You Have a Human Right Not to Be Tracked And Manipulated By Google And Facebook

- Human Rights / Law / Law Enforcement / Liberty / Society

> *"There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time." George Orwell, 1984.*

Timothy Clement-Jones introduced a private member's bill in the House of Lords mandating a moratorium on and review of the use of facial recognition technology in public in the United Kingdom. The bill comes as legislatures around the world are responding to a technology that is fundamentally reshaping the relationship between governments and citizens, and has the potential to massively restrict citizens' right to lead private lives in public places.

In an exclusive interview for Technical Politics, Lord Clement-Jones explained the need for a moratorium on and a review of mass facial recognition technologies in public spaces in the UK. In the interview, given on 1 October 2019, we asked first about the source of our right to privacy.

"Just because you are walking in a public place it does not mean your privacy can be invaded. For instance, what about RFID technology where you walk past a shop and they say, "Hi, come in inside!" I don't think that's a right that a commercial organisation has, and I don't think that it's a right that a public organisation has.

"I think you have the right to know when your data are being shared, and you have the right to know when technology is being applied to your identity. It's obvious when you go through passport control, but, for instance, in King's Cross in London for two years, people had facial recognition cameras pointed at them. ***They were collecting data on individuals, and people didn't know about it.***

"It breaches all the rules of transparency and consent, and quite apart from that, the technology is faulty in any event. The Home Office Biometrics and Forensics Ethics Group reported on this, and they questioned the accuracy and the potential for biased output.

"I think that on about four different counts it fails, and there is no proper regulation in terms of determination of the circumstances in which it is appropriate to use facial recognition.

"In my private member's bill, I've actually excluded the security services' use of facial recognition, in circumstances where a high court judge has permitted it.

"The irony of it is that there is no certainty about when other services can use it. Security services can use it under Section 28 of the Regulation of Investigatory Powers Act 2000, but there is no determination of when our civil police can use it. Now that seems to me to be a massive omission."

A unique characteristic of privacy as a right is that it can often easily be infringed without the subject being aware that they are suffering a harm, and some have speculated that this aspect of the right to privacy lies behind popular apathy about privacy issues in general. Lord Clement-Jones related the issue of popular apathy to a lack of understanding of the value of the data collected by technology companies.

"There is an apathy, but it is partly because people don't understand the trade-offs between getting something free and the personalisation of advertising using their own data.

*"**In the case of facial recognition, you have the right not to be tracked as you go about your business, if you are not a criminal or a terrorist. That seems to be a fundamental right.** Are we saying that the state has the right to observe every single individual? That seems to me to be the big brother state quite honestly.*

"We have found that the police forces sometimes are actually sharing data with the private sector, because the private sector is providing the technology. Are we saying that that is acceptable? I don't think so."

"So, I think it fails on a number of counts basically in terms of proper justification. I think we need to know for what purpose facial recognition is being used. At the moment, it is a bit out of control quite honestly."

If there is anywhere in the world that one would expect there to be deep popular understanding of the power of contemporary information communications technology, it is San Francisco, and so it is instructive that this city has taken a lead among US city governments in banning the use of facial recognition technology in public. In an Ordinance passed 8-to-1 by the San Francisco Board of Supervisors on 22 May 2019, it is stated that facial recognition technology will "threaten our ability to live free of continuous government monitoring", and the Ordinance specifically places controls on surveillance technology's use by San Francisco City departments.

Not all jurisdictions are demonstrating similar caution. On 30 October 2019, Technical Politics carried a story on Aruba Happy Flow, an initiative which "will allow travellers [to Aruba] to trial the application of biometric technology at every stage of the travel process, from arrival, border management, collecting the car rental and checking in at the hotel".

In reality, between enthusiastic adoption and outright bans, most legislatures have been content to let police forces and private companies aggressively expand facial recognition programmes with little oversight or regulation, and when legislation is passed, it sometimes reflects a limited understanding of the most advanced technologies and their applications, and of the potential harms to civil society.

Lord Clement-Jones was stark in describing the consequences of the misuse of data on private citizens today.

*"**We are in circumstances that the use of our private data is one of these existential issues. It's heavily under debate.** It's not just Cambridge Analytica. It's Facebook's use of data to personalise advertising back at you, **the whole surveillance capitalism agenda** and so on."*

"So, the fact that we've got a technology such as live facial recognition which is being used in this way, this is a massive diminution of public trust, if people feel that this technology is being abused, or is being used to their detriment in some way. That is not the way to build public trust."

Although a Joint Statement promoted by Big Brother Watch on police and private company use of facial recognition surveillance in the UK was signed by representatives from many of the major

UK parties, including David Davis of the Conservatives, Diane Abbott of Labour, Jo Swinson, Leader of the Liberal Democrats, and Caroline Lucas, Co-Leader of the Green Party of England and Wales, it was not clear to Lord Clement-Jones that this cross-party support would translate into positive government action. In fact, recent statements from Baroness Williams of Trafford in the House of Lords indicated that the outgoing Government was distinctly cool on the idea of additional restrictions on the use of the technology. Lord Clement-Jones explained the position of the Government thus:

"I know that the Science and Technology Select Committee has recommended a moratorium. You may have seen the comments from the Metropolitan Police Commissioner about the potential for a police state. You may have seen reports that the Information Commissioner's Office came out with yesterday, which I haven't had a chance to look at yet, but which seem to be saying that there is a serious issue and that police need to slow down in their use of live facial recognition technology."

"Government may not be in favour. Baroness Williams even went as far as talking about people who might be on a watch list, and who it would be quite legitimate to be tracking. I thought that was absolutely extraordinary that she went as far as that."

Looking at how the bill would will work in practice, we next asked about where liability would lie in the instance that images were taken by a member of the public in one country, stored by a company in a second, and processed by another company in a third. In response, Lord Clement-Jones made it clear that regular members of the public would be unlikely to be affected by his bill under such circumstances.

"You would probably have to have some regulation of apps that process facial recognition technology, but … you've got to be proportionate. We're really talking about public authorities. I'm not talking about people taking photographs on their iphones, and uploading them to photos or iphotos or whatever it is, and then iphotos saying this is the person that you've taken a photo of, for a private person. I think you have to be proportionate about this.

"The thing that I am talking about really is live, bulk facial recognition technology. Let's face it, Apple photos does precisely that. It's not live in quite the same way. We're talking about the potential for real issues in terms of tracking and so on and so forth, which I think is the most serious aspect. And of course, you don't have to have watched the Capture, to see that there is a whole bunch of issues that could surround how you, in a sense, pervert the way that facial recognition technology is used by deep fake technology and so on. That's another step just beyond the ordinary.

Following heavy lobbying, the United States recently relaxed restrictions on the maximum resolution that images of earth from space could be collected from 50 cm to 25 cm. As early as 2015, DigitalGlobe, a provider of commercial satellite images whose customers include Google and the National Geospatial-Intelligence Agency, was at it again, lobbying for the maximum resolution to be lowered to just 10 cm. According to the Science Explorer, "if the 10-centimeter resolution laws get approved, DigitalGlobe will be able to sell commercial high-resolution images to any companies willing to pay, meaning your smartphones, license plate numbers, and faces could soon have a price."

With facial recognition technology from space the next Orwellian prospect on the horizon, we asked Lord Clement-Jones about whether a scenario where foreign companies using foreign satellites to monitor individuals in the UK would be covered by his bill.

"I don't that [scenario] would even be extraterritorial in many ways. If the result of that data is used in the UK, that would not be according to regulation.

"At the moment, I am saying 'a moratorium', so I think if there was evidence of that, wherever the camera is situated, whether in space or terrestrially, I don't think that alters the situation, quite honestly."

We next asked about the ideal balance between new technology and respect for our fundamental right to privacy.

"That's the task of politicians to judge what is proportional and what is not. Generally, I am against regulation. I am not someone that has a knee-jerk reaction of saying that you've got to regulate everything. If you broadly operate in accordance with a code of ethics, and you've got your corporate governance right, that broadly seems to me to be the way forward, but there are some technologies that are so invasive and have such widespread use that you have to do something. That's where we are with this.

"For instance, government at the moment is very heavily involved in algorithmic decision-making in all sorts of services. Again, we don't really have any central guidance and compliance by central government in terms of ensuring that that is done in the proper fashion: it's transparent; the decisions are explainable; and, the datasets used to train the algorithms are free of bias

"If you suddenly found on the internet-of-things that a particular new technology allowed external actors to breach multiple devices in the home, for instance, you would probably want to regulate that as well, and make sure it was a criminal offense.

"You have to respond in a proportionate way to these things as you see them and as you see the size of the threat, and I think that most people now believe that it is a big threat, that it is a real issue.

Widespread concern has been raised that aspects of China's 'chilling' Social Credit System (SCS) are in danger of being emulated in Western democracies. According to Business Insider, among the rewards for compliance with the Chinese system are discounts on energy bills, deposit-free rentals, and better interest rates at banks, while those who are caught failing to comply with monitored behaviours face being blacklisted, having travel restrictions imposed on them, or even having their dog taken away. We asked Lord Clement-Jones his view of the Chinese social experiment.

"I think it's pretty obvious, it's up to Chinese citizens to object to that themselves. I wouldn't countenance that in a Western democracy. If it's the shape of things to come, it's not something I want to happen. One has to be very clear and robust about these things. But you know, quite frankly, these things creep up on you, and they may not be overt in a Western democracy, but public agencies are very, very good at accumulating ways of acquiring more information and that's what we have to counteract.

"It's the old frog in hot water example. You may not notice that little bit of a use of technology, in certain circumstances – fingerprinting for the Passport Office or eyeball recognition – but then they use it for other things, not just for immigration purposes, and not just for

passports, but for social security purposes, and so on and so forth, and then you've got government departments sharing all their data, and ***before you know it, you've got a comprehensive surveillance system****.*

Finally, Lord Clement-Jones encouraged members of the public to make mass surveillance an issue in parliamentary hustings.

"I think it's an ideal thing for people to ask their parliamentary candidates who are standing for election. Ask them what their attitude to this kind of intrusive technology is."

"I don't think we will be getting more apathetic. One of the big agenda items for all parties – there's no doubt about it, this is a cross-party issue – is the whole question of digital literacy and digital understanding, and the more we are digitally literate as a society, the more we understand about the impact of new technology and what's happening to our data, the more concern will be expressed in this sort of area.

*"****This isn't going to go away. This won't become a cultural norm that everyone is spied upon basically.*** *I just don't believe that that is going to happen, and that is why I am a great believer in new technology if used in the right way. What I don't want is a modern form of ludditism to arrive, and if the government loses faith in the government regulators' ability to control new technology, then they're going to react against it.*

UK Legislative Action

On 30th October 2019, the Automated Facial Recognition Technology Bill was introduced by Lord Clement-Jones as a private member's bill in the British House of Lords.

If enacted, the bill will establish a moratorium on the use of automated facial recognition technology for overt surveillance of public places in the United Kingdom, and will also mandate that the Secretary of State commission a review of the use of automated facial recognition technology in public places in the United Kingdom.

In a subsequent debate in the House of Lords, Liberal Democrat peer Lord Strasburger chastised the Government for its lax stance towards facial recognition technology.

"The Government have previously confirmed that this highly intrusive technology is being deployed in a legal vacuum. Alarmingly, we have recently discovered that private companies have for years been secretly using automated facial recognition in public spaces, and the Commissioner of the Metropolitan Police has warned that we are sleepwalking into an "Orwellian … police state" and called for a code of ethics and a strict legal framework."

Crossbencher Lord Anderson of Ipswich highlighted the potential for facial recognition to be combined with "gait analysis, lip-reading technology, algorithms that can predict fights and sensors that can detect explosives and radiation" to provide more comprehensive surveillance, and called for greater oversight.

Liberal Democrat peer Lord Paddick raised the issue of whether detainees were being prejudicially affected by this technology when custody images were paired with civil facial recognition technologies.

In response to various criticisms of the Government's position, Baroness Williams of Trafford was resistant to any calls for

further action.

“As I said before, we must proceed very carefully with such developing technologies. It is very important that the police have clear legal frameworks within which to operate. However—not one month ago—the High Court said that there is a sufficient legal framework for police use of facial recognition technology. This consists of common-law powers, data protection and human rights legislation, and the surveillance camera code.”

***

Author: David McHutchon, Technical Politics