Stop the Creep of Biometric Surveillance Technology

*Lotte Houwing**

Facial recognition is a hot topic. The technology can be used in a lot of different ways, some more controversial than others. There's one use case that is particularly worrisome, namely the deployment of face surveillance in public spaces. Since there are other technologies that can be used in the same way, our concerns regard all types of biometric surveillance technology in the public space.

There are several reasons why the use of these technologies is so alarming.

First, there are two distinct ways in which it leaves no room 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. In addition to the impossibility to opt-out from public space, it is impossible to opt-out from your face, and difficult to prevent your face from being surveilled once the technology has been deployed on the streets. The extremely personal characteristics of your face cannot be changed or left at home in a drawer. In several countries, it is even forbidden by law to cover your face when in public space. On top of that, it is fairly easy to gather face information covertly and distantly. This allows others to identify and follow people through public space without their knowledge.

Second, although the intended purpose of the deployment might be targeted, the real-world effects of face surveillance in public space are in any case untargeted. For instance, in order to prevent all people on a particular watchlist from entering a specific place, you need to scan and analyse every person and compare them to your list. Also, thanks to insights into existing facial recognition law enforcement databases, we've seen that there's a tendency to collect as many faces as possible. A study from 2016 shows that half of all United States adults are already included in one,[1] and in the Netherlands the criminal database includes 1.4 million people,[2] which translates to 1 in every 12 citizens.

DOI: 10.21552/edpl/2020/2/5

* Lotte Houwing, researcher and policy advisor at the Dutch digital rights NGO Bits of Freedom, where she focuses on state surveillance. She graduated with distinction from the research master 'Functionality of the Law' at the University of Groningen. For correspondence: <lotte@bitsoffreedom.nl>.

1 Sam Levin, 'Half of US adults are recorded in police facial recognition databases, study says' *The Guardian* (18 October 2016) <https://www.theguardian.com/world/2016/oct/18/police-facial-recognition-database-surveillance-profiling> accessed 4 June 2020.

2 'RTL Nieuws - 19:30 uur' *RTL Nieuws* (24 January 2020) see the 12:37min mark <https://www.rtlnieuws.nl/video/uitzendingen/video/4997786/rtl-nieuws-1930-uur> accessed 4 June 2020 (in Dutch).

Third, facial recognition surveillance is discriminatory by design. A lot of attention has been given to the fact that the technology has an accuracy problem. It is less accurate when pointed at women, transgender and non-binary people and people of colour, meaning these people have a higher risk of being misidentified. It is unclear if this problem can be solved. Although it is completely legitimate to be concerned about the harms of this technology burdening some more than others – and hardly ever are the 'some' the people designing, engineering and signing off on the deployment of the technology – we should not forget that as long as technology that is built to identify, profile and analyse people in order to treat them differently, is deployed by people within societies that suffer from systemic inequality, the technology will most likely reinforce and exacerbate those inequalities.

Finally, with the introduction of certain technologies in society, the underlying assumptions of these technologies are brought along, shaping the way we look at the world. The word 'biometrics' means turning biological characteristics to metrics. However, in translating our faces into more easily computable data, people are reduced to walking barcodes.

Some technologies, like emotion detection technology, take it a step further, 'identifying' emotions or personality traits based on facial movements or dimensions. When 'objective' value or meaning is attached to these characteristics, we start to tread the waters of a discredited pseudo-science rightfully left behind: physiognomy. The idea is that it is possible to extract information about a person's character from the biological characteristics of their face.

Any of these concerns on their own, should be argument enough for why we should severely limit the use of facial recognition. Taken together, we believe they convincingly lay out why the costs of deploying biometric surveillance technology in the public space are too high, and adding this technology to states' surveillance capacity would constitute too big an infringement on our liberties,

So how do we properly address the dangers posed? In the discussions surrounding face surveillance, there are a few options most prevalent: a moratorium, new regulation and a ban. Although all present valid arguments, we'd like to briefly discuss the potential shortcomings of each.

Brought back to its core, the purpose of a moratorium is to postpone the deployment of face surveillance technology until the most pressing concerns are mitigated. The first of those concerns is that of inaccuracy and bias. Our worries as regards to arguing for a moratorium on the basis of this concern, is that the technological deficiencies might be solvable over time, at least to an extent that brings the percentage of false positive and negatives within the realms of what our political leaders deem acceptable. More importantly, however, is that we might just be looking at a technology that becomes more dangerous, the better it works. Not when it's giving you access to your phone, but definitely when applied as a mass surveillance tool.

Another aspect that calls for a moratorium often focused on is the demand for a regulatory framework. This might imply to some that current legislation is ambiguous about the acceptability of face surveillance. We need to be very clear that assessing face surveillance in public space in the 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, the required mass-scale processing of biometric data seems to be at odds.

Finally, we're concerned that for the duration of the moratorium, we will see the technology become normalized. We will see industry deploy its lobbyists. We will see the companies at the forefront of product development, search for and find product-market-fit. We will see civil society again and again mobilise citizens until those citizens become fatigued and weary, and disbelieving that their voice makes a difference. In other words: time might prove a threat to our ability to clearly and adequately assess this technology.

A concern we have about calling for new regulation addressing biometric surveillance in the public space, is that we will not be able to contain the use. The call for regulation is a call for a limited legal basis for the deployment of this extremely invasive technology. History has taught us never to underestimate a good 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. We have seen this before with other surveillance measures being introduced. Restricting 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, show that even non-violent citizen interests groups are classified as 'extremist' or 'terrorist' when more powers to surveil these groups are desired.[3] 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.[4] Why would facial recognition databases be exempt from this data hunger?

We have seen several cities in the United States ban the use of facial recognition. This might offer a lot of added value in terms of protection in the United States. When we look at the European context we find a more extensive legal framework that serves the goal of protecting our privacy. Biometric surveillance in the public space, in our view, is clearly incompatible with the principles laid down in the European data protection framework, since it inherently requires mass-scale processing of biometric data. This type of data is extremely sensitive and due diligence requires limiting the processing of this data as much as possible.

3 eg Vikram Dodd and Jamie Grierson, 'Non-violent groups on UK counter-terror list threaten legal action' *The Guardian* (22 January 2020) <https://www.theguardian.com/environment/2020/jan/22/minister-denies-government-considers-extinction-rebellion-extremist> accessed 4 June 2020.

4 eg SyRI in the Netherlands: 'Profiling and SyRI' (The Public Interest Litigation Project, 11 December 2015) <https://pilpnjcm.nl/en/dossiers/profiling-and-syri/> accessed 4 June 2020.

It would be preferable to address the problem of biometric surveillance technologies in the public space with strong enforcement of existing regulation over the creation of a new legal instrument that bans it. The reason for this is that it shows and strengthens the potential this framework has in terms of protecting our rights and freedoms, providing us with a strong and extensive framework in the long run. Unfortunately, a few factors complicate this.

The Law Enforcement Directive additionally sets the high demand of strict necessity, suitable safeguards should be in place and the processing must be permitted by European Union or Member State law.[5] It is questionable whether it is possible to formulate a legal basis that meets these requirements while allowing for the mass-scale processing of biometric data inherent to these surveillance technologies. However, the protection of our fundamental rights and freedoms does not benefit from the possible disagreement or a long trial-and-error process.

Another problem is that these legal frameworks in themselves offer just theoretical protection. The actual protection they have to offer is as strong as their enforcement mechanisms. It is exactly these mechanisms that might be the weakest link in the chain.

As we see the deployment of facial recognition in public space in several Member States, it might be needed that authorities provide some extra clarity and invigorate the existing framework with an explicit ban on biometric surveillance technologies in public space. 44 digital rights organisations, including Bits of Freedom, called for a ban on biometric mass surveillance.[6]

The one thing we know for sure, is that to protect our free societies and our fundamental rights and freedoms, we cannot let biometric surveillance technology sneak up on us.

Corona-update: As we see more often, crises offer momentum for the introduction of infringing surveillance measures. In several states digital and biometric immunity passports are mentioned as part of the strategies of societies to exit their lockdowns and open up their economies. We should be very aware of the inherent risks this technological solutions bring along. Digital and biometric immunity passports not only put the integrity of our bodily and health data at stake, but also pose a great risk to equality by introducing so-called immunoprivilege.[7] Creating a stratified society where access to spaces and services can be distributed along the lines of the possibility to prove immunity, exacerbating existing structural inequaliaties.

---

5 Law Enforcement Directive 2016/680, art 10.

6 European Digital Rights (EDRi), 'Ban biometric mass surveillance!' (Position paper, 13 May 2020) <https://edri.org/blog-ban-biometric-mass-surveillance/> accessed 9 June 2020.

7 Kathryn Olivarius, 'The Dangerous History of Immunoprivilege' *The New York Times* (Opinion, 12 April 2020) <https://www.nytimes.com/2020/04/12/opinion/coronavirus-immunity-passports.html#click=https://t.co/QcXDROj5IL> accessed 9 June 2020.