FREEDOM OF SPEECH AND FAKE NEWS

A future with no secrets

Technology, surveillance, rights and freedoms

Stephen Armstrong

A cyberactivist with her computer. Picture by Jordi Borràs

“In the future there will be no secrets,” according to BBC security correspondent Gordon Corera. “In the future, we will all be spies, and we will all be spied on”.

Is Corera’s vision utopian or dystopian? When we consider the slow push for open government by democrats and philosophers from the enlightenment to today, we cannot ignore the panopticon – the ‘perfect prison’ imagined by English philosopher Jeremy Bentham, who believed that power should be visible and unverifiable. Through constant surveillance, Bentham believed, morals would be reformed, health preserved and industry invigorated.

Bentham’s vision was limited to the technology of his times –he described cells stacked around a central tower, ever door wide open, every room flooded with light–. French philosopher Michel Foucault hated the idea; he called it a “cruel, ingenious cage”, a dungeon where deviation means death.

If Corera is correct, we are already living in a technological panopticon –and yet, in Bentham’s vision, the surveillance only went one way–. If all of us are also spies, then there is some power in our gaze. Therefore, what do we think about when we think of technology, surveillance, rights and freedoms? The mass searching of e-mails to track and monitor

dissenters? Government agencies taking control of our smartphones to record our most intimate moments? Or the TikTok K-pop fans capturing right-wing hashtags to support Black Lives Matter and the Catalan independence activists using airplane mode to build secret communications hubs?

In a sense, we are battling for the soul of the Computer. To be there at this soul's creation, we must soar back through the history of freedom and technology to the day they switched on Colossus, the world's first programmable computer, in its rural home at the UK's World War II code and cypher school Bletchley Park. Colossus was built with one purpose –surveillance. It was designed purely to decipher the Lorenz-encrypted messages between Hitler and his generals during World War II. The computer, it seems, was built to spy on us.

> Many of the founders of the Internet were counter-culture idealists who saw the computer as a liberator. Were they wrong?

Yet, many of the founders of the Internet were counter-culture idealists like the team surrounding 1980s and 1990s US cyberculture magazine *Mondo 2000*, the founders of the *Electronic Frontier Foundation* or even Tim Berners-Lee, who created the World Wide Web and now campaigns for net neutrality, internet freedom and democracy. They saw, and still see, the computer as a liberator. Were they wrong?

Has the net set us free?

"The premise was that the net will set us all free –but soon it became a hunting ground for law enforcement and a space where the commercial world is king," argues Alan Pearce, a personal privacy advocate and advisor. Philosopher and psychologist Shoshanna Zuboff calls this "surveillance capitalism" –where our lives are spied upon as much for profit as for control. "Someone hijacked our dream," says Pearce. "But people are irrepressible –and we are playing catch up. So now we're in a never ending game of cat and mouse –we find a way to hide, they discover it, we move on, always changing, always protesting".

The Catalan government and pro-independence activists have already survived an online game of cat and mouse with the Spanish state. On 13th September 2017, the Spanish government used a court order to shut down sites holding information about the forthcoming referendum on Catalan independence. Activists cloned sites as fast as the government could block them until Guardia Civil officers raided the headquarters of the .cat registry on 20th September, seizing computers and arresting the company's CTO Pep Masoliver.

"The Spanish government used an anti-phishing technical infrastructure to stop people going to certain websites," explained John Graham-Cumming, CTO of web security company Cloudflare. Troy Hunt, the Australian web security consultant who founded data breach site *Have I Been Pwned* shared his shock. "This is not something that you normally see in a

modern democracy," he argued. "It's the kind of thing you see in Turkey, Egypt, China and Iran".

In response, activists set up channels through encrypted messaging apps like Telegram, guiding internet users to access the affected sites using Virtual Private Networks and proxy services. During the October 1st, referendum polling station volunteers communicated through clandestine data networks created by routing smartphones through VPNs to operate without internet access. In the street, activists and referendum officials chanted "airplane mode", urging voters to preserve network bandwidth for people working inside the polling stations.

> The exponential scale of digital technologies penetration of our lives means that Google, as Eric Schmidt said in 2010, can look at enough of your messaging and your location, use artificial intelligence, and then predict where you are going to go

On the one hand, this is just the latest in the long battle between elites and democrats over the control and use of information technology. In 1501, Pope Alexander VI promised excommunication for anyone who used the printing press without the church's approval. Over the next 40 years, Martin Luther printed his *95 Theses*, John Calvin mass-produced the theories of Protestantism and Copernicus published *On the Revolutions of the Celestial Spheres*, triggering the scientific revolution. Controlling the printing press meant controlling information – the most powerful weapon in the religious wars that shook the continent. Little has changed.

On the other hand, the exponential scale of digital technologies penetration of our lives means that Google, as Eric Schmidt said in 2010, can "look at enough of your messaging and your location, and use artificial intelligence, and then predict where you are going to go. Show us 14 photos of yourself and we can identify who you are. It is possible that all that information could be made available to the authorities. If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place".

Unprecedented control

This new, unholy alliance between corporate capitalism and the imperial might of the state means the potential for both control and freedom is vast beyond historical precedent. We exist in a world where the European Data Retention Directive requires EU member states to store citizens telecoms data for between six months and two years, where China's Social Credit System records 'good' and 'bad' behaviour, denies air tickets to 'untrustworthy' people and allows the Communist Party to measure and suppress dissent, and where the US government deploys so many different systems to monitor e-mails, web traffic, search engine data and 'suspicious activity' that it's lost control of some projects, loosing malware like Stuxnet into the hands of hackers, where it has been used to shut down the UK's health

system in a ransomware attack.

“The tanks, rifles and ammunition used against us for generations are disguised as new technology accomplishing the same colonial purposes,” according Yeshimabeit Milner, founder and executive director of the *Data for Black Lives Movement* –and yet, she believes, at this moment the struggle is far from over and the victor is still in contention. “We need data and technology to be used to fulfil its true promise of social change –to be liberatory, to be part of a new form of activism that could truly change conditions and empower us”.

For years, democrats and liberals have been pushing for transparency –the light of discovery to disinfect the secrecy and lies of the elites. As a result, a long tradition of radical secrecy disappeared –swept aside by the drive for and practice of openness. Historically democracy has needed secrecy in times of trouble –to organise and to conceal that organising from those who would prevent it. From street slang to radical publications like *Berthold’s Political Handkerchief* –an 1831 radical newspaper printed in London on a cotton handkerchief to avoid the stamp duties on paper and allow those who bought the publication to simply dip it in water if the police came calling –there have been conversations that took place out of sight.

When faced with increasing social control, many activists argue that these techniques are protestors’ best defence. “The way the world is going governments, even liberal democracies, are increasing surveillance and control over the public because the technology is there and they’d be stupid not to,” says Pearce. “It’s possible for activists to disappear into the dark web but as soon as you do, they’ll think you’re hiding something. Always give them something to monitor.”

Pearce suggests the equivalent of chaff and flares – making so much noise and hiding in the midst of that noise. There is *TrackMeNot*, a browser extension that makes countless random search queries to hide user’s actual activity in a cloud of meaningless questions, or *OpenStego*, free opensource software that can disguise text, film or sound files by coding them into selfies or music tracks. Journalists, says Pearce, could conceal a video of mass graves inside Beethoven.

> Historically, democracy has needed secrecy in times of trouble to organise and to conceal that organising from those who would prevent it. When faced with increasing social control, many activists argue that these techniques are protestors’ best defence

However, argues Dr Clare Birchall, author of *Radical Secrecy*, the traditional nature of these techniques at best leaves us trapped in an eternal cycle and at worst may prove insufficient for these explosive times. She believes that the transparency activists, democrats and radicals pushed for in the 20th century has lost its power in the 21st. “We have no faith in revelation when we have leaders who are immune from shame,” she argues.

When transparency seems exhausted as a political tactic that does not mean a return to old school secret societies created to discuss democracy, she suggests. Instead, we need to experiment with forms of opacity and obfuscation to create spaces for thinking about a radical future.

“It might mean digital spaces; it might mean a change in the way we think about secrecy, but we must get beyond the grip that both secrecy and transparency hold on politics,” she explains. “Privacy is this liberal/conservative idea of property and rights – moving back from the light of demos into the shadows. It does not encourage collectivity. The right to opacity is the right to not be readable. In that unreadability you can come together to fight the surveillant gaze”.

Forms of radical opacity

As protestors battle governments, young protestors in particular are creating improvised forms of radical opacity. In America, the Black Lives Movement protestors faced police who were armed with fake mobile phone towers grabbing information from protestors phones, monitoring their emails, Facebook and Twitter pages and –in extremis– software that takes over phones and uses them to spy on their owners. To fight back, young protestors used temporary short form videos on sites like TikTok –a teen pop site– to organise actions. Hashtags on videos that were rapidly deleted co-ordinated activists to swamp police apps that asked citizens to report illegal activity.

At the height of the protests over the death of George Floyd, the Dallas Police Department, for instance asked people on Twitter to submit video of “illegal activity from the protests” to its IWatch Dallas app. Instead, the app was inundated with videos of South Korean pop stars, blocking all reporting of crimes. Eventually the police department tweeted, “Due to technical difficulties iWatch Dallas app will be down temporarily.” Meanwhile, the video posters digital trails had disappeared – so tracking them was impossible. In June, anti Black Lives Matter hashtags like #WhiteLivesMatter, #WhiteoutWednesday and #BlueLivesMatter were linked to endless pictures and performances of K-pop groups, drowning out the original users. At the end of June, protestors used TikTok to organise mass registration for hundreds of thousands of tickets for a Donald Trump election rally in Tulsa, leading to empty seats in front of TV cameras.

Codes, hidden meanings, e-mails that vanish after ten minutes, hashtags that swamp out right wing messaging –the new way of organising may stay one step ahead of the less nimble state enforcers, but what might Birchall’s radical spaces produce in terms of radical futures? Yeshimabeit Milner from *Data for Black Lives* Movement argues that it is only by taking control of technology’s means of reproduction –for her, that means its data and the biases by which that data is processed– that society can find its true self online.

“Tools like statistical modelling, data visualization, and crowd-sourcing, in the right hands, are powerful instruments for fighting bias, building progressive movements, and promoting civic engagement,” she argues. “But history tells a different story, one in which

data is too often wielded as an instrument of oppression, reinforcing inequality and perpetuating injustice. Redlining was a data-driven enterprise that resulted in the systematic exclusion of black communities from key financial services. More recent trends like predictive policing, risk-based sentencing, and predatory lending are troubling variations on the same theme. Today, discrimination is a high-tech enterprise".

Milner was first radicalised at her Miami school, which was run like a prison – students were sent home for forgetting their ID and could be suspended for wearing a 'gang colour' if they broke uniform rules. When students organised a protest after staff member put a student in a choke hold the city sent in SWAT vans with fully armed police officers. CNN reported a 'Riot at Miami Senior High School'.

Milner was incensed. She joined a local group, the Power U Center for Social Change, and set out to do their own data collection on treatment of black students. They surveyed 600 students and published the results in a comic book: *Telling It Like It Is: Miami Youth Speak Out on the School-to-Prison Pipeline*.

> Young Black Lives Matter protestors used temporary short form videos on sites like TikTok to organise actions, coordinate themselves and to swamp police apps that asked citizens to report illegal activity

After graduating, she worked on a campaign to collect data on the high rate of black infant mortality – twice the rate of white babies, according to the Department of Health and Human Services. She learned that breastfeeding was linked to infant health, and that hospitals discouraged black mothers from breastfeeding in favour of infant formula given through by formula companies. Based on her research, the hospital fired the head of its maternity unit.

She soon realised that this sort of bias was at the core of apparently neutral algorithms. In 2019, for instance, an algorithm widely used in US hospitals to allocate health care to patients was found to have systematically discriminated against black people. Research published in the journal *Science* showed the algorithm was, when faced with equally ill patients, less likely to refer black people than white people to programmes that improve care for patients with complex medical needs.

Changing algorithms

But how do we change the algorithm? First by realising it is only a recipe – a list of instructions to make a dish that could be healthy or unhealthy, tasty or foul depending on the ingredients – or data – we choose to include. Just as we would not let the state choose our ingredients, so we should have control over the data and thus we slowly change the outcome.

“The weaponisation of data cannot be changed by policy change alone,” she argues. “This is not a call for the end of all data just as the call to abolish prisons is not a call to end accountability, but to end a punitive violent system that is not working for our society. It is a new way of understanding the world that begins in our minds, organisations and academic institutions. It is about building coalitions, developing more skills, more empathy. We have an opportunity to abolish, re-imagine, and recreate new structures of knowledge production, new forms of decision making, and new ways of relating to each other. The possibilities for the future are infinite”.

Stephen Armstrong

Stephen Armstrong is a freelance journalist and author. He writes for the Sunday Times, the Daily Telegraph, Wired and the Guardian, among other media. He authored five non-fiction books: *The White Island* (2004), *War plc*: *The Rise of the New Corporate Mercenary* (2008), *The Super Rich Shall Inherit the Earth* (2010), *The Road to Wigan Pier Revisited* (2012) and *The New Poverty* (2017). He also founded the Wigan Pier Workshops in collaboration with English PEN and is a trustee of the Orwell Youth Prize and a fellow of the RSA.