Gilbert and George.[31] To these one might add (hardly of recent vintage) performance art and so-called "land art", whose practitioners, many motivated both by artistic and ecological concerns, set out, so to speak, to tread lightly upon the earth, creating forms and patterns that are eventually erased by the elements. The court found it neither "necessary [n]or appropriate to answer that question".[32]

At this point the court might as well have concluded, "I may not know much about art, but I know what I like!". Mechanistic modes of thought have driven the creative imagination into exile. This is a vision of art as mere entertainment and it simply reaffirms the status quo, one in which "the base [has] forc[ed] all human energy into a competition of mere acquisition".[33]

Are We Sleepwalking into Giving Up Our Facial Data Rights? We Need a Public Conversation and New Laws

Dina Shiloh
CONSULTANT, SIMONS MUIRHEAD & BURTON

LT Data collection; Data protection; Data subjects' rights; Facial recognition software; Minorities; Police powers and duties

Recently three British media outlets managed to mislabel a series of photos of black female Labour MPs by confusing them with one another. As shocking as that is, the inability to recognise black faces is even worse when machines are involved: witness the 98% error rate at the 2017 Notting Hill carnival, where the system falsely alerted officers on over a hundred occasions it had spotted a suspect.

That's just one reason why we should be very concerned about facial recognition technology. Live Facial Recognition (LFR) is being used increasingly in our local high streets, in shopping centres and at sports matches. Authorities around the world like these systems: they allow them to watch thousands of people, often at some distance, and scan their faces against a "watchlist" of suspects. How is the data being used? How long are the images kept for? How accurate is the scanning? Who compiles the watchlist and decides who's on it?

Use of LFR continues despite these questions. The technology has been "trialled" by the Met, South Wales Police, Leicestershire, Humberside, and Greater Manchester Police. The Met has now openly said it is doing so operationally; it was deployed earlier this year in Oxford Circus underground station. In Wales recently, fans arriving at a football match were greeted by two surveillance vans roving around Cardiff City's stadium. The fans showed them what they thought of the vans by wearing hoods, sunglasses, scarves and even masks.

Shop owners in several UK cities are now regularly using the technology. If a shoplifter is caught on camera or by a staff member, their image can be stored; if they are then seen in that shop again, the shop manager will get an alert. These private "watchlists" are compiled by the management of the shops themselves and kept for as long as they see fit.

But not everyone is embracing the technology.

Civil rights organisations have voiced their concern at the speed at which the technology is being adopted. The UK's own data protection watchdog, the Information Commissioner's Office, has urged caution on the use of what it describes as an "intrusive" technology. The House of Commons Science and Technology Committee has called for British police to stop using LFR until regulation is in place.

In Brussels in January, a European Commission white paper was produced which suggested temporarily banning the use of facial recognition technology in public places including train stations, sport stadiums and shopping centres. A ban of 3–5 years would be put in place to allay fears about the creeping surveillance of European citizens. Meanwhile San Francisco, the base of so many tech companies, has banned the use of facial recognition technologies by the police and other government agencies; that should tell us something.

We should also take note of who does like the technology: China has embraced facial recognition, using it to implement a national surveillance system. It is pervasive in Chinese society, with facial recognition used for airport check-ins, cash withdrawals and even to monitor the attention of school students.

There are concerns over the increasing use of facial recognition to aid the oppression of ethnic minorities, with the state collecting their biometric data, including face scans to build a tool that could be used to justify and intensify racial profiling and other discrimination.

Supporters of the technology argue that this sort of use would not be tolerated in Britain. But the software's inability to recognise people of colour has been documented widely, especially women of colour. In other words, the technology can lead to unlawful arrests, and to discrimination.

Supporters also argue that the systems will get up to speed and public security will be improved. But there are still concerns about automated blanket surveillance

[31] See above.
[32] *Creation Records Ltd v News Group Newspapers Ltd* [1997] E.M.L.R. 444 ChD at 12.
[33] See R. Williams, *Culture and Society 1780–1950* (Penguin, 1958), p.201 (quoting D. H. Lawrence).

tracking every individual's move, and that private companies and law enforcement agencies are now sharing our images to build watchlists of potential suspects without our knowledge or consent.

The building of such databases will inevitably lead to a chilling effect on our political culture, as people are frightened to demonstrate or gather on the streets.

The law regulating the technology now being used is remarkably thin. The GDPR stipulates that watchlists need to be shared in a "proportionate" way; can we really say the technology is now being deployed—and the data collected and saved—proportionately? It's clear that obtaining people's sensitive biometric data to identify a small number of people is entirely disproportionate.

The current lack of legal or regulatory framework has been flagged by the very organisation which would be enforcing the rules. The Information Commissioner's Office has made it clear that "processing of personal data" takes place whenever law enforcement organisations deploy facial recognition technology in public spaces. And your face is not just personal data; it involves the processing of biometric data for the purpose of uniquely identifying an individual, and so it counts as sensitive processing. That includes images of faces which are captured and deleted quickly.

The law also says that an assessment should take place when the technology is used and an "appropriate policy document" must be in place. Even if this is taking place in every case, this gives the users of the technology an enormous amount of responsibility and power, and it will be very difficult to monitor those monitoring us.

It's now accepted by many that we have sleep walked into providing troves of personal data about our health, our sex lives and our personal relationships to various tech companies via social media. Many users have pushed back, by deleting their social media accounts or at least limiting the amount of personal information they provide.

Can we afford to give up our highly personal and unique facial data in the same way? We urgently need a public conversation on its impact on our rights and civil liberties, so that the law can provide a fully comprehensive framework for the new technologies which are being deployed.