Essay by Scott Ludlam
published May 2019 in *Griffith Review 64: The New Disruptors*

Cypherpunks and surveillance power

The global struggle for our digital rights

ON THE SURFACE, the global digital rights landscape is a depressing and forbidding place. US technology giants. The phrase 'data is the new oil' captures this ethic perfectly: our collective private lives are now assets to be stripped, refined and sold. The so-called Five Eyes alliance - the US, UK, Canada, Australia and New Zealand - continues its reign of driftnet surveillance and corporate espionage, and here in Australia, on the last parliamentary sitting day of 2018, we suffered a bipartisan assault on the cryptography standards that underpin privacy and security. Further down the curve, Chinese authorities have unleashed a deeply dystopian surveillance and behaviour modification regime against a sixth of the world's population. Social networks have been deployed to tilt whole electorates in the US and to fan ethnic cleansing in Myanmar.

Anchored by these dramatic expansions of state and corporate power, the truth remains as it was set out in journalist and essayist Quinn Norton's memorable 2014 piece for The Message, 'Everything is Broken': 'Your average piece-of-shit Windows desktop is so complex that no one person on Earth really knows what all of it is doing, or how.'

Norton describes how the whole digital medium - from desktops to the internet itself - is glued together with a tangle of hacks and patches as new features are added and security vulnerabilities are discovered. A surreal and lucrative market for information on how to exploit these vulnerabilities has sprung up between software developers, hackers and state intelligence agencies. To make things much worse, an exploding number of 'internet of things' devices with negligible security standards are being forced into our lives, magnifying the consequences when things go wrong.

Overwhelmingly, the tech industry is still culturally and politically dominated by white males from the global north, with the consequences reflected everywhere from gender bias among Wikipedia editors to deep discrimination in hiring practices and a sector-wide gender pay gap. And it isn't just a case of deleting our Facebook accounts and walking away, because many of us will be walking under a network of street cameras feeding facial recognition algorithms that report directly to security services.

My own interest in digital rights stems from late 2008, when the Labour government's proposal for a wide-ranging internet filter made headlines, provoking a spirited and ultimately successful campaign against the measure. Since then, we've been forced onto the back foot through an onslaught of terrible bipartisan initiatives from data retention to December's attack on cryptography. For this reason, much of the debate over digital rights over the last decade has been defensive in tone, and so instead of raking over this ground again, let's try something different. Let's go looking for the best examples of how peoples, states and companies are building something better, something that delivers on the internet's original promise of seamless connectivity for an emerging global community. Let's signal boost the good stuff for a change.

TO HELP ORIENT ourselves, it's worth briefly sketching out the simplest theoretical terrain, a map drawn along political and economic axes. Politically, it is still valuable to recall the original cypherpunk maxim from the mid-1990s, towards the end of the internet's long Precambrian era:

transparency for the state; privacy for the rest of us. You can align a lot of concepts along this gradient, if you agree with the basic premise: freedom of information laws, lobbyist registers, donations disclosure, data breach notifications, strong cryptography. It goes to the understanding that concentrations of power almost always go rancid without strong oversight and formal transparency, and to the complementary principle that the freedom of holding private thoughts and private communications with one another is a fundamental human right. In authoritarian states, these poles are inverted: the state withdraws itself and its operations behind firewalls, while turning surveillance and coercive capabilities against domestic populations in order to suppress dissident thinkers and fragment community organising. We'd be naive not to recognise multiple signs of this inversion here in Australia, and to an even greater degree in the United States. The way these debates are unfurling today reflects the digital dimensions of much older questions about how to constrain unaccountable power. On the upside, this means we don't need to reimagine countermeasures from the ground up: a lot of good thinking, creating and organising has already been done.

The economic axis goes more to the question of ownership. The surveillance capitalism model is hidden in plain sight, spelled out in twenty-page terms-of-service agreements that almost nobody reads. For the most part, we're signing over ownership of detailed imprints of our most private and intimate thoughts, relationships, movements and finances to very large extractive industries that now include the world's largest corporations. Their path to astonishing wealth accumulation lies in ever more granular on-selling of these digital profiles to advertisers and political parties, while forcefully sabotaging attempts at regulation. As a guiding theology, this is about as empty and devoid of human warmth as it’s possible to get. It is also diametrically at odds with some of the founding philosophies of the medium it is colonising: the availability of free and open-source software, and the existence of the digital commons. The idea of personal data sovereignty places these alternatives front and centre: what do these systems look like when we design tools that empower us, rather than mining us for marketable information?

Clarity over power and ownership goes some way towards neutralising the ways in which agency is increasingly ascribed to the technologies themselves, while those who build, own and wield them stay hidden behind the curtains. The best guides to this pervasive sleight-of-hand remain Adam Greenfield's Radical Technologies (Verso, 2017), which spotlights the business models and power dynamics behind common and emerging digital technologies, and Ellen Broad's Made by Humans (MUP, 2018), which unmasks some of the prosaic realities in the field of artificial intelligence.

When we go looking in these domains - transparency for the powerful, privacy for the rest of us; the digital commons and data sovereignty - we find a wealth of innovation and creativity built on decades of sustained effort. Since the mid-1980s, the free software movement has worked to ensure that the raw DNA of digital systems remains open to view and modification, starting with essential tools like text editors and compilers, and building towards the creation of the GNU operating system by Richard Stallman. As Stallman wrote in an online bulletin back in 1986:

> *The word 'free' in our name does not refer to price; it refers to freedom. First, the freedom to copy a program and redistribute it to your neighbours, so that they can use it as well as you. Second, the freedom to change a program, so that you can control it instead of it controlling you; for this, the source code must be made available to you.*

In the late 1990s, the free software movement branched into the open-source community, which holds a more pragmatic attitude towards the existence of proprietary software. 'Free software is a

social movement, and open source is a methodology,' as technology writer Klint Finley puts it. Between them, free and open-source developers have written some of the foundational architecture of the internet as we know it. Today, the Linux operating system kernel hums away in the brain stem of several billion Android smartphones and hundreds of millions of routers, as well as the vast majority of mainframes and web servers, supercomputers and home appliances. This astonishing popularity stems not just from the lower cost, but principally because the vastly larger number of eyes-on means the code is more robust and secure.

This ethic underpinned the astonishing growth in the world wide web from the late 1990s. HTML, the mark-up language that wove a web of self-published hypertext around the world, was designed to be written and edited by non-programmers, accounting for some of the early, explosive growth of the world wide web. Wikipedia, an open encyclopaedia that provoked the unexpectedly rapid extinction of its slow-moving paper ancestors, consistently rates in the world's five most heavily visited sites. None of these examples should even exist according to mainstream economic orthodoxy, which struggles to explain why so many people would plough their expertise into unpaid work. Nor do they operate according to an extractive mentality where human relationships are regarded as a kind of resource to be mined.

Free and open-source developers have also played an essential role in rebalancing the arms race between security and surveillance that rests on the question of cryptography standards. The global encrypted software market is predicted to continue expanding, rising to US$8.4 billion in 2024 from US$151 million back in 2013. For end-users, mobile messaging applications including WhatsApp and Facebook Messenger are rapidly becoming the dominant mode of electronic communication worldwide, and in the Western world these services are adopting stronger encryption standards one by one. In the wake of the Snowden revelations, outraged public demand has been met by a developer push to embed seamless cryptography in common messaging tools. But encryption is only as good as independent verification and auditing can prove it to be, which is why opensource apps like Signal are considered more reliable than closed proprietary systems like WhatsApp or Messenger. In an environment in which trust is in short supply, the ability of the wider developer community to test the claims of manufacturers counts for a lot.

Behind the technical standards lies an important political reality: whatever the industry says, people like privacy. And while keeping things genuinely private from determined state actors requires real skill, the ability of WikiLeaks staff to help orchestrate Edward Snowden's safe departure from Hong Kong in 2013 shows what's possible. For the rest of us, using Signal, starving Facebook of information and slowly divorcing Google in favour of DuckDuckGo and Searx, ProtonMail, firefox and OpenStreetMap raises the costs of indiscriminate surveillance and helps build an alternative software ecosystem. The website switching.social lays out a delightful menu of alternatives to everything from email to fair-trade smartphones. It's not an exhaustive list, but it is a healthy reminder that there are choices out there. The self-described 'grassroots website' points out that 'without wishing to sound overdramatic, if we do not control our own information then others will use it to control us.'

IS ANY OF this working? Trends are hard to spot in such a turbulent environment, but here's one indicator: 44 per cent of younger Facebook users in the US (in the eighteen to twenty-nine age bracket) told a Pew Research Center survey they had deleted the app from their phones in the last year, and 42 per cent of all US users said they had taken a break from checking the site for several weeks or more. It's much too soon to declare that Facebook is headed for a Myspace-style collapse, but for first time, the beleaguered platform seems vulnerable to upstart competitors.

Here in Australia, the self-inflicted debacle of the My Health Record system in 2018 demonstrates better than any survey the evolution of public attitudes towards governments' and the private sector's handling of their private information. The reservoir of trust has run dry: on the basis of a decentralised, leaderless information-sharing campaign and good media coverage, millions of people have opted out of a misconceived scheme and the issue has caused significant damage to an already wounded government. Similarly, the ferocious backlash against major party collusion to undermine encryption in December 2018 suggests that the political costs of abusing digital rights may be rising.

Slowly, the concept of personal data sovereignty is being honed as an alternative to aggressive surveillance capitalism. In something approaching a manifesto to this end, developer Arai Balkan sets out the boundaries:

> *... smart city architecture must be in the commons and data about the world around us ('data about rocks') must belong to the commons, while your smart car, smart phone, smart watch, smart teddy bear, etc, and the data they collect ('data about people') must belong to you.*

Global advocates of Indigenous data sovereignty point to ways in which this concept can be applied at scale. In the Australian context, the model was set out in a landmark statement in mid 2018 by the Maiam nayri Wingara Aboriginal and Torres Strait Islander Data Sovereignty Collective:

> *'Indigenous Data Sovereignty' refers to the right of Indigenous peoples to exercise ownership over Indigenous Data. Ownership of data can be expressed through the creation, collection, access, analysis, interpretation, management, dissemination and reuse of Indigenous Data.*

This work forms part of a reaction against processes in which Aboriginal people have become 'isolated from the language, control and production of data at community, state and national levels'.

Individual and collective data sovereignty only sounds radical when set against the bleak enclosure of the digital commons sold as a foregone inevitability by Silicon Valley oligarchs. It is entirely consistent with developed international human-rights frameworks and resonant with the original, open-source and free software underpinnings of the internet. Whole cities are now adopting these principles at scale.

Amsterdam is one city leading the way in integrating open data and strong privacy principles with a broader agenda of inclusive city building. Its 'Implementation plan: Participatory and digital' is a fascinating snapshot of how these principles can be put to work city-wide. Platform monopolies like Google and Uber are being rejected in favour of platform co-operatives, strong privacy protections and accessibility measures are being adopted, and new tools for civic participation and decision-making are being trialled. The city of Buenos Aires has opened its data holdings to the public through a graphical dashboard that residents can use to view budgets, municipal projects and environmental indicators in real time. Open Cities Africa is using OpenStreetMap - a free, open-source editable map of the world - for everything from flood resilience in the slums of Monrovia to participatory public health mapping in the Congo. In many parts of the world, OpenStreetMap is the only digital map available; the fact that it is free and can be updated collectively in real time makes it uniquely suited to this kind of work. In Australia, the open-source National Map project provides an elegant window into government geospatial data holdings across the states and territories - a singular example of government best practice amid the swamp of retrograde initiatives spawned by both the Home Affairs and Attorney General's departments.

Today, it is arguably the Barcelona Data Commons that is considered the gold standard. Combining open-data standards with strong privacy and data-sovereignty protections, Barcelona has steered directly away from the surveillance capitalism model to instead pursue a course to 'understand the value of data as a common asset and put citizens back in control'. And to look through the practical initiatives that make up the plan is to feel the spirit of transparency for the state, privacy for the rest of us at work across this city of more than 1.7 million people. In addition to opening the city's huge data holdings to developers and the general public, in 2018 the Barcelona City Council introduced a Data Protection Delegate to act as a guarantor of residents' privacy and data sovereignty.

At a continental scale, the implementation of the General Data Protection Regulation across the European Union from May 2018 has powerful implications worldwide. With the stated aim to 'protect all EU citizens from privacy and data breaches in today's data-driven world', the regulation applies to all entities with data holdings on EU citizens, whether they are based in Europe or not. Within hours of the new regulation coming into effect, US-based companies Google and Facebook were hit with lawsuits challenging the legality of forcing European users to consent to targeted advertising in order to use their services. At its heart, the regime levies huge fines for data and privacy breaches, strengthens the conditions for consent beyond unintelligible terms of service agreements, and strengthens EU citizens' right of access to data held on them by third parties. Critics have argued that the regulation is weakened by loopholes and introduces onerous compliance costs, but it nonetheless stands as a digital rights high-water mark.

AS YOU MIGHT expect, the private sector record on digital rights is mixed at best. US giants Google, Facebook and Amazon are predictably among the worst offenders, given their names are synonymous with the surveillance capital model. Even here, though, there are signs of hope - reminders that their operations are still occasionally circumscribed by acts of conscience. In June 2018, Google's engineers won an important concession when the company announced it would cease working on some of the US Defence Department's artificial intelligence research under Project Maven. The New York Times reported more than 4,000 Google employees signed a petition seeking 'a clear policy stating that neither Google nor its contractors will ever build warfare technology'.

These cracks in the armour are rare, and papered over by huge public-relations budgets and the evangelical aura of the companies' billionaire founders. But there are continual jarring revelations of Amazon's nineteenth-century work practices in which people are paid subsistence wages. There are repeated reminders of Facebook's slimy underside, from the Cambridge Analytica scandal to routine sharing of the private information of millions of people with other companies. These and many other examples have created a situation where even the giants may end up vulnerable to more ethical competitors.

There are exceptions to the rule, too, which prove that it's possible for tech companies to grow to significant scale without people losing their souls. Global software developer ThoughtWorks has more than 5,000 employees across fifteen countries, and a client base that runs from major government departments through to youth development organisation The Oaktree Foundation. Built on a foundation of diversity and pay equity, ThoughtWorks ploughs a significant fraction of its revenues into pro-bona work for not-for-profits and digital-rights organisations. The company's founder, Roy Singham, told CNN back in 2008: 'I believe the world should have access to the best ideas in software for free.' Since then, the company has provided technology and support to independent media around the world including Democracy Now!, and its developers contribute disproportionately to open-source software, including Bahmni, an open-source hospital information system built for low-resource environments that has partnered with Doctors Without Borders and others.

While positive examples from emerging and established businesses are inspiring, the dire state of the global digital-rights environment make it clear that it won't be enough to prevent whole new domains of exploitation under the surveillance capitalism model. Even as these hopeful alternatives are proliferating, so too are hundreds of millions of 'smart home' devices designed to gather information on the purchasing and social habits of whole populations in the name of 'convenience'. Taking back our digital rights can be as simple as choosing not to install spyware in our homes, but without deeper collective action, many trends will continue to run in the wrong direction.

Ultimately, this is a political project as well as a deeply personal one. Rights of any kind are never dispensed freely by the powerful: they have to be claimed through organised campaigns operating at many different scales. These campaigns will be controversial and occasionally polarising: witness the cold fury of the Western establishment when confronted with the sudden shocks of forced transparency that came courtesy of WikiLeaks and Edward Snowden. Defending and extending our rights is hard enough in a country like Australia, where the absence of a formal human-rights charter makes progress fraught and contingent on shaking up the stale cowardice of major-party politics. In more authoritarian parts of the world, an enveloping mesh of surveillance technologies are already tilting the balance further in favour of unaccountable power. We no longer need recourse to science fiction to see how dark things can get, because those futures are already here in Bahrain, China and Russia.

There is nothing in technology itself that makes it more or less prone to abuse by the powerful. These are questions of democracy and solidarity, and you don't have to be a cryptographer or software engineer to have a point of view. In Australia, well-established groups like Digital Rights Watch, Electronic Frontiers Australia and the Australian Privacy Foundation provide a solid starting point for people who are looking for advice, information or inspiration, meaning there's no need to feel alone in these campaigns. Digital rights are human rights, and that's a struggle with a lineage too strong and proud to be waived in anybody's terms-of-service agreement.

Scott Ludlam is a former Australian politician representing the Australian Greens. He served as a senator from Western Australia from 2008 to 2017, and as co-deputy leader of his party from 2015 to 2017. He is currently a columnist for The Guardian, and his first book on ecology, technology and politics will be published in 2019.