Constitutional principles in a networked digital society

Yeung, Karen

DOI:
10.2139/ssrn.4049141

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (Harvard):
Yeung, K 2022, 'Constitutional principles in a networked digital society', The Impact of Digitization on Constitutional Law, Copenhagen, Denmark, 31/01/22 - 1/02/22. https://doi.org/10.2139/ssrn.4049141

The Impact of Digitization on Constitutional Law

IACL Roundtable, 31 Jan-1 Feb 2022, Copenhagen, Denmark (hybrid)[1]

Keynote Address

'Constitutional Principles in a Networked Digital Society'

Professor Karen Yeung

Birmingham Law School & School of Computer Science

University of Birmingham

A. Introduction

My hosts have asked me if I could talk about constitutional principles and digitisation today, and I will seek to oblige. Hence in my short address today, I want to pose the following question: are our existing constitutional principles fit for purpose in an increasingly datafied, networked digital age? To attempt an answer to this question, we need to clarify at least two things. First, what do we mean by constitutional principles, and what is their point and purpose (which I will describe in terms of the aspirations of the 'rule of law project' to which liberal democratic polities aspire)? Secondly, how do the digital transformations sweeping across society, including the digitisation and datafication of government in particular, challenge the adequacy of our constitutional principles to serve the rule of law project and how can we understand the nature of those challenges?

In relation to the first matter, I am sure many of you know that we could get caught up in debates about what we mean by 'constitutional', what we mean by 'principles', and on what those principles are. But today I will glide swiftly over these debates and simply assume that constitutional law scholars broadly agree on what these principles are and their underlying purpose. In other words, I will proceed on the assumption that the purpose of constitutional principles within liberal democratic states is to ensure and maintain government under law so as to safeguard and protect individuals against the dangers of a despotic government, and to establish and foster democratic self-government. And I will assume that there is a widely shared understanding among constitutional lawyers about what these principles are: among others, they include principles of legality, transparency, due process, reason-giving, proportionality and respect for fundamental rights. Together, these principles play an important role in what David

[1] See https://jura.ku.dk/cecs/calendar/2022/hybrid-iacl-round-table/.

Dyzenhaus refers to as "the rule-of-law project" - one which he describes as a political project which, ideally, seeks to ensure that governmental power is always exercised within the limits of the rule of law.

> "The ideal of the rule of law project is a political one, the ideal of having in place a 'culture of justification' one in which 'every exercise of power is expected to be justified, in which leadership given by government rests on the cogency of the case offered in defence of its decisions, not the fear inspired by the force of its command"[2]

It is the second matter that I will focus on today. As you know, governments everywhere are enthusiastically embarking on projects of 'modernisation' that rely on wholesale networked digital transformation. I have referred to this movement as the **'***New Public Analytics'*[3] - a term chosen to reflect both continuity and discontinuity with the 'New Public Management' movement which swept through governments in many democratic states beginning in the early 1980s and the following two decades. Beguiled by promises of enabling governmental services to be delivered faster, cheaper, and better through reliance on automation, datafication and the population-wide profiling of users and citizens – the rule of law project faces an important and increasingly urgent challenge: the need to demonstrably bring these technologies, and the socio-technical systems into which they are embedded, under law. Here, my take home message is that our existing principles have the *potential* to fulfil their purpose, but whether they *in fact* live up to that potential depends critically on our governance institutions, and particularly our courts**,** to acquire a proper grasp of both (a) the critical technical features, capabilities and vulnerabilities of these technologies and (b) how these technologies and systems impact and implicate the opportunities and experiences our individual and collective lives in real-world settings in a manner that duly recognises their novelty, opacity and highly consequential effects, in ways that often seriously (and often radically) magnify the asymmetries in power between state and citizen.

B. The challenge: putting constitutional principles into real world practice

So, how does the New Public Analytics affect the capacity of our, constitutional principles to serve and sustain the rule of law project? The answer lies in recognising that constitutional principles (or indeed, any principles of any kind) are not self-executing. If one is to 'live by one's principles', it is not enough

---

[2] D Dyzenhaus 'Preventive Justice and the Rule-of-Law Project' in A Ashworth, L Zedner and P Tomlin (eds) *Prevention and the Limits of the Criminal Law*, 2013, Oxford University Press.

[3] I first spoke publicly of the New Public Analytics in 2018. See K Yeung 'Algorithmic Government: Towards a New Public Analytics?' ThinkBIG Workshop, *Ethical and Social Challenges posed by Artificial Intelligence'* (25 June 2018) Cumberland Lodge, The Great Park, Windsor, UK and K Yeung 'Big Data Driven Government: Towards a New Public Analytics', Hong Kong Law School's 50th Anniversary Celebration Conference, ICON-S Annual Meeting, *Identity, Security and Democracy: Challenges for Public Law*, 25-27 June 2018, Hong Kong.

merely to espouse them: instead, we need to *translate* those principles into practices and actions in our daily lives. This is equally true of our constitutional principles. Unless our constitutional principles are capable of being translated and put into everyday practice, then our principles count for little, and contribute nothing to the project of democratic governance, including the need to protect individuals against the abuse of governmental power. Indeed, this is – in my view – why the grand statements of principle that have proliferated in the form of 'ethical codes' promulgated by the tech industry, are little more than an exercise in marketing and public relations: all talk, no serious action to put noble statements of aspiration into practice.[4] In other words, our constitutional principles must be *operationalised* if they are to serve their purpose. It is here – in the process of interpretation, application and enforcement of these principles into real-world practice, that enables them to serve their purpose. But, it is precisely this process of *interpreting and applying* our constitutional principles, that we encounter several serious and related challenges.

In particular, as public anxiety concerning the power and practices of Big Tech has continued to grow as their adverse impacts have become impossible to ignore, contemporary policy-makers everywhere are now wrestling with questions about how to govern our powerful digital technologies. While considerable energy and effort is now being devoted to devising new regulatory governance regimes (and which I very much welcome), in the meantime, the pace of public sector take-up of digital technologies has continued unabated. And, like any other governmental tool, digital tools are prone to overreaching and misuse, quite apart from their potential to be weaponised against disfavoured groups and individuals, by both authoritarian and self-described democratic states alike, particularly in the name of security and efficiency.

C. *The compulsion of legality - bringing digital tools and systems under law*

My starting point for exploring the challenges which the New Public Analytics poses for constitutional principles begins with what David Dyzenhaus, the 'compulsion of legality', referring to the widely shared acceptance by democratic governments that it is a necessary condition of legitimate state action that public officials who perform the action have a legal warrant – that there is in pre-existing law an authorisation for public officials to act in the relevant manner. Yet despite the sophistication and power of networked digital technologies, governments appear to be embracing them without pausing to consider whether their proposed deployment is authorised by law. How do we explain this apparent indifference to the need for legal authorisation in relation to public sector digital transformation? My guess is that this

[4] Yeung, K, Howes, A and Pogrebna, G. 'AI governance by human rights-centred design, deliberation and oversight: An end to ethics washing.' In Dubber, Pasquale and Das (eds) *The Oxford Handbook of AI Ethics*, Oxford University Press (2019).

is due to an unexamined assumption that the technological tools and systems upon which the New Public Analytics relies fall within existing warrants of legal authority because they are considered 'equivalent' to existing technologies. In other words, it is assumed that digital technologies enable the performance of *existing* tasks and functions already carried out by public authorities, simply with greater speed, efficiency. Put differently, the networked digital tools employed by government are, for the purposes of our constitutional principles (including the requirement of prior legal authorisation), assumed to be no different from old tools: they merely perform the same functions - just faster, better and, thanks to the power of automation, more cheaply. On this logic, existing warrants of legal authority thereby provide the legal basis upon which they may be used.

But reasoning of this kind in order to ground the legal basis upon which digitisation in the public sector has proceeded is both mistaken and dangerous. It is based on false analogies. Most of us would laugh at the suggestion that there is no difference between a machete and a machine gun. Likewise, I shall subsequently explain why a notepad and pen in the hands of a police constable cannot be equated with the same constable equipped with a smart device with the capacity to capture images in real time and linked to a powerful facial recognition technology run on a central server connected to national database to which the public have no access. In other words, if we are to take the requirement of legality seriously in a networked digital age, we should *not* accept at face value claims that existing warrants of legal authority provide a sufficient basis upon which the use of powerful digital technologies can claim to be authorised by law. Instead, we must subject these claims to critical scrutiny – and to do this, a clear-eyed understanding of the technical capabilities of these digital technologies and hence their novelty and power in real-world practice, is absolutely essential. In other words, I am suggesting that governmental actors do not appear to be taking seriously the basic constitutional principle of legality in their rapid embrace of networked digital technologies.

D. Courts and constitutional principles in a digital age

While the responsibility for upholding and giving expression to constitutional principles in the practices of governments falls to *all* our governmental institutions (and to which I will return in my concluding comments), the judiciary occupies a unique role as the authoritative interpreter and, in effect, primary custodian of these principles. The question which arises, then, is whether courts are up to the task of interpreting and applying constitutional principles in a manner that serves and fosters the rule of law project as networked digital technologies are taken up across government, if we assume (as I think we must) that adoption and application of specific technological applications will be subject to legal challenge.

In other words, judges will be called upon to act as critical interpreters of existing laws, and this will require them to bring constitutional principles to bear in identifying how existing laws apply to novel digital applications, particularly in the absence of bespoke legal governance regimes that are currently being formulated and discussed at the policy-level. Hence courts will be required to consider whether a particular technological application is authorised by law, and if so, then they must also authoritatively determine how existing laws (including data protection laws, administrative law and legal duties to ensure respect for fundamental rights) restrict or condition the lawful use of these technologies. And in making *these* determinations, they must be guided by the full range of constitutional principles, including principles of proportionality, transparency, due process, and the duty to respect fundamental rights, particularly the right to privacy, and so forth.

This takes me to the heart of the question which my address sets out to answer, and this requires consideration of both the capabilities of the principles themselves, and the capabilities of our courts to apply to the New Public Analytic applications that are proliferating. This, in turn, requires consideration of two important matters:

> First, are our existing constitutional principles capable of being interpreted and applied in a manner that serves the rule of law project?
>
> Secondly, if so, are courts capable of undertaking that task in performing their crucial role as critical interpreter and custodian-in-chief of our constitutional principles?

My answer to the first is a reasonably confident 'yes': the high level of generality of our constitutional principles means that they have the potential to be interpreted and applied to new settings and novel situations in a manner that remains faithful to the animating spirit and purpose. But, I am less optimistic about the second, particularly in light of recent judgements of British courts. My pessimism stems from recognising that acquiring an understanding of the novelty, power and significance of the public sector's embrace of networked digital technologies is not a straightforward matter: it requires particular care when invoking familiar analogical reasoning frequently resorted to in common law reasoning. Although judges may be well-acquainted with the task of interpreting and applying constitutional principles to familiar public policy interventions, the, distinctive and novel functional capacities of many of our contemporary digital technologies (particularly those that rely on machine learning applications trained on historic data sets) when deployed in real-world settings in ways that affect individuals, groups and populations in significant and sometimes highly consequential ways. These consequences include threats to the very

foundations upon which our rights and democratic freedoms are ultimately rooted, while radically exacerbating the asymmetries in power between the state and citizen, yet may be difficult for judges to fully grasp. In other words, a proper understanding, appraisal and evaluation of the relevant technology that takes due account of its functional capabilities and limitations in *light of* the nature, extent and significance of its impact upon individuals, populations and the larger socio-cultural and political environment is an essential pre-condition of any attempt to evaluate its legality and, in turn, its conformity with constitutional principles. This is true not only of the basic question whether the state's use of the technology in question is authorised by law but also in authoritatively determining how existing laws restrict or condition the lawful use of these technologies. In making these latter determinations, courts must be guided by the full range of constitutional principles, including principles of proportionality, transparency, due process, and the duty to respect fundamental rights, particularly the right to privacy, and so forth.

In order to illustrate this, the remainder of my talk will critically examine the reasoning of the Court of Appeal in *Bridges v South Wales Police*[5] – a judicial review application challenging the legality of the use of live facial recognition technology (FRT) in public settings on multiple occasions on a 'trial' basis by the South Wales Police[6]. As you are no doubt aware, the use of live FRT by police forces has provoked intense controversy, with many civil liberty groups calling for legal prohibition on its use in public, particularly by law enforcement agencies, following the lead of taken by several US states. While police forces around the world have been keen to trial these technologies – unlike some US states, which have banned its use - the British police have simply pressed ahead, as early adopters of these technologies: particularly because the FRT software can easily be parachuted onto the very extensive CCTV camera infrastructure already in place in Britain, and which has become normalised in the eyes and experience of the British public. Although the Court of Appeal in *Bridges* overturned the lower court's decision[7] in 2020, finding that the specific circumstances of use were unlawful – their reasoning displayed serious failures to understand the novel and distinctive capabilities offered by the technology and its concomitant dangers. It refused to rule on the legality of the use of this technology for the purposes of mass surveillance by the police in general, thereby paving the way for the London MPS to announce its decision to roll-out the technology in London on a permanent and on-going basis in early 2021[8]. Rather than engage in a comprehensive case analysis, I

5 [2020] EWCA Civ 1058.

6 Live FRT trials have also been conducted by the London Metropolitan Police Service. See Fussey, P and Murray, D (2019). *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. Essex.

7 [2019] EWHC 2341 (Admin).

8 https://www.computerweekly.com/news/252477334/Met-Police-to-launch-facial-recognition-operationally/

will focus my attention on how the Court understood the functions, capabilities and limitations of the technology in question. My aim is to demonstrate how the court's reasoning is marked by a failure to properly understand the novelty, significance and power of the relevant technology – and thus its potential for abuse and overreaching. And, as a consequence, it fails to apply constitutional principles in a manner that enables them to serve their purpose in securing and nurturing the rule of law project.

E. The Bridges case: challenging the legality of police use of live FRT in public settings

While FRT software has been used by the British police for some time for forensic investigations in order to facilitate the identification of individuals from historic digital images in which criminal activity was reported or believed to have occurred, advances in machine vision technologies have made it possible to deploy FRT in open public settings. This technology has advanced to the point where commercially available software can be deployed to analyse live video capture of faces passing in front of the camera in busy, open, dynamic settings and then algorithmically compared with facial images uploaded to a pre-figured 'watchlist'. These technologies are touted as significantly enhancing the ability of law enforcement and security officials to 'catch terrorists' and 'find missing children'. In what I understand is the first attempt challenge the legality of these technologies, by Mr Bridges, a Welsh civil liberties campaigner, supported by Liberty, initiated a judicial review application challenging the use of a system called 'AFR Locate' (and a system called 'AFR Identify') which had been deployed in a number of public settings in Wales by the South Wales Police (SWP).

Beginning from 2017, SWP undertook a number of 'live trials' of AFR Locate at a variety of live public events[9] using facial recognition software produced by commercial software developer NeoFace, to assist in the finding and apprehending 'persons of interest'. AFR Locate is capable of scanning 50 faces per second[10]. The image watchlists compiled by SWP for these purposes comprised of between 400-800 people, although the maximum capacity of the software is approximately 2000 facial images[11] and it was SWP's stated intention during each deployment to allow AFR Locate to process as many individual faces as possible. Over the 50 deployments were conducted by SWP between May 2017-April 2019, resulting in approximately 500,000 faces being scanned.[12] Whilst the deployment of AFR was overt, evidenced by the

9 2020] EWCA Civ 1058 at para 11.

10 Ibid, para 16.

11 Ibid, para 13.

12 Ibid, para 16.

various channels through which the SWP sought to publicise its use, the Court of Appeal reasoned that a large number of people whose facial biometrics are captured and processed by SWP's use of AFR Locate were unaware that this was taking place.[13]

The judicial review application was based on several grounds, alleging that that the deployment of the technology:

- unlawfully interfered with the applicant's right to privacy under Art 8 of the European Convention on Human Rights (ECHR);
- violated aspects of the data protection legislation (particularly the Data Protection Act 2018 and its predecessor which implemented the EU Law Enforcement Directive into British law); and
- was not conducted in accordance with SWP's obligation to discharge its public sector equality duty (PSED) imposed by section 149 of the Equality Act.

To evaluate these claims, the court needed to understand the how the AFR Locate system was used in open public settings by the police to identify and apprehend individuals whose faces had been uploaded to the system's image 'watchlist'. This necessitated an appraisal of the technology itself, in order to identify its salient features for the purposes of legal analysis. Rather than engage in a comprehensive analysis of the case, I will focus my attention exclusively on how the Court of Appeal sought to understand the technological system - its functions, capabilities and limitations. If I had more time, I would also consider how that technological appraisal then affected how the Court applied the law, and – in turn – the constitutional principles animating the relevant laws upon which the judicial review claim rested. But today I only have time to critically examine the Court's appraisal of the technology, in order to ask: does its approach suggest that courts have the necessary capabilities and competence to undertake this kind of appraisal that I believe is required in order to faithfully apply constitutional principles? My short answer is no. Although there are some aspects of the Court's approach which are commendable and welcome – for example, its analysis of the technology's properties was far more careful and considered than that adopted by the court below it. In particular, the Court of Appeal explicitly rejected the argument made by the SWP that the use of live FRT is analogous to the taking of photographs or the use of CCTV cameras[14] – a finding that reflects a partial recognition that automated identification of individuals is a distinctive, powerful and new capability. Nevertheless the Court's analysis still fell well short of the kind of appraisal I believe is required, which I will now seek to demonstrate.

13 Ibid, para 20.
14 Ibid, paras 84-85.

The legal context for its technology appraisal

Attempts to understand and appraise AFR locate, in both the High Court and Court of Appeal, took place in the context of considering whether the interference with the right to private life under Article 8(1) ECHR that it entailed was nevertheless legally justified within the terms of Article 8(2). This required, among other things, the need to demonstrate that the technology's use was 'in accordance with law'. As many of you may know, however, this legal test is *not* a test of express legal authority. Rather, it is concerned with evaluating the 'quality' of the law – understood in terms of whether there are rules in place which meet the legal tests of 'accessibility' and 'foreseeability' in which the European Court of Human Rights jurisprudence has emphasised that applicable laws and guidelines should be both publicly available and sufficiently clear so that individuals can know them in advance.[15] For this purpose, the relevant legal framework includes not only laws enacted in the form of primary and delegated legislation but also includes codes of practice and 'local policies'. In evaluating the quality of the relevant law for this purpose, the Court of Appeal accepted that a 'relativist' approach was appropriate – in other words,

> 'the more intrusive the act complained of, the more precise and specific must be the law said to justify it'.[16]

This meant that the Court was required to assess the technology to determine its 'intrusiveness', in order to evaluate whether its deployment was 'in accordance with law', which consisted of two analytical steps. First, it identified the following features of AFR locate as salient:

- its novelty
- its capacity to capture and processes the digital images of a large number of members of the public, the vast majority of whom will be of no interest to the police,
- that the data it collects and processes is institutionally recognised as particularly sensitive, owing to its character as 'sensitive' data under the DPA 2018 (which implements EU legislation into domestic law), a

[15] It is worth noting that although judicial review application included a claim that there was no legal basis for SWP's use of AFR locate (for the purposes of Art 8(2) ECHR, but the Divisional Court held that its use was authorised under the common law powers of police and Police and Criminal Evidence Act 1984. This argument was not pursued on appeal, so that it was 'common ground that SWP do have the power to deploy AFR locate' (para 38). Likewise, the High Court rejected the applicant's argument (supported by) concerning the need for express legislation, stating "it is neither necessary nor practical for legislation to define the precise circumstances in which AFR Locate may be used, e.g. to the extent of identifying precisely which offences might justify inclusion on a watchlist as a subject of interest or precisely what the sensitivity settings should be.

[16] This statement of the principle in issue was based on an earlier ruling in *R (Wood) v Metropolitan Police Commissioner* [2009] EWCA 414.

feature which is *not* present, for example, for ordinary photographs (although the court does not explain what it means by an 'ordinary' photograph), and

- it processes data in an automated manner.

Secondly, the Court then compared the SWP's use of AFR locate with other technological interventions utilised by police that had previously been subject to legal challenge. To this, end the Court compared it with both:

(a) other biometric information, via fingerprint matching and DNA identification. Here, it noted that a police policy of routinely subjecting all persons arrested for a recordable offence to DNA sampling from which a digital DNA profile was then stored in the National DNA Database, and retention of that biometric identification data regardless of whether they are charged and convicted, was held unlawful by the ECtHR in *S and Marper v United Kingdom*.[17] This subsequently led to the introduction of a statutory regime to regulate and restrict the lawful use of DNA and fingerprinting biometrics.

(b) the common law power of police to collect and store personal data (names, addresses, digital photos) based on records taken by human officers whilst policing and observing individuals at public protests, the details of which were then included on the UK's 'extremism database' and held to be in 'accordance with the law' in by the Supreme Court in *Catt*[18] (although subsequently held unlawful by the ECtHR[19]).

It is on the basis of these two short analytical steps, that the Court concludes that the case:

> falls somewhere in between the two poles on a spectrum which are represented by *S v UK* on the one hand and *Catt* on the other (para 85)

In other words, the Court appears to characterise AFR Locate as *less* intrusive than fingerprinting and DNA identification technologies and practices but *more* as intrusive than police practices involving the retention of personal data about individuals attending public protests. Yet this reasoning is inadequate and incomplete for at least two reasons. First and foremost, the Court makes no attempt to explain *why* these features are significant, particularly for the purposes of identifying the technology's "intrusiveness". No

17 [2008] ECHR 1581.

18 [2015] UKSC 9.

19 *Catt* v *United Kingdom* [2019] ECHR 76

reasoned analysis is provided concerning the legal and constitutional significance of these technological features. While the Court offers a comparison between other identification technologies that have previously been subject to legal challenge, and concludes that the AFR locate system lies 'somewhere between the two', the nature and parameters of the comparison are woefully under-specified, offering a very limited analysis of what 'intrusiveness' is assumed to mean: intrusiveness in relation to what, whom, and how?[20] Let us consider both of these shortcomings together, drilling down into the comparisons which the Court makes with AFR locate and existing police identification technologies. This allow us to identify both (1) the salient features of the technology and (2) their real-world significance: both of which *must* be properly grasped if we are to hold the government to account for their use in a manner that is faithful to our constitutional principles.

First, the Court appears to regard DNA and fingerprinting biometrics for identification as 'more intrusive' than live FRT. Although no reasons are given for this view, presumably it is because these conventional biometric identification technologies require either the taking of a bodily sample or bodily contact with the individual (the taking of a fingerprint, the provision of a sample of hair or saliva swab). But, if we consider the full range of technological capabilities of FRT compared with DNA and fingerprinting biometrics for identification purposes, the latter are far *less* 'powerful' than FRT biometric identification technologies, because:

1. Live FRT may be deployed *remotely at a distance*: this means that it is capable of being deployed covertly, or even if overtly used, it will often operate without awareness of those whose faces are subjected to it;
2. Live FRT is capable of identifying *multiple* individuals of interest whose images a captured in a single digital image and thus technologically capable of undertaking many-to-many matching and identification. In contrast to DNA and fingerprint identification technologies can only operate on a 1-1 basis *and* also requires a human operator to manually procure the relevant biometric imprint before it can be used as the basis for undertaking identification matching.
3. Live FRT utilises a process of *automated identification,* which enables detection and identification of multiple individuals to be undertaken *at scale* in open public, unconstrained settings. In contrast DNA and fingerprinting biometric identification technologies cannot be deployed at scale cannot be used identify multiple individuals at a distance, and with such speed, convenience in open public settings.
4. Live FRT undertakes the identification matching process at very high speed, so that it can be deployed to identify individuals in dynamic settings *in real time*: unlike DNA and fingerprinting identification which

[20] The Court noted that 'a significant difference, however, is that AFR technology enables facial biometrics to be procured without requiring the co-operation or knowledge of the subject or the use of force, and can be obtained on a mass scale' [para 23] although it is not clear whether, and if so in what way, this acknowledgement affected the Court's legal analysis.

are useful for the purposes of forensic criminal investigations but, due to their technical limitations, cannot be used for the purposes of real-time identification;

Taken together, it becomes clear that live FRT is far more powerful than DNA or fingerprinting biometric identification technologies, due to a number of technological properties which enables the police to engage in an entirely novel and extraordinarily powerful new practice: that is, to engage in mass surveillance of populations as they go about their lawful activities in public, at scale, on a continuous basis, for the purposes of identifying multiple 'persons of interest' in real time. But by failing to properly grasp the true novelty and power of AFR Locate, the court's evaluation of the legal arguments was necessarily inadequate.

Unfortunately, I do not have time today to critically examine the legal reasoning employed by the Court that followed from its technological appraisal. However, there is one element of its legal analysis that I consider deeply worrying, and which is worth mentioning before I conclude. It concerns the court dismissal as 'trivial' the fact that many members of the general public would have their faces were photographed and algorithmically matched by the technology against the Watchlist without their consent and often without their conscious awareness. The appellant argued that, for the purposes of determining whether the interference with Art 8 was proportionate for the purposes of Art 8(2), account must be taken of the interference with the Article 8 rights not only of the individual applicant, but *all other members of the public* at the two venues in question when AFR Locate was deployed. Although the Court of Appeal deliberately side-stepped this question on highly technical grounds: focusing on the way in which P had formulated the basis of the challenge in terms of a violation of *his* rights, it nevertheless endorsed, by way of obiter dicta, the lower court's acceptance of the argument put forward by the police that the impact on each member of the public had a negligible impact of 'very little weight' on P's Article 8 right to privacy which "cannot become weightier simply because other people were also affected."

> 'It is not a question of simple multiplication. The balancing exercise which the principle of proportionality requires is not a mathematical one; it is an exercise which calls for judgement. (para 143)

This kind of reasoning is deeply troubling, for reasons I will shortly return in my concluding remarks.

Before doing so, however, I should acknowledge that there *are* some promising signs for optimism in the Court of Appeal's judgement. In particular, in response to allegations that the technology operated in a manner that was biased against female and non-white faces, the Court *was* willing to strike down the police's use of the technology on this ground, refusing to accept at face value the private software developer's claims that the software was not biased. While the Court recognised that it was 'understandable' that the manufacturer did not wish to divulge further details of the training data upon which the software was

trained, this meant that its claims that the software was free from bias could not tested. And this, the Court reasoned, was not sufficient to enable a public authority to discharge its own, non-delegable, duty under section 149 of the Equality Act to 'satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias'.

F. Concluding thoughts

I will conclude by returning to the question I posed at the outset: are our existing constitutional principles fit for purpose in an increasingly datafied, networked digital age? I have argued that our existing principles have the *potential* to fulfil their purpose, but whether they *in fact* live up to that potential depends critically on our governance institutions, and particularly our courts**,** to acquire a proper grasp of both:

(a) the technical features, capabilities and vulnerabilities of these technologies, and
(b) a proper appreciation of how these technologies and systems impact and implicate the opportunities and experiences our individual and collective lives in real-world settings in a manner that is novel, opaque and highly consequential, in ways that often seriously (and often radically) magnify the asymmetries in power between state and citizen.

I have critically scrutinised the technological analysis performed by the UK's Court of Appeal to demonstrate this*,* highlighting its failure to reckon with the extraordinary technological power, fallibility and social and political implications of its application for citizens, and the effects on the distribution and exercise of power between state and citizen power and novelty which the rise of the New Public Analytics portends. But I am not*,* however, suggesting that the Court's approach to technical appraisal in *Bridges* is typical or representative of the analysis taken by other courts, and in particular – there appears to me great untapped potential in contemporary European data protection law as a vehicle for upholding constitutional principles – and the CJEU has been at the vanguard of protecting the fundamental rights of European citizens.

In closing, I want to emphasise the way in which these powerful networked digital technologies may be directly eroding our collective culture and environment, prompting the need to ask what it means to take rights seriously in a networked digital age? In earlier work[21] I have emphasised the importance of taking seriously the collective impacts and implications of these technologies and their implications for the

[21] Council of Europe, A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework. Rapporteur: Karen Yeung. Available at https://www.coe.int/en/web/freedom-expression/msi-aut. Adopted by the Council in October 2019

'sociotechnical foundations of political freedom'. In this respect, in order to reckon with the power of this technological infrastructure to profoundly alter our collective social, political and cultural environments in ways that are completely at odds with the aspirations of the rule of law project, then we must move *beyond* the interference with the rights of a single individual. Hence the Court of Appeal's acceptance in *Bridges* of the claim that the use of live FRT by police in public spaces has a 'negligible' impact on those members of the public whose faces are photographed and algorithmically matched against a database of images of 'wanted' individuals so that it is of no legal consequence is seriously troubling. At the same time, these powerful, population-wide surveillance technologies are being embraced by democratic states based on promises that it will enable our public authorities to 'catch terrorists' and 'find missing children' without *any evidence* that they in fact do so. The unrestrained take up of these technological interventions are surely ones that our constitutional principles must guard against[22].

While I believe that our constitutional principles, including our rights discourse, has the *potential* to adapt to meet the altered conditions of our increasingly digitised and datafied age, whether they will succeed in doing so remains an open question. In this respect, we must bear in mind that the rule of law project does not lie solely in the keeping of the courts. Rather, it is our governance institutions more generally that bear that responsibility. In particular, courts may (understandably) lack the requisite technical competence to properly understand how these technologies actually work 'under the hood', and hence to properly grasp the full extent of their power, and potential for abuse. As constitutional lawyers and legal scholars, we too have a responsibility to maintain and foster the rule of law project. But if we are to do this effectively, we also need to acquire the necessary technological competence and to understand their real-world implications. We cannot and should not accept at face value the promises made by those who exhort our governments, law enforcement authorities and national security agencies to take up these technological tools. We, too, need to look inside the 'black box' of these technologies if we are to take our constitutional principles seriously. In particular, because these technologies are already exerting revealing the ways in which they are adversely affecting our collective life in profound ways, they are *not* simply more advanced versions of our existing technologies. Hence it should primarily be for the community at large to debate and determine whether to permit their use and if so, on what terms. In other words, our democratic institutions must play a pro-active role that nurtures and fosters meaningful public debate and participation if these powerful networked digital technologies are to be our servants and not our masters. My final word, then, is about the need to create and maintain institutions and regimes of governance that

[22] Consider, for example, the opportunities provided by the 'necessity' test: Gerards, J., "How to improve the necessity test of the European Court of Human Rights." *International Journal of Constitutional Law* 11.2 (2013): 466-490.

have both the necessary technical competence and democratic legitimacy to ensure that our constitutional principles are translated into meaningful safeguards that can be operationalised and enforced on the ground. It is not enough for us to champion the value of constitutional principles in a networked digital age: we need to make them real.

Karen Yeung

3 March 2022