mar/31/story-cities-12-paris-baron-haussmann-france-urban-planner-napoleon

de Zwart, Hans: 'Geen gezicht'—De Big Brother Awards speech van Hans de Zwart. In: Bits of Freedom of November 15, 2016, https://www.bitsoffreedom.nl/2016/11/15/geen-gezicht-de-big-brother-awards-speech-van-hans-de-zwart/