University of BRISTOL

Law Research Paper Series
Paper #003 2020

CCTV, Data Analytics and Privacy: The Baby and the Bathwater

Professor Andrew Charlesworth
University of Bristol Law School
Wills Memorial Building
Queen's Road
Bristol
BS8 1RJ

bristol.ac.uk/law/research/legal-research -papers

ISSN 2515-897X

CCTV, Data Analytics and Privacy: The Baby and the Bathwater

Andrew Charlesworth, Professor of Law, Innovation & Society, University of Bristol Law School

Abstract

While it can be criticised for polemic and hyperbolic language, the casual and inconsistent use of statistics and the trailing of unsupported conspiracy theories, commentary on the use of CCTV analytics by campaigning groups and others can raise important points. There is clearly a need for a defined regulatory approach to developing appropriate processes and safeguards to permit such analytics to be accountably incorporated into legitimate surveillance practices in public and private sectors. The problems with the nature of such commentary lie in its largely undiscriminating and scattergun approach to the technologies, and in the tendency of legislators and regulators to respond to its polarising rhetoric rather than promote critical review. The danger is that by conflating the capabilities of technology with wider systemic problems of poor organisational processes, lax regulatory standards and inadequate oversight, campaigning groups consistently overlook the fact that advances in the technology may contain the seeds of effective regulatory control. A more nuanced and thoughtful approach is required to the issue of CCTV analytics to avoid potential regulatory gains via the technology itself being lost in a wave of underinformed and poorly focused reaction.

Summary

The public debate over the use of CCTV analytics, such as automated facial recognition and other AI-supported techniques, is currently distorted. Both the media and relevant regulators have had their attention captured by commentators whose approach to the technologies appears to be, or is presented as, unfailingly negative. There often seems to be little interest in engaging in a debate about the effective regulation of CCTV analytics in the wider context of appropriate controls to be placed on the use of data and data analytics generally. It is suggested that this is because the dominant discourse chooses to promote CCTV footage, when used in 'artificial intelligence' or algorithmic sorting, as requiring different treatment from other forms of personal data. While images might perhaps be perceived as being more personal, more connected to the individual, than other forms of personal data, in practice there is no real justification for making such a distinction.

In particular, materials produced by campaigning groups tend to be more concerned with driving home their authors' viewpoint than they are in engaging in wider critical thinking about the problem they address. The issue is painted starkly in black and white – surveillance is bad, CCTV analytics in the form of Automatic Facial Recognition (AFR) is bad, police use of AFR is expanding "rapidly and recklessly" (BBW 2018, p.25), therefore UK public authorities should "immediately stop using automated facial recognition software with surveillance cameras" (BBW 2018, p.41). The evidence to support such conclusions is often cherrypicked, selectively and inconsistently presented, and almost exclusively negative. As a result, campaign group coverage tends to be a curious melange of credible argument, dramatic hyperbole or unsupported polemic, and in places, out-and-out conspiracy theory.

This type of rhetoric has come to dominate the debate about AFR because of the UK government's apparent reluctance to provide a detailed regulatory strategy, which has created a regulatory policy lacuna. This reluctance is exemplified by the recently published Home Office *Biometric Strategy* (2018). This long-delayed strategy document has been criticized by regulators and campaigning groups alike as containing little more than promises of future law and standards for AFR, without any details about what such law and standards might contain.

One might reasonably surmise that it is in the nature of pressure group publications to be partial in their review of a topic, partisan in their presentation, and polemic in their tone. It is problematic,

however, when the discourse around a topic becomes so polarised that there is little room for alternative viewpoints, ideas or evidence. In the debate around privacy and surveillance, this polarisation can be seen in views expressed by campaigning groups such as Liberty and Big Brother Watch - that surveillance is automatically repressive, that developments such as AFR are "fundamentally incompatible with human rights" (BBW 2018, p.9), and in the common countervailing argument of their opponents that "if you've got nothing to hide, you've got nothing to fear". The problem with such polarisation is that, despite the rhetoric, it is inevitable that an accommodation will have to be reached between the responsible and accountable use of CCTV analytics and human rights. Leaving the debate to the representatives of those polarities leads to the risk that innovative ways of achieving that accommodation are sidelined or rejected because they don't fit within one of the prevailing orthodoxies.

Ultimately the balance between acceptable implementation and protection of rights may be achieved through traditional legal means such as legislation, legal action and regulatory rules, but this is a slow and unpredictable process. Even where elements of legal protection are in place, as is the case with AFR, these can still be dismissed by critical observers as insufficiently robust, or inadequately overseen. Regulatory theorists would argue that seeking to regulate the use of CCTV analytics solely by legal intervention indicates a failure to make effective use of the full regulatory toolkit. To draw upon the work of Lessig and later writers, it is important to consider the use of other methods, or modalities, of regulation in tandem with the law. Lessig, writing in his 2000 book, *Code and other Laws of Cyberspace,* identified four primary modalities - law, market forces, social norms and architecture. It is the last of these that this paper identifies as a key neglected modality for the regulation of CCTV analytics. It is suggested that in the short to mid-term, key concerns about issues such as privacy and discrimination can be allayed by cultivating an understanding of how regulatory objectives can be hardwired into the developing technological architecture underpinning modern CCTV analytics. This will be a crucial step in ensuring such technologies can be accepted as controlled and legitimate tools for public and private sector activities.

Fear, Uncertainty and Doubt

When it comes to discussion of the future use of CCTV analytics, campaigning groups and academic commentators often take a deeply dystopian line, focusing on speculative abuses rather than on any positive aspects. For example, in the *New Scientist* magazine in June 2018, a report on a new drone camera surveillance/AI system that can identify violent behaviour in crowds contains the following comment from an academic: "What if this technology is used by non-democratic regimes to identify dissidents? Or by gangs to identify enemies?" One might reasonably respond, "What if it is? Do these potential negative uses instantly negate the potential beneficial uses?" Non-democratic regimes or gangs may make use of all kinds of otherwise socially useful technologies. ISIS uses drones to drop grenades, China uses firewall technologies to control access to information, the US uses medicinal sedatives and anaesthetics to execute prisoners. But we don't respond by banning those technologies (although we may, for instance, decide to regulate the sale of those technologies to certain types of customer). While journalists tend to seek quotable quotes from academics, simply publishing this type of what-if response suggests a failure to canvass critical thinking about how to obtain social benefits from a data technology while restricting the possibility of abuses.

In part, this is probably because images are often perceived as being more personal, more connected to the individual, than other forms of personal data. This perception tends to bring a higher level of emotional reaction to the debate, overshadowing the fact that, in terms of the use of AI, images are no more and no less than a dataset that can be processed automatically. As such, they can be, and are, given legal protection via the same forms of personal data protection practices that are used to protect other personal data datasets. Their use can also be regulated by mechanisms other than the law, as discussed below. However, if the regulatory debate becomes unnecessarily polarised through

recourse to misleading rhetoric, cherrypicked examples and statistics and unsupported assertions, then the opportunity for constructive consideration of novel regulatory options may be lost.

It is instructive to consider in detail a prime example of the difficulties in arguing a balanced and reasoned case for better regulation of a highly emotive subject. The publication in question is *Face Off: The Lawless Growth of Facial Recognition in UK Policing* (May 2018), which is allied to a high-profile media campaign and, according to *The Guardian* (June 2018), the threat of one or more future legal actions. In the pamphlet, the pressure group Big Brother Watch takes aim at the increased use of automated facial recognition technologies by police forces in the UK. The particular area of concern identified is the use of technology by state agencies, notably the police, to surveil large public gatherings, such as demonstrations, public festivals and football matches. The argument presented problematises the use of facial recognition technology, terming it intrusive, repressive, chilling, discriminatory and abusive. It emphasises the lack of explicit legislative control of the technology, and the lack of regulation and oversight of the image databases that are required for facial recognition to be viable. Yet, at the same time as drawing a worrying picture of the uncontrolled expansion of this seemingly coercive technology, the piece describes a very limited number of case studies across three police forces (out of the 45 UK territorial police forces), the details of which hardly present a compelling case for an impending dystopia. The case studies suggest that the police forces concerned have used the technology in a limited range of crowd environments and achieved less than impressive results.

The authors themselves appear vague both about what makes the technology so problematic and how this might be addressed. For example, they claim on the one hand that facial recognition algorithms are trained mainly using white faces and that this leads to more errors with minority faces (p.16), but on the other hand are opposed to its use in scenarios, like the Notting Hill Carnival, where the opportunity to improve that training might arise (p.17). They also express concern that biometric tracking might be used “in day-to-day policing for 'intelligence' purposes” (p.29). It is unclear why current non-algorithmic-based police surveillance, based perhaps on the use of CCTV and ‘super recognisers’ (individuals who have an above average ability to recognise faces), is fundamentally different in practical terms. Much emphasis is also placed on the notion that when AFR is used on live footage of public space citizens are “effectively asked for their papers without their consent or awareness" (p.7) or “increasingly subjected to identity checks while going about their daily lives” (p.30). This deliberate linking of a technology to totalitarian imagery is superficially powerful, but misleading; neither the existing use of CCTV analytics, nor the current UK legal and political framework, lends itself to the plausible realisation of such an outcome.

The evidence gathered in support of the authors’ arguments may appear similarly startling, until one starts to question its context and presentation. For example, when discussing the use of AFR in public spaces, the piece cites the example of football grounds. Even if one leaves aside the fact that football grounds are often not public spaces, any more than shopping malls or other privately-owned structures, the evidence of likely impact of AFR is sketchy – “supporter groups made clear the chilling effect it would have ... facial recognition cameras would result in “empty stands”” (p.14). Supporters’ groups, a largely self-selecting sample, have made similar claims in the past for compulsory seating (on safety grounds) and ID checks for ticketing (to prevent touting and hooliganism), yet football attendance in the UK appear buoyant. Is the use of a technology that permits the targeting of persistent disruptive or violent attendees really something that would concern the average fan? One thing is certain, the current cost of policing football is significant. An ITV report in 2017 suggested that policing football matches in London alone costs £12 million a year. At a time of police budget cuts, researching and trialling CCTV analytics that might reduce those costs in the longer term may seem like a reasonable option.

Equally, when reporting on the use of AFR at the Notting Hill Carnival (p.15), the authors claim that "Many of the people Big Brother Watch, StopWatch, and Liberty spoke to at Notting Hill Carnival 2017, where automated facial recognition was in use, were shocked and felt both uncomfortable and

targeted." Social science researchers are well aware of deliberate or inadvertent bias that may be imparted to survey results by the interviewees' perception of the person asking the questions and the nature of the questions. Subjects may be primed by the affiliation of the interviewer, and respond in ways that they think will 'suit' the interviewer. Without access to contextual information on the questions asked and how researchers presented themselves, the purported evidence generated is simply anecdotal. And to apply a well-worn phrase in academic research, "the plural of anecdote is not data."

Evidence in the pamphlet relating to police practice also lacks context. For example, in South Wales, use of AFR at 18 events led the police to "stage interventions with 31 innocent members of the public. 31 people incorrectly identified by the system were asked to prove their identity and thus their innocence." (p.28-30). Unfortunately, the reader cannot ascribe much weight to that figure without juxtaposing it against the number of innocent people that the police questioned at previous similar events where AFR was not used. Would that number be higher or lower? On this point the document is silent. The use of statistics, particularly those relating to matches and false-positives is inconsistent in approach throughout the document, and often leaves the reader unclear as to what is being claimed. For example, "[Metropolitan Police] use of automated facial recognition has resulted in 'matches' with less than 2% accuracy" (p.25); "the [German] system correctly matched volunteer images only 70–85% of the time" (p.35). Does this suggest that the latter system is a massive improvement on the former?

The pamphlet includes vignettes of the use of AFR in other countries. Of these four countries, Germany, Russia, China and the US, it is notable that only Germany has comprehensive data protection and surveillance laws similar to those of the UK, and that the trial of the technology in Germany has been subject to considerable oversight and public scrutiny. It is unclear what lesson, if any, the reader is to draw from the use of AFR in China and Russia, beyond the lesson that authoritarian regimes will tend to use technologies for authoritarian objectives. The US, too, is of limited value as a comparator, as the structure of US policing is very different from that of the UK, and the nature of the balance between privacy and public/private surveillance techniques is more often determined in the courts rather than in State or Federal legislatures.

The contributions provided by third parties (p.17-19 and 38-40) pad out the document, but ultimately add little more than unfocused anecdote, uncontextualised statistics such as "where the technology was able to make a match it was wrong 12% of the time for black and minority ethnic men, and 35% of the time for black and minority ethnic women," and unevidenced assertions: "facial recognition has been used almost as a propaganda tool" and "use at Notting Hill Carnival ... was likely part of the usual strategy of trying to persuade people not to come." Again, there is much angst about the adoption of AFR alongside new CCTV technologies like body-worn cameras, but little actual coherent argument about why the technology would be problematic. Initial evidence suggests that adoption of body-worn cameras by police has improved police-public encounters and relationships, and decreased police misconduct through enhanced legitimacy and accountability. It is unexplained how the introduction of AFR would cause matters to change for the worse.

Interestingly, only one of those contributions recognises, in passing, that a primary contributor to the growth of the use of AFR will undoubtedly be the private sector (p.38). The wider report is also largely silent on private sector use of AFR. Given that the boundary between the public and private sectors for personal data, including imagery, has repeatedly been shown to be highly porous, it seems strange that this relationship has not been more explicitly explored. The rollout of AFR in Apple's iPhone X and in Android handsets is already normalising the use of facial recognition amongst the general public (not to mention normalising the collection, use and sharing of face data). The role of the private sector is perhaps hinted at where it is stated that "South Wales Police has indicated that it intends to implement automated facial recognition in future throughout the enormous existing CCTV network" (p.14), this presumably refers to CCTV coverage available through both public and private sector systems.

Some measure of the issues that this may raise can be gleaned from juxtaposing a quote from a commercial vendor in *SC Media UK*, “If smart authentication works as well as it's advertised, users wouldn't even know they are being authenticated” against Big Brother Watch’s dystopian concept of citizens being “effectively asked for their papers without their consent or awareness" (BBW, p.7). These provide two very different interpretations of the use of essentially the same technology, which in turn suggests a need for a much more nuanced approach to the regulation of CCTV analytics than “UK public authorities [should] immediately stop using automated facial recognition software with surveillance cameras” (BBW 2018, p.41).

Panning for Critical Gold

It is easy to be critical of the evidentiary and analytical weaknesses, and the recourse to polemic and hyperbole, found in some campaigning group publications. In the case of *Face-off*, adopting a more rigorous and evidenced approach would both add credibility to the authors’ arguments and focus attention on the legitimate and important concerns they raise about the introduction of AFR and other CCTV biometric analytics, such as gait recognition and behaviour or emotion pattern recognition. That said, they would remain open to the criticism levelled here: that they take too narrow a regulatory viewpoint with their arguments for a specific legal basis for use of AFR, an increased level of oversight, and greater coherence of policy.

The activity of the campaigning groups in calling for specific legislation and greater oversight to control police of AFR can be contrasted with the apparent inactivity on the part of government. The Home Office’s recent *Biometrics Strategy*, published in June 2018, has been delivered five years later than initially promised, and has been described as simply "...pull[ing] together previous announcements, while offering few concrete overarching policy objectives." (The Register 2018). Criticisms of the strategy include a lack of detail about the Home Office's future direction for the use of biometrics and the sharing of biometric data, no clear statement that facial image databases already been held to be illegal will be brought into compliance and a lack of recommendations for legislation. While the strategy contains positive measures such as requiring DPIAs for new biometric projects and the creation of a new advisory and oversight committee, to advise on policy and standards for AFR (Home Office, para.48), ultimately it contains only the promise that "law and standards ... [will be] in place to regulate the use of AFR in identification before it is widely adopted for mainstream law enforcement purposes." (Home Office, para.58) with little indication of what such law and standards might contain.

It is suggested that there is already sufficient legal basis for the use of CCTV analytics, and sufficient supply of oversight bodies for both public and private sectors. While a more coherent policy direction for AFR would undoubtedly be desirable, ultimately the key issue in this area is not whether greater legal regulation is required, but rather how regulation could be most effectively designed to meet public policy objectives. The primary problem is thus one of unimaginative regulation. The solution lies not in an unrealistic demand for a ban on AFR and future analytics technologies, or yet more legislation, but rather in establishing how those technologies, and the public/private practices that leverage them, can be designed and constructed to incorporate compliance with the requirements of human rights legislation and data protection law.

There is little doubt that the use of CCTV analytics could be used to breach individual and group privacy. As such, the UK’s privacy and data protection commitments require that use of the technology must respect the right to private and family life, and ensure that any restrictions on that right are "in accordance with law" and "necessary in a democratic society" under Article 8 of the European Convention on Human Rights (ECHR). Further, under Articles 7 and 8 of the EU Charter of Fundamental Freedoms (CFR), its use must respect the right to the protection of personal data, ensuring that data is processed fairly for specified purposes, and only under a legitimate basis laid down by law. The privacy elements are largely provided through the common law, in the form of the law of confidentiality and the right to the protection of personal information. The data protection

elements are explicitly provided for in the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018.

The authors of *Face Off* contend that these requirements are not met, citing the Minister for Policing in a written statement in September 2017: "There is no legislation regulating the use of CCTV cameras with facial recognition" (BBW 2018, p.9). Crucially, however, they omit the next part of the Minister's statement:

> "However, the Surveillance Camera Code of Practice requires any police use of facial recognition or other biometric characteristic recognition systems to be clearly justified and proportionate in meeting the stated purpose. The retention of facial images by the police is governed by data protection legislation and by Authorised Professional Practice produced by the College of Policing."

There is no requirement under Article 8 ECHR that there be specific legislation to regulate a particular technology or activity. What is required is that where a technology or activity infringes on those rights, there is legal provision that plausibly covers the potential infraction, that this legal provision is accessible to citizens, that it is sufficiently precise to enable a citizen to foresee the consequences of a given action, and that it provides an effective safeguard against arbitrary interference in the right to privacy. The State must also show that the permitted infringement is genuinely necessary, and that the interference with the right is proportionate.

Relating to clarity of oversight the authors note that there are three potential regulators – the Information Commissioner (ICO), the Surveillance Camera Commissioner (SCC) and the Biometric Commissioner (BMC). They suggest that responsibility for oversight has not been addressed: "the Surveillance Camera Commissioner raised this concern in his Review on the Surveillance Camera Code of Practice [in 2016]" (p.10). In fact, the SCC noted in that Review that the BMC had taken the lead in this area (SCC 2016, p.15). In terms of policy, the claim that the Westminster Parliament has been slow to address the issue compared to the Scottish Parliament, appears undeniable, and is the most plausible element of *Face Off's* claims.

It must be said that UK's history regarding the use and regulation of surveillance technologies, and of official databases, has been, to put it mildly, chequered. The Westminster Parliament has very often required strong judicial prompting from Strasbourg before moving to bring both public and private sector practices into conformity with the ECHR. However, it appears that for CCTV and CCTV analytics, the difficulty lies not so much with a lack of legislation or oversight as it does with the process of implementing the technology, and with factors inherent in the political and economic environment in which it is being introduced.

If one looks past the polemic in their literature, there is little doubt that the campaigning groups have identified a plausible array of organisational, administrative and technical issues that need to be fully examined and addressed before use of CCTV analytics in the public and private sectors can be described as compliant with the requirements of human rights law and data protection law. Many of these are legacy issues arising from existing systems and processes, and unless and until these are addressed, the effective use of CCTV analytics will inevitably be compromised.

Amongst the key issues that critics identify are:

- image databases that are not fit for purpose, and which do not appear to be compliant with either the 'necessary and proportionate' requirements of the ECHR, or the current data protection legislation;
- 'feature creep' for existing public-sector technology without any evidence that detailed and publicly accessible privacy/data protection impact assessments (P/DPIA) and 'privacy by design' planning have been conducted;

- lack of evidence that the image data collected is processed in conformity with data protection law, for example that access to the data is restricted to those that are specifically authorised to use it, that the data is sufficiently accurate and up-to-date for the purpose it is to be used for, and that the way in which the data is collected, the scope of the collection, and the retention of the data is proportionate to the objectives to be met;
- the use of CCTV/AFR systems without an adequate and transparent assessment of the issues surrounding the use of artificial learning techniques, for example machine learning algorithms, against which system operators and other parties in the criminal justice system can assess and weigh the likely value of the system outputs;
- that, in the public sector, a desire to reduce costs has driven the interest in utilising CCTV analytics, whilst simultaneously limiting the sector's willingness to adopt practical and procedural safeguards that would ensure conformity with the law and legitimise the use of the technology in the eyes of the public.

None of these issues require new laws, or a ban on the use of particular technologies. What they do require is a fundamental reappraisal of the seemingly *ad hoc* approach to the implementation of the technology. The recent past is littered with biometric technologies which, because they were poorly implemented, or poorly understood by the organisations using them, created injustices and, in some cases, miscarriages of justice. For example fingerprints have been used as evidence for over a hundred years, but as late as 2009, the US National Research Council was criticising analysis of fingerprints as lacking a proper scientific foundation, and a later study in 2016 by the US President's Council of Advisors on Science and Technology noted that while "latent fingerprint analysis is a foundationally valid subjective methodology", it had a "false positive rate that is substantial and is likely to be higher than expected by many jurors based on longstanding claims about the infallibility of fingerprint analysis." If a data processing technology cannot be used reliably and transparently, then laws permitting the retention of data to facilitate it will always lack support from the public.

In short, any system or process using CCTV analytics needs to demonstrate that:

- a new system or new use of an existing system has been subject to a prior P/DPIA, (ideally by an independent third party), and that any new system can be shown to have been designed with privacy protection as an integral element rather than as an add-on;
- the processing of CCTV analytics data is structured, as far possible, to ensure that it is compliant with UK human rights legislation and the data protection regime, showing that data is collected, processed and retained in the least privacy infringing way possible, the system can provide for the efficient and timely removal of images when no longer required, and data subjects can fully utilise their data protection rights;
- the algorithms used are subject to ongoing independent validation, to ensure that discriminatory biases can be identified and ameliorated;
- where algorithmic bias cannot be ruled out, that this is properly factored into the use of the data generated: for example, the reliability of forms of CCTV analytics, such as AFR, should be properly explained to system operators and other parties relying on the data;
- the use of the system is transparent to the public, so that information about the nature of the technology, its planned deployment and the safeguards attendant upon its use is readily available.

A regulatory toolkit for CCTV analytics

Regulation can be complex. But a simple definition might be 'an action seeking to enable, facilitate or adjust the conduct of individuals or organisations'. It is most often understood in terms of binding legal norms, whether these are derived from Parliamentary legislation or from Executive, administrative or judicial powers. This type of regulation often takes a direct 'command and control' form, such as a law stating that a behaviour is, or is not, permissible which is enforced by state actors. However, legal regulation may also establish, or facilitate, other regulatory approaches, including (but not limited to):

- incentive-based regimes, where the State rewards certain behaviours;
- disclosure regimes where the State may mandate or bar the disclosure of certain information; and,
- rights and liabilities regimes where the State grants rights that one party can enforce against others in order to regulate their behaviour.

The UK data protection regime contains elements of all three approaches. Organisations which co-operate with the Information Commissioner (ICO) on matters such as breaches, are treated more favourably than those who do not - this is an incentive to disclose. Data protection law requires that data controllers provide information about their processing - this is mandated disclosure. Data subjects can sue controllers and processors for breaches of their DP rights - this is a rights and liabilities regime.

The ability to 'enable, facilitate or adjust the conduct of individuals or organisations' is not limited to the use of binding legal powers. US legal academic Lawrence Lessig noted in his book *Code and other Laws of Cyberspace* that law is just one of several ways in which regulation might be achieved. He suggested three further 'modalities': the market, social norms and, in relation to the internet, software code - the architecture of the internet. Whilst Lessig's discussion in this book is relatively simplistic, it provides a useful starting point for exploring the breadth of approaches available when considering regulation of new technologies.

If we consider CCTV analytics, we can see that there is a legal framework surrounding the use of CCTV and the further processing of data captured through it. That framework is expressed in several pieces of legislation, including data protection legislation, and in codes of practice, including the SCC's Surveillance Camera Code of Practice. However, legal regulation is reliant upon those who are being regulated understanding and observing their rights and obligations, and upon an effective and efficient system of enforcing observance. In some areas of regulated activity, neither of those requirements may be present or adequate. For example, employees of a data controller/processor may misunderstand their employer's obligations or may inadvertently or deliberately ignore them. Ideally an employer would ensure that their employees are properly informed, and that there are suitable consequences for failure to comply. In practice, legal compliance alone, particularly if the threat of enforcement action is perceived to be limited, may be insufficient.

A data protection regulator might therefore seek to achieve the regulatory goal by another means. They could assess the activity of data controllers/processors and provide certification for compliant controllers with additional awards for good practice. Data controllers/processors could then use that certification in their dealings with clients and data subjects, perhaps giving them a competitive edge. This would address the market modality. The regulator might also use advertising and other mechanisms directed at the public or at employees of data controllers/processors to stigmatise poor data protection practice or to evangelise for good practice, with the aim of changing the public's perception about the value of data protection and good processing practice. This would address the social norm modality. An effective regulatory strategy might thus consider using a variety of legal strategies in combination with action targeting the non-legal modalities, and in doing so harness

various elements of the regulatory toolkit to allow a multi-faceted approach to achieving the regulatory objective.

In terms of technology, Lessig argued that the most effective form of regulation of activity mediated through technology might simply be to design a system so that the desired regulatory outcome or outcomes were hard-wired into its hardware or software. If the architecture of a technology does not permit an undesirable regulatory outcome, or automatically defaults to a desirable regulatory outcome, then this is likely to be a more effective approach to ensuring compliance than relying solely upon individuals to understand, remember, and act upon, a set of legally binding rules. A sophisticated system of technological control could be developed to permit a spectrum of discretion that varied between types or hierarchies of user, including scenarios where exceptions to normal regulatory requirements might be permitted as necessary or justified.

Designing architectural regulatory control into CCTV analytics at an early stage of its roll-out has the potential to provide a verifiable means of achieving practical enforcement of the legal framework. Government and industry can develop privacy and data protection standards for architectural regulatory control, and Government might then mandate that systems purchased by the public sector should as a minimum conform to such standards, while leaving open the possibility of industry offering more sophisticated controls. This would increase the likelihood that industry offerings of CCTV analytic systems for both public and private sector organisation would adhere to those standards, a concept sometimes described as 'regulation by contract', leveraging as it does public sector spending power.

Alongside embedded architectural regulatory control, greater attention should be paid to another regulatory aspect of CCTV analytics, that of information provision. Publications like *Face Off* highlight the lack of information available about the use of CCTV analytics by public and private sectors. This limits meaningful discussion of the risks and benefits of the technology and how these should be balanced, whilst fuelling concerns about ways that the technology might be misused. A discussion needs to take place, before widespread adoption of the technology, about the reasonable balance to be struck between matters such as commercial confidentiality and efficacy of CCTV analytics use, and regulatory transparency.

Conclusions and Recommendations

Development of regulatory strategy with regard to CCTV and associated technologies in the UK has lacked strategic vision. The result has been a fragmented regulatory landscape, a plurality of regulators, and an unfortunate tendency to revert to, or to call for, outdated and unsophisticated 'command and control' style regulation.

- Key problems identified stem not from the data technologies being utilised such as CCTV and CCTV analytics, but from:
    - inappropriate legacy administrative practices and systems, including image database systems and outdated data management processes;
    - short term cost savings being prioritised over the development of good processes and practices for the long term;
    - variations on the technologies being rolled out piecemeal across different police forces without a clear coherent and publicised national strategy, or adequate funding to effectively verify and validate outcomes such as assessment of algorithms for fair application;
    - a lack of clear public information and guidance about the technologies provided both by parties using CCTV analytics and by regulators.

- Critical commentary on the use of CCTV and CCTV analytics is disproportionately focused on the public sector, notably policing, and takes little account of its implementation by private sector organisations. This means that:
    - the extent and effect of image data transfers between public and private sectors is largely ignored;
    - the implications of adopting the types of measures suggested for the public sector for private sector use are inadequately considered;
    - innovative good processes and practices in the private sector are overlooked as potential exemplars for public sector models, or as fertile ground for public/private collaborations.
- Effective regulation of new technology is being hampered by a dogged insistence on focusing on a limited and dated set of inflexible regulatory techniques, resulting in:
    - a polarising of the debate into a polemic where special interest groups with narrow-focus agendas have come to dominate the discussion;
    - a failure to consider how other modalities than the law, such as social norms, competition and technological factors, might be harnessed;
    - a lack of meaningful tripartite regulatory engagement – the regulators, those regulated, and the wider public are not effectively engaged in the process of determining appropriate use, and effective regulation, of the technologies.

With the increased use of digital CCTV and the development of new analytic tools, it is time for a reconsideration of regulatory practices, and a reappraisal of the regulatory tools available. The aims and objectives of regulatory reform are clear, but the means of achieving those aims and objectives remain open to debate. It would be unfortunate if the scope of that regulatory discussion were to be confined to the limited parameters espoused in the pages of publications like *Face Off*. So many regulatory alternatives are available that could do a better job of capturing the positive elements of the technology whilst actively incorporating appropriate safeguards.

With regard to the use of AFR by the Home Office and its partners, it is clear that the process of developing regulatory controls is at an early stage. Ideally, the new oversight and advisory board to coordinate consideration of issues relating to law enforcement's use of facial images and facial recognition systems, promised by the Home Office in the *Biometric Strategy* document (para.42), will take a broad view of the regulatory choices. It will certainly be advisable for the oversight and advisory board to consist of representatives with a wider range of expertise and viewpoints than simply "the police, Home Office, the SCC, the Biometrics Commissioner (BC), the ICO and the Forensic Science Regulator (FSR)". Recourse to technical, regulatory theory and private sector expertise outside those bodies will undoubtedly result in a more innovative approach to the deployment of non-legislative elements of the regulatory toolkit. It will also ensure that there is consistency of policy rationales and regulatory controls across public and private sector implementations and deployments of AFR.

Recommendations for a more constructive approach include:

- Not regulating new models of CCTV and CCTV analytics based on assumptions derived from flaws and abuses in legacy systems and administrative practices, nor adding unnecessary technology-specific regulation in areas where existing general legal regulation, such as data protection or human rights law could be effectively applied.
- Ensuring that existing general legal regulation is effectively overseen and enforced, and that organisations processing personal image data are both compliant and accountable. Personal image data should be treated no differently than any other type of personal data.

- Taking a holistic view of the use of CCTV and CCTV analytics to capture the full range of use cases across public and private sectors to ensure that:
    - the impact of regulatory measures can be predicted across different types of use by different actors;
    - proposed regulation is flexible enough to encourage innovation, but capable of practical implementation, and where necessary, enforcement;
    - it is possible for industry to create products which can be used in both public and private sector scenarios.
- Thinking outside the current regulatory box, and certainly beyond simplistic calls for bans on the use of technologies by the public sector simply because they utilise personal image data. There is a need to:
    - consider the positive use cases for the technology, as well as the negative, and work towards a regulatory framework that aims for a proportionate balance between the benefits and risks;
    - identify why there is a disconnect between the regulators, those regulated, and the wider public over appropriate uses and effective controls, and to work towards better public engagement through information and interaction;
    - adopt complementary regulatory strategies harnessing different modalities, for example seeking to change policing culture and practices, regulating through technological architecture, or requiring greater disclosure of policies and processes;
    - strongly encourage CCTV and analytics users to self-regulate through the deployment of appropriate technology architectures and systems.

Notes:

Anon. (2018). Premier League has highest cumulative attendance - EPFL study, *ESPN.com* (15 January 2018).
http://www.espn.co.uk/football/english-premier-league/story/3349601/premier-league-has-highest-cumulative-attendance-epfl-study

Beall, A. (2018) Drones to spot festival violence, *New Scientist* (3182: 16 June 2018): 15.

Big Brother Watch. (2018) *Face Off: The Lawless Growth of Facial Recognition in UK Policing* (May 2018).
https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

Bowcott, O. (2018) Police face legal action over use of facial recognition cameras, *The Guardian* (14 June 2018)
https://www.theguardian.com/technology/2018/jun/14/police-face-legal-action-over-use-of-facial-recognition-cameras

Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council (2009) *Strengthening Forensic Science in the United States: A Path Forward (*August 2009)
https://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf

Fowler, G.A. (2017) Apple is sharing your face with apps. That's a new privacy worry. *The Washington Post* (2 December 2017)
https://www.washingtonpost.com/news/the-switch/wp/2017/11/30/apple-is-sharing-your-face-with-apps-thats-a-new-privacy-worry/

Hill, R. (2018) UK.gov's long-awaited, lightweight biometrics strategy fails to impress (29 June 2018)
https://www.theregister.co.uk/2018/06/29/uk_biometrics_strategy/

Home Office (2018). Biometrics Strategy: Better public services, Maintaining public trust (28 June 2018)
https://www.gov.uk/government/publications/home-office-biometrics-strategy

Lewis, A. (2017). True cost of policing football in the capital revealed, *ITV.com* (10 November 2017).
http://www.itv.com/news/london/2017-11-10/exclusive-true-cost-of-policing-football-in-the-capital-revealed/

Lessig, L. (2000) *Code and other Laws of* Cyberspace, Basic Books.

Manzoor, S. (2016). You look familiar: on patrol with the Met's super-recognisers, *The Guardian* (5 November 2016).
https://www.theguardian.com/uk-news/2016/nov/05/metropolitan-police-super-recognisers

Maskaly, J. *et al.* (2017). "The effects of body-worn cameras (BWCs) on police and citizen outcomes: A state-of-the-art review", Policing*: An International Journal*, 40(4): 672-688.

President's Council of Advisors on Science and Technology (2016). Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods (September 2016)
https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf

Rowland, Kohl & Charlesworth (2017) *Information Technology Law* (5th ed.), Routledge, Chapter 10 Surveillance.

Secretary of State for the Home Department, *CCTV: Written question - 8098* (4 September 2017)
https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-09-04/8098/

Surveillance Camera Commissioner (2016). *Review of the impact and operation of the Surveillance Camera Code of Practice* (February 2016)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/502893/Draft_Review_FINAL.pdf

Vergara, D. (2017). "Smarter" authentication has arrived - with behavioural biometrics, *SC Media UK* (25 October 2017).
https://www.scmagazineuk.com/smarter-authentication-has-arrived--with-behavioural-biometrics/article/698996/