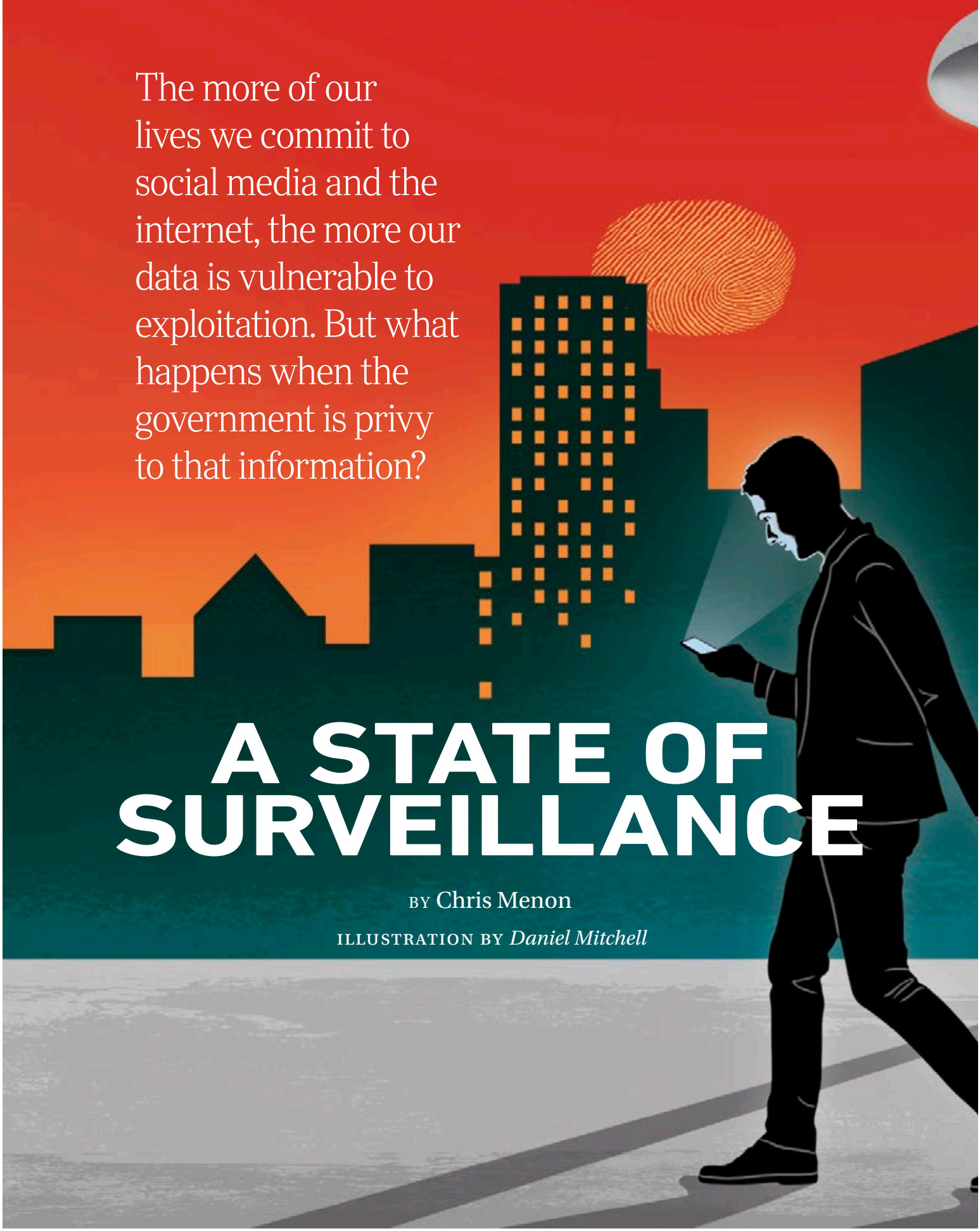
The more of our lives we commit to social media and the internet, the more our data is vulnerable to exploitation. But what happens when the government is privy to that information?



# A STATE OF SURVEILLANCE

BY Chris Menon

ILLUSTRATION BY *Daniel Mitchell*

IT MAY BE 2020 but for some it increasingly feels like *1984*, George Orwell's fictional dystopian world where citizens are spied upon 24/7, potentially guilty until proven innocent.

For instance, you've never committed a crime and are a peaceful, law-abiding citizen. Yet, your face may be routinely captured by live video and matched to a database of "persons of interest" to the police. If matched, the onus is then on you to prove your innocence.

This example isn't taken from China or some other despotic regime but here in Britain, as both South Wales Police and the Metropolitan police now use automatic facial recognition (AFR) to perform identity checks in real time.

"We now have cameras that are doing semi-covert identity checks en masse on hundred of thousands, even millions of people, who are innocent citizens going about their business. It is the hi-tech equivalent of "show me your papers." We don't have arbitrary identity checks in the UK but that is exactly what live facial recognition does," says Silkie Carlo, Director of Big Brother Watch.

The technology also has particular problems accurately identifying people, specifically darker-skinned individuals and women. "When we did our first report on trials by the Metropolitan Police it was 98 per cent inaccurate—I think it's now 96."

WE'RE CONFRONTED DAILY WITH NEW REVELATIONS ABOUT GOVERNMENTS USING TECHNOLOGY TO EXPLOIT OUR DATA

Big Brother Watch, founded in 2009, seeks to roll back the surveillance state and it isn't alone in calling for AFR surveillance to be outlawed. Other civil liberty groups, such as Liberty and Privacy International also want it banned.

## Presumption of innocence

"If you've done nothing wrong then you have nothing to fear", may be the knee-jerk response of some but Carlo points out that AFR, "completely subverts the presumption of innocence that you [are supposed to] have in a democracy".

Why is this so important? Tamsin Allen is a partner at law firm Bindmans and acted for Christopher Wylie, the Cambridge Analytica whistle-blower. She explains that while a citizen forgoes some of their liberty in return for protection by the State it should be the minimum necessary—a core principle of the Convention on Human Rights. "It is critical, particularly in the area of surveillance, that this delicate

balance is maintained and an individual does not give up more rights to the State than he or she has to in order to allow the State to carry out its functions."

Allen explains: "The fundamental right to the presumption of innocence is important in this context. The State usually has the burden of proving that an individual has been involved in wrongdoing, and the individual is presumed to be innocent. But, if the State has all the information and all the power, then the individual is effectively forced to prove they are not guilty. That is a major shift in the relationship between the individual and the State, and a very worrying one."

Dr Ilia Siatitsa

The secrecy that surrounds the ever-expanding collection and use of our data is an issue of great concern to many. Dr Ilia Siatitsa, Programme Director at Privacy International argues that this lack of transparency is a deliberate exploitative tactic increasingly used by companies and governments to escape traditional forms of scrutiny and safeguards.

This might sound like paranoia but, as both Siatitsa and Carlo point out, the release of the Snowden files in 2013 [see box 1] was one of the key moments in history when international media revealed the extensive secret mass surveillance operations of the US, UK and other intelligence agencies around the world, aimed at national and foreign citizens alike.

Siatitsa stresses that widespread abuses continue, stating: "We're confronted on a daily basis with new revelations about governments and corporations using technology to exploit our data at the expense of our liberties and protections."

For example, in 2018 Privacy International submitted a complaint to the UK Information Commissioner's Office (ICO) revealing how police forces across the UK have been taking data

from people's phones, including the victims of crimes, without an appropriate legal basis or oversight.

In response, the ICO issued a report in June calling for reforms and safeguards, such as a Code of Practice on mobile phone extraction to ensure people's rights are protected.

The increase in use of fake mobile phone towers (formally known as IMSI-catchers) also allows police forces, often without warrants, to collect mobile phone information from all protesters who happen to be located in their proximity.

## EDWARD SNOWDEN

Edward Snowden is a US whistle-blower who copied and leaked highly classified information from the US National Security Agency (NSA) in 2013 when working as a subcontractor for it.

His revelations alerted the world to numerous global surveillance programmes run by the NSA as well as the combined intelligence agencies of the US, UK, Australia, Canada and New Zealand, otherwise known as "Five Eyes".

He revealed that the US and British intelligence agencies have successfully cracked much of the online encryption relied upon by hundreds of millions of people to protect the privacy of their personal data.

For example, he revealed a secret programme known as "Tempora" under which the British Government Communications Headquarters (GCHQ) taps into transatlantic fibre optic cables carrying the world's phone calls and internet traffic data, which is then shared with the NSA. Tempora is said to include recordings of telephone calls, the content of email messages, Facebook entries and the personal Internet history of users. In an interview with the *Guardian* newspaper Snowden said of Tempora that: "It's not just a US problem. The UK has a huge dog in this fight...They [GCHQ] are worse than the US."

In addition, the documents claimed that the NSA via its "Prism" programme obtained direct access to the systems of Facebook, Google, Apple and other US internet giants. This allowed it to collect material such as search history, the content of emails, file transfers and live chat.

This was apparently done under secret agreements with these commercial companies, described in one document as "intercept partners", although publicly the companies have denied this.

## Terrorism


Diane Abbot, a Labour MP, points out that "a great deal of state surveillance has been introduced in the name of fighting crime in general and terrorism in particular." Those justifying the expansion of such surveillance argue that it prevents terrorism "because they know that it makes people afraid, that it's a threat we cannot see and the harm is acute", adds Siatitsa.

Richard Norton-Taylor, former security and defence editor at the *Guardian* and author of *The State of Secrecy* nevertheless questions its effectiveness. "Mass surveillance and data storage makes it more difficult for security and intelligence agencies to concentrate on potentially truly dangerous individuals. Bulk data storage may from time to time allow the agencies to connect a current threat with an individual whose communications they have intercepted in the past, but an assumption that they will find a lead or relevant connection from the past gives the agencies a false sense of security, dulling their senses."

Just as worrying is the revelation from Liberty that our intelligence agencies break the law and lie to the Investigatory Powers Commissioner's Office (IPCO), which is supposed to hold them to account. Liberty explains that the "security services have been breaking the law for years". They cite information that was revealed from documents MI5 had to disclose during litigation against the Snooper's Charter, otherwise known as the 2016 Investigatory Powers Act. [see box 2].

According to Liberty; "The documents reveal that MI5 not only broke the law, they failed to report this to IPCO, despite knowing about their non-compliance for years. They also gave IPCO false information to obtain warrants."

Given its failings and the dangers it poses to our basic freedom, Silkie

Carlo finds the lack of Parliamentary debate on state surveillance disturbing. Diane Abbott agrees and laments: "Once you utter the word 'terrorism' most British politicians do not question what is proposed. This is as true of Labour politicians as Tory politicians."

Asked about the lack of debate, Baroness Jones of Moulescoomb, a Green Party member who sits in the House of Lords, maintains: "We do debate these issues in Parliament, and there's a lot of us who are very concerned about the loss of civil liberties, but with a majority of 80-plus in the Commons the government can more or less do as it pleases."

Moreover, a lot of government legislation is pushed through "with virtually no scrutiny, through a mix of statutory instruments and by embedding ministerial control within bills," adds Baroness Jones.

Baroness Jones would like to see the government involve organisations such as Liberty and Big Brother Watch directly in the process of drawing up such legislation and also "ensure that when you give the security services surveillance powers, there are sunset clauses so they have to be constantly reviewed, that judges have to have sight of warrants and you abandon any legislation that allows general sweeps of the population."

Privacy International's Dr Siatitsa appears to be very much in agreement, arguing that: "Whenever a new form of surveillance is introduced we need to ask what its added value will be, and its impact

## THE 2016 INVESTIGATORY POWERS ACT

This law, widely known as the "Snooper's Charter", allows the UK security and intelligence agencies to intercept and store all of an individual's emails, texts, calls, location data and internet history.

According to Richard Norton-Taylor: "They can also hack into our phones and computers and create large 'personal data sets' on individuals, without the need to suspect any criminal wrongdoing."

These agencies are monitored by an Investigatory Powers Commissioner, a senior judge, and by a Security and Intelligence Committee consisting of peers (members of the House of Lords) and MPs vetted and approved by the Prime Minister. Although Norton-Taylor reveals: "The bodies are weak; what is needed are better resourced and independent bodies."

on human rights. We need to ask whether there is a publicly accessible legal framework and whether the measure is necessary in a democratic society and proportionate to the aim pursued. We must be sure that safeguards are there in place to mitigate the risks arising from increasingly intrusive powers. Mass surveillance isn't the solution."

In the opinion of Carlo, government secrecy and lack of oversight are ushering in "a shadow surveillance state" that makes use of authoritarian surveillance technologies that could have been lifted from the pages of George Orwell's novel *1984*. Will we wake up to the danger and reverse this trend?


**Edmond O'Brien as Winston in the 1956 adaptation of *1984***

IAN BOTTLE / ALAMY STOCK PHOTO

Norton-Taylor, who is familiar with the wiles of Whitehall and its spooks over the past 40 years, isn't confident: "The trouble, particularly in the UK, is that most people regard the state as benevolent, a force for good, rather than a threat in any way. I am not so optimistic."

That's not just bad news for those immediately threatened by the hard edge of the surveillance state, detailed by Carlo as those with mental health problems, peaceful protestors and young black men. Ultimately, she warns that surveillance could induce a fearful state of conformity among all citizens.

"If we really want to think about where the drift towards a surveillance state leads we just have to look to China, because that is the blueprint," she says.

Based on the evidence, it's hard to disagree with Diane Abbott MP's assessment—"There is a danger that Britain is becoming a surveillance state"

However, whether the nightmarish society predicted by George Orwell in *1984* becomes a reality in the UK still depends on us, the great British public. ■