

# ***Defending the Rule of Law from Threats Posed by AI-Enabled Surveillance Systems in the Hands of Law Enforcement Authorities\****

**Karen Yeung**

(Professor of Law, Ethics and Informatics, Birmingham Law School and School of Computer Science)

---

**ABSTRACT** This concluding article reflects on the preceding contributions taken as a whole. It argues that they reflect a troubling turn towards authoritarianism, and calls on scholars to take forward the task of critical inquiry to facilitate urgently needed democratic debate to help our communities decide on and establish the boundaries of legitimate and lawful use of facial recognition technologies.

---

**KEYWORDS:** Facial Recognition Technologies - Democratic Trust

---

**TABLE OF CONTENTS:** 1. Introduction. – 2. Setting the scene: what explains LEA's interest in FRT?. – 3. LEA experimentation at the local level with significant national variation. – 4. Rule of law 'gaslighting' and the authoritarian turn. – 5. What can we do?.

---

## **1. Introduction**

In concluding this invaluable and important collection, I must begin by expressing my gratitude and congratulations to Caroline Lequesne for her vision, commitment and tireless effort in convening an international scientific conference on the subject matter of this volume, hosted in true French style, at Le Saint Paul, Nice, earlier this year.<sup>1</sup> The rich, stimulating and occasionally confrontational discussions between legal scholars and those working at the 'sharp end' of law enforcement practice, including officials from data protection authorities and law enforcement authorities, drew into high relief both (a) the appeal of these technologies to law enforcement authorities (LEAs) entrusted with the unenviable task of responding to, investigating, prosecuting and seeking to prevent criminal offences and to keep the public safe from wrongful harm, and (b) the seriousness and significance of the threat which the prospect of widespread use of facial recognition technologies (FRT) by LEAs poses to basic democratic rights and freedoms, particularly given the ongoing lack of legal

certainty concerning the scope of its lawful and legitimate use. In keeping with the French tradition, I was invited to offer concluding remarks to close the conference. This prompted me to pay careful attention, taking notes while listening attentively to the presentations and discussions. In producing these concluding reflections, I have revisited those notes with the benefit of the written contributions which make up this volume, stepping back from their detail to take a more synoptic, bird's eye view to try and discern general directions of travel and recurring themes.

But before proceeding, I shall 'nail my colours to the mast'. I am not a disinterested and unbiased observer in debates about the use of FRT (and other AI-enabled biometric surveillance systems) by LEAs in self-described liberal democratic communities with well-established rule of law systems, to which I have the luxury and privilege of belonging. As a legal and regulatory governance scholar who has spent more than a decade of my thirty year academic career critically examining the governance of, and through, networked digital technologies, I have repeatedly highlighted the threats and dangers which the unthinking embrace of networked digital technologies (including but not limited to FRT) for ostensibly public purposes threatens to erode what I call the 'socio-technical foundations for political

---

\* Article submitted to double-blind peer review.

I am grateful to Emma Rengers for comments on an earlier draft. All errors remain my own.

<sup>1</sup> International Conference, *Law Enforcement Technologies in the Realm of Facial Recognition*, 13-14 March, Nice. Le Saint Paul. Hosted by the Université Côte d'Azur.

freedom<sup>2</sup> and their capacity to corrode the fragile bond of trust between individuals and the state, and between individuals *inter se*, upon which the contemporary rule of law rests. It is these foundational threats which the ill-considered embrace of digital transformation poses to the rule of law that I will return to in these closing reflections. But first, I will briefly contextualise the growing interest and diffusion of FRT systems by LEAs in contemporary democratic states, and draw out some common themes which emerge from looking across these contributions as a whole.

## 2. *Setting the scene: what explains LEAs' interest in FRT?*

The contributions in this volume testify to the growing enthusiasm of LEAs from across Europe and the USA to deploy FRT for various purposes across a wide range of settings, reflecting the embrace of data systems and practices in the public sector generally. To that end, I have argued that the take-up of digital automation, algorithmic decision-making and data-driven technologies (which I refer to as 'digital machines') in public administration across many countries from around 2010 onwards is sufficiently distinctive, important and widespread that it constitutes an emergent public sector reform movement which I call the 'New Public Analytics'.<sup>3</sup> This movement has been fuelled by a conjunction of technological advances and socio-economic factors, providing fertile soil in which the seeds for experimentation with networked digital systems, and their permanent deployment, have taken root. Chief among them have been a set of technical advances, including the emergence of the internet and the rise of cloud computing through which data can be stored, processed and managed on remote servers in real-time. These have enabled the rapid and widespread take-up and diffusion of internet-enabled

services and 'smart' devices that have become commonplace (at least in highly industrialised countries), which have, in turn, facilitated the ongoing 'data deluge'. Together with advances in machine learning, these technological developments have precipitated the rise of 'big data analytics' (or simply 'big data') including major advances in the field of computer vision thanks to the use of deep learning techniques, which entail the automated application of machine learning algorithms parsed on massive data sets to identify and analyse objects of interest, and to predict their likely behaviour, whether that be individual purchasing behaviours now routinely tracked by online retailers to inform automated ad delivery, to the automated identification of visual signs of urban decay to be prioritised for repair.

In the commercial sphere, these technologies have fuelled the rapid, meteoric rise of digital platforms and the so-called 'platform economy' which rely on automated digital intermediation, utilising machine learning algorithms to identify, distribute and deliver personalised media content and services to users in real-time. In the public sector, the promise of greater efficiency and effectiveness in carrying out a wide range of tasks through automation (which these technological advances enable) is especially alluring, as the pursuit of austerity policies have resulted in the savage reduction of public sector budgets. In addition, the extraordinary success of digital platforms in commercial settings and a pervasive rhetoric in which digital innovation is celebrated as an intrinsic good in and of itself (irrespective of its real world consequences including whether it in fact generates public benefits or any unintended adverse effects) has fuelled a desire by public authorities to cast themselves as tech-savvy 'innovators' rather than old-fashioned bureaucrats wedded to outdated practices, making them attractive prey to well-heeled global technology consultants eager to peddle their 'data-driven solutions' with glittering promises of better, faster, cheaper and more personalised public sector processes and outcomes. Although facial recognition technologies have been used for law enforcement purposes since the early 2000s,<sup>4</sup>

<sup>2</sup> K. Yeung, *A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework*, Council of Europe Report, DGI(2019)05, 2019, available at: <https://rm.coe.int/draft-study-of-the-implications-of-advanced-digital-technologiesinclu/16808ef255> (Accessed 15 July 2025)

<sup>3</sup> K. Yeung, *The New Public Analytics as an Emerging Paradigm in Public Administration*, in *Tilburg Law Review*, vol. 27, n. 2, 2022, 1-32, DOI: 10.5334/tlr.303.

<sup>4</sup> Facial recognition technology gained international attention when it was used during the Super Bowl in 2001 to scan the faces of attendees for potential criminals: <https://facit.ai/insights/evolution-of-facial-rec>

it was not until the development of ‘deep learning’ techniques and their application to machine vision through which major improvements in the accuracy of image recognition occurred, that automated facial recognition technologies began mainstreaming from 2010 onwards. In particular, Apple’s introduction of Face ID in 2017<sup>5</sup> brought FRT to millions of users worldwide, through which face unlocking became a popular means to conveniently and efficiently verify a user’s identity. It is the capacity to automate the task of recognising individual identities from facial images in real time, at a distance and at scale, and to facilitate the automated identification of individual’s behavioural patterns and of multiple individuals within crowded settings, that is critical to understanding its attractions to LEAs. Before examining those capabilities in the hands of LEAs, why they provoke controversy, and their implications for the rule of law, I turn first to the general trends and directions of travel that can be discerned by reading across the contributions in this volume.

### **3. LEA experimentation at the local level with significant national variation**

One of the most striking and significant contributions of this volume (and the Nice conference at which earlier drafts of many individual chapters were presented and discussed) lies in the broader landscape which is revealed by surveying the ongoing responses of LEAs to the ready availability of FRT systems. It offers an overarching and thus unique vantage point that is considerably more than the sum of its individual parts. For me, four features of the topography of this larger landscape stood out. Firstly, it reveals a keen interest by LEAs across the globe in adopting FRT (except for Canada), including western liberal democratic states in which respect for the liberty and freedom of the individual is claimed to be a cherished political and constitutional commitment. Secondly, that interest has taken the form of site-specific experimentation in local, urban environments, particularly where large numbers of people gather or pass by. Thirdly, there is a striking lack of appetite by national lawmakers to adopt FRT-specific laws to

govern and guide their lawful use, whether by law enforcement authorities or other organisations. Fourthly, there is a notable lack of transparency concerning these local level experiments which appear to have proceeded without, as Elizabeth Joh’s thought experiment highlights, the rigour and guardrails that apply to the conduct of research and experimentation on human subjects which is governed by the Declaration of Helsinki, which demands express and informed consent of each and every participant and for which institutional ethical approval is required before it can proceed.<sup>6</sup> Instead, the conduct of these local experiments appears to lack systematic oversight and accountability and may have been carried out without consultation with affected communities, or even—in some cases—data protection authorities. This lack of local-level transparency translates to a general, across-the-board lack of transparency, even across European states, in the absence of a pan-European public register of FRT usage by LEAs.<sup>7</sup> As Katy Kinsey remarked (albeit when commenting on the US experience) during the conference, LEA use of FRT is ‘widespread but unaccounted and unaccountable.’

The lack of clear legislative guidance has created an expansive ‘legal grey area’, providing hospitable conditions in which local-level experimentation by LEAs has proceeded largely hidden in plain sight. While lively contestation about the legality of FRT continues (as the contributions to this volume attest), these take place against the backdrop of general privacy and data protection laws established in an earlier technological era long before automated biometric sensing systems were readily available and easily configurable to meet the specific needs and preferences of organisations wishing to deploy them. In the European context, it has been left to data protection authorities to respond, while civil liberty organisations have found themselves

ognition-technology (Accessed 1 July 2025).

<sup>5</sup> <https://support.apple.com/en-gb/108411> (Accessed 11 July 2025).

<sup>6</sup> K. Yeung and W. Li, *From ‘Wild West’ to Responsible AI Testing ‘in-the-wild’: Lessons from Live Facial Recognition Testing by Law Enforcement Authorities in Europe*, in *Data & Policy*, 2025, in press.

<sup>7</sup> However, once the EU’s AI Act enters into force (which has now been thrown into doubt thanks to extensive tech industry lobbying) public authorities (or persons acting on their behalf) cannot lawfully deploy a high-risk AI system (which includes live FRT systems by law enforcement authorities) unless it has been registered in the EU database.

with little choice but to initiate legal proceedings petitioning national courts to intervene as fundamental rights protectors of last resort. Here we see considerable national variation. At one end of the spectrum, we see the ambitions of authoritarian states' technological ambitions in Saudi-Arabia's full-throated embrace of FRT and other biometric surveillance technologies in its visions for the NEOM megaproject. On the other, Canada's LEA's lack of keen interest in FRT governed only by generic privacy laws stands in direct contrast. The profile of LEA engagement with FRT in European states is mixed. On the one hand, the French and German data protection authorities have been vigilant in their approach to enforcement, backed by constitutional courts in upholding adherence to constitutional safeguards which condition and constrain interferences with fundamental rights and democratic freedoms, thereby preventing wholesale adoption in the absence of express legislative authority to proceed. On the other hand, law enforcement authorities in the UK and Greece have enthusiastically pressed ahead despite active and vocal opposition. More troublingly, we heard during the scientific conference that in both Britain and Greece, despite judicial rulings in which specific FRT deployments by LEAs have been ruled unlawful, this has not diminished LEAs' willingness to embrace and deploy them, dismissing assertions of illegality by claiming that they have complied with the conditions for lawful deployment but which, on closer inspection, are little more than superficial gestures that fall far short of meeting the conditions necessary to establish legal compliance.

#### **4. Rule of law 'gaslighting' and the authoritarian turn**

My overall impression from reading across this volume is that LEAs within democratic political communities have been taking up FRT by 'stealth' on a piecemeal, incremental basis, in the absence of a clear democratic mandate to proceed. Under conditions of significant uncertainty about what conditions (if any) FRT can lawfully be deployed, we see the appearance of familiar narratives of legitimacy. Hence law enforcement authorities insist that the deployment of FRT is necessary to preserve public safety and collective security, while civil liberties groups and public-spirited academics decry their use,

highlighting their capacity to enable mass surveillance by the state at scale with unparalleled chilling effects, stifling peaceful public protest, thereby amounting to a grossly disproportionate and unjustified interference with rights to privacy, freedom of assembly, and freedom of expression. On this familiar account, reminiscent of the debates which followed in the aftermath of the 9/11 attacks on New York's World Trade Centre, which precipitated a raft of draconian counter-terrorism measures that flew in the face of basic constitutional rights and freedoms, what is at stake is the legality of specific forms of executive action. Accordingly, it is the responsibility of courts to authoritatively determine whether specific actions taken by LEAs, including those entailing the use of novel technologies, transgress their warrants of legal authority.

But there is something more fundamental, and altogether more troubling, than the familiar tension between individual liberty and collective security provoking questions concerning the legality of executive action, dressed up in the latest technological garb. To understand what is at stake, we must dig below the surface to consider the meaning and significance of rule of law itself, in its 'thicker' foundational sense. Only then can we understand why the stakes are so high. Accordingly, we must return to the bedrock of constitutional principles upon which contemporary liberal democracies rest, back to the mid 18<sup>th</sup> century, long before computers or even photography had been invented. At that time, French political philosopher Montesquieu warned of the ever-present danger of the accrual of power without constraint and the threat of despotic rule. He argued that to guard against and prevent oppression of the people by the government, the latter's power must be limited, and this required institutional safeguards designed into the constitutional fabric to ensure that governmental power was distributed and constantly held in check. While first year students in British Law Schools typically encounter Montesquieu when introduced to the separation of powers as a principle of constitutional law, it is the emphasis Montesquieu places on the need for *institutional* restraint on the exercise of governmental authority which deserves emphasis. In liberal constitutional democratic states, the rule of law is inherently

asymmetrical. Hence, individuals are free and entitled to do as they please except that which the law prohibits, while the executive, on the other hand, can do nothing except that which the law allows.<sup>8</sup> Canadian constitutional and legal philosopher David Dyzenhaus refers to this asymmetry as the ‘compulsion of legality’, reflecting the widely shared acceptance by democratic governments that it is a necessary condition of legitimate state action that public officials who perform any action have a legal warrant: meaning that there is in *pre-existing law* an authorisation for public officials to act in the relevant manner. Yet attempts by LEAs to deploy FRT under the guise of local ‘experimentation’, particularly when used to parse the face of a single person, let alone tens of thousands of individuals who have committed no crime and pose no threat to anyone, has no clear pre-existing legislative warrant. For LEAs to proceed in this way constitutes an assault on the rule of law, through which the executive branch of government seeks to arrogate to itself warrants of legal authority which have not been conferred upon them by the community’s democratic legislature.

But a further assault on the rule of law can arise when law enforcement authorities deploy FRT due to its novel and sophisticated capabilities with the aim of identifying individuals who are ‘of interest’ to them, particularly when used for real-time surveillance of tens of thousands of people en masse in open public settings, the overwhelming majority of whom are going about their own business in an entirely law-abiding manner. In so doing, the basic and ancient presumption of innocence is inverted.<sup>9</sup> Thousands of ordinary people are, in effect, placed under suspicion by technological default so that it then becomes incumbent upon them to demonstrate that their actions were in fact benign should they be singled out for attention. What makes this rule of law assault so disturbing is not merely the way in which it betrays one of the oldest and cherished legal principles designed to protect

the innocent from being convicted for crimes they did not commit, but because, in the interconnected, datafied world that is now our everyday experience, it also inverts and radically magnifies the asymmetry in power between the executive and the ordinary person.

As we have already noted, the basic contours of the relationship between the executive and the individual in constitutional democracies is constructed asymmetrically in favour of the individual, in recognition of both the opportunities and temptations for executive authorities to overreach the proper limits of the state’s coercive power, thereby leading to oppression and injustice. Yet it has become apparent since the meteoric rise of global digital platforms that those who have the technological, organisational and practical capacity to gather and aggregate data about individuals across a population in real-time thereby acquire extraordinary power, enabling the data-collector to acquire a synoptic view of an entire population at a highly granular level, in real time, while the individual who is parsed by the system may be completely unaware that they have been flagged as worthy ‘of interest’, let alone challenge or contest how or why they have been flagged. The net effect is to invert the democratic constitutional compact through which state-citizen relations are constructed. Thus, although asymmetry in power between the executive and the individual is *formally* allocated in favour of the individual, in social, organisational and technological *reality*, the deployment of FRT on a mass basis shifts the distribution of power firmly and decisively in favour of the executive. As Sellinger and Frischmann argue in their contribution to this volume, FRT is the perfect tool for authoritarian control.

But, for me, the most egregious assault on the rule of law evident can be found in selective instances in which FRT deployment by a LEA has been successfully challenged in court, yet this has failed to curb or significantly temper LEA adoption of FRT in the relevant state. In the UK and in Greece (at least according to the contribution in this volume), law enforcement authorities have been undaunted by these judicial rulings. Rather than proceeding cautiously, taking particular care to ensure that they put in place systematic safeguards to demonstrate that they have not exceeded their lawful authority based

<sup>8</sup> As British constitutional lawyer Adam Tomkins puts it, ‘the executive may do nothing without a clear legal authority first permitting its actions’: A. Tomkins, *Public Law*, Oxford, Oxford University Press, 2003, 78.

<sup>9</sup> The right to the presumption of innocence has a long history in the French and English legal traditions, but can be traced back to ancient times to the Code of Hammurabi in Ancient Babylon, and the legal systems of ancient Greece and early Roman Law.

on the conditions set out in the court's judgement, we heard during the conference that they have instead continued and even expanded the frequency and scale at which FRT is deployed. To pre-emptively defend themselves against claims of illegality, these LEAs have simply pointed to various activities that they claim demonstrates their compliance with the law. On even a cursory inspection, such superficial indicators are in substance nothing of the sort. A vivid example of this 'rule of law gaslighting'<sup>10</sup> can be found in news reports of the Essex police use of FRT highlighted by Computer Weekly based on journalistic investigations referring to police documents obtained by Big Brother Watch through a series of freedom of information requests.<sup>11</sup> In response to powerful evidence demonstrating the lack of relevance and evidential foundations cited by the Essex police to demonstrate that they had conducted a mandatory equality impact assessment, in accordance with UK equality law (and which was one of the grounds upon which the Court of Appeal had found the earlier use of FRT by the South Wales police to be inadequate and thus unlawful), the Essex police spokesman simply responded 'We take our responsibility to meet our public sector equality duty very seriously' while boasting that '[t]here have been more than 50 deployments of our LFR vans, scanning 1.7 million faces, which have led to more than 200 positive alerts, and nearly 70 arrests.' Yet no account is offered concerning what kinds of offences those 70 people were arrested for, nor any attempt to explain why those deployments satisfied the legal test of necessity and proportion in a democratic society to justify the privacy intrusion of 1.7 million people. When invited by the investigative journalist to comment on why its equality impact assessment relied on the testing of a completely *different algorithm* (produced by an entirely different software firm) to the one employed by Essex police, and why it had not conducted or otherwise commissioned its own testing before

operationally deploying FRT, no explanation was forthcoming. Moreover, my own examination of the documents obtained from Big Brother Watch's FOI request left me appalled by just how baseless and completely inadequate those documents were in demonstrating that basic legal requirements articulated by the Court of Appeal in the *Bridges* case had been met.<sup>12</sup> If that documentation is intended to demonstrate how 'very seriously' law enforcement authorities in Britain take their responsibility to meet their public sector equality duties, then it reveals both a profound level of ignorance about their legal obligations, and a reckless disregard for their moral and legal obligations to demonstrate respect for the rights of women and ethnic, racial, religious and other minorities and the basic right of *all* British peoples to expect British police to obey and uphold the self-same law that citizens are expected to abide by.

It is this 'rule of law gaslighting' by LEAs that is, for me, the most disturbing assault on the rule of law. In my view, this constitutes an egregious breach of public trust and a serious dereliction by the police of their moral duty to uphold and ensure their obedience to law. It reflects a complete failure by LEAs to recognise that they hold a privileged and exclusive monopoly to wield the coercive power of the state against the people and which, in constitutional democracies, is and must be constrained by law, and which they are morally and constitutionally obliged to exercise with great care in acting, as essence, as fiduciaries for and on behalf of the British public.<sup>13</sup> As I shall shortly explain, the logical consequences and corollary of this reckless indifference to legal obedience is to invert the entire foundation of the 'social contract' articulated centuries earlier by distinguished liberal political philosophers, thereby embarking upon a slide towards

<sup>10</sup> The Oxford English Dictionary defines gaslighting as 'The action or process of manipulating a person by psychological means into questioning his or her own sanity'.

<sup>11</sup> S.K. Skelton, *Essex Police discloses 'incoherent' facial recognition assessment*, in *Computer Weekly*, 23 May 2025, available at: [www.computerweekly.com/news/366624473/Essex-Police-disclose-incoherent-facial-recognition-assessment](http://www.computerweekly.com/news/366624473/Essex-Police-disclose-incoherent-facial-recognition-assessment).

<sup>12</sup> The Computer Weekly report cites me as stating that 'There are many platitudes about being ethical, but there's nothing concrete indicating how they propose to meet the legal tests of necessity and proportionality... In liberal democratic societies, every single decision about an individual by the police made without their consent must be justified in accordance with law. That means that the police must be able to justify and defend the reasons why every single person whose face is uploaded to the facial recognition watchlist meets the legal test, based on their specific operational purpose.' *Ibid.*

<sup>13</sup> D. Galligan, *Law in Modern Society*, Oxford, Oxford University Press, 2006.

authoritarianism which is rapidly and terrifyingly being played out in the USA under Trump's presidency as this volume goes to press.

### **5. What can we do?**

What, then, are we to do to halt the ongoing assault on the rule of law wrought by LEAs' embrace of FRT by stealth? One of the most significant contributions of this volume lies in revealing what is going on across the board, while highlighting the serious and systematic lack of transparency concerning how FRT is being taken up by LEAs across contemporary democratic states without any sustained and open public scrutiny or discussion about whether, and to what extent, they serve the interests and needs of the community and if so, at what cost. It demonstrates why collaborative initiatives between scholars from across the globe is so important, enabling us to see, and call attention to, this larger landscape. So, at the very least we owe it to the world to continue these vital and invaluable collaborative conversations.

But that is not enough. Although we are right to celebrate successful litigation challenging specific FRT deployments, in which the courts have insisted on ensuring that LEAs eager to deploy FRT respect the limits of the law in the absence of clear warrants of legislative authority to proceed, judicial protection is insufficient for several systematic and structural reasons. First, as is well known, judicial decision-making is sporadic, piecemeal and reliant on the willingness of others who have the commitment, ability and, most importantly, the resources to support the costs and commitment involved in litigating a case through to judgement. Yet we all know that the capacity of civil society organisations and digital activists is limited and dwindling, and cannot fairly be expected to stem the tide of FRT embrace by organisations in the face of an ever-growing digital tech industry and the global management consultants who champion the virtues of software 'solutions' to address the challenges faced by cash-strapped law enforcement authorities. Secondly, due to the separation of powers principle, courts are constitutionally required to demonstrate deference to the substantive discretion of the executive, including law enforcement authorities. Accordingly, in evaluating

whether the 'necessity' test is met to justify an interference with the right to privacy, for example, this only requires that the executive demonstrate a rational connection between the proposed rights-intrusive measure and the legitimate collective goal (typically, to protect public safety). This is not a terribly demanding test.<sup>14</sup> Thus, courts are not the most suitable forum in which invocation by LEAs that 'FRT enhances public safety' can be tested, given the absence of systematic and demonstrable evidence that FRT actually delivers on the promise of enhanced security in real world practice. Finally, as I pointed out in an earlier lecture, judges typically lack the level of technical competence necessary to recognise and properly appraise what is 'at stake' in debates about the legality of a specific technological deployment.<sup>15</sup>

Rather, discussion and debate concerning whether it should be legally permissible for LEAs to deploy FRT and if so, on what terms, is for our communities to discuss and debate on an open and informed basis. Accordingly, we can play an important role by supporting our democratically elected representatives and institutions by nurturing and fostering meaningful public debate concerning the benefits and threats posed by these powerful networked digital technologies so that the community can decide for itself to what extent they are willing for law enforcement authorities to deploy them, and on what terms. Yet this collection indicates that legislative reform initiatives have often withered on the vine, with our legislatures showing little appetite to engage in these debates let alone initiate draft legislation to establish concrete safeguards to guide and govern the use of FRT by LEAs or their more general take-up by other public and private deployers. In this respect, our law-makers have let us down. The absence of specific legislative rules to guide and govern their use has provided ample practical opportunities for LEAs to proceed with local FRT experiments.

Why have our legislators been so reluctant to convene and foster democratic deliberation and take the legislative initiative? For EU member states, reluctance to introduce

<sup>14</sup> See J. Gerards, *How to improve the necessity test of the European Court of Human Rights*, in *International Journal of Constitutional Law*, vol. 11, n. 2, 2013, 466-490.

<sup>15</sup> K. Yeung, *Constitutional Principles in a Networked Digital Age*, 2022, available via SSRN network.

national-level laws might be explained on the basis that the EU AI Act has been under negotiation for some years, so it was quite reasonable for national legislators to wait until the EU legislative framework was in place.<sup>16</sup> I would not be surprised, however, if what Julie Cohen has called the ‘surveillance-innovation’ complex has played a significant role. Cohen argues that the emerging surveillance-innovation complex is a contemporary variant of the surveillance-industrial complex, the latter referring to the symbiotic relationship between state surveillance and private sector producers of surveillance technologies.<sup>17</sup> She describes the surveillance-innovation complex as a:

‘new, politically opportunistic phase of this symbiosis, one that casts surveillance in an unambiguously progressive light and repositions it as a modality of economic growth.... and ...a discursive and ideological formation...to advance the instrumental goal of holding the regulatory state at arm’s length’.<sup>18</sup>

I suspect that there is indeed both ideological and political capture by the tech industry lobby at work in seeking to account for legislative inaction in the face of sustained and strident opposition to the wholesale take-up of FRT by LEAs. If so, then our work as lawyers and legal academics is even more urgent and important. It becomes incumbent upon us and our collaborators to inform and carry forward public debate concerning the use of FRT in society, including their use by LEAs, in a manner that will best facilitate wise, informed democratic debate and collective decision making. In this way we can serve our communities, and our law-makers, by helping them to acquire a clearer and clear-eyed independent view, based on analytically rigorous independent research, of what is at stake, and the extent to which our communities are willing to permit, or even

encourage, the use of FRT by LEAs.

In supporting and facilitating public debate, we must do more than decry the ever more powerful surveillance apparatus which the executive appears eager to embrace. Rather, we need to undertake sustained, independent and analytically rigorous research that can help the public, and our law-makers, better understand these technologies and their capabilities and limitations. That should, in turn, allow them to arrive at a more informed view of what, if any, and on what terms, we wish collectively to support and to limit FRT use by LEAs in carrying out their functions. To this end, I offer the following suggestions and lines for productive inquiry.

Firstly, we must vigorously contest assertions by both the tech industry and the LEAs keen to deploy FRT and other digital technologies that do not withstand critical scrutiny. This includes unthinking belief that innovation of any kind is intrinsically good,<sup>19</sup> but it is especially important to highlight the need for evidence claims that FRT use by LEAs ‘makes us safer’. Although LEAs claim that FRT considerably enhances their ability to investigate crime and prevent violence more effectively, efficiently and precisely, there is little by way of sustained evidence to demonstrate that it delivers these alleged benefits in real world contexts and in what way. This evidential gap remains unaddressed. At the very least, we should draw attention to this gap and demand that LEAs provide us with evidence to support the claim made by General Perrow at the Nice conference that if we do not allow our LEAs to deploy FRT, ‘you will not be safe.’<sup>20</sup>

Secondly, we must engage in more fine-grained, nuanced analysis which examines the specific technological and organisation configurations in which FRT can be embedded for use by LEAs. This entails paying close attention to the specific ‘affordances’ of FRT systems, particularly their novel capabilities and the specific configurations and applications through which

<sup>16</sup> Unfortunately, the AI Act ultimately failed to provide a set of clear, bright-line rules identifying the specific conditions under which biometric technologies are legally permissible, preferring instead to regulate them as ‘high-risk AI systems’ which must be subject to a set of ‘essential requirements’ before they can be placed on the market, except in relation to the use of live FRT by LEAs which was ultimately permitted, albeit with a number of specific ex ante and ex post safeguards.

<sup>17</sup> J. Cohen, *The Surveillance-Innovation Complex: The Irony of the Participatory Turn*, 2015, available via SSRN network.

<sup>18</sup> *Ibid.*

<sup>19</sup> K. Yeung, *Dispelling the Digital Enchantment: how can we move beyond its destructive influence and reclaim our right to an open future?*, in *Prometheus*, vol. 39, n. 1, 2023, 8-27, DOI: 10.13169/prometheus.39.1.0008

<sup>20</sup> P. Perrott, *Law Enforcement Perspectives*, Session III. International Conference, *Law Enforcement in the Realm of Facial Recognition Technologies*, Nice, 13-14 March, 2025.

FRT can be deployed.

In particular, in a research report which I wrote for the Council of Europe in 2019, I endorsed Cohen's claim that to ensure that human rights can be operationalised in an era of smart environments, we need to 'take affordances seriously', otherwise our rights will be ineffective. According to affordance theory, the design of our technological objects and environments conditions and constrains the possibilities for action, including the range of actions and responses which the design of the object 'affords' to the user. Thus, Cohen argues that once we recognise that smart digital technologies continually, immanently and pre-emptively mediate our beliefs and choices, then our legal discourse about human rights (including privacy) can be understood as incomplete. This means more than merely extending our rights discourse. Rather, she calls upon us to develop a different vernacular for rights discourse that recognises the central role of socio-technical configurations in affording and constraining the freedoms and capabilities that people in fact enjoy and encompass our socio-technical architecture, in which rights can be conceived in terms of affordances as a practical matter in ways that 'speak with effective force to new kinds of material and operational considerations.'<sup>21</sup>

This is precisely what we must do in subjecting FRT to critical scrutiny in reflecting on their implications for the rights, interests and the democratic health of our communities. As Claude Castelluccia observed in his conference presentation, 'there are fifty shades of FRT, so clarify what you mean when you talk about it'. He is absolutely right. I therefore encourage researchers to focus their inquiries on specific technological configurations, to investigate FRT through the development of more fine-grained taxonomies based, for example, on their:

- (i) *law enforcement purpose*, ranging from identifying 'wanted' or 'interesting' individuals in real time, predictively identifying emerging sites of public unrest and unruly behaviour, or for retrospective automatically reviewed video footage of criminal activity to identify, investigate and prosecute those involved;
- (ii) *temporal dimensions*, whether retrospective, real time or aimed at predicting

future-criminal conduct;

(iii) *geographic and spatial dimensions*, including the nature, kind and contours of the places and locations in which FRT is deployed. For example, how effective is FRT in promoting legitimate law enforcement purposes when deployed in dynamic, open and chaotic spaces in comparison to environments that are stable or controlled, and to what extent is that space capable of being 'avoidable' by individuals who wish to avoid being parsed by the FRT cameras involved?

(iv) *who has authority to deploy the technology, and for what purpose and subject to what kind of constraints, legal or technological?* For example, recent pilot projects in the UK enable individual police officers to use their smart devices to photograph an individual while 'on the beat', and automatically match that image against a centralised facial database to identify that person in real time (so-called 'Real Time Recognition'). Given the egregious abuse of trust and power by the London police officer Wayne Couzens who kidnapped, raped and murdered 33 year old Sarah Everard in 2021 while she was out walking in London alone one evening, by falsely claiming she was wanted by police before handcuffing her. I find it staggering that any responsible senior police officer believes that this technology should be made available to each and every police officer, let alone considers it a necessary and proportionate interference with privacy in a democratic society;

(v) *what are the dimensions and contents of the reference databases ('watchlists') against which automated facial matching is to be parsed?* Whose faces are uploaded to LEA FRT reference databases, and on what basis and legal grounds can their inclusion be justified?

By undertaking more fine-grained analysis which attends to affordances and social contexts of deployment, we can investigate in a more targeted and precise fashion how the technological capabilities and affordances of FRT systems are translated into real world effects. This can help to produce evidence to assess whether, and under what conditions, FRT can genuinely contribute to a specific, lawful and legitimate law enforcement purpose, whether that be to more effectively and efficiently investigate the commission of

<sup>21</sup> J. Cohen, *Affording Fundamental Rights*, in *Critical Analysis of Law*, vol. 4, n. 1, 2017, 1-13.

crimes and bring offenders to justice, or whether it does in fact facilitate the more efficient identification of those wanted for serious crimes who are known to be at large in and around a particular location, and under what conditions the potential for over-reach should be considered unnecessary and/or disproportionate. At the same time, this kind of fine-grained analysis can help inform the development of ‘human rights by design’ measures through which technical safeguards can be introduced and mandated as a condition of lawful deployment. For example, in a forthcoming paper I argue that FRT systems intended for live deployment in public spaces by LEAs could be designed to strictly limit the number of facial images that are uploaded one-by-one (thereby preventing ‘bulk import’) when accompanied by a completed template outlining the legal justification for upload and a description of the source image. Such measures would eliminate ‘by design’ the temptation faced by law enforcement authorities to upload as many faces as they wish rather than restricting themselves to persons of interest for whom rights-intrusive measures can be legally justified, while deterring the unlawful images scraped from public websites. Analysis of the kind that I am advocating for is also necessary to help inform the responsible testing of FRT systems in real-world conditions. Experimentation and testing of FRT systems in real world conditions is necessary and welcome, but only if they are undertaken on a legally, ethically and epistemically responsible basis, that is strictly supervised, controlled and fully accountable.<sup>22</sup> Research insight and independent evidence of this kind can then provide the foundations to advocate for a more specific set of policy guidance and blueprint for our law makers in producing clearer legislative guardrails and oversight measures to guide and govern the use of this powerful but dangerous technology. Research insights of this kind should, in turn, enable us to identify the conditions in which FRT deployment by LEAs should be regarded as illegitimate and therefore legally prohibited. This kind of insight will enable us to identify and articulate the specific safeguards and governance mechanisms that must be in place,

both of a technical and organisational kind, to prevent, restrict and hold accountable those who develop, distribute and deploy them. So, for example, the most serious threats to democracy, including real-time FRT deployment on peaceful protestors, should be prohibited outright in the absence of evidence to indicate that it is likely to turn violent. On the other hand, we might be willing to allow the use of drone-mounted FRT cameras that are configured with watchlists that are technologically restricted to allow the uploading of only a very limited number of facial images, to identify a specific individual who is known to be on the run following the commission of a serious, violent criminal act and is reasonably believed to pose an imminent and serious threat to public safety, particularly if prior authorisation from an appropriate judicial officer is obtained in advance and the terms of a systematic record of approved deployments is retained and made publicly available.

In short, there is much work to be done. In encouraging you to continue this important work, with all of the analytical, legal, technical and intellectual resources you can muster, I recognise that we can find ourselves in a climate of despair. But in the face of on-going assault on the rule of law entailed by the take-up of FRT by LEAs in the absence of clear legal authority to proceed is something we must continue to oppose and resist. What makes the rule of law gaslighting that some LEAs have displayed so egregious is the ignorance and contempt which it displays towards the fragile bond of trust upon which the rule of law ultimately rests. According to law and society scholar Denis Galligan, the willingness of both governors and the governed within modern legal orders to accept that the law rules, and what gives law its legitimacy lies ultimately in the *reasons* for their acceptance. And these reasons lie, ultimately, in the social goods that modern societies expect the legal system to generate: that is, the social goods of security of person and property, and the stability of private arrangements and transactions as displayed in contracts and promises. Galligan points out that the willingness of both governors and governed within modern legal orders to subscribe to these reasons lies in the special bond of trust between them, which can be understood in terms of public trust in which officials (particularly our law enforcement

<sup>22</sup> K. Yeung and W. Li, *From ‘Wild West’ to Responsible AI Testing ‘in-the-wild’*.

officials) hold power – not for themselves or for the interests they serve, but on trust for and on behalf of the people they are expected to serve and whose power they ultimately exercise.<sup>23</sup> As I have previously highlighted, this bond of trust is a fragile and unstable one. It cannot be manufactured or artificially fabricated because it is ultimately rooted in the norms and habits that are deeply ingrained in each individual, and, although characterised in different ways by constitutional scholars such as Dicey, Oakeshott and Habermas, they all regard the rule of law as *learned* rather than inherent, that is necessarily specific to a time and place. Although conventional legal enforcement is underpinned by the coercive power of the state to compel compliance, ultimately the effectiveness of the legal guarantee rests on the *uncoerced acceptance* of legal subjects to respect its commands.

This brings me to the concerns which I referred to at the beginning of this short conclusion, highlighting the dangers which the unthinking embrace of advanced digital technologies poses to the socio-technical foundations of political freedom, and why the stakes in the uncertainty about the lawful and legitimate use of FRT by LEAs are so high. If our public safety comes to rely on the deployment of ubiquitous real-time FRT systems to provide the collective goods we currently associate with the stability and security provided by the rule of law that underpins modern legal orders, we may be in danger of losing the fundamental, mutual self-restraint that forms the bedrock of the rule of law in modern legal systems that is made possible through the gradual emergence over time through what Alexander de Tocqueville elegantly termed ‘the habits of the heart’ and which is deeply engrained in each individual. It is on these fragile yet enduring social foundations through which sovereign power within modern legal orders is constrained and rendered accountable. The creeping adoption of FRT systems by our law enforcement officials without open public debate, deliberation, and clear and effective safeguards, particularly in the context of a resurgence of populism and far-right sympathisers, reveals a deeply troubling slide towards authoritarian reconfiguration of the

social contract to which we have not consented. We are at a critical juncture in the ongoing digital transformation project. We must work to help our communities, law-makers and law enforcement authorities understand why FRT offers us a seductive false promise: beckoning us to place our faith in technological prowess rather than the capacity for mutual respect and self-restraint upon which the rule of law ultimately rests, undermining the very foundations of democratic community and threatening to invert the social contract upon which our cherished freedom under law depends.<sup>24</sup>

<sup>23</sup> P. Finn, *The Forgotten “Trust”: The People and the State*, in Malcolm Cope (ed.), *Equity: Issues and Trends*, Sydney, Federation Press, 1995.

<sup>24</sup> M. Loewe, A. El-Haddad, M. Furness, A. Houdret and T. Zintl, *Drivers of change in social contracts: Building a conceptual framework*, in *Mediterranean Politics*, 2024, 1-27, <https://doi.org/10.1080/13629395.2024.2379733>.

