CHAPTER 2

To be a face in the crowd

Surveillance, facial recognition, and a right to obscurity

SHAWN KAPLAN
DEPARTMENT OF PHILOSOPHY, ADELPHI UNIVERSITY, USA

ABSTRACT
This chapter examines how facial recognition technology reshapes the philosophical debate over the ethics of video surveillance. When video surveillance is augmented with facial recognition, the data collected is no longer anonymous, and the data can be aggregated to produce detailed psychological profiles. I argue that – as this non-anonymous data of people's mundane activities is collected – unjust risks of harm are imposed upon individuals. In addition, this technology can be used to catalogue all who publicly participate in political, religious, and socially stigmatised activities, and I argue that this would undermine central interests of liberal democracies. I examine the degree to which the interests of individuals and the societal interests of liberal democracies to maintain people's obscurity while in public coincide with privacy interests, as popularly understood, and conclude that there is a practical need to articulate a novel right to obscurity to protect the interests of liberal democratic societies.

KEYWORDS: surveillance, facial recognition, privacy, right to obscurity in public, anonymity

Kaplan, S. (2023). To be a face in the crowd: Surveillance, facial recognition, and a right to obscurity. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillance* (pp. 45–66). Nordicom, University of Gothenburg.
https://doi.org/10.48335/9789188855732-2

Introduction

The proliferation of video surveillance cameras is astounding. It was approximated that there would be over 1 billion surveillance cameras globally by 2022, with China accounting for over half and the US for 85 million (Lin & Purnell, 2019). Though many have voiced privacy concerns over ubiquitous video surveillance, opinion has been divided in the philosophical literature as to whether this practice violates a right to privacy. The reasons for the philosophical debate range from fundamental disagreements about the existence of a distinct right to privacy (Thomson, 1975), to more specific concerns about whether a right to privacy can be properly extended to what people do in public (Nissenbaum, 1998; Ryberg, 2007), or whether discreet video surveillance ever wrongs individuals who are unaware of being observed (Alfino et al., 2003), or whether the mining of personal information wrongs anyone if the information is not misused (Alfino et al., 2003; Ryberg, 2007). In this chapter, I explore how the emergence of highly effective facial recognition technology reshapes the debate over video surveillance.[1]

We are on the cusp of a radically altered surveillance landscape, as facial recognition programs are used to augment, for example, our extensive video surveillance infrastructure, body cameras worn by police, and video cameras deployed on drones. Until recently, real-time video surveillance required a human monitor to assess security risks. Quite often, however, video surveillance data has been used *post-factum* to investigate criminal cases or to redesign security procedures.

Two fundamental things change when video surveillance is augmented with facial recognition: 1) the data collected is no longer anonymous but is linked to specific individuals, and 2) the data can be powerfully aggregated to produce detailed profiles of individuals. In the first instance, as opposed to obtaining data via CCTV regarding crowd numbers, facial recognition surveillance (FRS) can catalogue every person who participates in public protests, political rallies, religious observances, or any socially stigmatised activity. These individuals will no longer be nameless faces in the crowd but will be clearly identified, and their participation will become part of their digital record. In the second instance, using our publicly observable movements, behaviours, preferences, and associations, FRS data can be aggregated and analysed to produce immensely detailed profiles that will disclose much of our intimate details –including psychological propensities. Though profiling is not novel to FRS, I argue that the breadth and depth of this form of surveillance profiling is novel in the degree of the harms it threatens to cause.

Both troubling practices are ongoing in China. In Chongqing, a program connects "the security cameras that already scan roads, shopping malls and transport hubs with private cameras on compounds and buildings, and integrate them into one nationwide surveillance and data-sharing platform" (Denyer, 2018: para. 6). By augmenting this integrated system of video sur-

veillance with facial recognition, Chinese authorities hope to track the movements, beliefs, and associations of their citizens to generate aggregate profiles. The larger ambition of the Chinese government is to combine this surveillance data with criminal, credit, and medical records, as well as online activity, to derive a "social credit" score by which each citizen's "trustworthiness" will be ranked (Botsman, 2017; Denyer, 2018). It is also suspected that FRS was used to track and arrest dozens of dissidents, petitioners, and journalists prior to the 2016 G-20 summit meeting in Hangzhou (Denyer, 2018).

Police in London, South Wales, Detroit, and Orlando have been testing FRS (Burgess, 2018; Harmon, 2019; Kaste, 2018), and it has been credited for over 300 arrests in Dubai over one year (Al Shouk, 2019). In addition, a leading manufacturer of police body cameras has added facial recognition capabilities to their products (Harwell, 2018). While assurances are given in the US that this surveillance technology would only be used to locate wanted criminals or missing persons, few jurisdictions have laws limiting the usage of FRS. In contrast, the EU has attempted to regulate FRS through the GDPR (European Parliament, 2016) and the recently proposed guidelines for harmonising rules on artificial intelligence (European Commission, 2021). Regardless, law enforcement in both Sweden and Finland have been judged to use facial recognition tools that fail to protect individuals' data (Skelton, 2021; Yle News, 2021), and a Swedish school district was fined for using FRS to track student attendance (Swedish Data Protection Agency, 2019). In addition, EU regulations have been interpreted to allow a Danish football team to use FRS to identify low-level offenders entering their stadium (Overgaard, 2019) and for Swedish stores to track shoppers' movements (Roos & Källström, 2020).

Considering the ability to use FRS to generate detailed profiles of individuals and to catalogue every individual participating in protests, political rallies, religious observances, or any socially stigmatised activity, Jake Laperruque (2017) has advocated for legal restrictions on facial recognition technology to protect our "right to obscurity" – that is, to remain a nameless face in the crowd. Insofar as the aim is to obscure individuals' identities when engaged in mundane, religious, and political activities *while in public*, a right to obscurity might appear entirely distinct from a right to privacy, which is conventionally assumed to restrict access to our non-public activities and intimate information. Whether the concerns raised by these two uses of FRS amount to a violation of a right to privacy, or a violation of a right to obscurity, or fails to amount to a rights violation at all, depends both upon what values or interests are threatened by FRS and which theory of privacy one accepts.

In the next section, I detail the values and interests threatened by the widespread use of FRS. My initial task is to distinguish how obscurity, as a public mode of anonymity, is distinguished from privacy. My analysis shows that widespread FRS will eliminate our obscurity while in public and that this

institutional practice will unjustly impose risks of harm upon both individual members of the public and society. I consider potential justifying purposes of FRS and show that the associated risks imposed upon individuals and society are either unnecessary or disproportionate to the proposed benefits unless FRS is effectively regulated to protect our anonymity while in public.

In the third section, I consider whether the interests under threat from widespread FRS are best conceived of as privacy interests or whether the value of preserving our obscurity in public is best articulated as being distinct from privacy. Answering this question does not alter the normative arguments from the second section, nor does it call into question the regulatory policies proposed there. I propose that the question has pragmatic political significance for how we can most effectively advocate for policies and laws that will protect those interests and values under threat by FRS. Answering this question is, however, complicated by the lack of anything in the literature approaching a consensus for how to understand privacy. Considering the conceptual disarray surrounding privacy, I identify when the interests under threat by FRS coincide with plausible conceptions of privacy, and I assess whether the controversies surrounding those conceptions of privacy prove problematic when advocating for FRS regulation. I argue that the interests under threat from amassing detailed, aggregate profiles of individuals coincide with some conventional theories of privacy. In contrast, I show that the interests in need of protection when considering the use of FRS to catalogue participants in protests, political rallies, religious observances, or any socially stigmatised activity fall beyond the typical domain of privacy protections. I conclude that this discontinuity indicates a practical need to articulate a novel right to obscurity, as opposed to further broadening our conception of privacy.

Anonymity and obscurity in public

In this section, I provide an account of anonymity as obscurity in public and the general value it may offer. I then use this account to describe the way FRS eliminates our obscurity in public and the potential harms this poses to both individuals and to liberal democracies more generally.

The general value of obscurity in public

If anonymity is lost when FRS is broadly deployed, the question remains what exactly this loss amounts to. What is anonymity and what inherent or instrumental value does it hold? To be an anonymous face in the crowd is to enjoy broad obscurity regarding one's identity. Obscurity in public is a mode of anonymity wherein publicly observable information about each person (e.g., location and behaviour) is dissociated from their identity.

The inability to link some information to an individual identity is what

differentiates anonymity from privacy. According to Julie Ponesse (2014), our personal information may become part of the public sphere and no longer be private but, insofar as the identifying markers have been sufficiently removed from that information, it can be dissociated from our identity, preserving anonymity. To illustrate, consider a traveller who tells everyone he encounters abroad that he is John Smith from England. Given the commonality of the name, it is only an opaque identifier and is readily dissociated from any identity; he still enjoys significant anonymity. His name and nationality are known to those to whom he revealed them, but all other aspects of his identity remain anonymous because, for this specific population, his other personal information remains dissociated. In a mirror image, the traveller who reveals her personal views and reasons for traveling to a stranger remains anonymous to the stranger insofar as her name and other identifying information remains dissociated.

The individual who is perceived by others as a mere face in the crowd enjoys broad anonymity because nearly all their identifying information remains dissociated and, thus, concealed from others. Is there something inherently valuable about this anonymity or obscurity while in public? To anonymously glide through a crowd can be a liberating experience, especially when compared to moving through a closed community where everyone knows who you are and takes note of your activities. Though such anonymity can be recognised as valuable, it may not be a universal good, as prolonged periods of anonymous obscurity might lead to a sense of alienation. The positive value of anonymity in this context is instrumental insofar as it removes inhibitions that can diminish an individual's autonomy. The absence of obscurity in public can create psychological pressure to conform to social expectations. However, we have no reasonable expectation that others who know us will not observe our public activities. Thus, nobody can claim a right to be an anonymous face in the crowd at any time they crave such obscurity. If a right to obscurity exists, it would be a conditional right.

The value of obscurity in public vis-à-vis facial recognition surveillance

Using this analysis of anonymity, we can quickly recognise how FRS would eliminate much of the anonymity people currently enjoy while in public. All FRS data is associated with an individual's identity, and an FRS network makes countless observations of individuals' movements, modes of transport, social contacts, purchases, attitudes, tastes, and behavioural idiosyncrasies. Much of the content of these individual data points will be ethically innocuous, but they will *not* be anonymous. However, the ease in which this non-anonymous raw data can be aggregated and analysed makes individuals vulnerable to significant harms.

This concern conforms to a focus upon the "inferential fertility" of information (Manson et al., 2007), as opposed to the ethical relevance of the informational content. Adam Henschke (2017) has made an extended argument for why we must take due care with how seemingly innocuous personal information is collected, analysed, shared, and used. He describes that, as this seemingly innocuous personal information is aggregated and integrated, a virtual identity is created, and this is ethically significant insofar as a virtual identity shapes how institutions and other persons interpret that individual or group. Of course, our virtual identities are already being constructed, without the use of FRS, based upon our purchasing records and online activities. Our virtual identities are commodified and sold, typically to those interested in marketing products or finding an audience susceptible to a political message or misinformation. FRS data would be a powerful source for constructing virtual identities by compiling our movements, behaviours, interests, social contacts and associations, demonstrated beliefs, psychological propensities, as well as political and religious activities. The creation of such detailed profiles makes people vulnerable to a range of possible harms. Following Robert Goodin (1985), Henschke interprets vulnerability as being under a threat of some harm and asserts that, if we make others vulnerable to us, we have a special duty to protect them from these potential harms. According to Henschke (2017: 223), we have a special duty to take due care with the personal information gained via surveillance technologies and that due care requires that "surveillance technologies with a potential to construct Virtual Identities ought to be designed and used in such a way as to minimise the probability and magnitude of information harms".

I agree that, when our actions or policies make others vulnerable to harms, we have a special duty to minimise the probability and magnitude of those harms. However, this seems to be a moral concern secondary to the question of whether we have wronged individuals by imposing an unjust risk of harm upon them in the first place. (Risk of harm is here understood as the product of the probability of a harm and the magnitude of that harm.) To show how FRS imposes an unjust risk of harm, I describe the harms this form of surveillance makes us vulnerable to, and then I show these risks of harm to be unjustly imposed. To do so, I must show that one of the following three necessary conditions for justified risk imposition is not satisfied: 1) the action or policy creating a risk of harm must serve some justifying purpose; 2) the imposed risk of harm must also be *necessary* for accomplishing that purpose (i.e., if there is a way to attain the same justifying purpose without imposing, or imposing a lesser, risk of harm, then the risk is unnecessary and unjust); and 3) the imposed risk of harm must be proportionate to the benefit of the justifying purpose.

Much of the vulnerability for the subjects of FRS results from its ability to create nuanced and detailed psychological profiles of individuals. Some

might contend that the creation of such detailed and *intimate* psychological profiles would directly harm individuals. To technologically pry into people's heads by aggregating and analysing their publicly displayed behaviour might easily feel like a violation of their privacy. In the next section, I return to this concern when considering popular conceptions of privacy and how they relate to FRS. For the present, I focus upon how the collection of this surveillance data makes people vulnerable to two types of harms and whether these risk impositions are just or unjust.

First, people become vulnerable to the harm of psychological manipulation as a result of these detailed psychological profiles. Similar concerns have been raised by the way that social media data is analysed to target specific psychologically susceptible individuals with false information (Rosenberg et al., 2018; Vélez, 2021). A significant distinction between the cases is that people have a choice to opt in or out of social media use. The practical ability of individuals to effectively mask their identity while in public every day is minimal. A second significant difference is the diversity of surveillance data available from FRS, where facial and bodily expressions provide a broader range of personal responses (e.g., anxiety, calmness, attraction, repulsion, pleasure, pain, interest, disinterest, depression, happiness, etc.) than online activity (e.g., search and click history, social media posts and reactions, and time spent hovering over online images, etc.). The vulnerability to psychological manipulation from FRS is not different in kind from what we already face, but it is different in degree. Online activity can reveal one's psychological propensities and inclinations but pales in regard to detail when compared to what would amount to countless hours of surveillance data from tracking our everyday activities while in public.[2] It is reasonable to suppose that, as the dataset grows and the tools of analysis become more nuanced, the resulting psychological profiles will allow for much more diverse, powerful, and coercive forms of psychological manipulation. Psychological manipulation which coercively triggers the target to adopt beliefs and actions is a violation of individual autonomy and a clear harm.

Second, detailed psychological profiles make individuals vulnerable to opportunity losses. Potential employers would no doubt pay handsomely to know the psychological propensities of job candidates, including their ability to focus or stay calm under pressure, their sociability, their lifestyle choices (e.g., substance use and abuse), their propensities for depression, anger, and violence, or their fit with management's religious and political views. If individuals' profiles indicate them to be statistically "riskier" hires, they could find many employment opportunities closed off. Parallel limits could be found when applying to schools and universities, or when seeking housing, insurance, and public assistance. Limiting a person's reasonable range of opportunities based upon what is publicly observable about them would stand as a harm insofar as a reasonable range of opportunities is required

for living any conception of a good life. Even if opportunity loss does not rise to the level of denying individuals a reasonable range of opportunities, we can still acknowledge that the accumulation of micro-scaled opportunity losses can pose a morally serious harm.

It might be objected that, while the creation of detailed psychological profiles makes individuals vulnerable to harms from psychological manipulation and opportunity loss, that does not indicate an ethical problem with FRS but rather a concern about the misuse of the FRS data. Similar claims have been made regarding other surveillance and data-gathering technologies (Alfino & Mayes, 2003; Marmor, 2015). Ryberg (2007) argued that collecting data from non-augmented CCTV surveillance fails to wrong individuals if it is used for crime prevention. If the data were used differently, then we might very well have a reasonable moral complaint: "If CCTV administrators start working as some sort of private investigation company passing on or selling information to employers or other parties, then surely they are engaging in activities that go far beyond mere crime prevention" (Ryberg, 2007: 141). Nissenbaum (1998) describes this specific sort of misuse of data as a failure to respect the "contextual integrity" of the information by shifting it from a legitimate context (e.g., crime prevention) to another context without the subject's consent or providing justification.

No doubt, individuals can be harmed and wronged by such misuse of personal information gained by various forms of surveillance. However, this ignores the inferential fertility of the data being collected from FRS and how easily this data can be aggregated and analysed into profiles that put individuals at risk of serious harms. The mere collection of this non-anonymous data puts people at risk of psychological manipulation and opportunity loss. To echo Henschke (2017: 260), the degree of ease by which data can be aggregated into a virtual identity "tells us how far off it is from simple data". The collection of "simple data" might be morally neutral but, as data is more easily aggregated into a profile or virtual identity, this correlates with the growth of people's increased vulnerability to harms.

The objector might respond that we ought to simply respect the contextual integrity of the FRS data and not shift this data into the context of forming profiles or virtual identities. This response presupposes that there are justifying purposes for collecting FRS data. Perhaps it would be legitimate to use this technology to seek missing persons, track suspected criminals, or create profiles of suspected terrorists? Like other forms of targeted surveillance, FRS ought to require a court warrant and, if the courts are sufficiently rigorous, people will be less vulnerable. However, for facial recognition technology to effectively locate missing persons or carry out surveillance against suspected criminals, authorities cannot simply enter the face of the one person of interest. The accuracy of facial recognition machine learning is relative to the number and diversity of faces in the database. Even if FRS required

a warrant to target specific individuals, it would only be reliably accurate if the majority of citizens had their facial biometrics entered into the database.

Furthermore, if this system of surveillance is meant to locate and track targeted individuals efficiently, then not only will our video surveillance infrastructure need to be universally augmented with facial recognition, but everyone would need to be tracked constantly. To hope that one person can be identified within tens of millions of video feeds (or more) would be like seeking a needle in a haystack. While super-computers can help speed the process of sorting through massive amounts of data to find a person of interest, it would be far more efficient to constantly keep track of everyone's movements. This is only to suggest that there would be pressure from the standpoint of efficiency to engage in non-targeted FRS and to access this data only in a targeted fashion after receiving a warrant. If this were to become standard practice, people would have unnecessary risks of harm imposed upon them, unless the data from this surveillance were anonymised in two important ways.

One significant protection would be to anonymise people's whereabouts by dissociating this data from their identity (i.e., dissociating location data from their names and identification numbers) until a warrant is granted. A further stage of anonymisation could be attained by banning any additional analysis of FRS data beyond location. This means blocking any analysis of observed behaviour and social connections. If location data were anonymised and dissociated from other personal information – like psychological propensities and social connections – then having the capacity to target individuals with FRS when ordered by a court would make people less vulnerable to serious harms from psychological manipulation or opportunity loss. Given the potential ability to subvert these anonymity protections, vulnerability would not be eliminated. The remaining risk imposed would still need to be proportionate to the likely benefits. Interestingly, these two protections would largely preserve individuals' anonymity in public, allowing them to remain mere faces in the crowd. Put differently, if we only find FRS permissible when anonymity is preserved in the two ways described, we have arrived at a conclusion that there are no *general* contexts in which non-anonymous data can be legitimately gathered via FRS.

It might be objected that building such anonymity protections within FRS systems might limit the potential to prevent predictable violence and criminal activity. For example, if the behavioural patterns preceding suicide attempts or terrorist attacks can be recognised via machine learning and effectively used to analyse real-time surveillance data, then banning the analysis of surveillance data beyond location would appear to significantly limit our capacity to prevent such violence. This, however, is only an apparent drawback. If our machine learning systems could predict likely violent or criminal activity by using surveillance data, it could do this both by learning from anonymous

data and analysing anonymous real-time surveillance. If computers could analyse real-time surveillance better than human monitors for security risks, the resulting data could remain dissociated from any individual's identity. Once the automated system identifies a security risk, it could both alert a human monitor to look at the surveillance stream and have police dispatched to investigate. All of this could be done without linking observed behavioural patterns with individual identities. Thus, using such technology to help prevent violence and crimes does not mandate a loss of anonymity.

By dissociating location and behavioural data from specific identities, anonymity is preserved in a way that keeps personal information from being aggregated into psychological profiles. This, in turn, diminishes people's vulnerability to harms that FRS would otherwise create. Thus, real-time FRS which fails to serve these justifying purposes or imposes unnecessary risks of harm, by failing to anonymise the data and its analysis, would be an unjust imposition of risk. At the same time, if it is unlikely that governments will effectively protect people's anonymity by keeping the information gained from FRS dissociated from their identities, then it would be prudent from the standpoint of practical politics to ban states altogether from coupling video surveillance with facial recognition.

Thus far, I have considered the powerful capacity to form detailed profiles of individuals via FRS. I now focus on the second concern named at the start of this chapter: the ability to use FRS to catalogue individuals participating in protests, political rallies, religious observances, or any socially stigmatised activity. To join a large group to express dissent via protest or rally for common political cause, or to join in common religious belief and practices, obscures the participants' identities, as each appears as a mere face in the crowd. If participants fear repercussions as a result of being identified any time they engage in socially stigmatised activities or ones disapproved of by government authorities, then the increased negative social pressure will likely correspond to reduced individual autonomy.

This chilling effect of FRS is not equivalent to a *direct* violation of the rights to free expression, assemblage, or worship. Unlike cases where individual rights are directly violated (e.g., the mass arrest of protesters), cataloguing the identities of group members is an act of implicit intimidation where repercussions are made possible but are not explicitly threatened.[3] (However, if the same technology were used by the surveillance state to overtly intimidate its citizens, then this would easily rise to a violation of these civil rights.) This implicit intimidation undermines the *effective* ability of people to exercise their rights to free expression, assembly, and worship.

Given the vast power asymmetry between those carrying out surveillance and those who are the subject of this cataloguing, one could not easily blame the intimidated party for their psychological response. My point is not that this response is perfectly natural (though it may be). Instead, insofar as citi-

zens are vulnerable to the state's asymmetric power which could deny their rights or impose negative repercussion for exercising their rights, the state and its law enforcements agencies have a special obligation towards those citizens. Beyond the responsibility of the state and its law enforcement authorities to avoid directly violating citizens' rights to free speech, assemblage, and worship, the state has a special obligation to create institutional practices that reassure citizens that they are not vulnerable to negative repercussions when they exercise these rights. Unless this special obligation is met, citizens will have their effective ability to exercise their rights undercut.[4]

When the effective ability to engage in free speech, assembly, and worship is diminished by the implicit intimidation from FRS, we must consider whether this inflicts a broader societal harm. When individuals feel so intimidated that they are reticent to either express dissent in peaceful protests or to assemble with others who share common political or religious beliefs, then the ability of a liberal democratic society to function well is diminished. For example, when the free expression of political dissent in protests or of political convictions at rallies is diminished, citizens will not be able to effectively challenge the political views of their compatriots, and democratic institutions will not be able to optimally represent the people's will because it remains partially silent. Also, when individuals are reticent to make their religious affiliations public, society appears more homogenous and is less capable of approximating the liberal ideal of supporting diverse ideas of the good. Without citizens being able to exercise these rights in a more optimal manner, broad societal interests of liberal democracies are undermined in significant ways, thus harming society.

By undermining the ability of liberal democracies to function well, the practice of cataloguing political or religious participants via FRS would be unjust, unless this societal harm were necessary and proportionate for attaining some justifying purpose. Perhaps FRS is permissible for cataloguing participants in riots or in group demonstrations of hate or bigotry? Regarding public demonstrations of hate or bigotry, our answer will hinge upon whether hate speech is protected under the right to free speech. If free speech rights protect hate speech, then cataloguing hate speech participants via FRS would unjustifiably undermine people's effective ability to exercise their right to free speech. If hate speech is *not* protected as free speech, then we can consider it in conjunction with the case of cataloguing rioters. These cases would involve employing facial recognition to identify criminals, and this can only be done *after* the crime has been committed. Since the aim is not crime prevention but a criminal investigation, *real-time* FRS is unnecessary. Instead, a warrant could be required to identify individuals engaged in criminal activities post factum. Thus, there are no obvious contexts for legitimately using real-time facial recognition to catalogue participants in any group activity. In the absence of a context where real-time cataloguing serves a legitimate justifying

purpose, the harms imposed upon liberal democratic societies by such FRS would always be unjust.

In this section, I have developed an account of anonymity as obscurity in public and uncovered what is valuable about obscurity in public both for individuals and society. Though it may be liberating to be an anonymous face in the crowd, the incidental loss of one's obscurity in public does not constitute a significant harm. However, FRS would effectively eliminate all anonymity while in public. I have highlighted two worrisome contexts for the loss of one's obscurity while in public: the creation of detailed individual profiles based upon publicly observable behaviour and the cataloguing of individuals participating in protests, rallies, religious observances, or any socially stigmatised activity. I have argued that, in the first context, the mere collection of non-anonymous FRS data makes people vulnerable to harms due to the ease by which this data can be aggregated and analysed to create nuanced psychological profiles. By disclosing individuals' psychological propensities, they are made vulnerable to psychological manipulation and opportunity loss. Hence, anonymity as obscurity in public is linked to our individual interests in preserving our autonomy and maintaining a reasonable range of opportunities or, at minimum, avoiding regular micro-scaled losses of opportunities.

Though I acknowledged the ways FRS can positively serve societal interests in crime prevention and locating missing persons, I have argued that these apparently legitimate aims can be embraced while preserving much of our anonymity by setting the following limits: First, facial biometric data ought to be dissociated from individual identities until a court warrant is provided. Second, the gathering of this anonymous data ought to be limited to location. Any further behavioural analysis of FRS data ought to be banned unless that analysis is of anonymous data. Since the justifying purposes can be attained while imposing lesser risks of harm, I concluded that FRS, in the absence of the limits described, imposes unjust risks of harm.

In the second context, I have emphasised how preserving anonymity as obscurity in public serves the societal interest of liberal democracies to optimise citizen's free speech, free assembly, and free religious worship. While cataloguing participants in political or religious activities does not directly violate these rights, I have argued that the implicit intimidation of such surveillance tactics would undermine the effective ability of individuals to exercise their rights. Cataloguing individuals can only be justified for the sake of a legal or criminal investigation, and this does not require real-time FRS. Instead, a warrant could be required to identify criminal suspects post factum. Insofar as the real-time cataloguing of participants serves no legitimate purpose, this practice would impose unjust harms upon society.

I next consider whether these various interests fall under privacy interests or whether anonymity as obscurity in public is best kept distinct from

privacy. Privacy advocates have long drawn a connection between privacy and individual autonomy; however, privacy is not typically associated with maintaining a reasonable range of opportunity, nor with the societal interest in supporting the effective ability of individuals to freely express dissent, assemble, and engage in worship. Does this discontinuity with conventional conceptions of privacy indicate a need to broaden our concept of privacy, or does it indicate that anonymity as obscurity in public is best kept distinct from privacy?

Obscurity, privacy, and rights

Judith Jarvis Thomson (1975: 295) famously stated, "Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is". She argued that the cluster of rights that we associate with privacy can be reduced to other rights clusters, like property rights and rights over the person. Thomson's point was not that privacy is vacuous or unimportant, but that the concept has no independent explanatory power for *why* we have the rights in the privacy cluster. In opposition to Thomson, many privacy theorists have attempted to isolate what is fundamental and common to privacy claims and that makes privacy a distinct concept with explanatory power of its own. We remain far from anything like consensus or even broad agreement. As Daniel Solove (2008: 1) stated:

> Privacy, however, is a concept in disarray. Nobody can articulate what it means. Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.

If privacy does cover such a broad range of interests, then the search for a single defining characteristic of privacy might prove impossible. Is privacy the right to: be left alone (Warren & Brandeis, 1890), limit access to the self (Van Den Haag, 1971), keep secrets (Posner, 1981), control personal information (Fried, 1968), protect the integrity of personhood (Reiman, 1976), or protect an essential condition for intimacy (Rachels, 1975)? These defining characteristics of privacy proposed in the literature can each be criticised as being too broad, too narrow, too vague, or all three (Solove, 2008). This situation has led some recent privacy theorists (Henschke, 2017; Nissenbaum, 2010; Solove, 2008) to propose pluralistic accounts of privacy, where diverse conceptions are included under the umbrella concept of privacy. Though the pluralistic approaches are advantageous in capturing the wide uses of the term privacy, they struggle to explain the normative force of the concept or how the diverse conceptions of privacy properly limit one another when they potentially conflict with one another.

It is beyond the scope of this chapter to resolve the conceptual disarray surrounding privacy. Instead, I attempt to show when the interests in maintaining one's anonymity as obscurity in public readily coincide with some popular conceptions of privacy and which controversies are linked to those conceptions of privacy. I assess whether the controversies associated with the relevant conceptions of privacy create complications when advocating for protecting our obscurity in public. Where there is no direct overlap, I consider whether that obscurity interest in fact clashes with privacy conceptions or can be incorporated into a yet broader pluralistic conception of privacy.

Whether the limited claims to anonymity as obscurity in public outlined in the previous section coincide with a right to privacy or stand independently of privacy will not change the normative conclusions already drawn. At the same time, determining whether these obscurity interests coincide with already established conceptions of privacy, or require us to expand the umbrella concept of privacy, or stand independently from privacy claims, will make a difference at the level of policy and law. Resistance to the type of protections suggested in the previous section will likely come from those who find that protecting individuals' obscurity while in public exceeds what the right to privacy can reasonably protect. By mapping out the relationship between privacy and anonymity as obscurity in pubic, I hope to be able to remove resistance to establishing policy and law that will protect against the risks imposed by FRS. My goal is not to address all possible sources of political resistance to protecting our obscurity while in public, but those elements of resistance that are rooted in controversies surrounding how we conceive of privacy protections.

To start, aggregating and analysing FRS data into detailed psychological profiles violates a popular conception of privacy. While each individual data point may not coincide with what people typically think of as personal or intimate information, the resulting psychological profiles would very much fit such a description. The conception of privacy as control over personal information captures this concern. According to Charles Fried (1968: 482), "Privacy is not simply the absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves".

There are some immediate controversies related to this conception of privacy. First, if one were to consider control of personal information as *the* defining characteristic of privacy, then privacy rights would not protect us from physical or legal interference regarding what we do with our own bodies or how we raise our children. However, if we adopt a pluralistic concept of privacy, other conceptions which fall under the umbrella of privacy could address these other aspects. Second, this conception suffers from vagueness regarding what information is "personal" and what is meant by "control". If privacy were to mean complete control over all personal information, then this conception seems too broad. One reply is that privacy is control over

"intimate" information (Inness, 2003), but this too suffers from vagueness. While we can debate where to draw the line between intimate and non-intimate information, some information lands clearly within the bounds of what is intimate, for example, what consenting adults do in their bedrooms and medical records (including the clinical notes of psychotherapists). If the profiles resulting from aggregating and analysing individuals' publicly surveilled behaviour discloses their psychological propensities and inclinations, then this discloses incredibly intimate details about the individuals that is analogous to their mental health records.

In regard to what is meant by control of information, there can be many cases that fall within a grey area (e.g., control over Internet activity data); but, it is widely acknowledged that intimate information from mental health records can only be released with the consent of the individual or under a court order. Similarly, consent or a court order is required for a mental health professional to produce a psychological profile in the first place. The target of FRS thus loses control over intimate information both when the psychological profile is created and when it is disclosed or sold. Hence, to the degree to which we conceive of privacy as control over intimate information, our initial case seems to coincide with this conception of privacy.

One potential objection is that there is little that is intimate or personal about what one does while in public. Again, it is not the observation of innocuous, individual data points that in themselves violate a person's privacy. It is only when these data points are aggregated and analysed that intimate information about the individual is uncovered. However, the non-anonymous nature of this data makes the control over the intimate information that can be inferred from it vulnerable, and, under this conception, privacy is equated with control over intimate information. In this sense, the protections recommended for preserving anonymity as obscurity in public can readily be interpreted as privacy protections.

Second, if we turn our attention to the potential harms of psychological manipulation and opportunity loss from FRS, obscurity protections against these potential harms overlap with other privacy conceptions. Jeffrey Reiman (1976: 39) conceived of privacy as what protects the integrity of personhood:

> Privacy is an essential part of the complex social practice by means of which the social group recognizes – and communicates to the individual – that his existence is his own. And this is a precondition of personhood. To be a person, an individual must recognize not just his actual capacity to shape his destiny by his choices. He must also recognize that he has an exclusive moral right to shape his destiny.

Reiman claims that, in the absence of privacy, the social group fails to demonstrate respect for the individual's exclusive right to be self-determining regarding both body and thoughts. He suggests that self-ownership is estab-

lished through the social ritual of communicating respect for privacy. These complex social practices aren't uniform across cultures but, before one can have rights to property or rights over the person, self-ownership of body and thoughts must be socially recognised and communicated. Psychological manipulation enabled by FRS profiling is contrary to respecting the individual's personhood and self-ownership of their own thoughts. For society to communicate to individuals that they have the exclusive right to determine their own destinies, it must establish legal restrictions upon FRS to minimise individuals' vulnerability to psychological manipulation.

One immediate complaint regarding this conception of privacy is that it reduces privacy interests to autonomy or basic liberty interests. This criticism seems to echo Thomson's (1975) claim that privacy lacks independent explanatory power, and privacy claims can be reduced to other more fundamental rights claims. Thomson may be right to the extent that we don't need the right to privacy to explain why people ought to be protected from psychological manipulation. We need only consider the way people's autonomy would be violated by such manipulation to recognise the need for legal protections. Reiman argues in opposition to Thomson that the right to privacy is more fundamental and a precondition for establishing the right to property and rights over the person that Thomson argues all privacy claims can be reduced to:

> The right to privacy is the right to the existence of a social practice which makes it possible for me to think of this existence as *mine*. This means that it is the right to conditions necessary for me to think of myself as the kind of entity for whom it would be meaningful and important to claim personal and property rights [emphasis original]. (Reiman, 1976: 43)

Reiman's counter to Thomson is convincing, *if* we assume Thomson means that privacy can be reduced to an interest in merely not having one's autonomy directly interfered with. (It is not clear to me that this assumption is warranted, as Thomson may be employing a richer notion of autonomy; however, this fine point in the debate is not central to my argument.) As a right to a series of social practices, Reiman's conception of privacy cannot simply be reduced to a protection from direct interference. More central to our concerns, if the aim of privacy rights is only the protection of individual autonomy from direct interference, then this would not protect against the collection of non-anonymous FRS data nor restrict the creation of psychological profiles but only protect against the use of the profiles to directly manipulate individuals. In contrast, Reiman's conception of privacy as a complex social practice whereby recognition of self-ownership and autonomy is communicated to members of the group maps more directly with regulations that protect individuals' obscurity while in public from FRS. Reiman's point is that, without communicating their recognition that individuals have

an exclusive right to their own thoughts and to be self-directing, the state fails to respect individuals' right to privacy. By not minimising individuals' vulnerability to psychological manipulation, a state would indeed fail to clearly communicate a recognition of every individual's exclusive right to shape their own destiny.

Opportunity loss maps less directly to any common conception of privacy. The creation of profiles that detail individuals' psychological characteristics and behavioural patterns could be used to screen individuals when they apply for jobs, schools, housing, insurance, or public assistance. One interpretation of the interest under threat is that we seek to protect individuals' reputations such that their opportunities are not unfairly limited. Though the connection between reputation protection and privacy is not well theorised, the disclosure of *some* intimate information can be damaging to one's reputation and can lead to opportunity loss. In the absence of adequate privacy protections in general, people's reputations and opportunities will certainly be vulnerable. Just as we sometimes value privacy as a means to protect individuals' reputations, we can value our obscurity in public for concerns over reputation and opportunity loss. Thus, even if protecting our obscurity in public for the sake of avoiding unjust opportunity loss does not seamlessly coincide with privacy claims, such protections do correspond to conceptions of privacy that are linked to protecting reputation.

Unlike the way FRS can be used to form detailed psychological profiles, cataloguing the participants of public activities does not disclose intimate information about them. Their religious and political affiliations are publicly displayed and can be observed by anyone. Nor does it *directly* make them vulnerable to psychological manipulation or some other way of undermining the individual's ability to shape their own destiny. (Of course, the data from cataloguing people's public participation could be aggregated into a broader profile that could be used to manipulate people's beliefs and actions; however, the cataloguing by itself does not have this potential.) The implicit intimidation produced by such cataloguing of participants does not violate an individual's bodily or mental self-ownership. Cataloguing political and religious participants is not antithetical to the group still communicating the recognition of an exclusive moral right of individuals to the integrity of their personhood. Instead, it fails to communicate to citizens that they are not vulnerable to negative repercussions when they exercise their rights to free speech, assembly, and religious worship. This failure violates the broad interests of liberal democracies, as opposed to the privacy interests of individuals.[5]

In the absence of any clear lines connecting the cataloguing of public participants within political and religious group activities with privacy interests or connecting privacy to the societal values made vulnerable by this surveillance practice, it may be best to view the right to anonymity as obscurity in public as distinct from privacy rights – at least in this context. Given the

conceptual disarray privacy suffers from, I do not suggest that the independence of this obscurity interest is definitive. Instead, our interest in preserving anonymity when publicly engaged in protests, political rallies, religious observances, or any socially stigmatised activity can only be tangentially thought of as a privacy concern. The apparent independence of this right to obscurity is not a problem for my argument but indicates that advocacy for policies and laws banning real-time facial recognition to catalogue participants in protests, rallies, religious observances, or socially stigmatised activities ought to be made *without* appealing to privacy, to lessen political resistance to establishing policy and law that will protect societies from the harms imposed by real-time FRS.

Conclusion

When considering non-augmented CCTV, there has been significant resistance in the literature to claims that widespread video surveillance violates people's privacy or that such public surveillance wrongs individuals in some other way. It has been argued (Alfino et al., 2003) that, if those being surveilled via CCTV are unaware of being observed or recorded, then their autonomy is not negatively affected, nor can we claim a right to not be observed while in public (Ryberg, 2007). Nissenbaum's (1998, 2010) work on privacy in public has helped to show that privacy interests are not limited to what happens in the "private realm". While she convincingly argues that individuals can be wronged when the contextual integrity of their data is not preserved – and that this holds for data mined from public or Internet activities as much as from more private settings – this does not capture what is new about FRS.

The integration of facial recognition programs into our already extensive video surveillance infrastructure – as well as it being deployed in police body cameras and drones – promises to eliminate our anonymity as obscurity in public. It is precisely this loss that is novel about this technological development. Some might associate their unease with this development with a violation of privacy, but anonymity and privacy are not the same thing. Anonymity involves dissociating the identity of the person from some information about them. Anonymising data can be a means of preserving privacy interests but, as examples like anonymous peer review show, anonymity can serve other ends besides privacy. In addition, the anonymity of being a mere face in the crowd can be valuable in itself, though this liberating value is not sufficient to ground an unconditional right to obscurity while in public.

I have made the case that we have a right to maintain our anonymity such that our mundane activities, behaviours, and associations are not recorded and linked to our identity by means of FRS. The mere collection of this non-anonymous data makes us vulnerable to significant harms in the forms of psychological manipulation and opportunity loss. In addition, I have argued

that this right to obscurity is not outweighed by social interests in preventing crime and violence or locating missing persons. These social interests could be equally served while still preserving individuals' anonymity by dissociating location data from personal identities and by only analysing behavioural patterns from anonymous data – until a court order requires the removal of these anonymity protections. Since the risks of psychological manipulation and opportunity loss could be greatly reduced by maintaining these protections to public anonymity, implementing FRS without protecting people's anonymity as obscurity in public would impose unnecessary – and, thus, unjust – risks of harm.

I have also made the case that we have a right to obscurity in public when we are engaged in political, religious, or socially stigmatised activities. The implicit intimidation generated by the state or its law enforcement agencies cataloguing such participation would have a chilling effect, but it may not qualify as direct interference with people exercising their rights to self-expression, assembly, and worship. Merely observing and cataloguing participants is not the same thing as stopping them from protesting. I have argued that the right to anonymity as obscurity is here grounded in the broader societal interest within liberal democracies that individuals can effectively exercise their civil liberties. The implicit intimidation arising from using FRS to catalogue political and religious participants fails to communicate to individuals that they are not vulnerable to the state's power to impose negative repercussions for their activities and convictions.

Given the power asymmetry between those under surveillance and the institutions carrying out the surveillance, the state has a special obligation to reassure individuals that they will not be subject to negative repercussions when they exercise their rights to free speech, assembly, and worship. Reassurance here can only take the form of banning the use of real-time FRS to catalogue participants in political, religious, or socially stigmatised activities. This second right to obscurity in public is also not overridden by competing social interests. The only justifying purpose for such cataloguing is for the sake of a criminal or legal investigation and, for such instances, real-time FRS is not required. A warrant can be required to apply this technology post factum to the video recordings.

If we recognise these two rights to anonymity as obscurity in public, how radically will this alter how we conceive of privacy? This question proves difficult to answer given the conceptual disarray surrounding privacy. However, I have shown that protection against collecting non-anonymous FRS data that can so easily be aggregated and analysed into detail psychological profiles maps closely to two popular conceptions of privacy: control over intimate information and protection of the integrity of the person. That these obscurity and privacy interests coincide so closely may indicate that anonymity is here a means of protecting privacy – but this is a matter for

later investigation. On the other hand, it appears that the societal interest in protecting the anonymity of people publicly engaged in political, religious, or socially stigmatised activities is not readily connected to privacy interests. The apparent independence of this right to obscurity is not a problem for my argument but indicates that advocacy for protections against using real-time FRS to catalogue participants in protests, rallies, religious observances, or socially stigmatised activities ought to be made without appealing to privacy to avoid muddying the waters.

Acknowledgements

I would like to thank the participants of the Association for Political Theory Workshop on Interpreting Technology and the ECPR Panel on Big Data, Mass Surveillance and Social Control for their helpful comments on earlier versions of this chapter.

References

Alfino, M., & Mayes, G. R. (2003). Reconstructing the right to privacy. *Social Theory & Practice*, *29*(1), 1–18. https://www.jstor.org/stable/23559211

Al Shouk, A. (2019, March 18). How Dubai's AI cameras helped arrest 319 suspects last year. *Gulf News*. https://gulfnews.com/uae/how-dubais-ai-cameras-helped-arrest-319-suspects-last-year-1.62750675

Botsman, R. (2017, October 21). Big data meets big brother as China moves to rate its citizens. *Wired*. http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

Buolamwin, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification Proceedings of the 1st Conference on Fairness, Accountability. In *Proceedings of Machine Learning Research*, *81*, 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html

Burgess, M. (2018, May 4). Facial recognition tech used by UK police is making a ton of mistakes. *Wired, UK*. https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival

Del Greco, K. J. (2017, March 22). *Law enforcement's use of facial recognition* [Statement Before the House Committee on Oversight and Government Reform, Washington, D.C.]. FBI. https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology

Denyer, S. (2018, January 7). China's watchful eye. The *Washington Post*. https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/

European Commission. (2021). *Proposal for laying down harmonised rules for the regulation of Artificial Intelligence* (SEC(2021) 167 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:SEC(2021)167&from=EN

European Parliament. (2016). *General data protection regulation* (Regulation (EU) 2016/679). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Fried, C. (1968). Privacy. *The Yale Law Journal*, *77*(3), 475–493. https://www.jstor.org/stable/794941

Friedersdorf, C. (2013, March 28). The horrifying effects of NYPD ethnic profiling on innocent Muslim Americans. *The Atlantic*. https://www.theatlantic.com/politics/archive/2013/03/the-horrifying-effects-of-nypdethnic-profiling-on-innocent-muslim-americans/274434/

Goodin, R. E. (1985). *Protecting the vulnerable: A reanalysis of our social responsibilities*. University of Chicago Press.

Harmon, A. (2019, July 8). As cameras track Detroit's residents, a debate ensues over racial bias. *The New York Times*. https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html?smid=url-share

Harwell, D. (2018, April 26). Facial recognition may be coming to a body camera near you. *The Washington Post*. https://wapo.st/2vN7CPr?tid=ss_mail&utm_term=.d955165fd135
Henschke, A. (2017). *Ethics in an age of surveillance: Personal information and virtual identities*. Cambridge University Press. https://doi.org/10.1017/9781316417249
Inness, J. C. (2003). *Privacy, intimacy and isolation*. Oxford University Press. https://doi.org/10.1093/0195104609.001.0001
Kaste, M. (2018, May 22). Orlando police testing Amazon's real-time facial recognition. *NPR*. https://www.npr.org/2018/05/22/613115969/orlando-police-testing-amazons-real-time-facial-recognition
Laperruque, J. (2017, October 20). Preserving the right to obscurity in the age of facial recognition. *The Century Foundation*. https://tcf.org/content/report/preserving-right-obscurity-age-facial-recognition/
Lin, L., & Purnell, N. (2019, December 6). A world with a billion cameras watching you is just around the corner. *The Wall Street Journal*. https://www.wsj.com/articles/a-billion-surveillance-cameras-forecast-to-be-watching-within-two-years-11575565402
Manson, N., & O'Neill, O. (2007). *Rethinking informed consent in bioethics*. Cambridge University Press.
Marmor, A. (2015). What is the right to privacy. *Philosophy & Public Affairs*, *43*(1), 3–26. https://doi.org/10.1111/papa.12040
Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy*, *17*(5/6), 559–596. https://www.jstor.org/stable/3505189
Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
Overgaard, S. (2019, October 21). *A soccer team in Denmark is using facial recognition to stop unruly fans*. NPR. https://www.npr.org/2019/10/21/770280447/a-soccer-team-in-denmark-is-using-facial-recognition-to-stop-unruly-fans
Ponesse, J. (2014). The ties that blind: Conceptualizing anonymity. *The Journal of Social Philosophy*, *45*(3), 304–322. https://doi.org/10.1111/josp.12066
Posner, R. A. (1981). *The economics of justice*. Harvard University Press.
Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, *4*(4), 323–333. http://www.jstor.org/stable/2265077
Reiman, J. H. (1976). Privacy, intimacy and personhood. *Philosophy & Public Affairs*, *6*(1), 26–44. http://www.jstor.org/stable/2265060
Roos, F., & Källström, L. (2020, Oct. 26). *Facial recognition technologies from a Swedish data protection perspective*. International Network of Privacy Law Professionals. https://inplp.com/latest-news/article/facial-recognition-technologies-from-a-swedish-data-protection-perspective/
Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, March 17). How Trump consultants exploited the Facebook data of millions. *The New York Times*. https://nyti.ms/2GB9dK4
Ryberg, J. (2007). Privacy rights, crime prevention, CCTV and the life of Mrs. Aremac. *Res Publica*, *13*(2), 127–143. https://doi.org/10.1007/s11158-007-9035-x
Skelton, S. (2021, February 18). *Swedish police fined for unlawful use of facial-recognition app*. Computer Weekly. https://www.computerweekly.com/news/252496545/Swedish-police-fined-for-unlawful-use-of-facial-recognition-app
Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.
Swedish Data Protection Agency. (2019). *Supervision pursuant to the general data protection regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students*. (DI-2019-2221). https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf
Thomson, J. J. (1975). The right to privacy. *Philosophy & Public Affairs*, *4*(4), 295–314. http://www.jstor.org/stable/2265075
Van Den Haag, E. (1971). On privacy. In J. R. Pennock, & J. W. Chapman (Eds.), *Privacy & personality* (pp. 149–168). Routledge. https://doi.org/10.4324/9781315127439
Vélez, C. (2021). *Privacy is power: Why and how you should take back control of your data*. Melville House.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.
Yle News. (2021, April 23). *Finnish police denied, the admit using controversial facial recognition app*. https://yle.fi/uutiset/osasto/news/finnish_police_denied_then_admitted_using_controversial_facial_recognition_app/11899325

Endnotes

[1] I do not focus on the reasonable concerns over the inaccuracy of current facial recognition technology. In a study by the FBI, their facial recognition system produced false positives 15% of the time and only found an accurate match for the other 85% within the top-50 suggested matches (Del Greco, 2017). A study has also shown that the accuracy of facial recognition varies depending upon ethnicity and gender (Buolamwini et al., 2018). While false positives can easily wrong those targeted by this technology, I am generally concerned with whether people are wronged by the institutional practice of FRS.
[2] As the recent Covid-19 lockdowns illustrate, it is conceivable that people's online activity can far out-measure their public activities. However, under more normal circumstances, this will not be the case, on average.
[3] The chilling effects of surveillance in general on free speech, free assembly, and free religious practice is easily observed. For example, when it became known that the New York City Police Department had video cameras aimed at Mosques after the 9/11 attacks, the number of people attending services, classes, and other events at the Mosques dropped dramatically (Friedersdorf, 2013).
[4] As an anonymous reviewer pointed out, this duty might be cast in terms of the state's obligation to optimally support citizens' individual autonomy by reassuring citizens that there will be no negative repercussions for exercising their autonomy within legal limits. I am not prepared, however, to defend a claim that states have an obligation to optimise individual autonomy, as opposed to states having an obligation to protect citizens' ability to effectively exercise their civil rights.
[5] Carrisa Vélez (2021) has claimed that privacy has a political value – especially in our current data economy – insofar as it can protect against data holders maintaining vast power asymmetries over data subjects. She argues that such power asymmetries are antithetical to well-functioning liberal democracies. However, insofar as she conceives of privacy as intimate information, and the damage to liberal democracies she describes comes from profiling and manipulating individuals, her account does not make a clear connection between privacy and the societal harms that I argue result from cataloguing people in public who are engaged in group activities.