tni
transnationalinstitute

State of Power 2023

Digital Power

Subscribe to our newsletter:
www.tni.org/en/subscribe

or scan the QR code:

AUTHORS: Tina Askanius, Mizue Aizeki, Tomás Balmaceda, Laura Bingham, Kean Birch, Chris Byrnes, Cory Doctorow, Roberto J. González, Maximilian Jung, Anne Kaun, Anastasia Kavada, Alice Mattoni, Santiago Narváez, Karina Pedace, Nils Peters, Tobías J. Schleider, Julia Choucair Vizoso, Julie Uldam

EDITOR: Nick Buxton

COPYEDITOR: Deborah Eade

EDITORIAL ADVISORY BOARD: Sofia Scasserra, Deepti Bhartur, Nuria del Viso

ILLUSTRATORS: Zoran Svilar and Anđela Janković

INFOGRAPHIC RESEARCH: Hannah Hasenberger

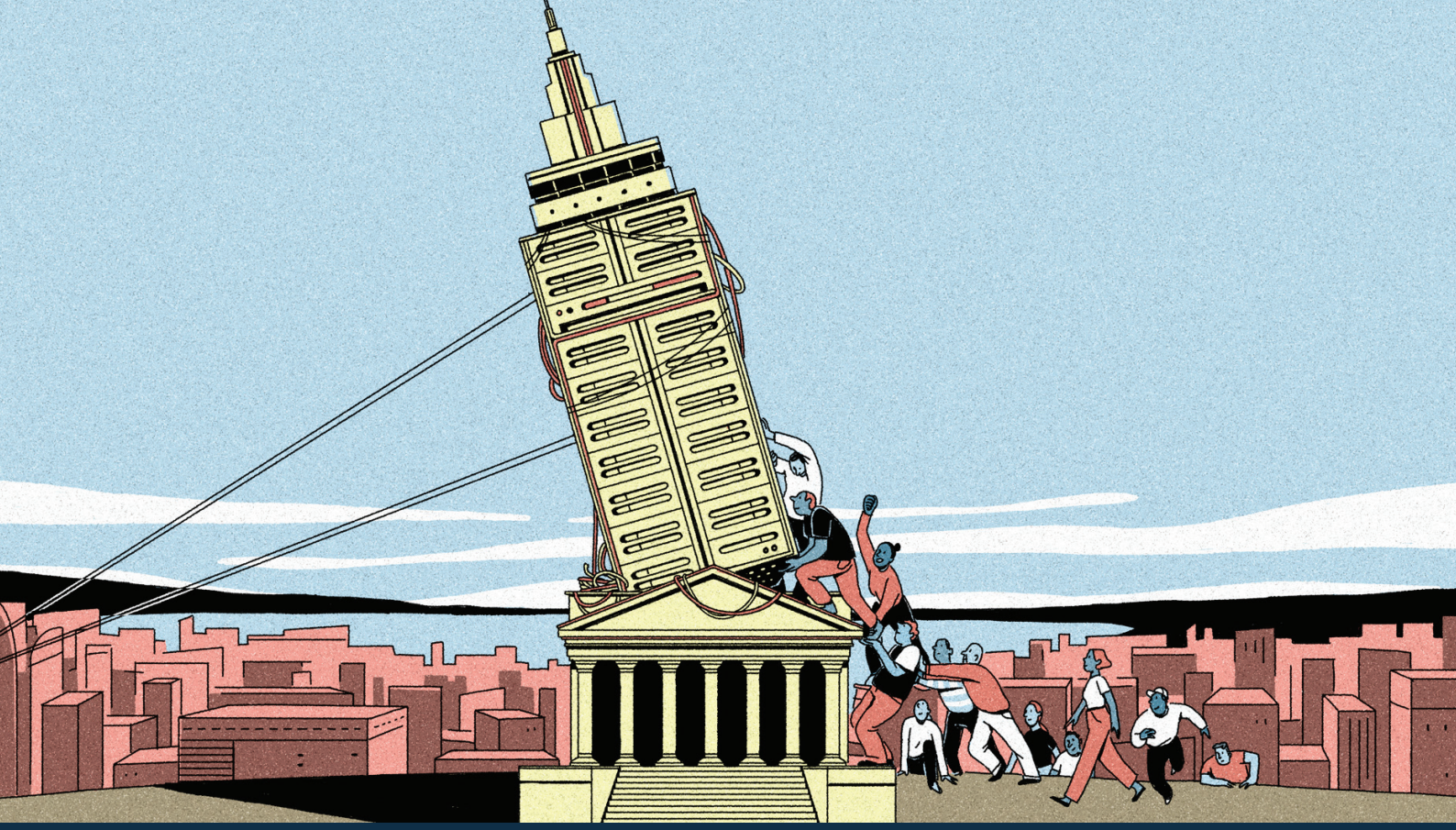
DESIGN: Evan Clayburg

PUBLISHED BY:

Transnational Institute – www.TNI.org

February 2022

Contents



Seizing the means of computation

How popular movements can topple Big Tech monopolies

Interview with Cory Doctorow

Cory Doctorow is a prolific writer and a brilliant science fiction novelist, journalist and technology activist. He is a special consultant to the Electronic Frontier Foundation (eff.org), a non-profit civil liberties group that defends freedom in technology law, policy, standards and treaties. His most recent book is Chokepoint Capitalism (co-authored with Rebecca Giblin), a brilliant expose of how tech monopolies have stifled creative labour markets and how movements might fight back. Nick Buxton, editor of TNI's State of Power report and Shaun Matsheza, host of the State of Power podcast, chatted to Cory in the wake of floods in his hometown of Burbank, California. This is an edited excerpt of the interview.

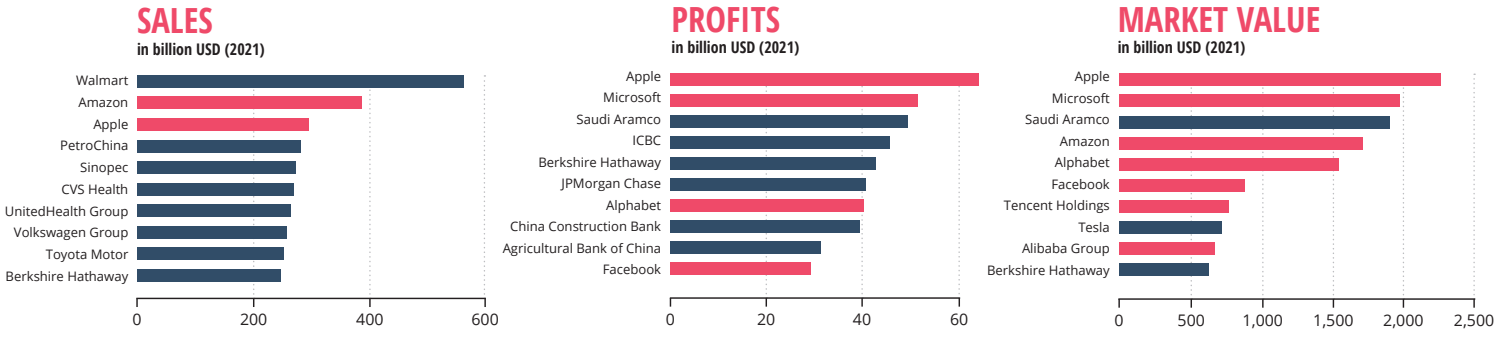
TNI: We want to start with a big open question that is at the heart of TNI's State of Power report: Who has digital power today?

Cory: That is an excellent question. As Tom Eastman, a software developer in New Zealand, has observed: the Web has devolved into five giant websites filled with screenshots of text from the other four. A small number of extremely powerful firms, namely Google, Amazon, Facebook, Apple, Microsoft, have what the European regulators call gatekeeper power—the right to decide who can speak, who can reach one another, how it works. This is a marked departure from the early ethos that birthed these firms, which was characterised by the idea that the internet would be a new kind of network where anyone who wanted to speak to anyone could do so without any third-party intervening. We now have any number of 'chokepoints' in which speech or similar activities like fundraising can be controlled by one of a very small number of firms.

And it's important to note that the reason those firms were allowed to grow as large as they have, the reason that state regulators turned such a blind eye, is because states view those firms as potential deputies for their own exercises of power. It is highly unlikely, for example, that the US National Security Agency (NSA) could have gotten regulatory authority or convinced us to carry beacons that broadcast our location all over the world. By allowing firms to do that, by failing to step in and demand regulation, the US government has accomplished a future in which the NSA doesn't need to wiretap us all. It can just ask Facebook or Google or Apple for information that it couldn't otherwise reach. And so this really needs to be understood as a public–private partnership.

BIG TECH IS THE MOST PROFITABLE AND VALUABLE INDUSTRY

Top ten companies according to sales, profits and market value



Source: Forbes Global 2000, 2021

Big Tech giants are often abbreviated as GAFAM – Google (Alphabet), Amazon, Facebook, Apple, Microsoft). With the rise of Chinese counterparts, Alibaba and Tencent, we need a new acronym: GAFAAMT?

TNI: How does this interplay of power between the state and corporations take place?

Cory: Well here's a very clear example. Google gathers your location data in a way that is plainly deceptive. If you turn off location tracking in your Android or iOS device, it will not stop tracking your location. There are at least 12 different places where you have to turn it off to stop the location tracking. And even then, it's not clear if they're really doing it. Even Google staff complain that they can't figure out how to turn off location tracking. Now, in any kind of sane world, this would be a prohibited activity. Section Five of the Federal Trade Commission Act gives the agency broad latitude to intervene to prevent 'unfair and deceptive' practices. It's hard to defend the idea that if you click the 'Don't track me' button and you're still tracked that that practice is fair and non-deceptive. This is clearly the kind of thing the law prohibits. And yet governments have taken no action. We haven't seen legislation or regulation to impede this.

At the same time, we see increasing use of Google location data and what the state calls either geofence warrants or reverse warrants. This is where a law-enforcement agency goes to Google, sometimes but not always with a warrant, and describes a location—a box, this street by street—and a time frame, say 1pm to 4pm, and demands to know everyone who is in that box. This was used extensively against Black Lives Matter demonstrators and then against the 6 January rioters. So, you can see here how the state has a perverse incentive not to prevent this deceptive, unfair conduct.

But it's very dangerous conduct, because a company as big as Google is always going to have insider threats, such as employees who will take bribes from other people. Twitter, for example, is well understood to have had Saudi operatives who infiltrated the company and then stole Saudi users' data and provided it to Saudi intelligence services so they could both surveil these activists and take reprisals against them in the most violent and ghastly ways imaginable.

There are also the risks that any data you collect will eventually leak and could be taken over by criminals. Sound regulation would involve snuffing this conduct out. The only way to understand why it trundles on is that there are too many stakeholders within the government who rely on these very dangerous and deceptive databases to make their jobs easier. So, not only do they fail to support efforts to rein in Google and other firms, they actually brief against doing so both publicly and then behind the scenes. It's very hard, as Upton Sinclair once observed, to get someone to understand something when their pay-check depends on them not understanding it.

TNI: What are the implications of this state–corporate relationship at a global level?

Cory: Well in the mid-2000s to early 2010s, we saw tech firms moving in to establish local offices in countries where the rule of law was very weak. There was a watershed with Google moving into and then out of China, and then we saw lots of firms setting up shop in Russia after its accession to the World Trade Organization (WTO). We saw Twitter setting up an office in Turkey. And all of this was important because it put people in harm's way. It gave the national governments of these countries the power to literally lay hands on important people within that corporate structure and thus to coerce cooperation from those firms in a way that would be much harder if, say, Erdogan wanted to shake his sabre at Google officials in California. If the nearest Google executive was an ocean and a continent away, Google would have a very different calculus about its participation in Turkish surveillance than when there are people that they care about who could be physically rounded up and chucked in prison.

There is a similar story of the proliferation of great firewalls, first in China and then as a turnkey product [installed and ready to operate systems] elsewhere, as Chinese and Western companies sold their turnkey solutions to governments with very little of their own technical capacity.

This has led governments to say to companies that unless you put someone in this country and store your data here, we will block you at our border. And they cite data-localisation rules from the European Union (EU) that that says that US firms operating in the EU can't move Europeans' data to the US, where the NSA can get at it. This is a perfectly reasonable regulation for the EU to have made. But depending on the nature of the government, it may be that they have even less respect for privacy than the NSA, or are even more apt to weaponise their own citizens' data than the US. I'm thinking, for example, of how the Ethiopian state has used turnkey mass-surveillance tools from Western firms to round up, arrest, torture and murder—in some cases, democratic opposition figures. So, to understand how it is that that data is within reach of Ethiopian authorities, you have to understand the interplay of data localisation, national firewall technology, and the imperative of firms to establish sales offices in countries all over the world in order to maximise their profits.

TNI: And how does Artificial Intelligence or machine learning fit into this?

Cory: I don't like the term artificial intelligence. It is neither artificial nor is it intelligent. I don't even really like the term machine learning. But calling it 'statistical inference' lacks a certain je ne sais quoi. So, we'll call it machine learning, which is best understood as allowing for automated judgment at a scale that human beings couldn't attain. So, if you want to identify everything that is face-shaped in a crowd by looking through a database of all the faces that you know about, a state's ability to conduct that would be constrained by how many people they had. The former East Germany had one in 60 people working in some capacity for the intelligence services, but they couldn't have come close to current scales of surveillance.

But that brings up a couple of important problems. The first is that it might work, and the second is that it might not. If it does work, it's an intelligence capacity beyond the dreams of any dictator in history. The easier it is for a government to prevent any opposition, the less it has to pay attention to governing well to stop opposition from forming in the first place. The cheaper it is to build prisons, the fewer hospitals, roads, and schools you need to build and the less you have to govern well and the more you can govern in the interests of the powerful. And so, when it works, it's bad.

And when it fails, it's bad because it is by definition operating at a scale that's too fast to have a human in the loop. If you have millions of judgments being made every second that no human could ever hope to supervise, and if there's only a small amount of error, say it's 1%. Well, 1% of a million is 10,000 errors a second.

TNI: So, has anything changed since Snowden's revelations?

Cory: I do think that we have an increased sense that surveillance is taking place. It's not as controversial to say that we are under mass surveillance, and that our digital devices are being suborned by the state. It has created the space for firms and for non-profits to create and maintain surveillance-resistant technologies. You can look at the rise of the use of technologies like Signal as well as the integration by large firms such as Facebook of surveillance technology in WhatsApp.

And within industry there is an increased sense that this mass surveillance is bad for it because the core mechanism used by government surveillance agencies is to identify defects in programming and rather than reporting those defects to the manufacturers, hoarding them and then using them to attack adversaries of the agency. So, the NSA discovers some bug in Windows, and rather than telling Microsoft uses it to hack people they think are terrorists or spies or just adverse to US national interests.

And the problem with that is that there's about a one in five chance per year that any given defect will be independently rediscovered and used by either criminals or a hostile government, which means that the US government exposed its stakeholders, firms and individuals to a gigantic amount of risk by discovering these defects and then not moving swiftly to plug up these loopholes. And that risk really is best expressed in the current ransomware epidemic, where pipelines, hospitals and government agencies and whole cities are being seized by petty criminals.

So that's the kind of blowback that we've seen for mass surveillance and it has created the spark of an anti-surveillance movement that is gaining steam, even if it hasn't come as far as you would hope, given the sacrifice that people like Ed Snowden made.

Anything that can't go on forever will eventually stop. And mass surveillance is so toxic to our discourse, so dangerous and reckless, that it can't go on forever. So, the question isn't whether it will end, but how much danger and damage will result from it before we end it. And moments like the Snowden revelations will bring that time closer.

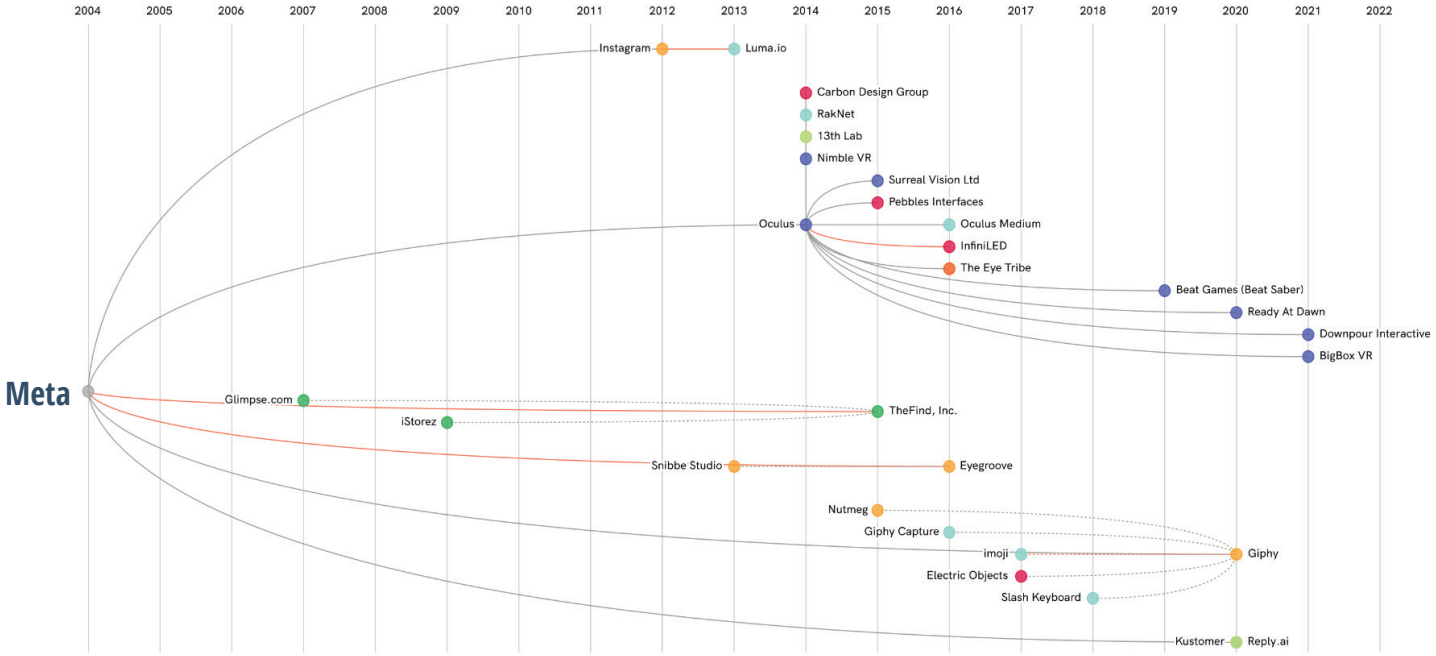
TNI: I'd like us to return to the companies that are in charge of this technology. How would you characterise the problem of Big Tech? Are we talking about a few companies or individuals that have too much power like Elon Musk or Mark Zuckerberg? Or is the problem that of their business models, the mass surveillance? Or is it that Big Tech is operating within a much broader structure that's problematic?

Cory: The first thing we need to understand about Big Tech is they're not very good at innovation. Take Google. This is a company that made three successful products. They made a very good search engine 30 years ago, a pretty good Hotmail clone, and a kind of creepy browser. Everything else that they've made in-house has failed. And every other success was achieved by buying another company. When Google video failed, they bought YouTube. Their ad tech stack, their mobile stack, their server-management tools, their customer-service tools: with the exception of those three tools, every part of Google's enterprise they bought from someone else.

Historically, anti-trust regulators would have prevented these anti-competitive mergers and acquisitions and have forced these companies to either figure out how to innovate on their own or get out of the way while people who had better ideas race past them. Google is not unique: Apple, Facebook, Microsoft are all company-buying factories that pretend to be idea-generating factories. We have frozen tech in time by allowing firms that have access to the capital markets to decide what the future of tech is going to look like. It's a planned economy, but it's one that's planned by a few very powerful financiers and the executives of a few large companies, not by lawmakers or democratically accountable government—or indeed by an autocrat, or at least an autocrat in office. We get autocrats in boardrooms these days.

BIG TECH GREW BY GOBBLING UP SMALL TECH

Companies bought by Meta (Facebook) 2007–2022



Source: gafam.theglassroom.org

"Competition is for losers. If you want to create and capture lasting value, look to build a monopoly."

– Peter Thiel, co-founder of PayPal, first outside investor in Facebook

And once you understand that these firms' major advantage is in being able to access the capital markets and buy and extinguish potential rivals before they can grow to significance, then we start to understand where their power lies. It's a mistake to believe the hype of Google and Facebook who go out and tell potential advertisers that we've built a mind-control ray that we can use to sell anything to anyone if you pay a premium. People have been claiming to have built mind control since Rasputin or before, and they were all lying. Their extraordinary claims require extraordinary evidence—and the evidence is very thin. What we see instead is firms that have a monopoly. Facebook can target 3 billion people because it spies on them all the time and because it's basically impossible to use the internet without using Facebook. Even if you're not a Facebook user, every app you're using has a good chance of being built with Facebook's toolkit, which means that it's always gathering data on you. The same is true of Google. It's not the case that the surveillance business model is what gave these companies power. It is their power that let them adopt a surveillance business model that would otherwise have been prohibited under any sane system of regulation, or would have been undermined by competitors.

For example, lots of people like having a great search engine but very few of us realise how Google spies on us. Historically, if you have a company whose digital products do three things that its customers like and one thing they despise, then someone will make an after-market module that gives you all the things you like and none of the things you don't. However, whenever a company

tries to build something like that, they're either bought out by Google or Facebook or Apple or one of the other big companies, or they're sued into oblivion for engaging in conduct that's very similar to what these firms themselves engaged in when they were growing. When they do it, it's a legitimate process. When we do it, it's theft.

TNI: What about those who say it's about the business model of surveillance that the likes of Google are adopting?

Cory: I don't think it's related to the business model. There is this idea that if you're not paying for the product, you're the product. Well, Apple has rolled out some really great anti-surveillance technology that blocks Facebook from spying on you. But it turns out that even if you turn on the Don't Spy on Me tools in your iOS device, your iPhone or your iPad, Apple still spies on you. They deceptively gather an almost identical set of information to what Facebook would have gathered, and they use it to target ads to you. The single biggest deal that Apple does every year that's negotiated in person between Apple's senior executive, Tim Cook, and Google senior executive, Sundar Pichai, is the one that makes Google the default search tool on iOS, which means that every time you use your iPhone, you're being spied on by Google.

So, the idea that there is a good company and a bad company or that the surveillance business model turns good, honest nerds into, you know, evil crepuscular villains, doesn't bear scrutiny. Companies will treat you how they can get away with treating you. And if they can find a way to make money by treating you like the product, they will. And if you think giving them money will make them stop, you're a sucker.

TNI: I have to say, Cory, your response is the first one that's somewhat encouraging when we understand Big Tech's digital power as based on mediocrities who happen to get a monopoly. So essentially, if we're able to break their monopoly, then perhaps we can reclaim their power?

Cory: Yeah, I think that's very true. The problem with the mind-control ray theory that you see advanced in books like Shoshana Zuboff's *Age of Surveillance Capitalism* is that it's a counsel of despair. There's a section where she says, 'Well, what about competition law? What if we just broke these companies up and made them less powerful?' She argues that won't make them less powerful because now that they've got mind-control rays even if you make them small again, they'll still have the mind-control thing. And rather than having one mind-control ray out being controlled by an evil super-villain, you'll get hundreds of evil super-villains like suitcase nukes being wielded by dum-dum terrorists instead of our current coldly rational game theory played by superpowers.

That that would be true if they had, in fact, built super weapons. But they haven't. They're not even good at their jobs. They keep making their products worse and they make lots of terrible blunders. And like lots of powerful people, they can fail up and because they've got a great big cushion—market power, capital reserves, access to the capital markets, powerful allies and government agencies and other firms that depend on you for infrastructure and support—they can make all kinds of blunders and kind of motor along. Elon Musk is the poster child for failing up. A man who is so insulated by his wealth, his luck, and his privilege that it doesn't matter how many times he screws up, he can still land on his feet.

TNI: So where did the left go wrong? I came of age in the 1990s where it very much felt that the internet was an emancipatory tool and that left-wing progressive forces were very much at the cutting edge of it, whether it was challenging structures like the World Trade Organization or overthrowing undemocratic governments. But now we live in a time where the big corporations have got a choke point of control, and where internet discourse is very much populated by disinformation and it's the far right who seem to be much more successful in using digital technologies. So, what do you feel has happened to cause this and what are the lessons?

Cory: The flaw was not about seeing the liberating potential of technology or failing to see its potential for confiscating liberty and power, but rather to fail to understand what had happened to competition law and not just in tech, but in every area of law, which began with Ronald Reagan and accelerated through the tech age. Remember that Reagan was elected the year the computer Apple II Plus hit the shelves. So, neoliberal economics and the tech sector can cannot be disentangled. They are firmly inter-penetrated. We failed to understand that something really foundationally different was happening in how we allowed firms to conduct business, letting them buy any competitor that got in their way, and allowing the capital markets to finance those acquisitions to create these monopolies which would change the balance of forces.

My own history is that I got an Apple II Plus in 1979, which I fell in love with and became a young, technology-obsessed kid. At that time, the companies that were giant one day were collapsing the next with some new company that was even more exciting coming up behind it. And it was easy to think that that was an intrinsic character of technology. In retrospect, it was the last days of a competitive marketplace for technology. The Apple II Plus and personal computers were possible because of anti-trust intervention in the semiconductor industry in the 1970s. The modem was made possible by the breakup of AT&T in 1982.

As a result, we now have this world where that foment and dynamism has ended. We live in an ossified time. A time when tech, entertainment and other sectors have merged not just with each other, but with the military and the state, so that we have just an increasingly concentrated, dense ball of corporate power that is intermingled with state power in a way that is very hard to unwind.

TNI: So, would you say the genie is out of the bottle? There seem to be some moves towards regulation in the last few years, such as the General Data Protection Regulation in Europe, the Digital Markets Act. You're seeing some anti-trust discussions in the US and generally people are now awake to this. How would you view these efforts by lawmakers and the greater public awareness?

Cory: We're living through an extraordinary moment, a regulatory moment, on Big Tech and other kinds of corporate power that is long overdue and been a long time coming. I think that is down to a growing sense that Big Tech is not an isolated phenomenon, but is rather just one expression of the underlying phenomenon of increasingly concentrated corporate power in every sector. So that when we say we want Big Tech tamed, we are participating in a movement that also says we want Big Agriculture tamed and Big Oil and Big Finance and Big Logistics and all of these other large integrated, concentrated sectors that provide worse and worse service, take larger and larger profits, inflict more and more harms, and face fewer and fewer consequences.

We can also draw hope from the way that digital technology is profoundly different and genuinely exceptional from other kinds of technology, which is that digital technology is *universal.* There's really only one kind of computer we know how to build. It's the Turing complete von Neumann machine. Formally, that is a computer that can run every programme that we know how to write, which means that if there is a computer that is designed to surveil you, there is also a programme that can run on that computer that will frustrate that surveillance. That is very different from other kinds of technology, because these programmes can be infinitely reproduced at the click of a mouse and installed all over the world. Now, this means on the one hand, that criminal organisations are able to exploit technologies in all kinds of terrible ways. There is no such thing as a hospital computer that can only run the X-ray machine and not also run ransomware. But it means that what we used to call hacktivism and what is increasingly just being called good industrial policy as contemplated in things like the European Digital Markets Act, has the potential to tip the balance in which the infrastructure of these large firms and the states that support them are suborned to support people who oppose them.

TNI: So, what do you think is going to be needed to make the most of this moment? How can we provide the push to make it a proper tipping point?

Cory: Tipping point is maybe the wrong way to think about this. There's something in stats called the scalloped growth curve. You've probably seen these, where you have a curve that goes up, hits a peak, goes down to a higher level than it was at before, and then comes up to a new peak and then to a higher level than it was before. So, it's a kind of punctuated growth.

And the way to think about that in terms of suspicion of corporate power is that corporate abuses—which will inevitably happen as a result of concentrated power—will gradually build its own opposition. For example, last month, a million flyers were stranded during Christmas week by Southwest airlines which was part of the $85 billion airline bailout and which has declared a $460 million dividend for its shareholders. The secretary of state who is supposed to be regulating them, Pete Buttigieg, did nothing even though he had broad powers to intervene. And this has created lots of partisans for doing something about corporate power. Now, those people have other things to do with their lives. Some will drop out, but some of them are going to nurse a grudge and will be part of this movement for taming corporate power. And because these firms are so badly regulated, hollowed out, and exercise power in such a parochial and venal way, they will eventually create more crises and even more people will join our movement.

So, I don't think it will be a tipping point so much as a kind of slow, inexorable build-up of popular will. And I think that our challenge is to get people to locate their criticism in the right place, to understand that it's unbridled corporate power and the officials who enable it, that it's not the special evil of tech or a highly improbable mind-control ray. Or, I'm sure it goes without saying: it's not immigrants, it's not George Soros, it's not queers. It's unchecked corporate power.

TNI: I've been enjoying your book, *Chokepoint Capitalism,* and I guess a lot of our conversation has been focused on us as consumers or activists. We haven't touched so much on workers. You have some good stories in your book about how activists and workers have confronted and rolled back corporate power. Could you share one of the inspirational stories that we should learn from?

Cory: Sure. My favourite one is actually by Uber drivers, whom we talk about as an exemplar in the book. Here in California, Uber was engaged in rampant wage theft of Uber drivers, not the normal wage theft of worker misclassification, but a separate form of wage theft where they were just keeping money that they owed. In California, Uber drivers had to sign a binding arbitration waiver in order to drive for Uber, in which all disputes would be heard by an arbitrator on a case-by-case basis.

An arbitrator is a fake judge who works for a corporation employed by the company that wronged you, who unsurprisingly rarely finds against the company that pays his fee. But even if they do, it doesn't matter, because usually that settlement is confidential and is not precedential, which means that the next person can't come along and use the same argument to get a similar outcome. Most importantly, a binding arbitration waiver forbids a class action, which meant that every Uber driver would have to individually hire counsel to represent them, which would never be economically sensible or feasible. All this meant that Uber could get away with stealing all this money.

So, the Uber drivers worked with a smart firm of lawyers, and they figured out how to automate arbitration claims. And hiring an arbitrator, which Uber has to pay for as the entity that is imposing an arbitration waiver, costs a couple of thousand dollars. So, if a million people demand arbitration of their claims, then just rejecting those claims would cost more than doing the right thing and paying up. So, facing hundreds of millions of dollars in arbitrator fees, Uber settled with the drivers and gave them a $150 million cash money, which is pretty goddamn amazing.

TNI: Oh, that's really cool. It's a sign that change is somewhat possible.
And to follow on that, I want to ask, do you think it's possible to reshape digital power, broadly defined as you described at the beginning in the public interest, and to use it to address the big crises such as environmental collapse?

Cory: I think that technology that's responsive to its users' needs, technology that that is designed to maximise technological self-determination, is critical to any future in which we address our major crises. The main thing that digital technology does, the best way of understanding its transformative power, is that it lowers transaction costs—the costs you bear when you try to do things with someone else.

When I was a kid, for example, if I wanted to go to the movies with friends on a Friday night, we would either have to plan it in advance or we did this absurd thing where we would call each other's mothers from payphones, leaving messages and hoping they somehow got through. Of course, now you just send a text to your group chat saying, Anybody up for a movie? That's a simple and straightforward example of how we lower transaction costs.

The internet makes transaction costs so much lower. It allows us to do things like build encyclopaedias and operating systems and other ambitious projects in an easy, improvisational way. Lowering transaction costs is really important to fomenting social change because, by definition, powerful actors have figured out transaction costs. If you're a dictator or a large corporation, your job is to figure out how to coordinate lots of people to do the same thing at once. That's where the source of your power is –coordinating lots of people to act in concert to project your will around the world.

So, while these transaction costs mean the cost of figuring out who is at a protest has never been lower for police cops, the cost of organising a protest has also never been lower. I spent a good fraction of my boyhood riding a bicycle around downtown Toronto pasting posters to telephone poles, trying to mobilise people for anti-nuclear-proliferation demonstrations, anti-apartheid demonstrations, pro-abortion demonstrations and so on. So, whatever fun people might make of clicktivism, it is riches beyond our wildest dreams of just a few decades ago.

So, our project needs to be not to snuff out technology, but to figure out how to seize the means of computation, how to build a technological substrate that is responsive to people, that enables us to coordinate our will and our effort and our ethics to build a world that we want—including one with less carbon, and with less injustice, more labour rights and so on.

Here's an example of how it can do that to address the environmental crisis. We are often asked to choose between de-growth and material abundance, so we're told that de-growth means doing less with less. But there is a sense in which more coordination would let us do significantly more with less. I live in a suburban house outside Los Angeles, for example, and I have a cheap drill because I only need to make a hole in my wall six times a year. My neighbours also own terrible drills for the same reason. But there is such a thing as a very good drill. And if we had a world in which we weren't worried about surveillance because our states were accountable to us, and we weren't worried about coercive control, then we could have drills that were statistically distributed through our neighbourhoods and the drills would tell you where they were. That is a world in which you have a better drill, where it's always available, always within arm's reach, but in which the material, energy, labour bill drops by orders of magnitude. It just requires coordination and accountability in our technology.

There are no markets anymore

From neoliberalism to Big Tech

Kean Birch

Google's original motto was 'don't be evil'. Today, it struggles to live up to this noble principle, as a recent and ongoing court case brought against Google amply demonstrates. The most recent litigation document even states that 'it seeks to ensure that Google won't be evil anymore'. You may not have heard of this lawsuit, but it provides an important insight not only into Google but also into the whole edifice Big Tech has built up over the last decade or so, and which has gradually taken over our economies and undermined our markets.

The case against Google is being led by the State of Texas, along with 16 other US states. It is an antitrust suit called *In Re: Google Digital Advertising Antitrust Litigation* and was announced in 2020 by the Texas Attorney General, with its most recent amended version published in January 2022.[1] It is running alongside a better-known antitrust case against Google brought by the US Justice Department at the end of 2020.[2]

At the heart of *In Re: Google Digital Advertising* is the claim that Google is monopolising the technologies and market information underpinning online programmatic advertising,[3] including the use of our personal data to try to sell us stuff. Programmatic advertising is a tangled beast of a system which Google sits astride as both buyer and seller of online advertising space. Similarly, Facebook (now Meta) sits at the centre of this online advertising market.

Here's a quick description of how programmatic advertising works, and how this market has been exploited.

Let's pretend you're an advertiser: say you want to sell your book—although it could be any product or service—so you probably want to reach people who will actually buy it. Google offers to connect you to the online advertising space best suited to that purpose through its 'ad exchange'. It does this by collecting and aggregating an enormous amount of our personal data from our searches, emails, smartphones, third parties using their analytics applications, and so on. We are largely unaware that we are handing over our personal data; it is hidden in the small print in the terms and conditions that most people simply sign in order to use digital products and services.

Using our personal data, Google can make inferences about our personal preferences—for instance, I like science fiction—and decisions—I'm likely to click on an online ad. With this information, they automate the buying and selling of adspace in the microseconds between our opening a webpage and seeing an advert. Google sells online adspace to you, the advertiser, to target your advert precisely at each viewer. A third party, such as a newspaper, sells adspace on its website to Google. In other words, Google both buys and sells adspace, also mediating between buyers and sellers through an auction exchange it controls—and from which it takes a cut.

The Texas lawsuit makes two critical allegations:

First, that Google and Facebook have colluded to monopolise the online advertising market, thereby excluding competitors from the market; this agreement was codenamed 'Jedi Blue'.

Second, that Google launched a secret programme in 2013 called 'Project Bernanke', allegedly designed to deceive advertisers and website publishers.

Project Bernanke revolves around Google's design of the auction system used to buy and sell adspace.

Auctions can be designed in different ways. For example, auctions using *sealed bids* are often presented as a key feature of market competition because they enable market actors to reveal their true preferences without fear of being exploited or the system being gamed by other market actors. This is because no one sees the other bids until these are revealed at the end of the auction process; thus no one can change their bid in light of what other bidders are doing. Sealed bid auctions should, then, be the most efficient mechanism for determining 'ideal' prices in a market economy.

Economists have long sought to theorise the best design for auctions, with William Vickery famously winning a 'Nobel' Prize for his work on the benefits of second-price auctions, now called *Vickery auctions.* A second-price auction is designed to ensure that the highest bidder wins but also pays the second-highest bid, thereby incentivising bidders to reveal their true preferences (i.e. they won't fear bidding too much). There are also third-price auctions, where the highest bidder will pay the third-highest price bid.[4]

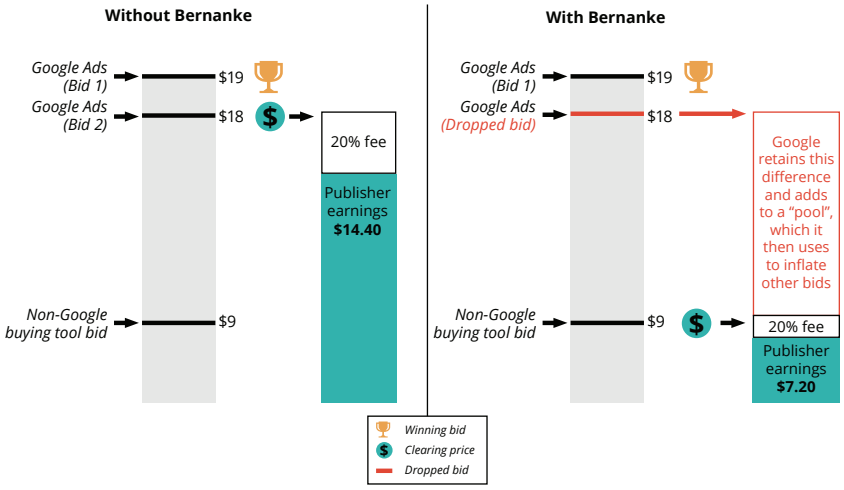
To return to Google and Project Bernanke. According to the Texas lawsuit, Google designed their ad exchange as second-price auctions, and told everyone that. However, according to the lawsuit, Google 'surreptitiously switched Google's AdX exchange from a second-price auction to a third-price auction on billions of impressions per month'.[5]

Although this might sound complicated, it's not. Basically, Google told advertisers that they would pay the second-highest bid, and told publishers they would be paid the second-highest price. It is alleged that in fact Project Bernanke changed the system so that publishers would receive the third-highest bid, while Google would net the difference. According to the claims, this meant that publishers lost up to 40% of their revenues as a result, but knew nothing about it. Google then 'pooled' these extra revenues and used them to 'inflate the bids of advertisers bidding through Google Ads to help them win impressions they would have otherwise lost to advertisers bidding through non-Google buying tools'.[6]

As one commentator noted, Google basically overcharged advertisers and underpaid publishers by controlling the market-pricing technologies and architecture; they designed the market to benefit themselves and drive out competitors.

Image: Googles' Bernanke Programme

The Bernanke program caused AdX to drop the second bid from the auction and lowered publisher earnings. Google retained the difference and adds it to a "pool" to use it to inflate other bids.



Source: Texas Attorney General, 2022, p.107

Markets and the Long Tail of Neoliberalism

The takeaway from all of this is that their control over digital platforms enable Big Tech firms like Google to design markets in ways that best suit them. The lack of transparency in these platforms means that markets can deviate quite significantly from the assumptions of pro-market thinkers and policy-makers who have dominated how we understand economies and societies since the 1970s.

Often defined as 'neoliberalism', the underlying assumptions of this worldview can be described as a political-economic and moral project to redesign societies to put markets at the centre of decision-making, whether by governments, organisations, or individuals.[7] Harking back to the work of thinkers like Friedrich Hayek—the famous peripatetic Austrian economist—neoliberalism is premised on the idea that no one agency (e.g. government) can coordinate the economy or society because it lacks the cognitive capacity to process all the information we individually produce and use to make everyday decisions. For Hayek and other neoliberals, markets are the best information processors for efficiently coordinating our societies. As Hayek put it:

'The reason for this [economic problem] is that the "data" from which the economic calculus starts are never for the whole society "given" to a single mind which could work out the implications and can never be so given'.[8]

Hence, markets are the best way to coordinate society since they can provide us with information to make the *right* decisions. They do this through the price mechanism, where prices are proxies for information telling us what and when to produce, when to change our preferences, and how best to manage our collective resources. Markets are, in this framing, both a factual *and* a moral mechanism; they tell us how to decide and what decisions are best to make.

Within this neoliberal narrative, information becomes a critical component in the working of markets. People cannot reveal their preferences or make decisions without information. Since Hayek, the problem of information permeates much orthodox economic thinking.[9] However, it is precisely in neoliberal thinking about information that its assumptions about markets start to come unstuck. This is because, at least in the policy and legal spheres, neoliberal thought gradually shifted from Hayek's view that societies will gradually evolve towards markets and market thinking to a perspective in which societies are simply assumed to operate like markets with everyone behaving as if they are market actors responding to incentives, defined by prices as proxies for information.

This is wonderfully outlined by S.M. Amadae (2016) in her book *Prisoners of Reason.*[10] Her basic argument is that the goal of neoliberal thought and policy-making is that once you have worked out what markets *should* do, then you no longer need to let markets emerge spontaneously, in a Hayekian fashion. Rather, you can design markets to achieve what they need to do to achieve your desired policy outcome.

And this is exactly what happened; the various ideas about market or mechanism design—like second-price auctions—became wedded to assumptions about what our individual and collective goals should be so that policy-makers could design markets to that end. So, when governments

seek to privatise public assets, or deregulate electricity supply, or auction off radio or cell phone spectrum, they use mechanism design.[11] Results are varied, sometimes generating enormous government revenues (e.g. UK G3 spectrum licensing), but sometimes leading to significant problems (e.g. Californian electricity deregulation).

Such market or mechanism design has a relatively short history, going back to work by economists like Vickery in the 1960s, but it was not until the 1980s when it really took off and became a staple of policy-making.[12] Second- and third-price auctions, explained above, are an example of how to design markets; such auctions are configured by the assumption that we are rational and self-interested beings who seek to maximise our own interests, which in turn will generate collective, social benefits. For example, cell phone spectrum auctions are supposed to generate as much government revenue as possible, while not discouraging innovation.

The key, then, is to create market mechanisms that get us to reveal our preferences through the design of 'choice architectures', like auctions, ensuring that we are always *truthful* about our desires in making our choices. Many contemporary conceptions of markets—and not just the neoliberal version—depend on this idea that markets reveal information upon which we can all act as individuals, without the (assumed) distorting interference from a central planner (e.g. government). Market design, however, actually turns all of this on its head. Market designers can create whatever markets they want to achieve whatever outcomes they want; individual preferences and decisions are sidelined here, since market designers can construct whatever market architecture they need to incentivise us to do what *they* want (e.g. increase revenues, welfare, or efficiency).

The Ascendance of Big Tech

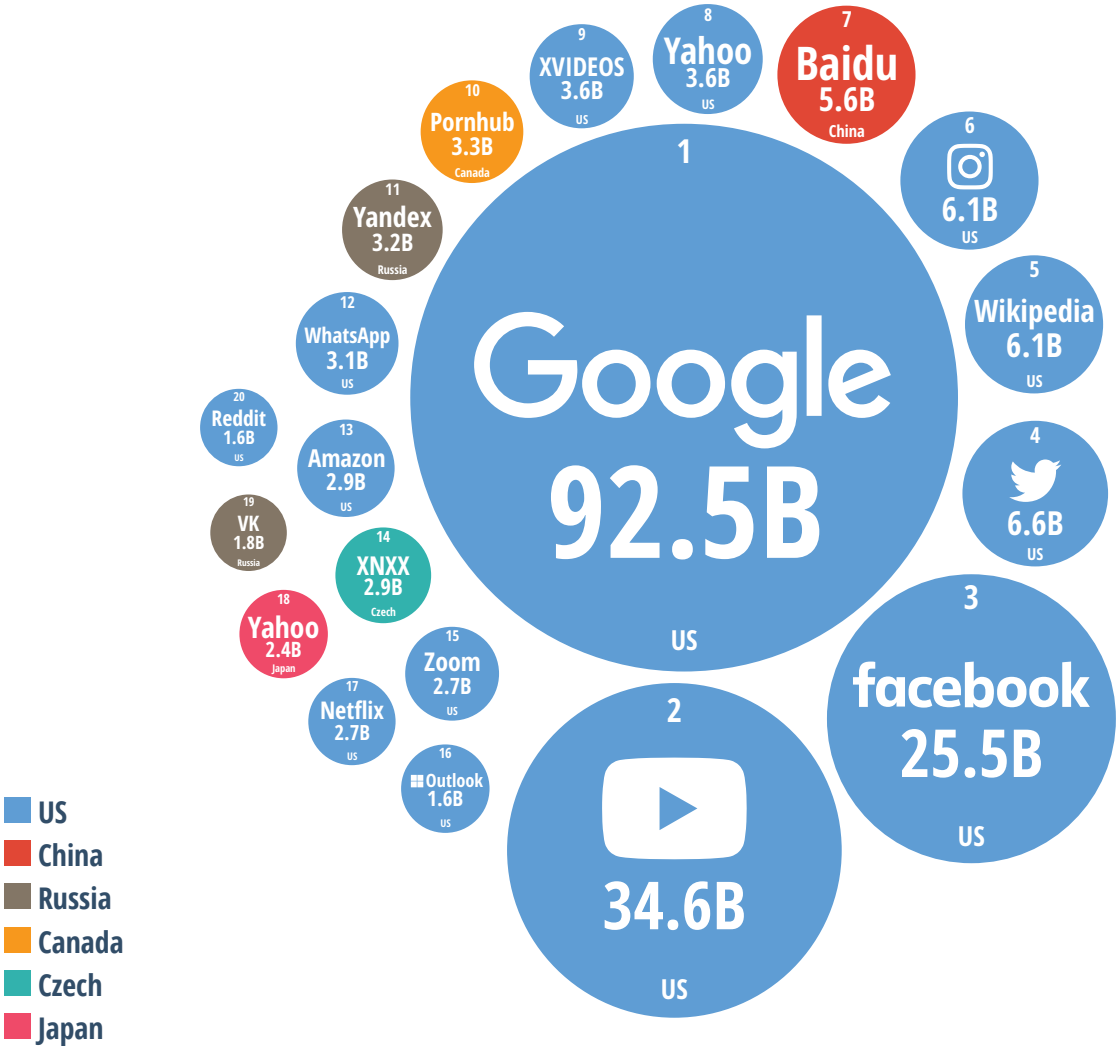
Until relatively recently, it wasn't really possible to extend market design beyond a particular goal or outcome. All of this changed, however, with the rise of Big Tech firms, such as Apple, Amazon, Alphabet/Google, Microsoft, and Meta/Facebook .[13] They have transformed the way our economies and societies function and, increasingly, dysfunction—such as fears about misinformation, cognitive impacts, dark patterns, and such like. I shall return to some of these later.

Today, it is safe to say that Big Tech are *the* key intermediaries in our daily lives and the information on which we rely: they connect us to one another, they operate the infrastructure we use for work and leisure, they provide us with useful goods and services, and far more besides. Much of this mediation relies upon digital platforms, such as those that match you with others (e.g. Uber), with content (e.g. YouTube), or with ads (e.g. Facebook/Meta). Obviously, they don't do this out of the goodness of their heart; they take personal, commercial, and user data from us in exchange for what they provide, which they then turn into further products, services, and infrastructures.

Increasingly, they have designed and reconfigured their technologies, such as digital platforms or application programming interfaces, with the specific goal of collecting increasing amounts of our data, as they have become dependent upon their *data enclaves* for their success.[14] These enclaves represent the data holdings created by the spreading of Big Tech's influence through their ecosystem of devices, applications, software, and platforms.

TOP 20 MOST VISITED WEBSITES

Monthly traffic volume in billions



Source: Visual Capitalist, 2021

It is hard to comprehend the sheer size of Big Tech, to get a good sense of how their existence makes such a difference in our lives compared with other companies. Until recently, Big Tech were among five of the world's largest companies by market capitalisation at over US$5 trillion in 2020, representing almost 25% of the total market capitalisation of the US stock market. They have since fallen in market terms, but not because they have become any less important to our lives. According to a 2020 report resulting from an investigation by the US Congress, 81% of all general searches and 94% of all mobile searches use Google; 99% of smartphones use Android or iPhone operating systems; 80% of browsers are either Google Chrome or Apple Safari; Facebook, Instagram, Messenger, and WhatsApp have 2.47 billion daily active users between them; an estimated 50% of all US e-commerce goes through Amazon; and Amazon, Microsoft, and Google dominate cloud computing infrastructure.[15] Big Tech is so ubiquitous that it is now hard to live without them.

Image: Big Tech's Market Capitalization (US, S&P 500)

Source: Birch et al., 2021.

As critics, myself included, debated whether neoliberalism was dead, dying, or resurgent after the 2008 global financial crisis, Big Tech simply rode the wave of easy money unleashed by central banks through quantitative easing to establish themselves as the dominant players in our economies. This was especially true in the US where the Federal Reserve released more money between and 2008 and 2010 than in its previous 95 years' existence. The journalist Christopher Leonard outlines the unintended and negative consequences of this policy in *The Lords of Easy Money.*[16] As he points out, this flow of easy money resulted in a decade-long low interest rate regime—only stalling with the recent rise of inflation—in which central bankers had hoped companies would leverage the cheap money to invest in new assets and jobs. Few did, preferring instead to use the money for share buybacks or investments in asset bubbles, including the booming tech industry, which saw spectacular growth in venture capital funding.

In contrast, Big Tech put that easy money to good use, especially increasing their stock of tangible assets like data centres, high-speed cables, and suchlike, enabling them to expand their data-collection activities and the computing capacity needed to turn that data into value and cement their market power.[17] Amazon, Google, and Facebook (Meta), in particular, significantly increased the share of tangible assets on their balance sheets.

The real kicker to all this, though, comes with the digitalisation of market design ushered in by the ascendance of Big Tech firms and their platform ecosystems. As Salomé Viljoen, Jake Goldenfein, and Lee McGuigan point out, market design has been turbo-charged by algorithmic technologies enabled by the mass collection of personal data and vast computing capacity of Big Tech firms.[18] They discuss how 'algorithmic or automated mechanism design' gives Big Tech firms a special and unprecedented ability to profile their users, customers, suppliers, and others.

Rather than worrying about policy outcomes, Big Tech has applied mechanism design to making money, as my starting example illustrates, across their various platforms and ecosystems. They

are using mechanism design to incentivise particular kinds of user engagement and impressions with and within their ecosystems, encouraging us to spend more time using their products and services.

As user experience designers note,[19] something as simple as constant scrolling, a defining feature of platforms like Facebook, Twitter, and Instagram, was designed and implemented precisely because companies knew it leads to addictive-like behaviour, keeping our attention glued to our screens; the same applies to notifications, 'likes', and other technologies of digital engagement. And the more time and attention we pay to our screens, the more value Big Tech can capture from our behaviour. By designing markets in this way, Viljoen and colleagues argue that Big Tech is able both to cultivate and exploit so-called 'informational asymmetries', meaning the information that Big Tech has but their users do not.

Does Big Tech Dream of Algorithmic Control?

Big Tech has designed markets and technologies to make us do things they want, even when it does little to benefit users or has highly negative impacts. The implications of this techno-economic configuration are often pernicious, to say the least, partly because soon Big Tech will be simply unable to distinguish between their perception of users as valuable assets and their goal of turning us into those valuable assets.[20]

There are two key concerns with this setup worth considering further, if we wish to challenge Big Tech in any way.

First, we have to counter the direct and damaging effects of mechanism design now built into many digital and algorithmic technologies. The most damaging and egregious forms include so-called *dark patterns* which are built into technologies to encourage us to spend more money online than we intend. The Australian Consumer Policy Research Centre think tank recently released a report on these dark patterns, examining specific examples, including:

- Hidden costs, or drip pricing, when we end up paying more than we first anticipate (e.g. service fees);
- Ads that are indistinguishable from content (e.g. clickbait);
- Trick questions to confuse us, especially in relation to opt-in or -out options;
- Fake scarcity claims to encourage us to make rushed decisions;
- Notifications telling us what others are supposedly doing; and,
- Requests for personal data not needed to access the product or service hidden in cookie requests.[21]

Many of these examples play on our psychology, though reinforced through techno-economic processes and infrastructures. Outlining dark patterns, however, offers limited insight into the broader social and health effects of companies locking us into using their digital and algorithmic technologies. The US-based Center for Humane Technologies highlights the damaging cognitive, health, and social effects and impacts of addictive technologies, including loss of attention, rising unhappiness, and increasing social anxiety.

Second, and despite the negative cognitive, health, and social effects of digital technologies, I argue that the most significant implication of algorithmic mechanism design is the way that Big Tech firms—and others that follow their business model—have managed to control and monetise the very information on which markets are meant to function. Data-driven companies like Big Tech can collect and analyse masses of personal, consumer, and user data to gain a major advantage when making market decisions. They can use 'brute force', as Viljoen, Goldenfein, and McGuigan put it, to achieve their goals because they have the massive processing power necessary to make inferences about how we, as their consumers, users, competitors, and so on, are going to act and behave.

Two things matter here if, as neoliberals and other economists argue, markets depend upon information to function properly *and* beneficially, and Big Tech has more information than any other market actors:

- There is a huge information asymmetry between ourselves as individual users and Big Tech; they can work out things like how much we would be willing to pay for a product or service, and then either sell that information to a third party or use it themselves. And they can even do this for people who spend little time on the internet sharing their personal data, because they can infer our likes and dislikes from all the people around us—our networks—who are in turn sharing their data.[22] For example, it is pretty obvious that I like science fiction from my Amazon buying habits or Google browsing history; this information can be used to price sci-fi books and films higher for me than for other people, in so-called dynamic or discriminatory pricing.[23] There are already clear examples of this in things like Uber's surge pricing[24] or Tinder's user charges[25], and it's likely to become more prevalent.
- More importantly, the information Big Tech collects and controls represents the very information we need for markets to function as markets (i.e. as information processors)—at least in basic economic terms. Big Tech monetises this market information, selling it to whoever is willing to pay. Our likes and dislikes (e.g. recommendations or rankings) are an example of this kind of market information; Big Tech can collect it, hoard it in their enclaves, and sell it to other companies that want to sell us stuff, or exploit that information for other purposes. Big Tech can do all this because they have the resources to invest in the necessary computing capacity, representing a huge entry barrier to the emergence of competitors.

My point here is not to individualise these impacts, but to emphasise that Big Tech firms have become, to all intents and purposes, markets unto themselves: they write the rules of the game for their respective ecosystems; they regulate their ecosystems; they can exclude or ban potential competitors from their ecosystems; and they can set and change the terms and conditions under which we engage with their ecosystems as they see fit (and change these without our consent). And their influence extends far beyond their own ecosystems as they can leverage the huge information asymmetries between their business operations and their competitors or individual users. As all this shows, they are incredibly powerful entities.

Challenging Big Tech?

Because of their social and market power, Big Tech are currently facing growing challenges to their dominance. Some of these are collective challenges, but others are emerging from the inherent and internal contradictions in their own strategies and operations.

The Texas lawsuit mentioned at the start is just one of many collective actions being brought against Big Tech, both by governments and competitors. More concerted efforts have been undertaken by sovereign jurisdictions to rein in Big Tech's power, some of which appear more effective than others.[26] The European Union (EU), in particular, has been active in this area as concerns about Big Tech's anti-competitive impacts have grown. Recently, the EU has introduced various policies and regulations, including:

- ***Digital Markets Act*** establishing ex ante regulations to control the behaviour of so-called 'gatekeeper' firms like Big Tech. It forbids certain actions like combining personal data from platforms with data collected for other services. It comes into effect in 2023;
- ***Digital Services Act*** designed to increase transparency in online advertising while reducing illegal content and misinformation. It comes into force in 2024; and,
- ***Data Governance Act*** to open up and standardise data sharing between organisations, limiting the ability of companies to hoard data. It is still in the legislative phase.

Other countries and jurisdictions are also taking action, such as Australia and the US, although there is stiff lobbying from Big Tech and other data-driven companies.

A different challenge, though, seems to be emerging from within the Big Tech firms themselves, namely the growing contradictory effects arising from their operations and strategies. As anyone who has used their products and services knows, Big Tech's offerings are becoming much less useful, and even dysfunctional. My personal experiences include: buying dodgy products via Amazon that are knockoffs or scams; using Google search but having to scroll halfway down the page to avoid advertising; browsing through Facebook but being put off by all the advertising (Knights Templar T-shirts anyone?); having to change settings on Microsoft products because of some bizarre automated effect; and avoiding Apple like the plague because I do not want to be locked into an enclave.

Others are having similar experiences—data-driven companies are finding it harder to achieve their stated goals: for example, ride-hailing companies like Uber and Lyft are having to raise prices to the same or higher levels as taxi companies[27]; food-delivery companies like Doordash or Deliveroo have been undermining the restaurants they rely upon for their very existence[28]; and Airbnb is plagued by scams and is transforming housing markets in problematic ways[29]. And don't even get me started on things like 'click farms'.[30]

Generally, we need to find ways to limit the collection and use of our personal data and I think there's a growing political space to do this as data-driven firms encounter a growing range of problems with their business and innovation models. We have options. One way is to channel pro-market sentiments by turning our personal data into our property[31]—which will probably not solve anything no matter how attractive it might sound since it is difficult to determine who

should own what information. Another option is to create centralised data trusts[32], perhaps run by governments or public agencies, providing access to all sorts of digital data while providing oversight of its use—this might help solve some issues and open up our data to uses for with which we agree, but would not necessarily stop Big Tech from accessing our personal information. A third option is to create decentralised data cooperatives or data communes[33], collectivising our personal data and enabling more local oversight and accountability—these could be run by specific groups, organisations, or communities, but would require significant effort to run and manage all the privacy concerns that people have about their personal data.

One thing is certain: we are going to see far more digital data in our lives, and if we want to use it for our collective benefit then we need to find ways to govern it collectively and democratically, rather than leave it in the hands of powerful corporations to do with as they will.

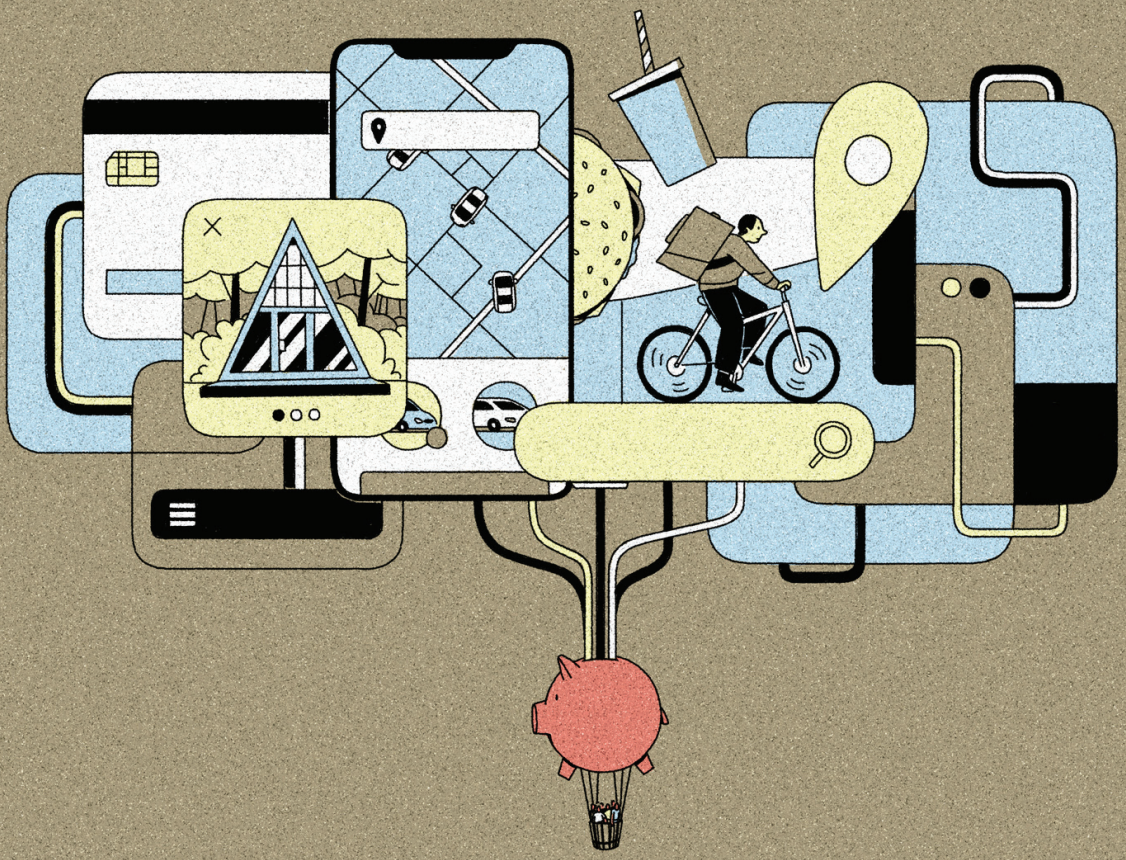
To Conclude

Market design has underpinned the ascendance of Big Tech firms over the last decade or so. A new array of digital and algorithmic technologies have enabled these and other data-driven firms to monetise the very information on which markets are supposedly dependent (e.g. who wants to buy X, what person Y would pay for Z, how many people view A); this market information is meant to be transparent and truthful to ensure competition, but it is increasingly hoarded and hidden in *data enclaves* constructed by Big Tech firms to secure their monopolistic positions. So, rather than simply monetising personal information, Big Tech firms have gone far beyond the 'surveillance' fears of many critical thinkers, such as Shoshana Zuboff.[34]

Today, however, Big Tech firms face challenges on different fronts: from politicians and policy-makers developing new frameworks to curtail their power; and from the internal contradictions and dysfunctions in their own operations. All of this raises the question: will markets come back with a vengeance, or is this the start of something new? An important point for activists, civil society groups, non-government organisations (NGOs), and publics to remember when raising awareness or engaging with governments about the power of Big Tech is that if there are no longer any markets, then regulators returning to their outdated ways of understanding the world to rein in Big Tech will not work. We have to think beyond the market.

BIOGRAPHY

Kean Birch is Director of the Institute for Technoscience & Society and Professor in the Science & Technology Studies Graduate Program at York University, Canada, where he researches the emergence and implications of technoscientific capitalism: http://www.keanbirch.net/



Holding the strings

The role of finance in shaping Big Tech

Nils Peters

'Web3' has surged onto the agenda of Silicon Valley's founders and financiers. The newest libertarian tech paradigm vaguely promises the decentralisation of the internet—using technologies such as blockchain—to save it from the clutches of current platform corporate control. A year since this hype, its track record is at best mixed.[35] But besides hacks and lacklustre engagement from the general public, insiders have identified a more profound problem with the next big thing in tech. Jack Dorsey, the co-founder of Twitter, pinpointed why the optimism of those boosting decentralisation is misplaced. On 21 December 2021, he tweeted: 'You don't own "web3". The VCs and their LPs do. It will never escape their incentives'.[36]

Venture capitalists (VCs) and their funders (limited partners, or LPs) receive little attention in the contemporary debate about digital power. Yet highlighting the financial actors behind tech revolutions is long overdue. How did Uber operate for almost a decade without making a profit? Why did Google create its advertising business in the first place? How did Facebook (now Meta) fend off its early competitors? Building and maintaining a platform is immensely expensive. Whenever we try to get to the bottom of digital power and start tracing the steps that companies took towards becoming so dominant, we need to address the question: How was this financed?

Venture capital is a high-risk, high-reward form of investing. Most investments fail, but a small number of highly successful ones generate outsized returns. A famous example of this is the VC firm Benchmark's original investment of $12 million in Uber, which rose to a value of $7,000 million.[37] Venture capitalists, in turn, raise the money they invest from pension funds, endowments, insurance companies, corporations and high-net-worth individuals. Upon their investment, these become LPs of a VC fund.

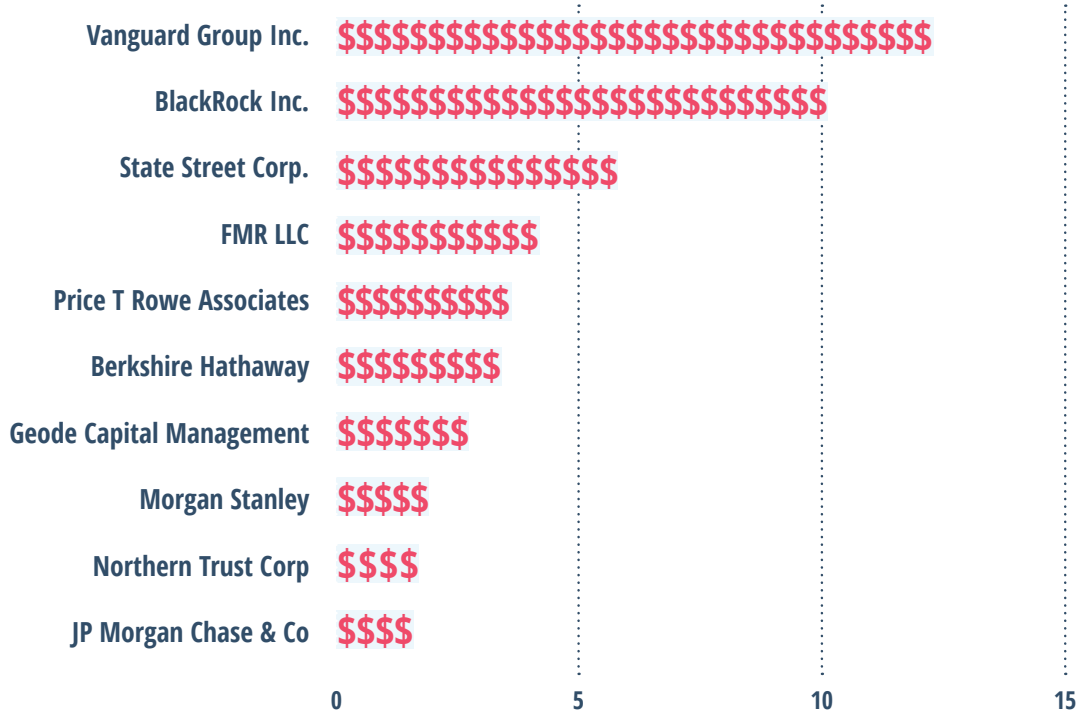
Financiers are far from neutral intermediaries that merely allocate capital. They face pressures to make returns for their stakeholders and shareholders, and are actively involved in shaping the world around them to accommodate their financial aims. Few major tech companies reach their scale without VC funding. Prominent examples are Amazon ($8 million received in VC funding)[38], Google ($36 million)[39], Facebook ($800 million)[40], Airbnb ($2,444 million)[41] and Uber ($6,523 million).[42] Given the magnitude of these cash injections, it is highly doubtful that it is even possible to build a large tech business without VC financing. How could any individual entrepreneur compete with a company that can draw on funds like this? And if you can't, shouldn't finance take a much more central role in our analysis of digital power?

Put simply, if we want to understand digital power, we need to understand how it is financed. Digital power, after all, is embedded in a financialised economy.[43] Ignoring the financial pillars of the platform economy risks missing how Big Tech affects us beyond the nature of work and privacy concerns. As this essay will show, financialised elements of everyday lives, from pension and insurance contributions to loans, are tied up with the fate of Big Tech.

WHO OWNS BIG TECH?

GAFAM (Google, Amazon, Facebook, Apple, Microsoft)

Approximate % ownership of GAFAM shares



Source: NASDAQ

We can learn a lot about the functioning of today's publicly listed Big Tech companies by studying their *private* market beginnings. I will not focus on the already established Big Tech companies like Amazon, Alphabet, Apple and Meta. Once companies have gone public, VC firms lose most of their influence over them. Yet for the crucial period between incorporation and going public in the stock market, these financiers play a critical role in shaping emerging tech companies. Understanding how the next generation of Big Tech companies is made can help inform our ability to safeguard against their power. By focusing attention here, this article aims to develop tools to understand and resist Big Tech as it unfolds.

Financing the Tech Boom

Larry Summers famously argued that since the early 2000s, Western economies are caught in a state of 'secular stagnation'.[44] This describes a state where excessive savings drag down demand as they are not being spent and generating new income. As others have shown, runaway wealth increases have led to substantial growth in savings among the top 1%. Excessive savings here reflect rampant inequalities in income and wealth distribution. In addition to that, Summers

explains that digital platforms conserve capital by further encouraging savings: 'Think about Airbnb's impact on hotel construction, Uber's impact on automobile demand, Amazon's impact on the construction of malls, or the more general impact of information technology on the demand of copiers, printers and office space'. The results of these two developments are low investment, low growth, a lacklustre recovery from economic downturns, and a capitalism devoid of dynamism. This is the financial backdrop against which the rise of the platform economy needs to be read.

This development became especially problematic after the 2008 Global Financial Crisis. Governments and central banks were tasked with containing the crisis and charting a recovery from what would become known as the 'Great Recession'. The key responses were fiscal austerity and expansive monetary policy. Major central banks like the Fed, Bank of England and the European Central Bank (ECB) lowered interest rates to near zero. Concurrently, central banks also deployed quantitative easing (QE) programmes.[45] Leaving most technical details aside, this meant that central banks started purchasing government and corporate bonds, which in turn raised the price and lowered the interest on those bonds. The intention was to spur investment and economic growth by making it cheaper to take out credit.

In effect, QE made it harder for many investors to rely on interest payments to make their desired returns. This was particularly true for institutional investors like pension funds, endowments, and insurance companies which increasingly scrambled to find profitable outlets for their capital, throwing them into the arms of the big asset managers like BlackRock. If significant growth was achieved in this environment, it came through capital gains on equity markets. This saw a debt-fuelled conversion of savings into unsustainably high investment levels. The flood of cheap capital further drove down yields on bonds and raised the yields on equities. In other words, buying the debts of governments and corporations (bonds), a proven but increasingly insufficient strategy for institutional investors, was supplemented by purchasing corporations' shares and stocks (equity).

This resulted in a decade-long bull market in publicly listed Big Tech stocks, and privately held shares of tech startups, where asset prices continuously rose. 'Unicorns'—private companies with a valuation exceeding $1 billion—became the highly publicised figureheads of the seemingly unceasing upward trajectory. In the UK, the number of unicorns increased from 10 in 2010 to 80 in 2020.[46] As was the case with excess savings, this shows that macroeconomic trends, finance and the fate of Big Tech are closely intertwined.

The Venture Capital–Platform Nexus

Venture capitalists buy minority stakes in early-stage, private companies. Typically, VC investors sit on these companies' boards and actively advise and consult them. They are particularly known for financing the next tech generation. For that reason, venture capital is often considered 'patient' because investors have to commit for up to a decade before they can expect a payoff. The only way for VC investors to realise their gains is when the investee company is either acquired (usually through some form of merger and acquisition) or goes public on the stock market through an initial public offering (IPO). In the case of Uber, ten years passed between incorporation and the IPO. Their 'patience' notwithstanding, VC funds usually have a limited lifetime, which means the understanding between investors and startups is that the latter have to pursue ambitious growth rates to scale up quickly.

In order to make returns, institutional investors increasingly turned towards riskier, alternative outlets for their capital. Venture capital stood to be a major beneficiary from this dynamic. The relationship between institutional and VC investors can be imagined as being like a chain of investments. Institutional investors conservatively manage very large investment portfolios. The returns they generate finance pension plans, insurance benefits, endowment expenses, or simply make rich people even richer. Venture capital funds handle much smaller volumes and portfolios, with an inverse risk–reward structure. They act as an intermediary between institutional investors and unproven tech startups, absorbing the risk mismatch and directing money into opaque private markets.

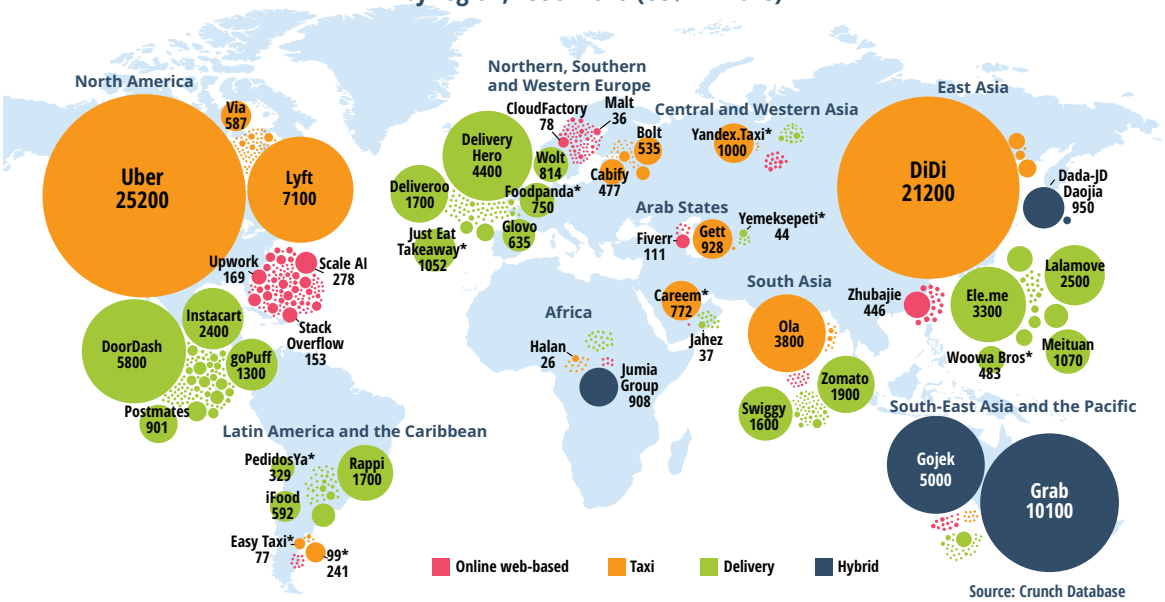
Besides macroeconomic push factors, the characteristics of venture capital further provided a pull for surging investments into their funds. VC firms are primarily invested in tech-related businesses, one one of the few sectors that still generated growth in a largely anaemic phase of capitalism.[47] Moreover, the VC industry understands how to sell their highly publicised successes. The most successful VC firms generate returns way above what the stock market could offer. As a consequence, venture capital saw steep increases in funding volumes from the late 2000s. In 2020, VC investment in tech companies in the UK stood at $14.9 billion.[48] This is still dwarfed by the US venture capital market, where investors dished out $144.3 billion. Globally, VC investments increased from $59 billion in 2012 to over $650 billion in 2021.[49]

On the back of cheap money at VC investors' disposal, new types of business models drew their attention. The dress rehearsal for today's platform economy was the 1990s' 'dot-com' boom, where e-commerce businesses pioneered many of the ideas that a decade later would become common sense. The dot-com bubble (and eventual bust) are often ridiculed for the laughable business ideas that were brought to public markets at sky-high valuations. Yet the business models and financing of companies like Pets.com (which delivered pet supplies ordered online) were not radically different from those of today's platform giants.[50]

The platforms' business strategies depend on investors who are willing and capable of shouldering year-long financial losses. By mutual agreement, platforms such as Uber are losing money because they prioritise rapid growth (or scaling) over profitability. Platforms pursue different strategies to supercharge their growth. On the one hand, there is user-driven growth through what are called network effects. Platforms' digital intermediary position between different user groups means that they create networks of users. Network effects occur when the value of the service or product the platform offers increases as more people start using the platform. For example, the value of using Instagram increases as more users sign up (direct network effects), and the value of hailing rides or driving for Uber increases as each group grows (indirect network effects). At some point, network effects essentially become a natural monopoly, similar to broadband infrastructure or railway systems, where users are increasingly locked into the service while competitors find it ever more difficult to enter.

PLATFORM ECONOMY HAS BOOMED ON FINANCIAL CAPITAL

Total funding from venture capital and other investors, selected categories of digital labour platforms by region, 1998–2020 (US$ millions)



Source: Crunch Database

Global financial investment in digital labour platforms: $119 billion (1998–2020)

Global revenue: $52 billion

Average worker pay: $3.40/hour

Alternatively, or ideally in addition to that, platforms can burn through investors' cash by doubling down on their expenses. They can use investors' money to acquire customers, such as through discounts or advertising. Through VC-fuelled growth, platforms can drive out competitors and fortify their 'moats'. Rather than an option, rapid growth is a necessary condition for many platforms to operate profitably at some point in the future, because profitability hinges on dominating the market.

In a nutshell, the platform model is built on large amounts of 'patient' capital that finance rapid scaling of platform operations. Network effects are a potent tool to advance this process. More than just desirable, market domination is a necessity for platforms to be sustainable—and for their VC investors to make sufficient returns on their investment. This was enabled by the post-2000 low-interest macroeconomic environment, which created conditions that sustained platforms for years without making any profits. While this funding arrangement predates the internet, digitalisation charged the speed and scale of investee companies' expansion.

The important takeaway here is that financial and platform capitalism are deeply entangled. The rise of platforms fulfils a function within a larger search for returns for investors. Institutional investors' problem of low returns was 'solved' by funnelling money towards VC funds. VC investors flocked to platforms for their ability to put to use large amounts of cash and little likelihood of very large returns. In turn, the availability of this capital pushed Big Tech into models that looked to become dominant and lock out competitors. The flipside of excess savings was a VC-led investment regime for which platforms became an ideal outlet. Finance plays a substantial role in who gets to advance in the digital economy, and digital power boils down to the power of finance.

Digital Power through the Financial Lens

Examining emerging platforms through the financial lens allows for a different reading of the current situation. Alphabet, Amazon and co. absorb most of the public attention. Yet dozens of platform startups currently attempt to carve out space for themselves and 'disrupt' legacy sectors. It seems that every year, investors' attention focuses on a new hype. A few years back, ride hailing inaugurated this tradition with a fierce standoff between Uber and Lyft. Since then, food delivery (JustEat, Uber Eats, Deliveroo), micro mobility on rentable bikes and scooters (Bird, Lime, Bolt), and challenger banks (Monzo, Revolut, N26) have joined the trend. More specifically in reaction to the pandemic, fast grocery delivery (Getir, Gorillas) and office collaboration tools have been swamped with investors' cash.

Each of these was presented to the public as a revolutionary change in how the economy and society operate. Uber is arguably the most prominent case here. While this is difficult to remember after years of corporate scandals regarding Big Tech, when it started up, Uber was mostly welcomed as a harbinger of the 'sharing economy'. For a brief moment, there was a genuine belief that platforms could usher in a more democratic, sustainable capitalism by letting people share their underused assets. On the back of this narrative, Uber raked in more than $6 billion in VC funding over coming years to self-fulfil this prophecy. Its list of investors reads like a Who's Who of private market investing, including the VC firm Benchmark, SoftBank's seismic Vision Fund and Saudi Arabia's sovereign wealth fund, The Public Investment Fund.[51]

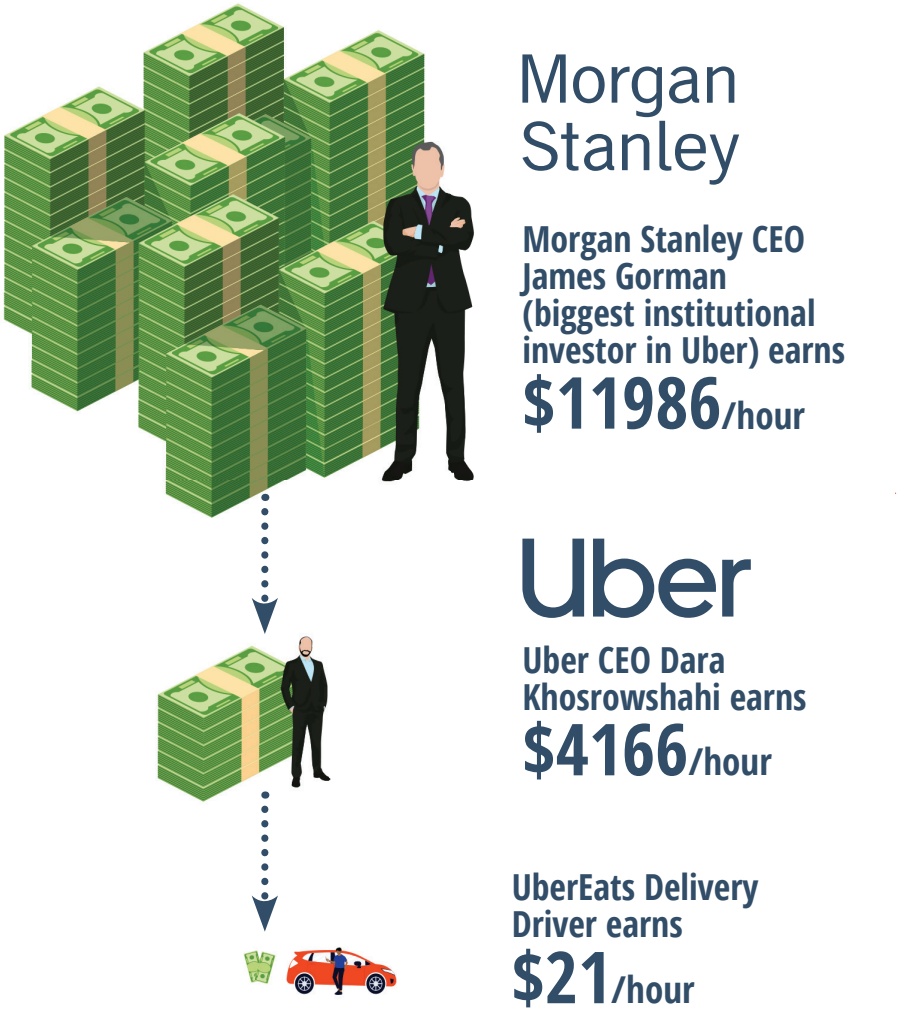
With its 'war chest' filled to the brim, Uber embarked on the typical platform strategy I outlined above. As the Uber files have more recently revealed, employees opted for aggressive strategies to drive legacy industries (i.e. taxi drivers) out of business.[52] Competitors were challenged on price, where Uber could afford to set fares below cost to increase their market share. To keep network effects going, the company was also able to use investors' money to uphold eyewatering acquisition costs. At one point, the company paid drivers a $750/$750 referral bonus: Give new drivers $750 for joining and $750 for the person who referred them. As the former Uber executive Andrew Chen boasts, 'we spent hundreds of millions just on driver referrals programs, and nearly a billion in paid marketing'.[53] In light of these strategies, Uber's infamous unprofitability comes as no surprise.

While in its early days Uber seemed almost unstoppable, a more sober look begs the question what would be left of its digital power without the lavish financial backing. 'Uber Technologies Inc' is the company's official registered name, yet what substantial changes did its technology effect? Granted, Uber built a sleek app with a good user interface. But this didn't solve any of the problems that taxi services have always been dealing with: empty backhauls caused by uneven geographic demand, the high cost of peak capacity or the risk of overcapacity.[54] The is emblematic of the wider platform economy, where a thin layer of tech often disguises the reality that platform companies are simply restating rather than solving long-standing problems.

So why are platform services so popular with consumers? In this reading, demand for platform services is largely explained by the price distortion that VC money enables. This means that at the outset, services are either free or unsustainably cheap. It's not all that surprising that people love free stuff. But demand at the 'real' price of the service that consumers will have to pay in the long run will inevitably be much lower. The challenge for the platform, then, is to damage competitors and engrave themselves in people's desire for convenience before they reach that point. As VC funding and the proceeds from Uber's IPO start to run out, the company has started raising prices steadily.[55]

A similar story has played out across different industries. Micro mobility platforms covered European cities in rental bikes and e-scooters, much to the dismay of local residents.[56] When we start to pierce through the narratives of easy access, sharing and convenience, many of these companies look more like an act of desperation to will the 'next big thing' into being.[57] This points to the limits of financially enabled platformisation. These limits now become increasingly obvious because of changing macroeconomic conditions. High inflation and rising interest rates have reduced the flow of cash into highly risky startups. With investors inclined to see positive cash flow instead of high 'burn rates', a number of 'disruptors' were thrown into disarray. A prominent example of this is the fast grocery delivery sector, where Gorillas laid off hundreds of workers and pulled out of four countries.[58] Even the Tech Giants Meta, Alphabet, Amazon and Twitter weren't spared and a layoff tracker estimates the number of jobs cut at over 130,000.[59]

Looking at the current state of emerging platforms through the financial lens challenges our conceptions of digital power. New services that are sold to us as a revolution in transport or shopping begin to look like investors' desperate attempts to make returns in a low yield environment. The ability of Uber, Bolt and Gorillas (to name but a few) to turn their shaky business model into a self-fulfilling prophecy hinged on torrents of capital from their VC investors. And these huge streams of capital were a function of a global economy awash with cash. The point here is that many platform services exist only because an abundance of capital needs to be channelled *somewhere.*



Sources: Reuters, Nasdaq, Business Insider, Glassdoor

De-financialise to de-platform: Implications and Resistance

We can't talk about digital power in isolation from the financial power behind platforms. This new angle reveals new dependencies as the change of macroeconomic tides in 2022 has put many tech companies under pressure. Rising inflation rates have prompted central banks to raise interest rates. This was immediately felt by investors who adopted a more conservative approach to high-risk investments.

This is not a reason for schadenfreude, however. If we follow the chain of investors, the slowdown in tech will have ripple effects for society at large. When money was cheap and markets were going up, startups kept VC investors happy. Rising VC portfolio values meant better returns for their LPs, the pension funds, insurance firms, endowments, etc. This ultimately ensured the viability of defined contribution pension schemes and insurance plans. Institutional investors allocate only a small share of their portfolios into risky asset classes and will not be drastically affected by the downturn in tech. However, it is important to note how our everyday decisions are linked with high finance.

Although venture capital is a highly speculative form of investing, investment decisions have concrete effects in the present. There are now significant sums of money tied up with companies that exist by burning through VC investors' cash. Irrespective of unsustainable financial strategies, platforms have inflicted lasting damage on competitors or legacy industries. Transport companies like Uber are an obvious example, and a similar case can be made for the effects of accommodation platforms on hotel chains (and family hotels), the impact of social media on newspapers, and streaming platforms' disruption of the music and film industries. In their absence, we might find ourselves in a position where we are lacking access to important services.

And beyond the platform–consumer relationship, platforms might also depend on each other: As many startups are each other's customers, one of them going bankrupt has potentially systemic consequences.[60] Cryptocurrency exchanges are a case in point. An extreme example of this is what the *Financial Times* dubbed the 'Tesla financial complex' with regard to its outsized impact on the stock market.[61] This describes a 'vast, tangled web of dependent investment vehicles, corporate emulators and an enormous associated derivatives market of unparalleled breadth, depth and hyperactivity'.

The upshot here is that if we want to de-platform and scale back digital power, we would first have to de-financialise. Digital power is the product of a distinct financial regime. Yet scaling back financialisation is a task of a much larger order of magnitude. Fiscal, monetary and legal changes that enabled financialisation more broadly, and encouraged flows of money into the VC industry more specifically, are tied up with a broader desire to reignite growth in stagnant economies. Curbing these flows would give rise to the need for a credible alternative growth regime. So, what *can* be done about this?

Despite being a tall order, challenging the power of established financial regimes is not without precedent. More recently, and especially with regard to the climate catastrophe, activism has focused much more squarely on financial actors implicated in this development.[62] Activist research has revealed how asset managers like BlackRock, Vanguard and State Street amassed power through concentrated share ownership.[63] BlackRock alone currently has $10 trillion under management. The company has put this money to use by purchasing shares in publicly listed companies. As significant shareholders in corporations across the entire economy, asset managers like BlackRock effectively indexed the market, by constructing a portfolio that tracks the performance of large parts of the economy. In other words, when the market goes up, so does BlackRock's portfolio. A 'side effect' of this is that BlackRock as shareholder has a say in corporate governance decisions of a vast amount of companies. How this power is used and to what ends has become increasingly politicised, as activist campaigns seek to coerce the asset managers into matching power with responsibility.

Challenges to asset manager capitalism show a way forward for resistance against the VC-led investment regime. Public market scrutiny needs to be combined with more attention to what is going on in private markets. Interestingly, a few major VC investors have started to mimic the indexing strategy of the big asset managers. For instance, Tiger Global and Softbank's Vision Fund have embarked on acquiring shares in a very large number of private companies.[64] Due to more lenient reporting requirements, private markets are more difficult to scrutinise. Yet a concerted effort to gather what is publicly available would help to paint a much clearer picture of the investment landscape.

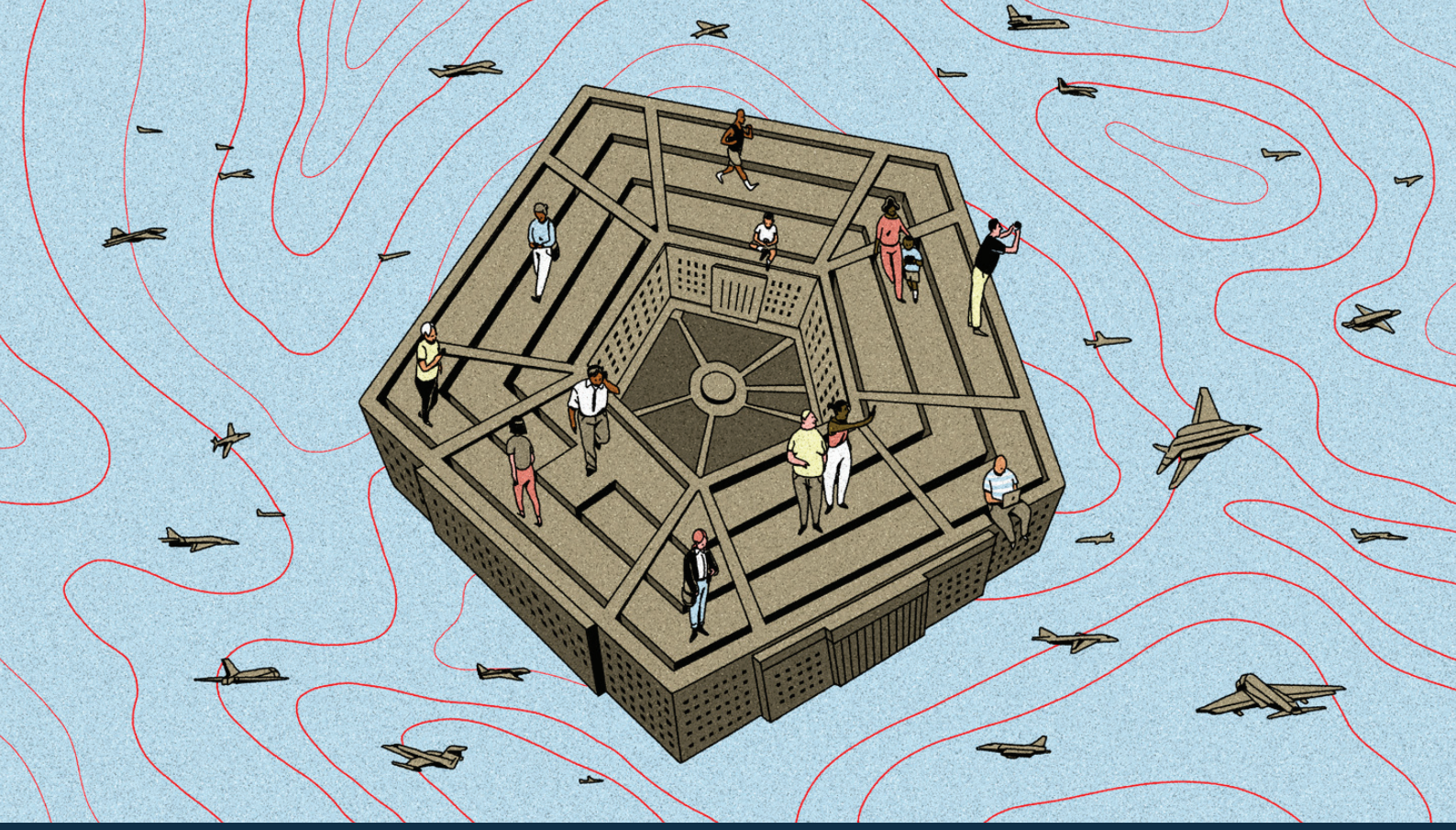
Further, we need a better understanding of what institutional investors supply capital to the VC industry. There remains a lot of work to be done in mapping such relationships and following the investment chain from institutional investors to VC funds to startups. Some institutional investors have public reporting requirements, which could be a starting point and further provide insight into the actual financial performance of VC funds.

Rather than reacting to existing crises, a focus on the financial actors behind Big Tech enables us to anticipate where future problems might emerge. If we want to see what's next, we should be looking at what kind of funds VC firms are raising, what their purpose is, and what companies are found in the portfolios of the most successful VC funds. This might give a hint to which industries will face pressures next and where the nature of work is about to undergo a major transformation. For instance, there have long been attempts to bring white-collar services under a platform labour system. Preparing for the impact might give workers an edge to organise and anticipate the coming disruptions.

The changing macroeconomic environment does promise change. What kind of change is impossible to say at this point. Challenging digital power starts with changing the supply of capital, and this is profoundly affected by tightening monetary policy. While this is largely beyond activists' control, historical lessons might be drawn from comparable episodes. Jack Dorsey's annoyance about the trajectory of web3 should be turned into an activists' rallying cry. At the heart of the desire for decentralisation is a yearning for the early internet, to restore web 1.0's noble ambitions before the web 2.0 corporate capture. This has progressive potential. Understanding the incentives of VCs and their institutional investors LPs can lead the way to challenge digital power and realise it.

BIOGRAPHY

Nils Peters is a Fellow in Economic Sociology at the LSE. He occasionally tweets @peters_nils.



Militarising Big Tech

The rise of Silicon Valley's digital defence industry

Roberto J. González

In September 2011, CIA and US military personnel jointly launched a drone strike authorised by President Barack Obama. The attack resulted in the assassination of Anwar al Awlaki—an ardent US-born Muslim cleric—in Yemen. Those who organised the drone strike targeted Awlaki based on geolocation data which was monitored by the National Security Agency as part of a surveillance programme.[65] Two weeks later, a CIA drone attack killed another US citizen using the same kind of data: al Awlaki's 16-year-old son, Abdulrahman al Awlaki.[66]

Although al Awlaki was deliberately assassinated by US forces, other US citizens—and thousands of civilians in Afghanistan and other parts of central Asia and the Middle East—have been inadvertently killed by drones.[67] These cases foreshadow a major flaw in the latest iteration of automated war: the imprecision of the technologies, and the great margins of error that accompany even the most sophisticated new weapon systems. In their most advanced form, the computerised tools make use of artificial intelligence and machine learning, and may soon have fully autonomous capabilities.

Handheld internet-ready digital devices have transfigured billions of people worldwide into atomised data-production machines, feeding information into hundreds, if not thousands, of algorithms each day. Although we have swiftly integrated smartphones and tablets into our lives, we very seldom reflect on how the data stored and transmitted by these gadgets can easily become militarised. For example, recent reports describe how the US Defense Intelligence Agency, affiliated with the Department of Defense (DoD), routinely uses commercially available geolocation data collected from individual cell phones—sometimes without warrants.[68] Military and intelligence agencies can use such data not only for spying, but also to reconstruct social networks and even to target individuals for lethal attacks.

Drones, geolocation software, spyware, and other such tools are emblematic of a new series of collaborations between Big Tech and Big Defence. Over the past two decades, the DoD and 17 US government agencies collectively known as the US Intelligence Community have attempted to capture technological innovation at its source: Silicon Valley. Military and spy agencies have done this by creating outposts along the West Coast; organising a high-profile advisory board that links the Pentagon to Big Tech firms; coordinating summits, forums, and private meetings with influential investors and corporate executives; and appealing directly to the hearts and minds of entrepreneurs, engineers, computer scientists, and researchers who are sometimes sceptical of government bureaucrats, especially those from the DoD.

In many ways, it is impossible to fully understand the US military today without an analysis of its deep connections to the tech industry.

The interconnections between the worlds of network technology and defence stretch back more than 50 years. For example, from the early 1960s, the DoD's Advanced Research Projects Agency (ARPA) played a crucial role in funding computer research that led to the ARPANET, the precursor to today's internet. Silicon Valley's early development was financed largely by defence and intelligence agencies, and the Pentagon was heavily invested in tech companies throughout the Cold War.[69]

What Is Virtual War?

Virtual warfare obviously means different things to different people. There is no agreed definition—which gives room to interpret the term broadly, holistically, and anthropologically. I take a wide-angle view, focusing on four different elements: robotic and autonomous weapons systems; a high-tech version of psychological operations or psyops; predictive modelling and simulation programmes, which some call 'computational counterinsurgency'; and cyberwarfare, meaning the attack and defence of critical infrastructures. These technologies and techniques are predicated on the production, availability, and analysis of massive quantities of data—often surveillance data –collected from drones, satellites, cameras, cell phones, electronic transactions, social media, email messages, and other internet sources.

We can think of this as war by algorithms. Increasingly, the technologies make use of artificial intelligence or AI to automate decision-making processes. The development of virtual weapons relies on the combined efforts of a wide range of scientists and technical experts—not only chemists, physicists, engineers, computer programmers, and data analysts, but also biotech researchers, political scientists, psychologists, and anthropologists. Much of the work is rather banal, and takes place in nondescript buildings in suburban office parks, tech campuses, or university laboratories. Silicon Valley has emerged as a major centre for this kind of defence and intelligence work.

In some ways, virtual warfare is a continuation of the so-called Revolution in Military Affairs or RMA, a doctrine that was articulated by the Pentagon's Office of Net Assessment in the 1980s and 1990s. It leaned heavily towards technology-based solutions. After 9/11, when the US waged its so-called Global War on Terror, and went to war against global networks of insurgents armed with relatively simple technologies such as improvised bombs, rifles, and grenade launchers, the RMA lost steam, and counterinsurgency became fashionable after a long hiatus. But now, in a period marked by rapid innovation, algorithmic modes of governance, and the rise to power of rival nations like China and Russia—each of which is pursuing its own virtual war-fighting technologies—computerised combat has once again taken centre stage among US military establishment elites.

The Intersection between Big Defence and Big Tech: Creating DIUx

Mountain View rests comfortably between the heavily forested Santa Cruz mountains and the southern shores of the San Francisco Bay. Through the first half of the twentieth century, it was a sleepy town with cattle farms, fruit orchards, and picturesque downtown streets. But after a team of scientists led by William Shockley invented the semiconductor there in 1956, it grew rapidly, along with the rest of Silicon Valley. Today, it's a bustling suburb with more than 80,000 residents.

At first glance, it seems like an odd place for military and intelligence agencies to set up shop. Mountain View is nearly 2,500 miles (4,024 km) away from the Pentagon. Direct flights from San Francisco to Honolulu take less time than flights to Washington, DC.

The Pentagon and Silicon Valley are not only geographically distant, but there are other differences too. The Defense Department is often considered a notoriously bloated, stuffy, wasteful bureaucracy,

with rigidly hierarchical organisational structures and inflexible workplace norms. By contrast, Mountain View's biggest employer is Alphabet, Google's parent company, one of the world's most valuable corporations. Its 26-acre campus, known as the Googleplex, includes more than 30 cafés, free food and drink for its employees, on-site fitness centres, and swimming pools. A life-size iron *Tyrannosaurus rex* skeleton, lovingly called Stan by Google employees, is prominently displayed outside a main building.

Despite these differences—indeed, *because* of them—Defense Secretary Ash Carter very publicly established a Pentagon outpost less than two miles (3 km) away from the Googleplex. The Defense Innovation Unit Experimental, or DIUx, was created in August 2015 to quickly identify and invest in companies developing cutting-edge technologies that might be useful to the military.[70] With DIUx, the Pentagon built its own start-up accelerator dedicated to funding firms specialising in AI, robotic systems, big data analysis, cybersecurity, and biotechnology.

DIUx's new home wasn't so out of place. Its headquarters was located in a building once occupied by the Army National Guard, on the grounds of the Ames Research Center, the largest of NASA's ten field sites, and Moffett Field, once home to the California Air National Guard's 130th Rescue Squadron. Defence giants Lockheed Martin and Northrop Grumman have offices less than 3 km away. In 2008, Google itself was encroaching on government territory: it entered into a 40-year lease agreement with NASA Ames for a new research campus. Then it signed a sixty-year deal with NASA to lease 1,000-acre Moffett Field, including three massive dirigible hangars.[71] Today, Google uses the hangars to build stratospheric balloons which might one day provide internet services to people living in rural areas[72]—or perhaps conduct high-altitude military surveillance missions.

DIUx's office was in close proximity to other tech firms: Amazon's Lab126 (where the Kindle reader, Amazon Echo, and other digital devices were hatched); LinkedIn's corporate headquarters; and Microsoft's Silicon Valley campus. Apple's corporate offices were located 8 km away, in nearby Cupertino. The Pentagon's newest digs were literally at the intersection of Big Tech and Big Defence. DIUx's office, housed in a squat brick building, embraced the contradictions of Pentagon West: 'The corridors are old-school drab, the doors secured with combination locks. But inside, the newcomers have revamped the spaces with blackboards, whiteboards, and desks arrayed in random diagonals, to match the nonhierarchical vibe of a Valley startup', reported an observer.[73]

Ash Carter's plan was ambitious: to harness the best and brightest minds from the tech industry for Pentagon use. The native Pennsylvanian had spent several years at Stanford University prior to his appointment as Defense Secretary, and was impressed with the Bay Area's innovative spirit and millionaire magnates: 'They're inventing new technology, creating prosperity, connectivity, and freedom', said Carter.[74] 'They feel they too are public servants, and they'd like to have somebody in Washington they can connect to.' Astonishingly, Carter was the first sitting Defense Secretary to visit Silicon Valley in more than 20 years.

The Pentagon has its own research and development (R&D) agency, DARPA, but it pursues projects that are decades, not months, away. Carter wanted a nimble, streamlined office that could serve as a kind of broker, channelling tens or hundreds of millions of dollars from the DoD's massive budget towards up-and-coming firms developing technologies on the verge of completion. Ideally, DIUx would serve as a liaison, negotiating the needs of grizzled four-star generals, the Pentagon's

civilian leaders, and hoodie-clad engineers and entrepreneurs. Soon, DIUx opened branch offices in two other cities with burgeoning tech sectors: Boston and Austin.

In the short term, Carter hoped that DIUx would build relationships with local start-ups, recruit top talent, involve military reservists in projects, and streamline the Pentagon's notoriously cumbersome procurement processes. His long-term goals were even more ambitious: to take career military officers and assign them to work on futuristic projects in Silicon Valley for months at a time, to 'expose them to new cultures and ideas they can take back to the Pentagon… [and] invite techies to spend time at Defense'.[75]

In March 2016, Carter organised the Defense Innovation Board (DIB), an elite civilian brain trust tasked with providing advice and recommendations to the Pentagon's leadership.[76] He appointed former Google CEO and Alphabet board member Eric Schmidt to chair DIB, which included current and former executives from Facebook, Google, and Instagram, among others.

Three years after Carter launched DIUx, it was renamed the Defense Innovation Unit (DIU), indicating that it was no longer experimental. Despite early challenges, DIUx was described as 'a proven, valuable asset' by Deputy Defense Secretary Patrick Shanahan. 'The organization itself is no longer an experiment', he said in 2018.[77] 'DIU remains vital to fostering innovation across the Department and transforming the way DoD builds a more lethal force.' In early 2018, the Trump administration requested a steep increase in DIU's budget for fiscal year 2019, from $30 million to $71 million.[78] For 2020, the administration requested $164 million, more than *doubling* the previous year's request.[79]

The CIA's Own Venture Capital Fund

Although Pentagon officials portrayed DIUx as a ground-breaking organisation, it was actually modelled on another firm established to serve the US intelligence community in a similar way. In the late 1990s, the CIA established a non-profit entity called Peleus to capitalise on innovations being developed in the private sector, with a special focus on Silicon Valley.[80] Soon after, the organisation was renamed In-Q-Tel.

The first CEO, Gilman Louie described how the organization was created to solve 'the big data problem':

> [CIA leaders] were really afraid of what they called at that time the prospect of a 'digital Pearl Harbor'… Pearl Harbor happened with every different part of the government having a piece of information but they couldn't stitch it together to say, 'Look, the attack at Pearl Harbor is imminent'… [In] 1998, they began to realize that information was siloed across all these different intelligence agencies of which they could never stitch it together… they were trying to solve the big data problem. How do you stitch that together to get intelligence?[81]

By channelling funds from the CIA to nascent firms building surveillance, intelligence gathering, data analysis, and cyber-warfare technologies, the agency hoped to get an edge over global rivals by co-opting creative engineers, hackers, scientists, and programmers. In 2005, the CIA pumped approximately $37 million into In-Q-Tel. By 2014, the organisation's annual funding ballooned to

nearly $94 million, and it had made 325 investments in an astonishing range of technology firms.[82]

If In-Q-Tel sounds like something out of a James Bond movie, that's because the organisation was partly inspired by—and named after—Q Branch, the British secret service's fictional R&D office, popularised in Ian Fleming's spy novels and Hollywood blockbusters. In-Q-Tel and DIUx were ostensibly created to transfer emergent private-sector technologies into US intelligence and military agencies, respectively. A somewhat different interpretation these organisations were launched 'to capture technological innovations… [and] to capture new ideas'.[83] Critics point to In-Q-Tel as a prime example of the militarisation of the tech industry.

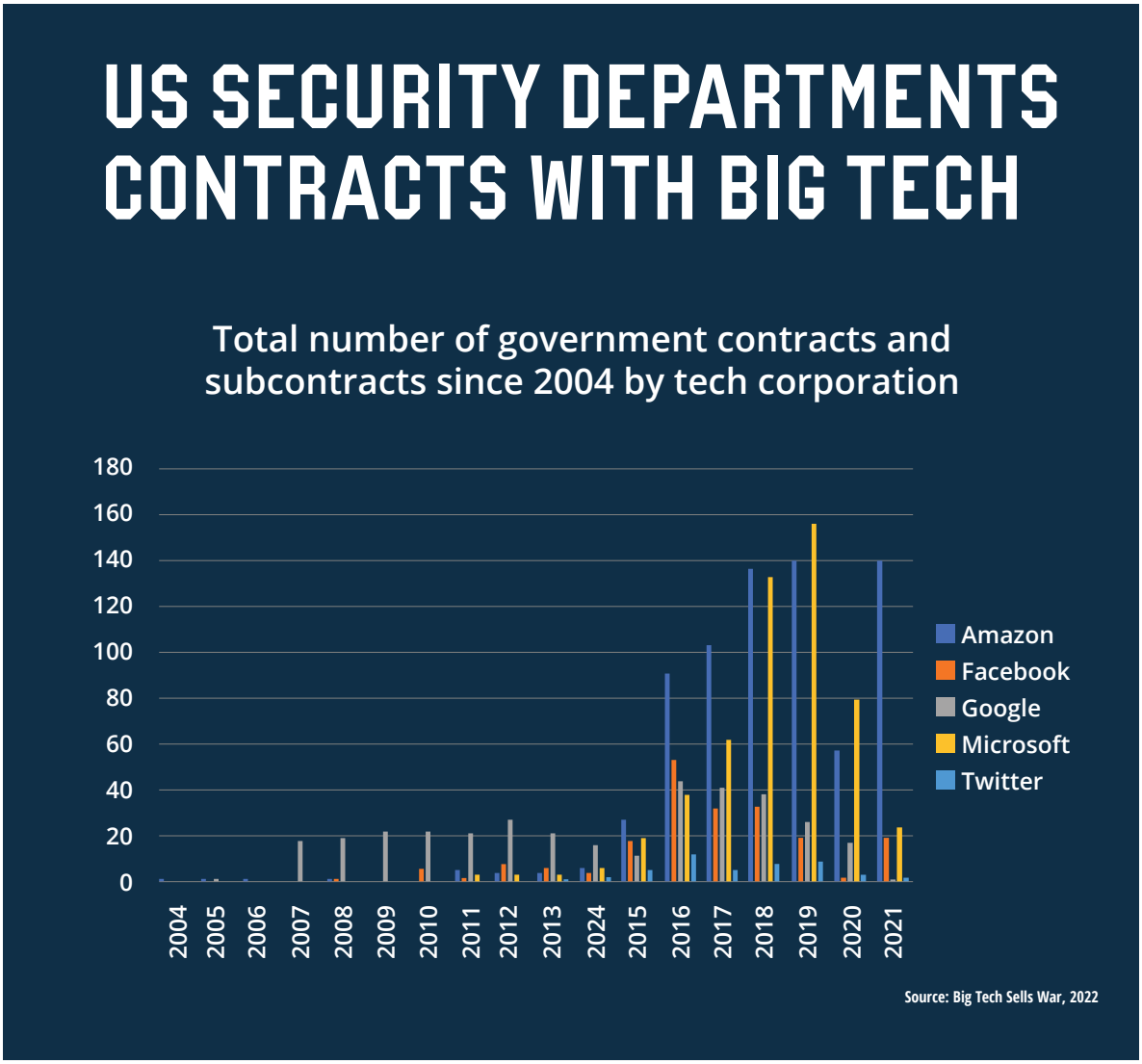
In monetary and technological terms, it's likely that the most profitable In-Q-Tel investment was Keyhole, a San Francisco-based company that developed software for weaving together satellite images and aerial photos to create three-dimensional models of the earth's surface. The programme could essentially create a high-resolution map of the entire planet. In-Q-Tel provided funding in 2003, and within months, the US military was using Keyhole to support US troops in Iraq.[84]

Official sources never revealed how much In-Q-Tel invested in Keyhole, but in 2004, Google purchased the start-up. It was renamed Google Earth. The acquisition was significant: Yasha Levine writes that the Keyhole-Google deal 'marked the moment the company stopped being a purely consumer-facing internet company and began integrating with the US government'.[85] By 2007, Google was actively seeking government contracts evenly spread among military, intelligence, and civilian agencies.[86]

Apart from Google, In-Q-Tel's portfolio includes firms with futuristic projects such as Cyphy, which manufactures tethered drones that can fly reconnaissance missions for extended periods thanks to a continuous power source; Atlas Wearables, which produces fitness trackers that closely monitor body movements and vital signs; Fuel3d, which sells a handheld device that produces detailed three-dimensional scans of structures or objects; and Sonitus, which has developed a wireless communications system, part of which fits inside the user's mouth.[87] If DIUx has placed its bets with robotics and AI companies, In-Q-Tel has pursued those creating surveillance technologies—geospatial satellite firms, advanced sensors, biometrics equipment, DNA analysts, language-translation devices, and cyber-defence systems.

More recently, In-Q-Tel has shifted towards firms specializing in data-mining social media and other internet platforms. These include Dataminr, which streams Twitter data to spot trends and potential threats; Geofeedia, which collects geographically indexed social media messages related to breaking news events such as protests; and TransVoyant, a firm that collates data from satellites, radar, drones, and other sensors.[88]

Some might applaud US military and intelligence agencies' successful recruitment of tech firms. Given the rapid development and deployment of high-tech weapons systems and surveillance programmes by rival nations such as China—which has deployed comparable technologies against its own citizens in Xinjiang province[89]—proponents often claim that the US military cannot afford to fall behind in an AI arms race. But such arguments fail to consider how merging Big Defence with yet another major industry will bind the US economy ever more tightly to endless wars abroad and militarised policing at home.



Project Maven

Many companies funded by In-Q-Tel and DIUx have been small start-ups in dire need of cash. But the Pentagon's interest in Silicon Valley also extends to the biggest internet-based companies.

Consider the case of Project Maven—known formally as the Algorithmic Warfare Cross-Functional Team. Deputy Defense Secretary Robert Work established the programme in April 2017, describing it as an effort 'to accelerate DoD's integration of big data and machine learning... [and] to turn the enormous volume of data available to DoD into actionable intelligence and insights at speed...'.[90] *The Bulletin of the Atomic Scientists* states the problem succinctly:

> US spy planes and satellites collect more raw data than the Defense Department could analyze even if its whole workforce spent their entire lives on it. Unfortunately, most of the imagery analysis involves tedious work—people look at screens to count cars, individuals, or activities... most of the sensor data just disappears—it's never looked at—even though the department has been hiring analysts as fast as it can for years.[91]

The Pentagon had spent tens of billions of dollars on sensors. Creating algorithms to sort and analyse the images made good economic sense, and at a projected cost of $70 million,

Project Maven must have seemed like a bargain. The scope of the work was staggering. In their current state, AI systems require massive data sets for 'deep learning', which essentially means learning by example. During the latter half of 2017, people working on Project Maven reportedly labelled more than 150,000 visual images to create the first datasets for training the algorithms. The images—photos of vehicles, individuals, objects, events—had to account for hundreds, if not thousands, of variable conditions—different altitudes, photo angles, image resolution, lighting conditions, and more.

What organisation could possibly take up such a task? Pentagon officials were quiet about which companies were involved, but some insiders provided oblique hints that significant Big Tech players were involved.[92] Marine Corps Colonel Drew Cukor, who headed Project Maven, noted that 'We are in an AI arms race… It's happening in industry [and] the big five Internet companies are pursuing this heavily. Many of you will have noted that Eric Schmidt [then CEO of Alphabet Inc., Google's parent company] is calling Google an AI company now, not a data company'.[93]

Just eight months after the Defense Department launched Project Maven, the military was using the programme's algorithms to support drone missions against ISIS in Iraq and Syria.

In March 2018, Gizmodo published a series of blistering exposés revealing that the Pentagon had quietly contracted Google for Project Maven work in September 2017.[94] According to internal emails from Google executives, the deal was worth at least $15 million, and was expected to increase to as much as $250 million.[95]

Some emails detailed meetings between Google executives and Deputy Defense Secretary Jack Shanahan.[96] More than ten Google employees were assigned to the project, and the company had partnered with several other firms including DigitalGlobe, a geospatial imaging company, and CrowdFlower, a crowdsourcing company. CrowdFlower (which has since changed its name to Figure Eight) paid so-called 'crowd workers'—people who complete repetitive tasks online, such as identifying photos—to label thousands of images for algorithmic 'deep learning'. Apparently, the crowd workers didn't know what they were building, or who would benefit as a result.[97]

Some of Google's internal emails implied that the company had ambitious plans going beyond what was initially suggested in the Pentagon's initial announcements. One suggested creating a 'Google-earth-like' spy system giving users the ability to 'click on a building and see everything associated with it' including people and vehicles.

Google officials privately worried about a potential public relations problem if the Project Maven project was leaked: 'I think we should do a good PR on the story of DoD collaborating with GCP from a vanilla cloud technology angle (storage, network, security, etc.)', wrote Fei-Fei Li, Google Cloud chief AI scientist, 'but avoid at ALL COSTS any mention or implication of AI'.[98]

But eventually, word got out.

Revolt of the Engineers

By February 2018, internal emails about Project Maven circulated widely among Google employees, many of whom were shocked and dismayed by what the company's senior executives had done. Within months, more than 4,000 Google researchers had signed a letter to CEO Sundar Pichai, demanding cancellation of the Maven contract. The letter, which was signed by several senior engineers, began with the statement: 'We believe that Google should not be in the business of war'. It also demanded that Google develop 'a clear policy stating that neither Google nor its contractors will ever build warfare technology'. By the end of the year, nearly a dozen employees resigned in protest of the company's military contracts and executives' lack of transparency.[99]

Astonishingly, the employees succeeded, at least momentarily. In early June, Google announced that the company would terminate its Project Maven work when the contract expired. Days later, Google released a set of ethical guidelines or 'AI principles', stating that the company 'will not design or deploy AI' for weapons systems, for 'surveillance violating internationally accepted norms', or for technologies used to contravene international law and human rights.[100]

Google's commitment to cancelling its Project Maven work was too good to be true. In March 2019, *The Intercept* obtained an internal Google email indicating that a third-party company would continue working on Project Maven using 'off-the-shelf Google Cloud Platform (basic compute service, rather than Cloud AI or other Cloud Services) to support some workloads'. Walker added that Google was working with 'DoD to make the transition in a way that is consistent with our AI principles and contractual commitments'.[101]

Other reports revealed that the Defense Department had awarded the Project Maven contract to Anduril Industries, best known for creating the Oculus Rift virtual reality headset. The previous year, Anduril had piloted a surveillance system developed for US Customs and Border Protection agents. The system uses AI to detect the presence of people attempting to cross the US border.

Although media reports implied that Google (and later Anduril) were the only firms that played a role in Project Maven, the reality is far more complex and troubling. A careful analysis by the non-profit research organisation Tech Inquiry documents the deeper involvement of numerous other contractors and subcontractors.[102] The Pentagon granted 'prime awards' to ECS Federal and Booz Allen Hamilton, and 'subawards' to a range of firms including Microsoft, Clarifai, Rebellion Defense, Cubic Corporation, GATR Technologies, Technical Intelligence Solutions, and SAP National Security Services, among others. These contracts were never widely publicised.

Although those Google employees who resisted Project Maven represented only a modest portion of the company's 70,000 employees, they succeeded in sparking discussion about tech industry military contracts, and a broader debate about the ethics of AI.

The Google revolt resonated throughout Big Tech and inspired others to follow. For example, in February 2019, more than 200 Microsoft employees demanded that the firm cancel a $480 million US Army contract to supply troops with more than 100,000 augmented-reality HoloLens headsets. The Pentagon's request for proposals outlined a need for a head-mounted display capable of giving soldiers night vision, stealthy weapons targeting, and the ability to automatically recognise threats. It would ideally give soldiers 'increased lethality, mobility, and situational awareness', according to the announcement.[103]

In an open letter to Microsoft CEO Satya Nadella, the workers expressed concern that in the hands of the military, HoloLens could be 'designed to help people kill' by 'turning warfare into a simulated video game'. The employees added, 'we did not sign up to develop weapons, and we demand a say in how our work is used'.[104] Microsoft executives refused to cancel the contract. Nadella said, 'we're not going to withhold technology from institutions that we have elected in democracies to protect the freedoms we enjoy'.[105]

During the summer of 2018, approximately 450 employees from tech giant Amazon signed a letter demanding that the company stop selling Rekognition—a facial-recognition software programme—to law enforcement agencies.[106] The employees' letter also asked that Amazon's Web Services division stop hosting Palantir, a tech company that provided data analysis software to US Immigration and Customs Enforcement, as the agency was targeting unaccompanied children and their families for deportation. Amazon CEO Jeff Bezos shrugged off the employees' letter. 'One of the jobs of the senior leadership team is to make the right decision even when it's not popular', he said in October 2018. 'If big tech companies are going to turn their back on the US Department of Defense, this country is going to be in trouble.'[107]

As tech workers expressed reticence about involvement in military projects, executives peddled their companies' wares to Pentagon officials. Microsoft announced Azure Government Secret, a cloud service for Defense Department and intelligence community clients requiring 'US Secret classified workloads'.[108] Oracle's websites boasted about how its products 'help military organizations improve efficiency, mission preparation, and execution'.[109] And Amazon created a slick, ninety-second promotional video in August 2018, titled simply 'Amazon Web Services for the Warfighter'.[110]

Fighting Back against the Merger of Big Tech and Big Defence

Silicon Valley's technologies illustrate the unpredictable consequences of unleashing new hardware or software. The idea that an invention can be used for either peaceful or military purposes—that is, the notion of dual-use technology—became widely accepted in US society over the past century.[111] Historian Margaret O'Mara reminds us that throughout the Cold War, 'the Valley built small: microwaves and radar for high-frequency communication, transistors and integrated circuits… Silicon Valley built elegant miniaturised machines that could power missiles and rockets, but that also held possibilities for peaceful use—in watches, calculators, appliances, and computers'.[112]

These technologies continue to have dual-use applications. Google Earth can be employed for mapping and geographic research, but it can also be used by Special Forces teams for targeting electrical power grids, bridges, or other infrastructures.[113] Microsoft first marketed HoloLens as an augmented-reality device for gamers, artists, and architects, but the most profitable consumers are likely to be infantry. Amazon's facial-recognition programme might be used for secure bank or ATM transactions, but they can also be used as surveillance technologies by military, intelligence, or law enforcement agencies such as US Immigration and Customs Enforcement. Cloud platforms offered by Amazon, Oracle, Microsoft, and Google can potentially store data for scientific researchers, public health officials, or commercial firms. But they can also increase the lethality of military forces.

Some might chide Google's dissident engineers and scientists as naïve Pollyannas. After all, didn't they know what they were getting into? If scientists generally understand that fact that once they produce knowledge, they will probably have no control over how it is used, then they must have surely understood that the devices and apps they were creating might at some point be weaponised. Or did they?

It is possible that many scientists and engineers now objecting to Silicon Valley's military work might have never imagined that they would be drawn into the military-industrial-technological complex. Perhaps they even decided to work for tech companies because they thought those firms were not in the weapons business. After all, the letter written by Microsoft's protesters states: 'We did not sign up to develop weapons'.

The researchers may also have placed inordinate faith in their company's executives. At Google, employees felt betrayed by secretive decisions that led to the Project Maven contract. The business press regularly recognises the firm as having the best 'corporate culture' in the US, not only because employees can bring pets to work and have access to organic meals prepared by professional chefs, but also because the organisation has a reputation for valuing employee collaboration.

Once Project Maven came to light, tech workers' false consciousness began to evaporate. Earning a six-figure income as an engineer or a programmer straight out of college makes it difficult to think of yourself as a proletarian, especially when you're enjoying the perks offered by the industry—free gourmet lunches, on-site gyms, and complimentary childcare, for example. For thousands of employees, being shut out of discussions about whether the company should collaborate in AI weapons development woke up a latent sense of class consciousness.

There was also another problem: Silicon Valley's long-standing entanglements with the Pentagon. As this essay accounts and as noted by Margaret O'Mara, 'Whether their employees realize it or not, today's tech giants all contain some defense industry DNA… This involves a much fuller reckoning with the long and complicated history of Silicon Valley and the business of war'.[114]

The divide between the Pentagon and Silicon Valley is mostly a myth—it's never really existed, at least not in any significant way. The differences are superficial and stylistic. For the better part of a century, the regional economy and culture have been shaped by what might be called the military-industrial-university complex. During the Cold War, the Pentagon helped build the computer industry by awarding military contracts in fields like microwave electronics, missile and satellite production, and semiconductor research.

Historian Thomas Heinrich reminds us that popular portrayals of 'ingenious inventor-businessmen and venture capitalists [who] forged a dynamic, high-tech economy unencumbered by government's heavy hand' draw attention away from the crucial role of 'Pentagon funding for research and development [that] helped lay the technological groundwork for a new generation of startups' in the twenty-first century.[115] From the 1950s until the late 1990s, Silicon Valley's biggest private-sector employer wasn't Hewlett Packard, Apple, Ampex, or Atari. It was defence giant Lockheed. Today the region faces a familiar pattern, albeit that the gargantuan size and influence of today's tech firms dwarf the computer companies of yesteryear.

This is likely to have major implications in the near future. Jack Poulson, a former Google senior research scientist and co-founder of Tech Inquiry, put it to me this way: 'I believe we're witnessing the transition of major US tech companies into defense contracts and would go so far as to predict them purchasing defense contractors in the coming years—something like Amazon buying Raytheon'.[116]

The real fault line isn't between the Pentagon and Silicon Valley. It's *within* Silicon Valley, where a modest contingent of politically awakened engineers and scientists have pushed back against the weaponisation of their work. When they face a full attack from PR messaging, hearts and minds campaigns, 'collaborative' discussion, more compensation and perquisites—and perhaps the tacit threat of losing their jobs or having them outsourced—will they capitulate?

At this point it's too early to know the outcome, but the future of virtual warfare and digital battlefields may well rest in their hands.

BIOGRAPHY

Roberto J. González is chair of the Anthropology Department at San José State University. He is the author of several books, including *War Virtually: The Quest to Automate Conflict, Militarize Data, and Predict the Future, Connected: How a Mexican Village Built Its Own Cell Phone Network,* and the co-edited collection *Militarization: A Reader.* He is a founding member of the Network of Concerned Anthropologists.

The everywhere border

Digital migration control infrastructure in the Americas

Mizue Aizeki, Laura Bingham and Santiago Narváez

In 2021, José Eusebio Asegurado, a farmer in El Salvador, was arrested by the Salvadoran National Civil Police for 'promoting human trafficking'. The basis for the arrest was a WhatsApp group chat that Asegurado and other migrants[117] were using to coordinate a caravan, which had been infiltrated by a police agent. According to the screenshots used to incriminate him, Asegurado's only participation in the chat was responding 'OK' to a migrant's message that he would be at a meeting point at around 5 o'clock. Police arrested Asegurado at the meeting point, telling him he was 'profiled' as a caravan organiser.[118]

The same day, the Salvadoran police also charged Fátima Pérez, a cook, and Juan Rufino Ramírez, a private security guard, with promoting 'human trafficking' based on messages on a WhatsApp group they had created to coordinate a caravan. Screenshots in Ramírez's case show him giving instructions to the 55-member group to meet at the bus station, and the prices of tickets to Guatemala. The police arrested Ramírez and Pérez the morning they were planning to leave.

These three arrests took place in the span of four hours. The then-US ambassador in El Salvador, Katherine Dueholm, promptly congratulated the General Prosecutor's office,[119] stating: 'I applaud the Salvadoran authorities who are taking action against those who want to deceive citizens with caravans and false promises. They promote only #UnViajeEnVano'—'a journey in vain'.

The arrests and Ambassador Dueholm's praise reflect the critical role of covert surveillance and data-driven 'smart' technologies in US migration-control practices operating deep within countries outside the US. Over the past twenty years, the US (and other wealthy countries) have made strides to externalise border-control regimes well beyond their actual territory. This often involves effectively enrolling agencies in other countries in migrant surveillance, policing, and exclusion.

The new digital infrastructure that enables border externalisation, however, is little understood. This digital infrastructure relies on both military-grade technology built by major weapons manufacturers and Silicon Valley innovation: inter-operable databases that share fingerprints seamlessly between police agencies across borders; biometric collection devices used by Mexican detention authorities to track migrants for US Customs and Border Protection (CBP); social media apps that serve as critical communications networks for migrants and surveillance tools for police; digital ID systems that enable access to essential services, but double as tracking devices.

Infrastructure—digital or material—has real sticking power; that's the point. Once a highway splits a community in half, a new permanence stifles the din of protest, and people move on. We use the term *digital infrastructure* to describe the establishment of a foundation that will be fundamental to how world powers will practise migration control; and, as it embeds itself, increasingly beyond challenge—a unified strategic intervention by powerful countries, with the US coveting the vanguard. While it may look like technological experimentation (like AI-powered robot dogs on the border) or one-off opportunistic data-grabs (like networks of international data-sharing agreements), the growth of digital border infrastructure is *by design.* This is enabled through joined-up digital technologies that settle into the kind of rigid, 'motiveless' permanence granted to other infrastructures, like submarine communications cables, protocols and servers that run the internet, an electrical grid or a superhighway.[120]

The profound implications of new infrastructures persist long after their creation, as is the case for the digital infrastructure deployed to police migrants in the so-called US 'backyard'. Its impacts are frequently rendered invisible. Governments promote border policing technologies as fundamentally safe, humane and non-violent while migrant advocates struggle to make visible the violence on the other side of this unseen 'borderland circuitry'.[121]

The implications range from digitally triggered violence and killings by local police in Central America to actions by the US, its allies and competitors in geopolitical contests over the control of global security. The US government and private industry have worked themselves into a largely covert entrepreneurial frenzy to own and control the migration policing interface of the future. Monitoring and control capabilities—a longstanding and routine part of US aid packages to fight organised crime—both expand domestic spying by partner governments for their own ends and serve US border externalization interests in controlling the movement of people and diverting them away from the US territorial border.

This essay will focus primarily on how digital infrastructure serves US interests. What do we know about this strategy and how it is already affecting mobility and human rights in the region? What are its historical foundations? What challenges lie ahead? It is impossible to answer these questions simply by dissecting the cruelty or provenance of any single technology, system or actor. We first need to understand the transnational motivations driving these incremental, more observable, facts on the ground. We need, in other words, to make visible the invisible digital infrastructure.

Digital infrastructure is key to border externalisation and a rise in unaccountable violence

Understanding border externalisation through the lens of digital infrastructure captures the true scale of border practices envisaged by the US (and its competitors and allies) as well as their envisaged permanence within the future world order. Digital border infrastructure feeds on histories of domination, control and atrocities in the name of transnational 'crime-fighting' projects, setting the stage for tremendous social costs.

First, as to scale, we are witnessing an escalation of US border imperialism and borderland violence[122]—both in terms of geographical reach far into national territories and the further extension of 'policeability' to an increasing number of individuals and groups through this digital infrastructure. This includes anyone an algorithm decides might be 'dangerous', those who might migrate, as well as humanitarian actors, migrant advocacy groups, and aid organisations. Scaling and the rapid growth it engenders is a quintessential property of digital technologies, regardless of their origin or application. The shifts to new targets under digital infrastructure are frictionless compared to earlier analogue-based border policing tactics. Asegurado, the farmer assisting migrants in El Salvador, was swept up in the US border externalisation dragnet with a simple 'OK' on a WhatsApp chat.

Second, as to permanence, advocates of digital borders in national capitals, industry and development agencies embrace the term 'digital public infrastructure' as a brand, to bestow (unearned) trust, normalisation and the inevitability of contested digital tools such as biometric IDs and payment

systems.[123] Ceding the privilege of defining 'digital infrastructure' to actors with vested interests in current migration-control practices is reckless. Without a counternarrative that articulates their violent disposition, digital border externalisation tools—including widespread biometrics collection, real-time transaction data-collection in payment systems, and the confiscation of smartphones at the border—can easily be normalised as 'digital public infrastructure', rather than resisted.

The scale and enduring impact of the rapidly hardening digital infrastructure that fuels border externalisation calls for urgent transnational organising. As writers and activists, we have come together to resist the use of digital infrastructure in US migration-control policy in Mexico, Central and South America, and the Caribbean. We have only traces and not the whole picture. Building on the work of others, we weave all this together to show how the fusion of state and digital power to construct digital border infrastructure is neither humane nor safe: rather, it is increasing unaccountable forms of violence.

Convergence: Drugs war, border externalisation, digital infrastructure and the militarisation of US' neighbouring regions

Economic and political initiatives since the 1970s have driven relentlessly towards US investments in more militarised, criminalising, and digitised migration-control practices. Since 9/11, the US convergence of 'national security' with unauthorised migration has fueled an ever expanding border externalisation regime—currently there are 23 CBP offices and 48 ICE offices worldwide[124]—and consequently has provided an especially lucrative market for digital surveillance corporations.[125] Through programmes such as the Mérida Initiative and the Central American Regional Security Initiative, the US has tied aid to countries such as Mexico, El Salvador, Guatemala and Honduras to increased militarisation, policing, incarceration, and migration control.

Yet migration patterns to the US from Mexico, Central America and the Caribbean cannot be divorced from the practices and policies that the US employed for over a century to dominate countries in these regions. Decades of US practices and policies have fuelled economic, political, and environmental instability—key factors that drive migration to the US. Over the past 20 years the number of people migrating from Central America has more than doubled, the largest increases coming from Guatemala, Honduras and Mexico. The US-backed 'war on drugs' in Mexico and Central America has dramatically increased violence and instability.[126] In Mexico, the fight against organised crime has resulted in 350,000 deaths and more than 72,000 disappearances between 2006 and 2021. According to the World Bank, 60% of rural Central Americans live in poverty. While the largest contributors to the climate crisis are wealthy countries, these already impoverished populations suffer the most acute impacts of climate change. For decades, prolonged droughts together with natural catastrophic events such as hurricanes and floods have deeply affected Central America. The number of people facing food insecurity tripled between 2019 and 2021, affecting 6.4 million people. Asegurado, Pérez and Ramírez—like many others—are grasping for alternatives to this intolerable situation.

Rather than acknowledge these underlying causes, the US response has been to extend its border ever further. General John Kelly, former Secretary of the US Department of Homeland Security (DHS), stated, 'I believe the defense of the Southwest border starts 1,500 miles to the south'. Mexico has long been central to the US border-externalisation regime, and digital infrastructure plays an increasingly critical role. Tony Crowder, former director of CBP's Air and Marine Operations, shared Kelly's sentiment 'We have taught the Mexicans how to fish… [but] even though we have all this surveillance capability, we don't have enough, we need more'.[127]

While part of a continuum of US efforts to enlist Mexico in support of its regional objectives, this 'security and rule-of-law partnership' accelerated following 9/11. In 2007, the US shifted the focus of its drug war from Colombia to Mexico, Central America, and the Caribbean. Under this frame of securitisation, the drug war merged with the migrant-control regime. In 2008, the Mérida Initiative was launched—a bilateral partnership between the US and Mexico in the name of the US war on drugs. It initially provided financing for Mexico to purchase equipment for its military and police forces and for intelligence gathering. In 2013, Mérida was revamped to include four pillars, incorporating the creation of a '21st century US-Mexican border, while improving immigrant enforcement in Mexico and security along Mexico's southern borders'. Effectively an extension of US policy, some $3.5 billion has helped shape Mexico's migration-control agenda since 2008.

In 2014, *Programa Frontera Sur* further securitised Mexico's southern border by increasing the migration policing and deportation apparatus. Consequently, Mexico now has one of the world's largest immigration detention systems. Between 2014 and 2017, Mexico deported more Central Americans than the US Border Patrol. Doris Meissner, the former commissioner of the Immigration and Naturalization Service (INS, the predecessor to ICE and CBP), underscored the importance of Mexican migration control, explaining in 2017 the need to look at both US and Mexican data to assess the effectiveness of US border enforcement.[128]

Under these agreements, the US Department of Defense has provided training and sold millions in military equipment to Mexico, including an array of 'smart border' technologies provided by corporations such as Dev Technology, General Dynamics, Amazon Web Services, and NEC.[129] The CBP and ICE have provided training on intelligence-gathering, info-sharing, and migration policing. A key element of US support to Mexico has been to develop an infrastructure to collect and share data—such as biometric and biographical information, and criminal history—in a manner that interfaces seamlessly with US databases.

The digital infrastructure that tracks and catalogues migrants is central to US migration policy in Mexico. The US-backed Instituto Nacional de Migración (INM) strategy relies on this infrastructure as the primary means to control migration rather than sealing Mexico's southern border with Guatemala. Biometric collection is essential to making migrants more legible to the state. In 2011, the US provided four biometric kiosks to Mexico's southern border, and 117 additional biometric scanners the following year. Between 2018 and the first half of 2022, the Mexican government gathered and shared information on over 360,000 migrants in detention facilities.[130] Information from CBP reveals that Mexican authorities shared information from 10,000 humanitarian visa applications with DHS. The release of approximately 1,800 unregistered migrants from a shelter in Piedras Negras was conditional on the registration of their data.[131]

An 'Information Sharing Environment' that includes inter-operable data-sharing systems is central to achieving the objectives of the homeland security state.[132] 'Inter-operability' enables seamless connectivity between police, immigration agencies, foreign governments, and more.[133] Key forms of US-initiated digital infrastructure rely on widespread information-gathering and seamless sharing of data for surveillance across borders.

This vast amount of data-collection and sharing has been fuelled by unleashing the power of the carceral state—including the centrality of the 'criminal alien', 'gang member' and 'drug trafficker' as threats to national security—at all geographic levels of the US migrant-control regime. For example, the Biometric Identification Transnational Migration Alert Program (BITMAP) allows DHS and its partner countries to know where and when an individual arrives in the Western Hemisphere and their travel patterns before they reach the southwest US border. BITMAP is currently deployed to 18 countries, including Mexico. DHS also has a Criminal History Information Sharing (CHIS) programme that allows for the global sharing of biographic, biometric, and descriptive information on individuals deported from the US (e.g. alleged immigration, employment, family, and criminal histories).

The structural criminalisation of poverty in both countries is amplified with CHIS. According to the National Survey of Imprisoned Population in Mexico, conducted by the National Institute of Geography and Statistics (INEGI) in 2021, nearly 44% of the respondents declared having been imprisoned on the basis of false accusations or incriminations. Forty-two percent claimed they had been forced to plead guilty or to incriminate someone else. Nearly half of those who are jailed have not been convicted,[134] and nearly half of all convictions are for theft of under US$100.[135] This is the kind of data that feeds CHIS.

In another example, DHS is developing the Homeland Advanced Recognition Technology System (HART) to replace its current centralised biometric database, IDENT, through a contract with Peraton (a subsidiary of Veritas Capital, a private equity firm). Hosted by Amazon Web Services, HART will enable DHS to aggregate and compare biographical and biometric data on hundreds of millions of people across the globe. This includes so-called encounter data from police stops, facial recognition, DNA, iris scans, and voice prints—usually gathered without the individual's knowledge or consent. The massive HART database draws from widespread biometrics collection in all realms—for example, the US DOS INL's development of integrated DNA databases in Mexico and Central America in the name of combating trafficking or the proposed national biometric digital ID in Mexico. In this way, multiple state initiatives merge, and the power of the state to police, track and control migrants and all people under their watch grows exponentially.

While the Mérida Initiative formally ended in 2019, its approach has been sustained by the Mexican government. In 2021, the Mexican government increased the military by 46% and the National Guard dedicated to stopping migrants by 300%. In July 2022, President López Obrador committed $1.5 billion in smart border infrastructure over the next two years.

For US partner states, any technological and data-sharing channels that are financed and exported to them become assets—not just for monitoring migrants, but to advance multiple agendas of coercive power-building. This infrastructure can therefore end up fuelling violence and criminalisation, undermining the right to asylum, exacerbating inequality, and expanding the power of paramilitaries and the police, while privileging securitised neoliberal and corporate prerogatives.

The geopolitical nature of digital infrastructure

In their research on digital payment systems, Marieke de Goede and Carola Westermeier use the term 'infrastructural geopolitics' to stress the growing centrality of infrastructure to geopolitics and the ways in which US economic power is rooted in financial infrastructures (which, like migration control, are rapidly digitising).[136]

The global financial messaging network SWIFT is an example of infrastructure that is invisible to most people and yet plays a major role, as the writers describe, in reinforcing power relations of the post-war global order in which it emerged. Seventy years after the Second World War and fifty years since SWIFT's establishment, bank messaging routes flow through former colonial capitals and map onto a 'core' of Western countries, leaving large swaths of Latin America, Africa, and the Middle East in a permanent, but effectively invisible, economic periphery. Similarly, digital IDs, social media monitoring and infiltration, and data-sharing platforms are essentially component parts, nodes, or partially visible layers of deeper, longer-term geo-strategic digital infrastructure projects.

Extension of borders through digital infrastructure serves US political and economic goals well beyond the policing of human mobility. Geopolitical contests for control over infrastructures play out across several domains. Military establishments covet 'identity dominance', an objective that drove US forces to gather massive stores of biometric data in Afghanistan and Iraq as a weapon of war.[137] US digital services giants like Amazon and Google mastered 'platformisation' by building e-commerce (digital advertising, search, social media, etc.) infrastructure to dominate the digital economy. Often, public and private-sector interests converge, including in the form of public–private partnerships (PPPs) to build infrastructure. In each case, the true contest among states and corporate giants centres on control over the interface, or the most essential, invisible, infrastructural methods of digital communication and control. As Michael Kwet explains, 'Transnational "Big Tech" corporations based in the United States have amassed trillions of dollars and gained excessive powers to control everything, from business and labor to social media and entertainment in the Global South. Digital colonialism is now engulfing the world'.[138] The US quest for domination through externalised migration policing infrastructure goes hand in hand with its geopolitical and corporate designs for economic power.

These forms of infrastructural digital power pose unique challenges for documentation and ultimately for any form of systemic change. Challenges include blurred lines of responsibility, mission, and function; governments and corporate actors are seen or presented as passive conduits or intermediaries in digital public infrastructure; and infrastructures can easily appear to be 'ahistorical' and motiveless. In Mexico and Central America, migration control converges with ongoing US foreign policing operations (such as the war on drugs, and gang wars). We explore the several simultaneous effects of this complex merger: the turn to digital infrastructure; its relationship to violence and human suffering; and its foreclosure of accountability for these harms.

Digital border infrastructure in your phone: Information and Communications Technology (ICT) policing techniques along migration routes

Surveillance infrastructure is tangible in physical migration detention centres and in police arrests: mugshots, cheek swabs, confiscation of the detainee's mobile phone. The deepening integration of daily life, telecommunications and computers open extensive avenues for more covert, opportunistic surveillance of private communications and activity by users who rely on social media, mobile communication and messaging apps. The surveillance of mobile phones and social media ranges from overt disclosure requirements for visa and benefits applications to government listing and tracking of protesters and other 'undesirable' actors. Migrant surveillance is immersed in these control schemes where surveillance technology serves as a silent tool for government violence and repression.

This has had an impact on how migrants travel and keep safe, such as through safety in numbers. Travelling in caravans has therefore become both a survival and a protest strategy: sources of both physical and economic security and opposition to the economic policies that contributed to their displacement. Social media and messaging apps are key tools for the coordination of caravans and for migrants more broadly. Migrants use these tools to identify routes, look for shelter and food, communicate with their support networks, warn each other about risks, and coordinate travel. Governments as well as organised crime understand these dynamics and use these same tools to monitor and extort migrants.

On 5 June 2019, Irineo Mujica, from *Sin Fronteras*—a civil society organisation (CSO) dedicated to the protection of human rights of migrants in Mexico and the US, and which has supported multiple migrant caravans—was arrested in Mexico, falsely charged with human trafficking. Mujica appeared in the CBP's watchlist database published in 2019 that contained photos, names, professions, and other details of journalists, activists, and social media influencers both from Mexico and the US with links to the migrant caravan.

A DHS Office of Inspector General (OIG) report on the database and other surveillance practices found that CBP established electronic alerts (lookouts) on journalists, attorneys, and advocates who were connected by social media to the migrant caravans.[139] Those tagged by the lookouts were constantly flagged for secondary screening when entering the US, and interrogated about their work, organisation, family, education, and political leanings.

The weaponisation of such information had grim effects on the Mexican side of the border. According to *Sin Fronteras* activist Alex Mensing, after the CBP shared information gathered through lookouts with the Mexican government, other members from his organisation who assisted migrant caravans in the same period saw an increase in border scrutiny and death threats. Organising and supporting migrants threatens lucrative operations that depend on the criminalisation of migration across the region. Civil society assistance makes migrants less prone to kidnapping and extortion, which therefore reduces the income for organised crime linked to these activities, and, as a domino effect, bribes to authorities also drop, pitting the collective interests of such groups against activists and those providing humanitarian assistance.

Surveilling anyone who might pose a threat to the system has long been a generalised and systematic form of government control in Mexico. A leaked document from the NSO Group, the Israeli company that created Pegasus, revealed that 50,000 people were possible surveillance targets in Mexico. The list included opposition politicians, journalists investigating government corruption and extrajudicial killings, activists advocating the taxing of sugary drinks, judges, academics, and international experts who investigated the case of the enforced disappearance and extrajudicial killing of the 43 students, among others.

In 2022, mobile phones from two journalists and an activist who investigated abuses committed by the Mexican army were found to be infected with the malware Pegasus. In 2020, the Mexican government sought to create a SIM card registry that would link to the card owner's biometrics and other personal data. This would have intensified government digital surveillance via ICT infrastructure, and was opposed by civil society.

CBP internal documents show that government agencies across the border continually share information about the location of migrants, their origin, and the number of people in each group, even before they start to migrate. In 2018, US DHS agents infiltrated a WhatsApp group of Honduran migrants travelling in a caravan of about 4,000. These policing practices are also being reproduced by the Mexican government.[140]

Impact: Infrastructural violence and accountability deficits in globalised migration policing

Roberto M., a young man in El Salvador, was shot and taken away by police shortly after being deported from the US. The rural police officers who shot Roberto also threatened an eyewitness at gunpoint, telling him that Roberto was a gang member and if he revealed what he'd seen, the same would happen to him. Police in El Salvador receive data on gang-member affiliation from the US, and share these lists with neighbourhood-level police where deportees plan to live. These databases have been found to be problematic and unreliable.[141] Police departments confirmed that this information is used to target people: 'We think that if a person wasn't wanted in the United States, it must be because the deported person is bad'.

Violence can increasingly be tied to digital border technologies, particularly in combination with one another and with physical and environmental realities that envelop them. Studies show the effects of integrated fixed-tower surveillance on migrant mortality rates in Arizona's Altar Valley. Here, digital infrastructure merges with the ineffective yet longstanding US deterrence policy that purposefully makes migration routes more dangerous, on the theory that migrants would not risk the journey. The fusion of technology and policies that inflict deliberate harm produces these predictable results of increased migrant deaths.[142]

The story of Roberto M. and the witness to his post-deportation shooting and disappearance in El Salvador reflects another pattern of violence tied to information-sharing through digital infrastructures. The criminologist Ana Muñiz documents a 'cycle of violent policing, migration, more violent policing, detention, deportation, violent policing, migration, and so on', in which the labels themselves ('criminal alien' or 'gang member') become inescapable vectors of precarity.[143] Such

labels channel individuals into a 'sort of statelessness' as constant, quantifiable scapegoats that provide an easy diversion for state security forces and corporations that produce and perpetuate the 'structural causes of violence'.[144]

Digital infrastructure merges not with a physical terrain, but with pre-existing social and political factors that make violence a foregone conclusion. Today's multipurpose digital infrastructure also permits the efficient incorporation of new undesirable criminalised categories, including 'caravan organisers' or 'migration promoters'—as in El Salvador's attempt to reform its penal code, criminalising the 'promotion of migration' on social media.

Challenges and way forward

We are interested in developing deeper knowledge about the political origins of these infrastructures to challenge the violence of global migration control systems. This essay only sets out the field of engagement. Far more collective work is required to document and design models of resistance to meet such challenges.

The diffuse and structural nature of power behind the seemingly ahistorical, and motiveless characteristics of digital infrastructures undermine classic approaches to accountability. Furthermore, the familiar national and international judicial avenues to hold perpetrators of these forms of indirect violence responsible—however imperfect or ineffective they may already be—are exceptionally ill-suited to the conditions at play in the migration policing context specifically, for several reasons.

First, the technologies *in use* such as biometric databases, and the *means of using* civilian technologies like social media and other ICTs, are simply not designed to respect or be held to democratic scrutiny; they are military-grade and converted for use in quasi-militarised spaces, by institutions permeated with military ideology. Nearly a third of CBP personnel previously served in the US military. Biometric surveillance technologies advanced by leaps and bounds within US military operations before being integrated with 'civilian' border policing. Private-sector military contractors play an integral role in this transition.

As journalist Annie Jacobsen documents, as part of the US military biometric data-collection in Afghanistan, Palantir Technologies served as a critical link between US intelligence operations to track and kill military targets and quasi-civilian policing operations like the piloting of rapid DNA samples from migrant families at the US border in 2019.[145] Today, the biometric kits used in Afghanistan, some still storing biometric data collected on the battlefield, are for sale on eBay.

Second, justice and oversight bodies are ill-equipped to serve their intended function in this ecosystem. Within criminal proceedings and investigations, the use of technologies that capture and record evidence of allegedly criminal activity or purport to biometrically match records are extremely difficult to challenge because of their scientific veneer and opaque data-collection and analysis methods, which leaves no practical room to impeach or exclude such evidence. The design of technologies that predetermine risk factors keyed to criminalised behaviour, including migration, contravenes the presumption of innocence. In the civil context, national-level justice mechanisms deny standing to non-nationals located outside the US who are victims of violations linked to digital surveillance.

Finally, there are huge incentives for both state and corporate power to hide violence. The political positioning of 'smart borders' as more 'humane' conceals the state's role in violence and insulates corporations from negative PR or constraints by participating in repugnant markets. Their task is made easy by rendering physical pain abstract rather than affecting real human beings,[146] and features of the data economy like the way corporates have helped the movement towards running government functions like private digital platforms.

Mitigation 'risk assessment' tools like data protection or human rights impact assessments provide cover, favouring the continuation of these business practices because firms undertake them voluntarily and face little or no consequences for a poor risk assessment. Unsurprisingly, these industry-led tools often fail to provide a means for real accountability; they reveal scant information that would be actionable if and when products do cause harm; and the burden of proving rights violations and finding an effective remedy after the fact is shouldered entirely by victims. The interests of powerful actors converge around a web of financial stakes in the system, leading to the aggressive harassment and potential silencing of activists as the case of Irineo Mujica and *Sin Fronteras* illustrates.

We need tools and methods for transnational cooperation to document, gather and share information safely, and organise. Fusing new understandings about how digital power functions within existing resistance movements transnationally, holds potential for challenges to the digital infrastructure of border externalisation.

We are in the initial stages of our collective effort to understand and expose this digital infrastructure. Through this analysis, we can begin to identify the interventions to start to tear it apart and break it down. Transnational organising against tech corporations offers opportunities for shared understanding and meaningful solidarity. This year, organisations in France and Kenya, with support from actors in other countries, sued biometrics giant IDEMIA for its failure to meet even minimum human rights standards of due diligence as it reaps billions in secret border security tech sales to low- and middle-income countries. This emerged from collaborative evidence-gathering and organising across borders.

As the US military establishment recognised decades ago: whoever dominates the field of externalised borders defines 'friend and foe' everywhere.[147] The faster the US establishes economic and political dominance over digital migration-control infrastructure, the greater its security in maintaining global digital power. Digital infrastructure serves multiple purposes at once, but the ultimate geopolitical function is raw, generalised power over global affairs. The tools examined here will 'contain' human life within spaces of catastrophic violence, by design.[148] This specific effect betrays the most fundamental commitments of international human rights and humanitarian law in the face of unprecedented challenges to human survival across most of the world. But this pernicious effect is also ruthlessly beside the point.

In reality, as facets of infrastructural power, the technologies that fix the 'calculation of who must live and who must die'[149] do not do so as an end in itself, but in the service of power and its reproduction in this digital age.[150] In this way the complicity of state and corporate actors in the production of violence is cast in the starkest relief. This geopolitical analysis is our starting point for building resistance towards transformation.

BIOGRAPHIES

Mizue Aizeki is Executive Director of the Surveillance Resistance Lab. For close to twenty years, Mizue has focused on ending the injustices—including criminalization, imprisonment, and exile—at the intersections of the criminal and migration control systems. Prior to the Lab, Mizue was a Senior Advisor at the Immigrant Defense Project (IDP) and the Project Director of the Surveillance, Tech and Immigration Project. Mizue is a co-editor of *Resisting Borders and Technologies of Violence* (forthcoming from Haymarket Books, Fall 2023).

Laura Bingham directs the Temple University Institute for Law, Innovation, and Technology. Prior to joining Temple Law, Laura served as senior managing legal officer with the Open Society Justice Initiative. She established and led a global program on data, technology, and human rights. Since 2017, Laura has taught courses on human rights and forced migration as an adjunct faculty member at New York University's Center for Global Affairs.

Santiago Narváez has been a researcher since 2016 at digital rights NGO "R3D: Red en Defensa de los Derechos Digitales" based in Mexico City where he researches how government surveillance is exercised and its impact on human rights. He has a degree in International Relations and a formation in data analysis.

Seeing the world like a Palestinian

Intersectional struggles against Big Tech and Israeli apartheid

Apoorva PG

In May 2021, as Israeli forces launched an intense wave of airstrikes on the besieged Gaza Strip—resulting in 256 Palestinian casualties and tens of thousands injured—Google and Amazon Web Services (AWS) signed Project Nimbus[151], a $1.2 billion contract to provide cloud services to the Israeli government and military. The two corporations would effectively provide the technological backbone of Israel's occupation of Palestinian territories. Three data centres are already underway for this project. Amazon Web Services also provided the cloud platform[152] for Pegasus spyware until the news on Pegasus Project broke, and continues to do so for the Blue Wolf app,[153] which allows Israeli soldiers to capture images of Palestinians across the occupied West Bank and then matches them with military and intelligence databases.

With its far-reaching and unprecedented impact, the contract is just one manifestation of the profound links between Israel and Big Tech corporations. Hewlett Packard Enterprise (HPE), for example, had an exclusive contract to provide servers from 2017 to 2020 for Israel's population database[154], which was also used to determine various forms of exclusion of Palestinian citizens of Israel and residents of occupied East Jerusalem. Big Tech has helped sustain an occupation built on military control and perpetual surveillance, which Palestinians have for decades denounced as a form of apartheid and as 'settler colonialism'.[155] Amnesty International[156] and other international organisations, the UN Special Rapporteur on human rights in the Occupied Palestinian Territories (OPT), and a growing number of governments believe that Israel is committing the crime of apartheid.

The ubiquity of digital technology and control, alongside the monetisation of personal data, have led to data becoming the new frontier of colonialism. Understanding the role of Big Tech in consolidating Israel's violation of Palestinian human rights brings into sharp relief the urgent need to challenge this global data colonialism. This is both because methods of repression tested on Palestinians are being adopted across the world, and because in questioning Big Tech, its collusion with military and surveillance agencies and its theft of our data enables us to build intersectional struggles against the *matrix of oppression*—of militarisation, neoliberal capitalism and Israeli apartheid—that Big Tech bolsters and from which it profiteers.

The deep ties between Israel and Big Tech have enabled a two-way flow of profit, crime and complicity. This enables Israel to deploy fast-innovating technology developed by transnational corporations (TNCs) and integrate it in its surveillance, control and repression of Palestinians. At the same time, Israeli technology developed to control the Palestinian people is made available for Israeli and international tech companies to scale up and export to other countries for repressive purposes. Consider some of these statistics compiled by Palestinian Stop the Wall campaign in its Digital Walls[157] report:

- During the last few decades, over 300 leading technological multinational corporations established R&D centers in Israel, accounting for about 50% of the business enterprise R&D [research and development] expenditure.
- These multinational corporations have acquired a total of 100 Israeli companies. A number of them, such as—Intel, Microsoft, Broadcom, Cisco, IBM and EMC—acquired over ten local companies over the span of their operation in Israel.
- More than 30 tech Unicorns—start-up companies valued more than 1 billion US$—are located in Israel. This is around 10% of the world's unicorns.

This symbiotic relationship drives Big Tech's investment in Israel, and reinforces the growth of militarised digital technology and surveillance, which has been pioneered by but is not unique to Israel.

Big Tech and Global Imperial Wars

The specific context of Big Tech and apartheid Israel is part of a global power structure of domination, racism and coercive states. Digital technology includes surveillance systems first used by the military, as the Digital Walls report argues[158]:

> Both processes—the digitalization and the militarization—are not only partially time wise parallel developments. They are deeply intertwined: the first computers emerged from World War II and the internet was developed in the Cold War by the US military. No wonder that military technology, research and industry is gaining huge profits from the start of the digital economy.

The Pentagon's Project Maven illustrates how these processes and their interlinkages continue to grow in tandem with global, imperial wars. Since early 2000, the US military has used drones to attack targets in other countries, also causing civilian casualties.[159] Project Maven is geared to further drone attacks by analysing surveillance footage with the use of Artificial Intelligence (AI). Google was initially contracted for this project, but withdrew in the wake of objections by its own employees. The contract then went to AWS and Microsoft,[160] and has since been transferred to the US National Geospatial-Intelligence Agency (NGA).[161]

The Big Tech Sells War[162] project, which has been tracking the collusion between US tech corporations and anti-Muslim violence and Islamophobia, noted that '(t)he [Patriot] act authorizes sweeping powers for the government to surveil Americans and even indefinitely detain immigrants who aren't charged with crimes. Its passage opened the doors for Big Tech to become, first and foremost, the brokers of our personal data, selling to government agencies and private companies at home and abroad and unleashing the era of the data economy'. The US National Security Agency (NSA), whose mass surveillance programme was exposed by the former contractor and whistle-blower Edward Snowden, had access to Microsoft servers in September 2007; to Google in January 2009; to Facebook in June 2009; to YouTube in 2010; and to Apple in October 2012, mandated by amendments to Foreign Intelligence Surveillance Act, which have since been renewed.

Decades of normalising mass surveillance, the introduction of remote drone attacks by the US military, and building walls and other border-control mechanisms to prevent the entry of immigrants, have depended on constantly advancing technology to classify, surveil and attack people. This runs parallel to Big Tech becoming the multi-billion-dollar industry that it is today. A timeline of both trajectories[163]—of evolving technologies of repression and the growth of Big Tech—can be found in the Big Tech Sells War campaign. In 2013, AWS won its first cloud contract[164] in the US with the CIA, the National Security Agency (NSA) and other US intelligence agencies. In April 2022, the NSA re-awarded[165] a (separate) $10 billion contract for cloud-based computing services to AWS. Microsoft protested against AWS winning this contract, the successor of the Joint Enterprise Defense Infrastructure (JEDI) IT contract, which Microsoft had in 2019. In March 2021, Microsoft signed up to provide HoloLens augmented-reality headsets to the US military[166] in a contract worth about $21.88 billion over 10 years.

Big Tech Sells War calculates that over the last 20 years, Big Tech contracts with the Pentagon and Department of Homeland Security (DHS) have amounted to approximately $44 billion. It also exposes the (unsurprising) revolving door between the US defence establishment and Big Tech executives: at the time of writing, the Director of Security at AWS, Steve Pandelides, had worked for the Federal Bureau of Investigation (FBI) for over 20 years, including at the National Counterterrorism Center and Operational Technology Division. Jared Cohen worked at Google where he founded Jigsaw, tasked with developing counter-terrorism tools for social media platforms among other things. He was previously Policy Planning Staff for the US State Department and now works at Goldman Sachs.

In many ways, Big Tech builds on the military-industrial complex model in creating a new tech-military complex. But unlike the brazen nature of the traditional arms-production industry, where weapons are obviously designed to kill and repress, Big Tech is more insidious because it simultaneously claims to be democratic and accessible. The blurred distinction between military and civilian use helps normalise its ubiquity and dulls our response to the urgent challenges it presents.

Israel's Apartheid Technology

Seeing the situation from the Palestinians' perspective helps clear the fog, given the complicity of Big Tech in Israel's apartheid system. Since before its establishment in 1948, through the ethnic cleansing of hundreds of thousands of Palestinians, Israel has deployed its military and surveillance apparatus to further dispossess, fragment and disempower them. The Intelligence Corps of the Israeli Occupation Forces, Unit 8200, was founded in 1952. Since then it has been tasked with collecting intelligence and decrypting code. Spying and mass surveillance of Palestinians is the driving force behind much of Israel's rapid development of new technologies. Here is how Israel's Innovation Authority talks about cyberwarfare[167]:

> Cyberwarfare has always been at the forefront of the Israeli high-tech industry. [...] The winning combination of graduates from IDF [Israel Defense Forces] technology units and an innovation environment supported by the Innovation Authority enables cutting-edge Israeli technology to shape the future starting today.

Israel exports this security paradigm—of manufactured fears justifying responses by authoritarian responses by states to ensure their 'security' and 'survival', along with its weapons and technologies. In the case of Israel's apartheid regime, this need for security extends only to the Jewish population while Palestinians live in varying degrees of disenfranchisement, stripped of security by Israel's policies.

Unit 8200 can tap any phone conversation in the Occupied Palestinian Territories. There are facial-recognition cameras installed—one for every 100 Palestinians—in occupied East Jerusalem. Private information is used to blackmail Palestinians[168] into becoming informants. Hawk Eye cameras designed to read license plates allow the Israeli police forces to obtain information and the location of vehicles in real time. Israeli checkpoints have facial-recognition technology installed, initially provided by HP. The 'Blue Wolf' app, dubbed the Israeli army's secret 'Facebook for Palestinians', captures images of Palestinians all over the occupied West Bank and matches them with the database run by Israeli military and intelligence. Israeli soldiers are rewarded for capturing[169] a large number of photographs of Palestinians under occupation.

Not even Jeremy Bentham's 'panopticon' captures this situation as it aimed only to *watch in order to control,* whereas Israel and its tech apparatus aims to *watch, coerce, blackmail and violate*—all within the framework of its apartheid regime.

Just like the arms industry, Israel's digital technology sphere is deployed within an apartheid system, whereby tools and applications are 'field-tested' on Palestinians before they are exported. Jalal Abukhater, in the article cited earlier, notes:

> For Israeli companies engaged in developing the surveillance and spyware technologies, the occupied territories are just a lab where their products can be tried before being marketed and exported worldwide for profit. For the Israeli government, this surveillance regime is both a tool of control and a money-making business.

Indeed, as the Pegasus Project revealed, the Israeli NSO Group's Pegasus spyware has been used across the world to spy on journalists and activists as well as government and opposition leaders. In India, for example, the list of those targeted by Pegasus spyware includes anyone articulating a serious challenge to Modi's right-wing government. That Israeli weapons and military technologies are used as a means of repression worldwide is well known. Still shrouded, however, is the role of Big Tech in Israel's production and export of repressive technologies.

Big Tech Profits from Apartheid

While its apartheid and settler colonial regime is the 'lab' for producing repressive weapons[170] and technology, it is Big Tech which provides the necessary investment and supports the proliferation of Israel's IT and cyber-security industry, from which it richly profits.

Major tech giants, from Microsoft to Google to AWS are actively engaged in Israel's tech industry. Microsoft reportedly acquired two Israeli cyber-security companies between 2015[171] and 2017[172]. Adallom, which was founded by a veteran[173] of the Israeli Intelligence special unit, was bought in 2015 for $320 million in 2015, and Hexadite for $100 million in 2017.

In 2019, AWS, contracted along with Google to build Israel's cloud platform along with Google, worked with local data centres to set up the cloud infrastructure. As part of the Nimbus project, Google has recently set up a local cloud region in Israel. According to the contract the two companies have 'committed to making reciprocal purchases and launching industrial cooperation[174] in Israel equivalent to 20% of the value of the contract'. Facebook's second largest R&D centre is also based in Israel.

States which buy Israeli spyware and digital technology to repress their citizens are entrenching Israel's apartheid regime and need to be challenged, along with exposing the complicity and profiteering by US-based Big Tech corporations.

Praxis of Intersectionality: The No Tech for Apartheid campaign

Big Tech's expanding control and complicity in military repression have been countered by diverse challenges and grassroots resistance. From the early phase of whistle-blowers' exposés to current campaigns exposing Big Tech's profiteering from war, there is a growing demand to end the weaponisation of technology.

In the US, for example, a grassroots-based No Tech for ICE[175] campaign highlights the key role played by Palantir and AWS in providing the infrastructure for Immigration and Customs Enforcement (ICE) along with other law-enforcement agencies involved in the Trump administration's brutal family-separation policy. Palantir gathered information on individuals, which enabled state agencies to track and build profiles of immigrants to be deported, while AWS provided servers to host Palantir's tools.

Community organisers are fast recognising and responding to the digital mode of militarisation and repression, seen not only in the tech giants' exports to repressive states but also in how digital censorship and silencing are used to crush the voices of resistance and amplify right-wing, regressive ideologies. This has also been highlighted by digital rights groups such as 7amleh, the Arab Center for Social Media Development, and Sada Social, which have shown how during the 2021 Gaza assault and in the ensuing popular struggle, Palestine-related content was censored[176] by social media platforms such as Facebook and Instagram. There is a growing discourse of digital rights which brings together grassroots organisers and tech experts who are working to make the digital sphere open and democratic rather than serving as a tool for subjugation.

Joining these forces are various current (and former) tech company employees, striking against their products being used to violate the rights of marginalised people, and for military purposes. They highlighted the profound ethical implications of any involvement in the automation of warfare. In 2018, a year before it was due to expire, Google announced that it would not be renewing[177] its contract with Project Maven. As stated earlier, Microsoft and AWS won the contract.

The campaign against Project Nimbus presents a crucial opportunity to bring together the struggles against Big Tech from various perspectives—Palestinians and solidarity activists, tech workers, digital rights, and labour and anti-militarisation activists.

Months after the contract was announced, 90 Google and 300 Amazon employees wrote an open letter condemning it and opposing their employers' decision to 'supply the Israeli military and government technology that is used to harm Palestinians'. Some of the protestors faced retaliation, such as Ariel Koren, who was given an ultimatum to relocate from the US to Brazil, despite large public petitions against this action. Koren left Google in August 2022, noting in her resignation statement that, 'Google systematically silences Palestinian, Jewish, Arab and Muslim voices concerned about Google's complicity in violations of Palestinian human rights—to the point of formally retaliating against workers and creating an environment of fear'. Others joined her in speaking out against the retaliatory action taken against those who supported this campaign.

Along with the deep complicity of AWS in Israel's IT and cybersecurity industry, and its support for repression elsewhere as seen in the ICE example, its track record in the inhumane treatment of workers and union busting[178] has been widely reported. The formation of the Amazon Labor Union on Staten Island was, therefore, a historic moment in the US labour movement. Taken together these employees' actions are likely to be causing some concern among today's Big Tech CEOs.

Beyond the support to military and surveillance agencies, in essence contributing to deepening militarisation of people's daily lives, there is also the question of Big Tech's control over our data. Aspects of our lives that leave traces in the virtual world—now all but inevitable—are woven into algorithms that profoundly influence our choices, political opinions and decisions. Digital rights movements call for the defence of our privacy and security and against the commercialisation of personal data, nowhere more evident than with Google. There is a growing challenge to the control of Big Tech over individual lives and choices codified into data. The alternatives to data colonialism have also prompted lively debates on open source, public ownership and so on.

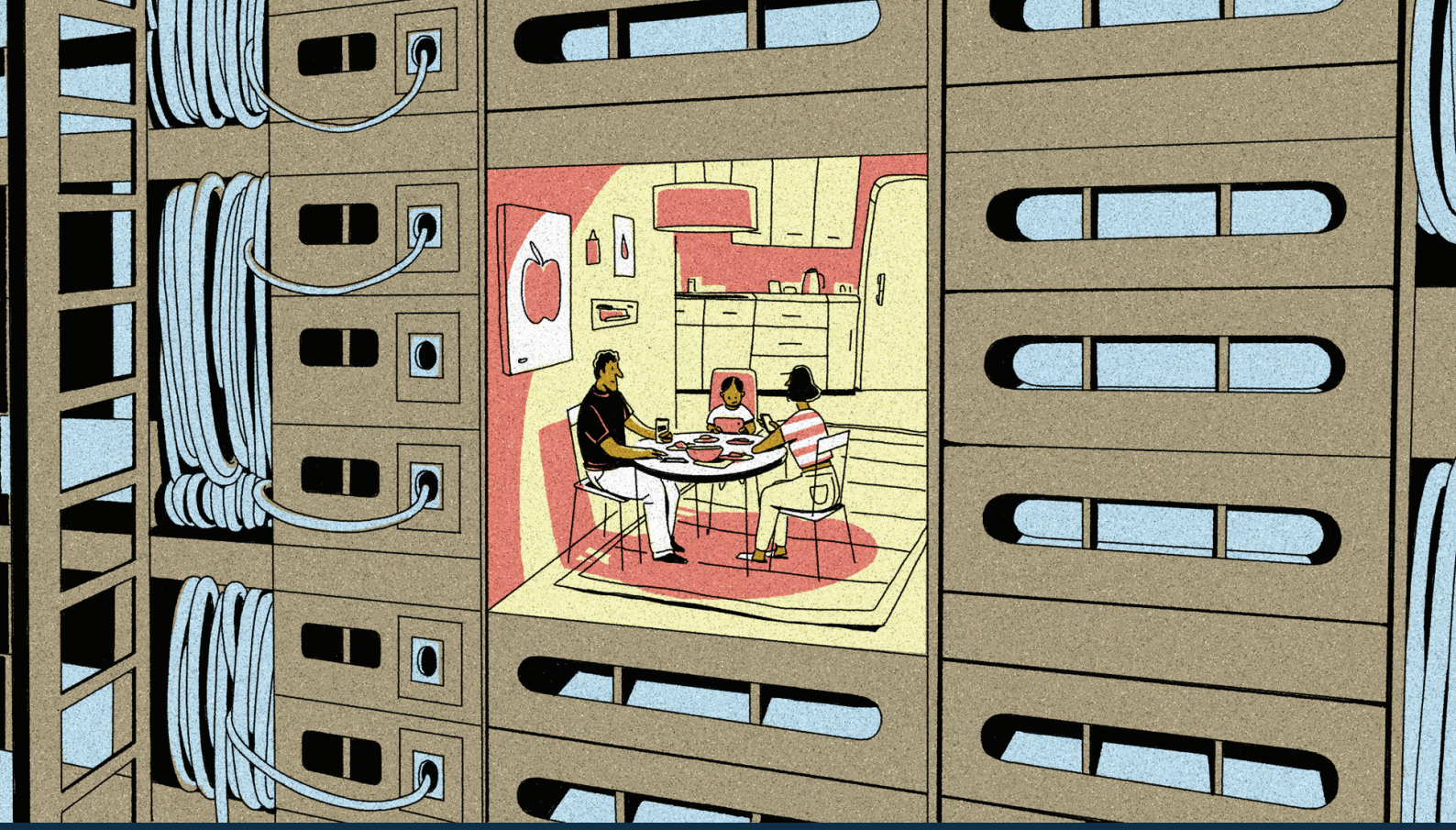
At the sharp end of digital colonialism, Palestine is therefore a sign of what is to come—and hence the point where we must first resist. In the name of bridging the digital divide, Big Tech is becoming more deeply entrenched, extracting data and profiteering from it. The COVID-19 pandemic exacerbated this as people around the world had to work and study from home, mostly without access to digital technology and equipment.

The growing interest of students and academics in questioning the control of Big Tech companies, such as Google, in the field of education, and its direct link with the oppression of Palestinians, prompted the global No Tech for Apartheid campaign to develop a toolkit for organising on university campuses.

The campaign against Project Nimbus stands at the intersection of Palestinian solidarity and anti-apartheid, labour rights, digital rights, decolonial and demilitarisation movements. In this evolving movement, it offers a clear look at the *matrix of oppression* of militarisation, neoliberal capital Israeli apartheid—all of which Big Tech bolsters and from which it draws massive profits. It builds on the understanding developed by campaigns against Big Tech in war, and brings together many struggling communities against a contract which has deep implications for everyone. Interlinked systems that oppress us demand that our forms of resistance also unite, to defy the forces that seek to isolate us. Solidarity exists only in action, and through its very existence as an intersectional force it undermines the violence inflicted by colonialism, patriarchy, racism and neoliberalism. Technology is not designed to be neutral, and as aspects of our lives move further into this sphere, and its operations and mechanisms remain far from democratic, with the force of global resistance its basic tools can yet be made democratic and accessible.

BIOGRAPHY

Apoorva PG is Asia Pacific campaigns coordinator for the Palestinian Boycott, Divestment and Sanctions (BDS) National Committee. She is among the organizers of BDS campaigns against HP Enterprises and Project Nimbus- the Google and Amazon contract to provide cloud services to the Israeli government and military. She has studied Sociology and was earlier part of access to education, copyleft and free software campaigns in India.



Digital capitalism is a mine not a cloud

Exploring the extractivism at the root of the data economy

Maximilian Jung

Berlin's largest data centre is located in a faceless, grey building, between a tax office, two used car dealers and a building materials store in the Siemensstadt neighbourhood. It meets its high energy demand from the Reuter West coal-fired power plant, which supplies electricity to one million households in Berlin and is not far from the data centre. From the outside, it looks nothing like the Big Tech portrayal of the cloud as an airy unreal digital space. Inside the building are countless stacks of servers, humming away and consuming large amounts of fossil-fuelled electricity and water in order to enable massive streams of data to circulate.

It seems unlikely that this place, operated by the Japanese telecommunications company NTT, might have any connection to the history of the neighbourhood, which was built by the industrial giant Siemens for its production and for housing its workers over 120 years ago. And yet, this building and the infrastructure it represents makes possible the world's wealthiest and most powerful companies. It is a manifestation of the exploitation of people and the extractivism that is ravaging the planet and that increasingly attempts to colonise our lives and social relations in the form of data.

Big Tech companies, such as Alphabet, Amazon, Apple, Microsoft or Meta, as well as their Chinese versions such as Alibaba, Tencent and Weibo, like to claim that data is a new 'raw' material that is there for taking. A reservoir that waits to be discovered by capable actors, who will tap into it and release data's potential for the benefit of humankind. The latest spin of Google's chief financial officer, for example, was to abandon the metaphor of data as the new oil in favour of likening it to sunlight, implying that data is a 'replenishable, inexhaustible (especially as compared to finite oil) and owner-less resource that can be harvested sustainably'[179]

This narrative naturalises and conceals the pervasive infrastructures that are built in order to generate data, and the corporate aspiration to transform potentially all human experience and social interaction into data to be extracted. This would not only violate our privacy, leaving us with no means to give any meaningful consent, but—as data is always relational—conscripts us to relations in which we participate in the oppression of one another.[180]

This narrative also hides the actors that appropriate, aggregate and sell this data for economic profit and, thus, their underlying choices about which data is worth being collected, how it is stored, tagged and analysed. It belittles the violence involved in extracting the materials used to create the digital transformation and the exploitation that makes it work, whether it be mining for metals, manufacturing parts, brutalising communities and depriving them of vital resources, dumping toxic waste in landfills or offloading the worst horrors of content moderation onto traumatised 'click workers'. And ultimately it depoliticises those decisions that brought about the digital economy and seeks to rob us of the means to envisage different futures.

Brought to the market, yet not produced for sale

Rather than regarding data as a resource we should understand it as human experience and social relations that are 'datafied' and thus transformed into a *commodity,* which then can be sold. This does not happen naturally, but requires a great deal of political intervention and violence and has grave consequences both for individuals and also for societies. We should turn to Karl Polanyi to guide our thinking through the process of commodification and its consequences. In his

classic *The Great Transformation* he describes the historical violence necessary to ensure that land, labour and money are transformed into commodities and to create the market society, an entirely separate and 'self-regulating' economic system, directed and controlled by market mechanisms. This economic logic, however, would soon come to colonise and dominate the social logic.[181]

The fundamental difference between ordinary commodities (such as oil or wheat) and land, labour and money is that labour and money are what Polanyi calls fictitious, as they are the essential basis of human life. Treating them as if they were ordinary commodities undermines the very preconditions to commodity production and is the cause of three interrelated crises—the disintegration of communities and the increasing strain on care work, the depletion of nature, and the financialisation of the economy, with its recurrent destruction of livelihoods worldwide.[182]

These developments would not have been possible without colonial processes of appropriation, possession, enslavement, and extraction. These processes are the foundation of the commodification of labour, land and money in Europe, and the creation of the market society and its subsequent expansion.[183] The violent expropriation of land in the Americas is the precursor to the privatisation of the commons. Without chattel slavery, the racialisation and the literal commodification of millions of Black people, the commodification of labour is unthinkable.[184] Enslaved work on plantations, plunder, and the emerging financial institutions intimately bound to slavery were key in providing the capital for industrialisation and the processes Polanyi describes.[185]

How did commodification work in Europe? Let's take Polanyi's description of labour. He argues that labour is essentially another name for an activity that cannot be separated from human life itself. In order to commodify it, commonly held land had to be privatised, its peasant population violently dispossessed, early and local forms of welfare provision abolished, and men, women and children compelled to migrate to work in the emerging factories in urban centres. Only when robbed of their means of subsistence and production, only when violently forced to do, would people sell their labour in an institutionalised, national market in exchange for meagre wages. Labour was finally commodified.

Technological innovation, paid with the capital that came from the colonies, needed this form of organising labour in order to function. Care work in this system—cleaning, feeding, caring for the elderly and bringing up children—becomes an activity appropriated by capital, that is about reproducing the workforce rather than about sustaining and nurturing human life.[186]

Since then, the market logic expanded both globally and into all areas of society. As Polanyi wrote: 'A market economy can only exist in a market society.[187] Although our communication with friends or family, sharing our intimate thoughts and experiences, or our bodily functions, simply what we do in our everyday lives, is not intended to produce data, under digital capitalism it has become a commodity, transformed through extraction, abstraction and aggregation. This data can be sold and played back to us in the form of targeted advertisements.

The three interrelated crises of labour, land, and money come together in the process of the commodification of data, in what we commonly understand as digitalisation. It exacerbates rather than alleviates the depletion of nature, through the extraction of manifold materials. It is built with exploited labour, while entrenching the surveillance of workers and heightening their precariousness. And it makes the financialisation of the economy possible, which in turn finances it.

The great transformation, the market society in the twenty-first century, intends to capture *human life itself* and to commodify it all the way down. This essay is about the history of this commodification, its relation to the ecological crisis, and ways out of it.

The making of data and its commodification

Digitalisation has a much longer history than is generally understood. The first computers—operated by women—were used to manage the huge volume of data that came from censuses at the turn of the twentieth century. Governments wanted to know about their citizens and the environment in order to govern them. Citizens, whose data was collected, were transformed and abstracted by bureaucrats into a 'population', with particular attributes that could be managed and administered. Likewise, militaries—now very decisive in shaping technologies essential for capturing data—wanted to predict the weather for war-purposes or for increasing the output of the industrialising agricultural sector.[188]

In order to understand the commodification of data, it is vital to understand the history of information and communications technologies (ICTs). The internet, and most other technologies—from microprocessors, to the global positioning system (GPS), and touchscreens that enable our smartphones and make them 'smart'—came about through state investment and research from military-industrial complex of the US (and to a lesser extent the UK).[189] The predecessor of the internet, the ARPANET, was envisioned to cement US hegemony and anticipate social upheaval, abroad and at home, which drew fierce opposition from the anti-war movement.

Efforts to create similar networks in the former Soviet Union[190] or in Chile[191] show that that there were alternatives to this development but that these networks were intended and used for central or democratic planning.[192] With the onset of neoliberal policies from the 1980s to the 1990s, these technologies were commercialised, along with many public provisions and infrastructures, which peaked during the Clinton administration with the privatisation and commercialisation of the internet. The mantra of self-regulation meant companies could shape early internet policies to their liking. While state surveillance continued, companies were given free rein to shape the internet in the decades to come.

This non-regulatory approach prevailed until the 2010s when policymakers in North America and especially Europe, confronted with the powerful Big Tech companies and threats to their democracies, decided to step in to curb the major excesses.

Since the 1970s the financial industry developed in tandem with the information and communications industry. Digitalisation makes financialisation possible, providing a wide array of applications in exchange for venture capital.[193] During the 1990s, for example, unprecedented volumes of venture capital were pumped into internet companies that promised business success. The dot-com crash in the early 2000s scuppered those dreams, but those based on advertising remained sturdy. Their models were based on collecting data that was supposed to make advertisements more relevant to (i.e. targeted at) users so they would spend more.

Thus, data collection was encoded in the very heart of the internet. In addition to state surveillance, private, for-profit surveillance was born, enabling the generation and digital enclosure of user

activity into data.[194] While the public is (rightly) highly critical of state surveillance, for-profit surveillance often evades such scrutiny, despite the ongoing cooperation between Big Tech and the military-industrial complex.[195] Users' increased engagement in their own surveillance is sought by every means possible, including strategies of gamification and addiction. As Blayne Haggart, digital policy scholar at the Canadian Brock University expressed it: 'We have constructed a data-driven economy and society, in which the list of what can be turned into data and commodified—heartbeats, conversations, our expressed preferences—is limited only by our imaginations'.[196]

Palimpsests of infrastructure

In popular perception technological innovations and computational advances are a story of progressing dematerialisation—a story that enables the belief in digitalisation as ecological salvation. Technologies such as 'the cloud' made its ubiquity, its disconnection from its physical environment, a key selling point. Invisibility is a central feature of large-scale infrastructural systems—they are not supposed to be seen. Unearthing these stories will help us better understand how the commodification of data is possible, the ecological cost of data, and how these entrench extractivist, colonial relations.

Looking back at the period when telegraph connections started to link empires and their colonies, particularly through submarine cables, the material nature of communication networks became visible.[197] While the unevenness of this global infrastructure still persists, the changing actors involved in financing the cables which are laid on the ocean floor also show the discontinuities of those wielding the power over global communication and its infrastructure. A hundred and twenty years ago, they were financed by empires, which imagined this would lead to a more efficient oversight and a more immediate command over their colonies and used colonial resources to build them.

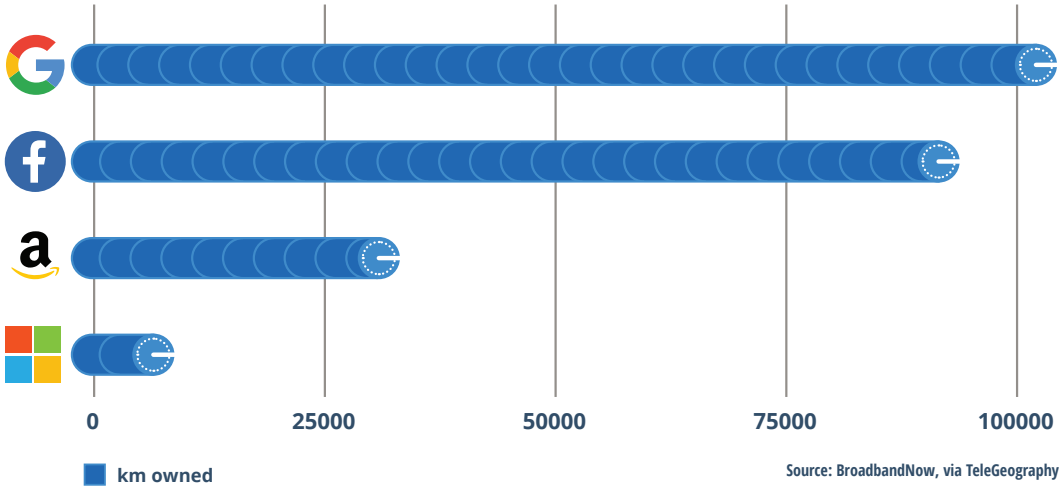
An important advantage for British cable companies to control the market throughout the nineteenth century was their ability to insulate underwater cables through their access to the rubber-like gutta percha gum—natural latex—from colonies in the Malay Peninsula. Malays shared their indigenous knowledge of their environment, and this specific tree sap and its properties, with British colonial officers, which in turn became indispensable to the very beginnings of internet history. Its extraction soon became an ecological disaster. The first transatlantic cable, laid in 1857 between western Ireland and Newfoundland, was isolated with 250 tons of gutta percha, while a single felled tree yielded on average 312 grams of this material. When the British imposed a ban on the tree felling in 1883 it had already become extinct in many regions of today's Malaysia. In the early twentieth century roughly 200,000 nautical miles (370,000 km) of cables criss-crossed the ocean floors, made up of the sap of an estimated 88 million trees.[198]

Nowadays, former colonised countries and peoples are treated first and foremost as resources that can be tapped into rather than connecting them in their own right. Many fibre-optic submarine cables still follow routes established during colonial times. Increasingly the global tech giants finance, build and control new cables. In 2010, Amazon, Google, Meta, and Microsoft owned only one long-distance submarine cable. By 2024, there will be more than 30. This number includes projects such as Google's Equiano cable connecting the entire West African coast or Meta's 2Africa

cable which circumvents the whole continent and branches off to the Gulf States, Pakistan and India, providing 3 billion people with as yet unparalleled capacity. Building their own cables gives Big Tech companies unprecedented technical and operational control—what data traffic is going where at what speed—and privileged access to the data and the attention of 1.4 billion potential internet users.[199]

Meta and Google can afford the huge capital investments needed for laying these cables even without having to sell the bandwidth since the potential revenues of a new user base are deemed a sufficient return on investment. Nanjira Sambuli, a digital rights advocate based in Nairobi, remarks: 'What's mostly interesting in techno-politics is the "rush to connect the unconnected" and to retain them on a certain platform [...] because it's all about the data. How much data can I get about people, so I can sell ads, to create predictions to keep them hooked to what I offer'.[200]

KILOMETRES OF SUBMARINE CABLES OWNED BY MAJOR CONTENT PROVIDERS



In 2010, Google, Meta, Microsoft, and Amazon owned only one long-distance submarine cable. By 2024, this number will be up to more than 30.

(Blum, A & Baraka, C. 2022)

(Data) extractivism

The colonial nature of the digital economy becomes most visible in the old and new arenas of extractivism all around the globe. Extractivism comes in many forms—the manufacture of an exponentially growing volume of electronic and digital (consumer) devices relies not only on the exploitation of rare earth elements, other metals and human labour, but also the fossil-fuelled logistics of their transport. Further, their production and discharge generate waste, pollution, and toxicity.

Mining is often the deadliest arena for human and environmental rights defenders, often from indigenous communities. Global Witness reports that 1,733 of these defenders have been killed in the past ten years, with many more assassinations going unreported, as they seek to defend their lands from exploitation.[201] Both the 'green' and the digital transition are increasing the extractive nature of the economy.

The devil's metal

Much of the public attention regarding crucial metals for the digital economy has rightly been preoccupied with lithium mining in Bolivia, child and bonded labour in 'artisanal mining' for cobalt in the Democratic Republic of Congo, or geo-political conflicts surrounding rare earths. Tin is usually associated with cans rather than computers, but half of the world's supplies are currently consumed by the electronics industry; and 30% is mined on the 'tin islands' of Bangka and Belitung of the coast of Sumatra, where unregulated mining turns rich rainforest ecosystems into toxic wastelands. Since the Dutch colonised the islands in the 1870s, the colonial administration sought to intensify and industrialise the pre-existing mining practices.[202] Today's low-tech, labour-intensive and dangerous mining has destroyed the coastal ecosystem, which provided a livelihood for local fishers, created stagnant pools of water which are breeding grounds for dengue and malaria, and proved deadly for miners.[203]

Small chips, big toxics

Even after resource extraction, high-tech manufacturing contaminates and poisons its workers and their communities. Microchip production, for example, which has been offshored from California and New York to cheaper, more leniently regulated, globalised sites on 'Silicon Island' (Taiwan) or in 'Silicon Paddy' (China), involves intensive chemical inputs in order to use extracted ores. In 2002, to assemble one microchip one required 630 times the mass of the final product as production input, and up to 300 processing steps. These require large amounts of electricity, water and chemicals. Taiwan Semiconductor Manufacturing Company (TSMC), for example, is set to consume 7.2% of Taiwan's electricity, and, amidst droughts caused by the climate crisis TSMC's facilities consume roughly 63 billion litres of water each year.[204]

In Endicott, New York, thousands of litres of carcinogenic solvents such as trichloroethylene (TCE) and perchloroethylene (PCE) ended up spilling into the ground, poisoning the groundwater and leading to increased rates of cancer and birth defects. During court proceedings, led by over a 1,000 of Endicott's residents, IBM had to disclose the contents of a 'Corporate Mortality File',

where it had tracked demographic data and the cause of death for 33,730 former employees. The data shows increased rates of respiratory, intestinal and breast cancer as far back as 1969. IBM tried to pump out the contaminated groundwater but it took 24 years and an order from the New York State Department of Environmental Conservation for the company to test the air quality and install mitigation systems in homes and public buildings. The pollution in Endicott is by no means unique.[205] The Santa Clara Valley, more commonly known as Silicon Valley, has 23 locations catalogued as 'Superfund' sites—contaminated with hazardous substances—the most of any county in US. Successful clean-up is by no means certain. Many more places face similar issues all over the world.

Cooling servers, heating water and the climate

Access to water plays a decisive role not only in the production of semiconductors, but also in the geographical allocation of huge server farms, insatiable in their hunger for power and water to ensure their operation and constant cooling. Companies often secure favourable deals with communal or state administrations to satisfy their thirst for water for decades. The effects become increasingly visible under drought-induced water stress. For example, the NSA Data Center in Utah (one of the driest US states), at the time of its construction the third biggest assembly of servers in the world, was estimated to use about 6.5 million litres of water per day, depriving local communities and habitats. The NSA initially even refused to disclose this data, citing 'matters of national security'. Contestation regarding the use of water has been unsuccessful as the city of Bluffdale had granted the NSA water at discounted rates for years to come.[206]

The 'ephemeral' cloud is often placed in rural areas such as Utah or in the hills of Guizhou, and 'cold' countries like Finland, Iceland, Ireland or Sweden. Here, imperial imagination and corporate advertisement presents such locations as remote, 'natural', which obscure their environmental impacts as well as the political intervention that facilitated their construction. As usual, the abstracted and dematerialised image of the cloud hides the opposite.

Disposable land, disposable people

Ultimately, electronic and digital devices, especially given their short lifespan, end up in the waste stream. Every year, the world discharges almost 50 million tonnes of e-waste. The overwhelming majority from the Global North ends up being exported to the 'Majority World', from North America and Europe to Nigeria or Ghana, from Japan to China, from Singapore to India. Most of the waste ends up in landfills, where heavy metals such as lead, mercury, cadmium, and other toxins leak into the ground and contaminate the groundwater and the food chain. Recycling and scavenging at these sites take place in precarious conditions and through crude and highly toxic methods, including smashing, open burning, and bathing electronics in acids, to collect small scraps of precious materials that can be sold. Exposure to toxic fumes is hazardous to the workers, often children, inhibiting development of the brain, nervous system and reproductive system. Many do not live beyond their twenties succumbing to their injuries, untreated wounds, respiratory diseases and cancer.[207]

Zygmunt Bauman says that this form of toxic colonialism is characterised by disposable land and disposable people.[208] It extends into the virtual world. Digital workers in the Philippines or India have to deal with pornographic, extremely violent or abusive content for social media giants. Reviewing videos of suicides, beheadings, massacres or sexual abuse of children causes severe trauma and other sychological harms, to the point where the workers themselves may attempt suicide. Unlike US-based moderators, workers in the Majority World do not get adequate psychological support, nor are they compensated after successful court cases in the US. Legal provisions often exempt Big Tech firms from many responsibilities for their employees, leaving the 'othered' global reserve army of labour in these countries struggling and making it clear to them that they are interchangeable and disposable.[209]

Data extraction

It is only when we look at (digital) capitalism through a colonial lens that we are able to understand these processes of extraction and dispossession and the contemporary frontier of capitalist expansion. In the drive to open up new markets, generate new growth and tap into ever more 'outsides', capitalism turned 'inwards'. Digital companies seeking to maximise profits have penetrated into ever more layers of human life itself enclosing and colonising previously non-commodified, private times and space.[210]

Returning to Polanyi, this transformation seems only logical. If, with the commodification of land, labour and money, the nascent market economy could only exist in a market society, the commodification of data also requires its own disrupting and violent social transformation towards a 'datafied society'. This transformation expresses itself in the many forms we have discussed.

Most importantly, however, social relations are no longer just embedded in an economic system, 'they *become the economic system,* [...] human life is converted into the raw material for capital via data.'[211] Human experience and social relations are reduced to a production input and transformed so that they generate ever more data, which can be extracted, abstracted, aggregated and sold.

This is what Big Tech ultimately aims for—turning everything into data which ultimately generates a profit. Even if the violence of data collection itself is not as overt and crass as it was under historical colonialism, the mass of captured and commodified data, particularly through its automated, algorithmic processing, has profound effects in entrenching the current forms of racialised, gendered, and class-based oppression. It is all justified through the ideology of 'knowing' the world through the 'objectivity' of data.[212]

The double movement—emancipatory data governance and de-commodification

No large-scale transformation or newly emerging social and economic order go uncontested. Polanyi describes a double movement: societies did not simply await the long marketisation of labour, land and money. Colonised peoples resisted colonial violence. The commodification of labour, land and money was followed by a countermovement of institutions and rules that protected society from the effects of unbridled marketisation. Many of these regulations, such

as workers' protection or welfare states, are in turn being challenged with the commodification of data and the transformation of society through data colonialism.[213] Likewise, communities at today's frontlines daily resist the corporations that seek to destroy their environments and turn them into sacrifice zones. Policymakers and digital rights activists around the world are continually fighting back against the power of Big Tech. Winning digital futures that are social, ecological, and just means confronting the commodification of data, but also the crises triggered by the commodification of labour, land, and money.

How could we find forms to govern data and its material infrastructure more democratically? One popular legal answer is the strengthen the right to privacy as, for example, in the European Union with General Data Protection Regulation (GDPR), or ban some of the data collection and targeted advertisements as under the Digital Markets and Digital Services Acts.

Simply regarding data commodification as a problem which pits individuals against corporations is not truly emancipating. Salomé Viljoen, a Michigan Law School professor, proposes reconceptualising data governance democratically so that it accounts for the insights generated at the level of populations, because, even if there were meaningful ways to withdraw individual consent from corporate or state data extraction, insights about that individual could still be inferred from aggregated data collected from people who were categorised as belonging to the same demographic group.

Acknowledging these data relations and understanding data governance in such a way opens a means to recast data as a common good or public utility. Data should be collected and used only in instances that are democratically agreed in advance and also that benefit citizens. It would allow for building counter-power and drastically reduce data extraction.[214] This would allow for data ownership via public trusts or common ownership, forms that are emerging from the bottom-up.[215] Existing data and data that is being collected by private entrepreneurs should be transferred to the public domain and institutions, similar to the expiry of intellectual property rights, before the latter are phased out entirely.[216] Such data trusts acting on behalf of data subjects could, when existing in plurality, already ensure our empowerment vis-à-vis powerful corporations under the current system.

Approaches to the treatment of data as a common good that involves citizens' contribution, access, use and ultimately empowerment are being successfully implemented in Barcelona, where city officials stress the need for transparency, accountability, and trust—and could be scaled (supra-) nationally through common property, public institutions that are subjected to scientific oversight and democratic accountability and that act independently from law enforcement or military institutions.[217] These pushes for different regulative legislation and the creation of community structures for the participation of data governance needs to be complemented by 'nowtopias', niches where a desirable future already is being implemented, such as subversive 'digital commoning' projects or through the 'contentious politics of data activism'.[218]

The issue with the digital economy does not lie exclusively in the ability of certain very powerful companies to extract data for their profit, but rather in the colonial and extractive logic on which capitalism rests. Therefore, the response from any radically transformative countermovement must be broader, more comprehensive, and challenging to the power relations inherent in the digital economy and capitalism in general, while also representing the plurality and heterogeneity of all reality.

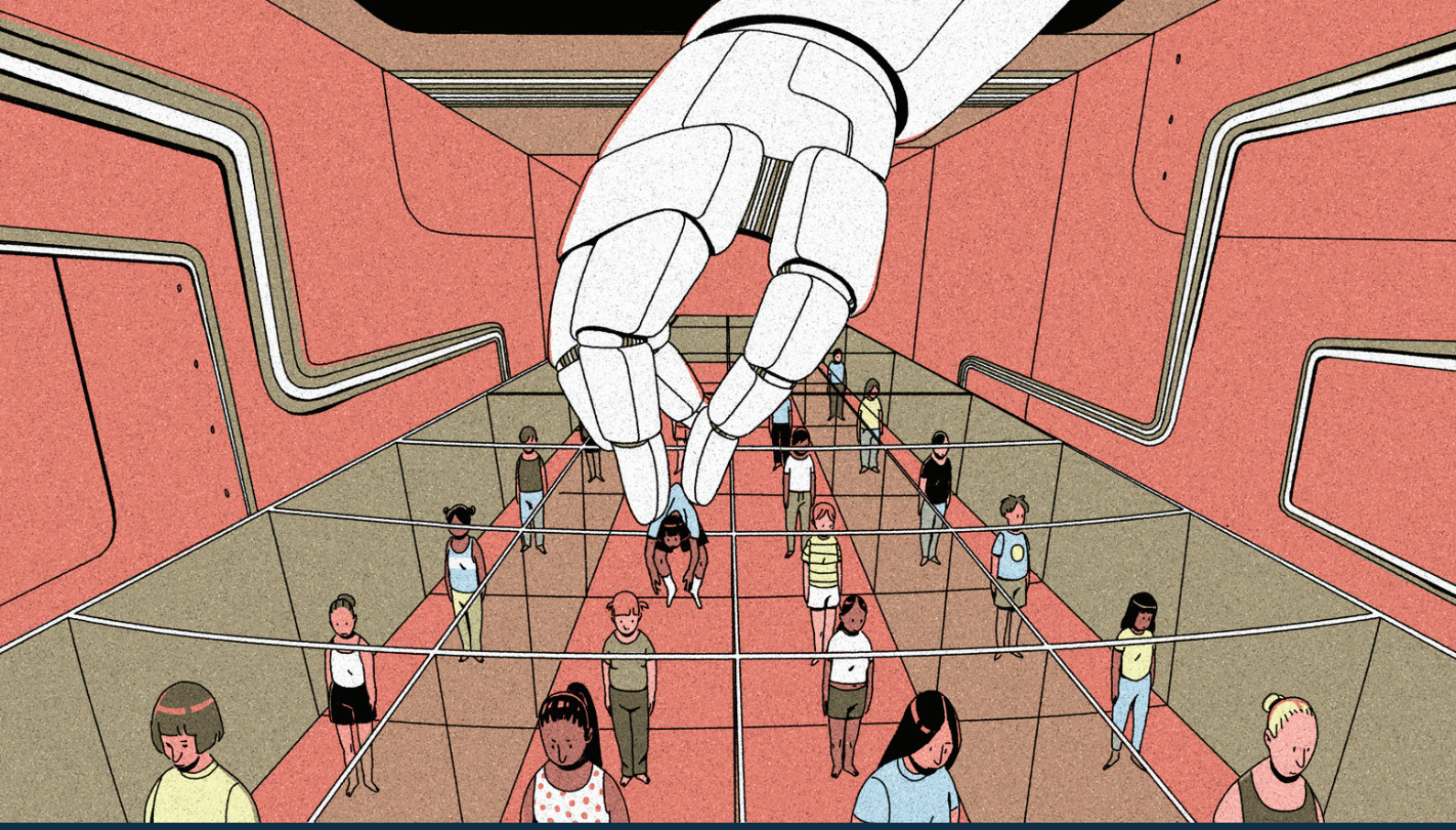
It will require struggles in many different areas. Platform workers all over the world are already expressing resistance through strikes, seeking and building solidarity and working class power, through unions, but also a continuum of strategies.[219] From these countermovements, new models of ownership in the digital economy such as cooperative platforms are emerging. Rather than just supporting this flourishing of local, small-scale cooperatives, legislators should seek to socialise existing platforms.[220] The latter also includes the (infrastructure of the) internet, which has to be geared towards serving as a and for the public good rather than having an ad-funded backbone.

While these proposals would not put an immediate end to the underlying phenomenon of the commodification of data, they would put us on a trajectory towards *de-commodification.* This de-commodification has to alongside the reduction of material throughput of the (digital) economy, a re-orientation towards sufficiency rather than efficiency. Degrowth proposals aptly identify the impossibility of decoupling resource intensity (and carbon emissions) from economic growth and the need for securing global well-being.[221] There is a need for binding targets for reducing resource extraction. Indigenous and local communities should have a real say in consultations about extractive projects affecting them.

Advocates for the de-commodification of data should seek alliances with and learn from environmental and climate justice groups who are at the forefront of often local struggles against extractivist projects, and for a post-extractivist model of development that contest the colonial logic, which the digital economy requires and which is devouring environments all around the world, in order to arrive at caring futures in which it is possible to sustain global ecosystems.

BIOGRAPHY

Maximilian Jung recently graduated from the Global Studies Program at the Universities of Leipzig and Gent. His interest lies in investigating the environmental, decolonial, and global histories of the digital economy. He is also an climate justice activist with Degrowth Belgium.



What Artificial Intelligence is hiding

Microsoft and vulnerable girls in northern Argentina

Tomás Balmaceda, Karina Pedace and Tobias Schleider

The film *The Wizard of Oz*[222] premiered in 1939. One of its star actors was Terry, the dog trained to play the role of Toto, who was then considered 'the smartest animal on the planet'. The subject of animal intelligence preoccupied many scholars of the time, while there was growing interest in understanding whether machines could think on their own. Such a possibility clearly challenged common sense, which ruled it out completely, but started to be challenged a decade after the film's debut in the work of the British mathematician Alan Turing.[223] For much of the twentieth century, the idea that animals or machines were capable of thinking was considered totally preposterous—so much has changed since then!

In early 2016, the governor of Salta in Argentina chose *The Wizard of Oz* as the book to hand out to students in his province who were learning to read. The girls discovered in L. Frank Baum's book that there is always a man behind the 'magic'. When they became adolescents, this lesson extended to other, more concrete, areas of their lives: that it is not magic, but men that lie behind poverty, promises, disappointments and pregnancies.

By then, artificial intelligence (AI) had gone from being Turing's challenge to become the preferred area of expertise of the world's most powerful and influential corporations. Thanks to attractive applications on personal devices such as mobile phones and streaming platforms, it gained broad popularity.

Until a few years ago, we used to only hear the phrase 'artificial intelligence' to refer to HAL 9000[224] from *2001: A Space Odyssey* or Data, the android from *Star Trek.* But today, few are surprised by its daily use. The consensus in the media and in certain academic literature is that we are witnessing one of the most important technological revolutions in history.

However, the awe inspired by this technology—which seems to be straight out of a fairy tale or a science fiction movie—conceals its true nature: it is as much a human creation as the mechanisms that the would-be Wizard of Oz wanted to pass off as divine and supernatural events. In the hands of the state apparatus and large corporations, 'artificial intelligence' can be an effective instrument of control, surveillance and domination, and for consolidating the status quo. This became clear when the software giant Microsoft allied itself with the government of Salta, promising that an algorithm could be the solution to the school dropout and teenage pregnancy crisis in that region of Argentina.

Algorithms that predict teenage pregnancy

A year after he distributed copies of *The Wizard of Oz* to the schools in his province, the governor of Salta, Juan Manuel Urtubey, announced an agreement with Microsoft's national subsidiary to implement an AI platform designed to prevent what he described as 'one of the most urgent problems' in the region. He was referring to the rising number of teenage pregnancies. According to official statistics, in 2017, more than 18% of all births registered in the province were to girls under 19 years of age: 4,914 children, at a rate of more than 13 per day.

While promoting his initiative, the governor declared,[225] 'We are launching a programme to prevent teenage pregnancy by using artificial intelligence with the help of a world-renowned software company. With this technology, you can predict five or six years in advance—with the first and

last name and address—which girl, future teenager has an 86% likelihood of having a teenage pregnancy'.

With almost the same fanfare as the Wizard of Oz's greetings to visitors who found their way along the yellow brick road, Microsoft heralded the announcement[226] of the deal, calling it an 'innovative initiative, unique in the country, and a major step in the province's digital transformation process'.

A third member of the alliance between the tech giant and the government was the CONIN Foundation, headed by Abel Albino,[227] a medical doctor and activist who fought against the legalisation of abortion and the use of condoms.

This alliance reveals the political, economic and cultural motives behind the programme: the goal was to consolidate the concept of 'family' in which sex and women's bodies are meant for reproduction—supposedly the ultimate and sacred purpose that must be protected at all cost. This well-known conservative view has been around for centuries in Latin America, but here it was dressed up in brightly coloured clothes thanks to the complicity of a US corporation Microsoft and the use of terms such as 'artificial intelligence' which were apparently enough to guarantee effectiveness and modernity.

The announcements also provided information on some of the methodology to be used. For example, they said that basic data 'will be submitted voluntarily by individuals' and allow the programme 'to work to prevent teenage pregnancy and school dropouts. Intelligent algorithms are capable of identifying personal characteristics that tend to lead to some of these problems and warn the government'. The Coordinator of Technology of the Ministry of Early Childhood of the Province of Salta, Pablo Abeleira, declared[228] that 'at the technological level, the level of precision of the model we are developing was close to 90%, according to a pilot test carried out in the city of Salta'.

What lay behind these claims?

The myth of objective, neutral artificial intelligence

AI has already become embedded in not only public discourse but also our daily lives. It sometimes seems as if everyone knows what we mean by 'artificial intelligence' (AI). However, this term is by no means unambiguous, not only because it is usually used as an umbrella under which very similar and related—but not synonymous—concepts appear—such as 'machine learning', 'deep learning' or cognitive computing, among others—but also because a closer analysis reveals that the very concept of intelligence in this context is controversial.

In this essay, we will use AI to refer to algorithm models or systems that can process large volumes of information and data while 'learning' and improving their ability to perform their task beyond what they were originally programmed to do. A case of AI, for instance, is an algorithm that after processing hundreds of thousands of pictures of cats can extract what it needs to recognise a cat in a new photo, without mistaking it for a toy or cushion. The more photographs it is fed, the more it will learn and the fewer mistakes it will make.

These developments in AI are sweeping the globe and are already used in everyday technology such as voice recognition of digital assistants like Siri and Alexa, as well as in more ambitious projects including driverless cars or tests for the early detection of cancer and other diseases. There is a very wide range of uses for these innovations, which affects many industries and sectors of society. In the economy, for example, algorithms promise to identify the best investments on the stock market. In the political arena, there have been social media campaigns for or against an electoral candidate that have been designed to appeal to different individuals based on their preferences and internet use. In relation to culture, streaming platforms use algorithms to offer personalised recommendations on series, movies or music.

The success of these uses of the technology and the promises of benefits that, until a few years ago, existed only in science fiction, has inflated the perception of what AI is really capable of doing. Today, it is widely regarded as the epitome of rational activity, free of bias, passions and human error.

This is, however, just a myth. There is no such thing as 'objective AI' or AI that is untainted by human values. Our human—perhaps all too human—condition will inevitably have an impact on technology.

One way to make this clear is to remove some of the veils that conceal a term such as 'algorithm'. The philosophy of technology allows us to distinguish at least two ways of defining it in conceptual terms. In a narrow sense, an algorithm is a *mathematical construct* that is selected because of its previous effectiveness in solving problems similar to those to be solved now (such as deep neural networks[229], Bayesian networks[230] or 'Markov chains[231]). In the *broad* sense, an algorithm is a *whole technological system* comprising several inputs, such as training data, which produces a statistical model designed, assembled and implemented to resolve a pre-defined practical issue.

It all begins with a simplistic understanding of data. Data emerge from a process of selection and abstraction and consequently can never offer an objective description of the world. Data are inevitably partial and biased since they are the result of human decisions and choices, such as including certain attributes and excluding others. The same happens with the notion of data-based forecasting. A key issue for government use of data-based science in general and machine learning in particular is to decide what to measure and how to measure it based on a definition of the problem to be addressed, which leads to choosing the algorithm, in the narrow sense, that is deemed most efficient for the task, no matter how deadly the consequences.[232] Human input is thus crucial in determining which problem to solve.

It is thus clear that there is an inextricable link between AI and a series of human decisions. While machine learning offers the advantage of processing a large volume of data rapidly and the ability to identify patterns in the data, there are many situations where human supervision is not only possible, but necessary.

Pulling back the curtain on AI

When Dorothy, the Tin Man, the Lion and the Scarecrow finally met the Wizard of Oz, they were fascinated by the deep, supernatural voice of this being who, in the 1939 film version, was played by Frank Morgan and appeared on an altar behind a mysterious fire and smoke. However, Toto, Dorothy's dog, was not as impressed and pulled back the curtain, exposing the sham: there was someone manipulating a set of levers and buttons and running everything on stage. Frightened and embarrassed, the would-be wizard tried to keep up the charade: 'Pay no attention to the man behind the curtain!' But, when cornered by the other characters, he was forced to admit that it was all a hoax. 'I am just a common man', he confessed to Dorothy and her friends. The Scarecrow, however, corrected him immediately: 'You're more than that. You're a humbug'.

When we take away the fancy clothes and gowns, we see AI for what it really is: a product of human action that bears the marks of its creators. Sometimes, its processes are seen as being similar to human thought, but are treated as devoid of errors or bias. In the face of widespread, persuasive rhetoric about its value-neutrality and the objectivity that goes along with it, we must analyse the inevitable influence of human interests at various stages of this supposedly 'magic' technology.

Microsoft and the government of Salta's promise to predict 'five or six years in advance, with names, last names and addresses, which girl or future adolescent has an 86% likelihood of having a teenage pregnancy' ended up being just an empty promise.

The fiasco began with the data: they used a database collected by the provincial government and civil society organisations (CSOs) in low-income neighbourhoods in the provincial capital in 2016 and 2017. The survey reached just under 300,000 people, of whom 12,692 were girls and adolescents between 10 and 19 years of age. In the case of minors, information was gathered after obtaining the consent of 'the head of family' (sic).

These data were fed into a machine-learning model that, according to its implementers, is able to predict with increasing accuracy which girls and adolescents will become pregnant in the future. This is absolute nonsense: Microsoft was selling a system that promised something that is technically impossible to achieve.[233] It was fed a list of adolescents who had been assigned a likelihood of pregnancy. Far from enacting any policies, the algorithms provided information to the Ministry of Early Childhood so it could deal with the identified cases.

The government of Salta did not specify what its approach would entail, nor the protocols used, the follow-up activities planned, the impact of the applied measures—if indeed the impact had been measured in some way—the selection criteria for the non-government organisations (NGOs) or foundations involved, nor the role of the Catholic Church.

The project also had major technical flaws: an investigation by the World Web Foundation[234] reported that there was no information available on the databases used, the assumptions underpinning the design of the models, or on the final models were designed, revealing the opacity of the process. Furthermore, it affirmed that the initiative failed to assess the potential inequalities and did not pay special attention to minority or vulnerable groups that could be affected. It also did not consider the difficulties of working with such a wide age group in the survey and the risk of discrimination or even criminalisation.

The experts agreed that the assessment's data had been slightly contaminated, since the data used to evaluate the system were the same ones used to train it. In addition, the data were not fit for the stated purpose. They were taken from a survey of adolescents residing in the province of Salta that requested personal information (age, ethnicity, country of origin, etc.) and data on their environment (if they had hot water at home, how many people they lived with, etc.) and if they had already been or were currently pregnant. Yet, the question that they were trying to answer based on this *current* information was whether a teenage girl might get pregnant *in the future*—something that seemed more like a premonition than a prediction. Moreover, the information was biased, because data on teenage pregnancy tend to be incomplete or concealed given the inherently sensitive nature of this kind of issue.

Researchers from the Applied Artificial Intelligence Laboratory of the Computer Sciences Institute at the University of Buenos Aires found that in addition to the use of unreliable data, there were serious methodological errors in Microsoft's initiative. Moreover, they also warned of the risk of policymakers adopting the wrong measures: 'Artificial intelligence techniques are powerful and require those who use them to act responsibly. They are just one more tool, which should be complemented by others, and in no way replace the knowledge or intelligence of an expert', especially in an area as sensitive as public health and vulnerable sectors.[235]

And this raises the most serious issue at the centre of the conflict: even if it were possible *to predict* teenage pregnancy (which seems unlikely), it is not clear *what purpose* this would serve. *Prevention* is lacking throughout the entire process. What it did do, however, is create an inevitably high risk of stigmatising girls and adolescents.

AI as an instrument of power over vulnerable populations

From the outset, the alliance between Microsoft, the government of Salta and the CONIN Foundation was founded on preconceived assumptions that are not only questionable, but also in conflict with principles and standards enshrined in the Argentinean Constitution and the international conventions incorporated into the national system. It is unquestionably based on the idea that (child or teenage) pregnancy is a disaster, and in some cases the only way to prevent it is through direct interventions. This premise is linked to a very vague stance on the attribution of responsibility.

On the one hand, those who planned and developed the system appear to see pregnancy as something for which no one is responsible. Yet, on the other hand, they place the responsibility exclusively on the pregnant girls and adolescents. Either way, this ambiguity contributes, first of all, to the objectification of the people involved and also renders invisible those who are in fact responsible: primarily the men (or teenagers or boys, but mainly men) who obviously contributed to the pregnancy (people often say, with a crude, euphemistic twist, that the girl or teenager 'got herself pregnant'). Second, it ignores the fact that in most cases of pregnancy among young women and in *all* cases of pregnancy among girls, not only is it wrong to presume that the girl or teenager consented to sexual intercourse, but this assumption should be completely ruled out. In sum, this ambiguous stance obscures the crucial fact that all pregnancies of girls and many pregnancies of young women are the result of rape.

With regard to the most neglected aspect of the system—that is, predicting the school dropout rate—it is assumed (and concluded) that a pregnancy will inevitably lead a pupil to drop out of school. While the opportunity cost that early pregnancy and motherhood imposes on women should never be ignored, the interruption or abandonment of formal education is not inevitable. There are examples of inclusive programmes and policies that have been effective in helping to avoid or reduce dropout rates.

From a broader perspective, the system and its uses affect rights that fall within a spectrum of sexual and reproductive rights, which are considered human rights. Sexuality is a central part of human development, irrespective of whether individuals choose to have children. In the case of minors, it is important to take account of differences in their evolving capacities, while bearing in mind that the guidance of their parents or guardians should always give priority to their capacity to exercise rights on their own behalf and for their own benefit. Sexual rights in particular entail specific considerations. For example, it is essential to respect the particular circumstances of each girl, boy or adolescent, their level of understanding and maturity, physical and mental health, relationship with various family members and ultimately the immediate situation they are facing.

The use of AI has concrete impacts on the rights of (potentially) pregnant girls and teenagers. First, the girls and teenagers the right to personal autonomy was violated. We have already mentioned their objectification and the project's indifference towards their individual interests in pursuit of a supposed general interest. The girls and teenagers were not even considered as rights holders and their individual desires or preferences were completely ignored.

In this Microsoft project, AI was used as an instrument to yield power over girls and teenage women, who were catalogued without their consent (or their knowledge, apparently). According to those who promoted the system, the interviews were held with the 'heads of the family' (especially their fathers) without even inviting them to participate. Moreover, the questionnaires included highly personal matters (their intimacy, sex lives, etc.) on which their parents would seldom be able to respond in detail without invading their daughter's privacy or—just as serious—relying on assumptions or biases that the state would then assume to be true and legitimate.

Other violations include the rights to intimacy, privacy and freedom of expression or opinion, while the rights to health and education are at risk of being ignored, despite the declarations of the authorities and Microsoft about their intention to take care of the girls and adolescent women. Finally, it is worth mentioning a related right that is of particular importance in the specific context of this project: the right to freedom of thought, conscience and religion.

We would not go so far as to claim that this episode had a happy ending, like the Wizard of Oz did. But the Microsoft project did not last long. Its interruption was not because of criticisms from activists, however, but for a much more mundane reason: in 2019, national and state elections were held in Argentina and Urtubey was not re-elected. The new administration terminated several programmes, including the use of algorithms to predict pregnancy, and reduced the Ministry of Early Childhood, Childhood and Family to the status of a secretariat.

What AI is hiding

The rhetorical smoke and mirrors of value-neutral and objective AI developments fall apart when challenged by voices that assert that this is impossible in principle, as we argued in the first section, given the participation of human analysts in several stages of the algorithms' development. Men and women defined the problem to be resolved, designed and prepared the data, determined which machine-learning algorithms were the most appropriate, critically interpreted the results of the analysis and planned the proper action to take based on the insights that the analysis revealed.

There is insufficient reflection and open discussion about the undesirable effects of the advance of this technology. What seems to prevail in society is the idea that the use of algorithms in different areas not only guarantees efficiency and speed, but also the non-interference of human prejudices that can 'taint' the pristine action of the codes underpinning the algorithms. As a result, people take for granted that AI has been created to improve society as a whole or, at least certain processes and products. But hardly anyone questions the basics—for whom will this be an improvement, who will benefit and who will assess the improvements? Citizens? The state? Corporations? Adolescent girls from Salta? The adult men who abused them? Instead, there is a lack of real awareness about the scale of its social impact or the need to discuss whether such a change is inevitable.

People are no longer surprised by the constant news on the introduction of AI into new fields, except for what is new about it, and just like the passage of time, it is treated as something that cannot be stopped or revisited. The growing automation of the processes that humans used to carry out may generate alarm and concern, but it does not spark interest in halting it or reflecting on what the future of work and society will be like once AI takes over much of our work. This raises a number of questions that are rarely asked: Is this really desirable? For which social sectors? Who will benefit from greater automation and who will lose out? What can we expect from a future where most traditional jobs will be performed by machines? There seems to be neither the time nor the space for discussing this matter: automation simply happens and all we can do is to complain about the world we have lost or be amazed by what it can achieve today.

This complacency with the constant advances of technology in our private, public, work and civic lives is thanks to trust in the belief that these developments are 'superior' to what can be achieved through mere human effort. Accordingly, since AI is much more powerful, it is 'smart' (the 'smart' label is used for mobile phones, vacuum cleaners and coffeemakers, among other objects that would make Turing blush) and free of biases and intentions. However, as pointed out earlier, the very idea of value-neutral AI is a fiction.To put it simply and clearly: there are biases in all stages of algorithm design, testing and application and it is therefore very difficult to identify them and even harder to correct them. Nonetheless, it is essential to do so in order to unmask its supposedly sterile nature devoid of human values and errors.

An approach focused on the dangers of AI, along with an optimistic stance about its potential, could lead to an excessive dependence on AI as a solution to our ethical concerns—an approach where AI is asked to answer the problems that AI had produced. If problems are considered as purely technological, they should only require technological solutions. Instead we have human decisions dressed up in technological dress. We need a different approach.

The case of the algorithms that were supposed to predict teenage pregnancies in Salta exposes how unrealistic the image of the so-called objectivity and neutrality of artificial intelligence is. Like Toto, we cannot ignore the man behind the curtain: the development of algorithms is not neutral, but rather based on one decision made from many possible choices. Since the design and functionality of an algorithm reflects the values of its designers and its intended uses, algorithms inevitably lead to biased decisions. Human decisions are involved in defining the problem, data preparation and design, the selection of the type of algorithm, the interpretation of the results and the planning of actions based on their analysis. Without qualified and active human supervision, no AI algorithm project is able to achieve its objectives and be successful. Data science works best when human experience and the potential of algorithms work in tandem.

Artificial intelligence algorithms are not magic, but they do not need to be a hoax, as the Scarecrow argued. We just have to recognise that they are human.

Translated by Karen Lang

BIOGRAPHIES

Karina Pedace teaches graduate and post-graduate students at the University of Buenos Aires and National University of Matanza, and is a researcher at the Institute of Philosophical Research of Argentinean Society (IIF-SADAF- CONICET). Her current research areas include the philosophy of technology, metaphysics of the mind and research methodologies. She is executive secretary of the UNESCO Latin American Network of Women Philosophers and co-founder of the Artificial Intelligence, Philosophy and Technology Research Group (GIFT). In 2022, she was recognised internationally as one of 100 Brilliant Women in AI Ethics https://womeninaiethics.org/the-list/of-2022/

Tomás Balmaceda has a PhD in Philosophy from the University of Buenos Aires. Currently he is Researcher in IIF (SADAF/CONICET) and part of the GIFT group which analyses technology and artificial intelligence through the lens of philosophy. Author of various books, his interests include the ethics of network influence, new longevity and financial education for the LGBTIQ+ population.

Tobías J. Schleider is a lawyer and specialist in criminal law for the National University of Mar de Plata and Doctor of the University of Buenos Aires in Philosophy of Law. He is a Professor at the National University of the South, where he directs the degree in Public Security. His current lines of research include technology-supported violence prevention, human action theory, causality and the influence of luck in the attribution of responsibility.

Abolitionist creativity

How intellectual property can hack digital power

Julia Choucair Vizoso and Chris R. Byrnes

The most influential real estate company in history does not own much real estate. It has made housing less affordable,[236] created housing crises in popular tourist destinations, hollowed out communities,[237] and reached a valuation of $113 billion[238]—all without owning the physical property.

Yet Airbnb has a great deal of property. What the company lacks in physical property it makes up for in intellectual property (IP), the legal and economic codes that govern creativity, information, brand, and reputation in the global economy. If you are one of Airbnb's half a billion users, when you browse listings, make a booking, pay, or contact customer support, you are interfacing with diverse types of IP, such as copyright-protected software code, trade secret-protected algorithms, and hundreds of the company's patents. As Airbnb expands into new markets, it explains to its investors that the company's long-term growth will come from the web of IP that surrounds the rental and housing market.[239]

Airbnb's intangible empire is far from unique. Physical property, commodities, resources, products—things you can touch—are increasingly marginal in market value. The shift has been seismic: 50 years ago, 80% of the value of the world's largest companies was in hard assets; now 90% is in intangibles.[240] And the shock waves keep coming. The value of intangibles has increased tenfold in the last seven years,[241] to $65 trillion, or more than 75% of the global economy.[242] No global supply chain, no trade agreement exists without intellectual property running through it. Digital power would not be possible without it.

We cannot understand digital capitalism today, and its many inequities, without understanding how it has transformed every act of the human imagination, every data point, past and present, into a potential commodity. A new generation of 'disruptive' tech firms have found ways to use IP as an important part of their arsenal to control and exploit the labour and data of digital workers and consumers alike in the so-called sharing economy.

Yet perhaps no other asset class is as ripe for revolution. For all its power in the economy, IP is also uniquely vulnerable. We can occupy the vulnerabilities of the current system, untether creativity and data from exclusion and personal possession, and forge it instead as a radically imaginative, generative, and socially productive community-building practice.

Abolitionist creativity

> *'Abolition is about presence, not absence. It's about building life-affirming institutions.'*
> – Abolitionist geographer Ruth Wilson Gilmore

Today, trillions of imaginary dollars are exchanged for rights to imaginary property, yet we lack the imagination necessary to transform the economy into something that could help life flourish. Now, more than ever, creativity is the way out of the deadlocks we face. But for it to thrive we must first abolish the economic and legal codes that shackle it.

Creativity enters the economy as intellectual property, the legal regime arising from seventeenth-century Europe, which formalised creative expression and invention into individual exclusive rights. As a catch-all term for copyright, patents, trademarks, and trade secrets, intellectual property is everywhere. The technology of the smartphone you may be using to read this could have as

many as 250,000 related patents.[243] The report of which this essay is chapter carries a copyright notice—in the form of a Creative Commons license—on the first page. Even the scribble you may have doodled on a napkin is automatically copyright-protected, whether or not you want it to be (and irrespective of its aesthetic prowess).

Copyright law does not care whether what we have created is any good from an artistic perspective. For work to be protected by copyright, it must be 'original' and 'creative', but the threshold is very low: slightly more creative and original than organising a telephone directory in alphabetical order.

Founded on concepts of labour and individualism developed by Enlightenment philosophers, IP was imposed throughout the globe through European colonial and settler-colonial projects and trade agreements. To this day, the IP system remains rigidly Euro-centric with no agreed means to recognise and respect non-European epistemologies or conceptions of the individual.

The regime is fortified by powerful and legally vindictive institutions whose jurisdiction extends to all members of the World Trade Organization (WTO). Under the banner of policing 'IP infringement', IP laws can block any good at the border and preclude even the most essential innovations from being made available to the public. And its power seems to only expand. Under pressure from a wide array of corporate lobbyists, exclusive rights that at one time elapsed have become perpetual and expansive, eroding the public domain.

Naturally, such a system inspires resistance. Critical voices resist the colonial capitalist worldview of property rights that undergirds the system. Pirates and free-culture advocates insist that 'information wants to be free', establishing alternative platforms for sharing culture. Even liberal defenders of IP regimes grudgingly admit that while the initial set-up was wise—it would promote 'the ideal of progress, a transparent marketplace, easy and cheap access to information, decentralized and iconoclastic cultural production, self-correcting innovation policy'– the system has been corrupted by corporate influence, undermining a culture of sharing and remixing.[244]

What is to be done? Eliminate IP altogether? Reform it through public policy? Develop legal technologies that allow creators to opt out? Champion online piracy and infringement campaigns? Though these debates are important (some more than others), they dangerously curb our imagination. By limiting our gaze to the inner world of what constitutes IP—whether and how creative works should be protected, what should be considered intellectual property—we are failing to do the radical work: to locate IP in the broader political economy, to question what role it plays in the larger structures of exploitation and oppression.

When we move away from the culture wars that have dominated debates on intellectual property itself, we are forced to contend more seriously with the materiality of creativity—with how it runs through every global supply chain and every international trade agreement one can think of, with how it makes digital power possible and pervasive. Capitalism recognises this power and moves to tighten its grip. Headline-grabbing capitalist cowboys like Jeff Bezos, Nathan Myhrvold,[245] and Martin Shkreli,[246] are innovating around the incongruities of this powerful asset class. Anti-capitalists have been asleep at the wheel.

The inattention is not surprising. The mention of intellectual property can cause even the brightest eyes to glaze over. It is one of many issues deliberately made to seem abstruse, overly technical,

legalistic, and irrelevant for the crises we face. One should not need a law degree to understand the terms upon which their creativity enters the economy. Freeing IP from its legalistic scaffolding, and waking up to its power, reveals that it is a uniquely vulnerable regime.

Here is the vital loophole: crucially, ownership and control of IP always belongs, in the first instance, to the artists, inventors, academics and creators who made it. Currently, this power lies dormant. Most IP producers uncompromisingly surrender their IP to corporations (both for profit and not-for-profit) through employment contracts, click-wrap terms and conditions, and IP licences that allow these institutions free rein to commercialise the IP in exploitative and oppressive supply chains. Others simply give their power away by using Creative Commons or Open-Source licences, but again do nothing to stop corporations from then aggressively and oppressively commercialising IP.

Could we imagine a different way? What if creators seized their IP rights, occupied them, and turned their logic on its head? What if we took the essence of IP—the economic and legal right to exclude others from an intangible—and opted to exclude only oppression and exploitation? Can we leverage our legal rights as creators to throw a spanner in the works of capitalism? What if creators did not simply protest the regimes that incarcerate the imagination but created, here and now, the grassroots systems, structures, and institutions to replace them?

Towards these ends, we are not primarily concerned with the abstract question of whether intellectual property should exist. Abolitionist creativity for us is not about eliminating the rights of creators or the protections afforded to creations; it is about ensuring that creativity enters the economy as a tool against oppression. In the words of the abolitionist geographer Ruth Wilson Gilmore, 'Abolition is about presence, not absence'.[247] We ask creators to show up and be present in the rights we have been afforded, to occupy them, and to put them together in service of the worlds we want to create. To use our creativity to build life-affirming institutions.

Inspired by the questions offered by abolitionists Mariame Kaba and Dean Spade in their thinking on 'non-reformist reforms' (the term originally coined by French economist-philosopher André Gorz in the 1960s),[248] we ask creators to ask themselves: What is the purpose of creativity, of information, of knowledge? Does it provide material relief to the oppressed and exploited inside the supply chains within which the creativity is commercialised? Does it build power, mobilising ongoing struggle among those affected by the creative works? Does it leave out marginalised groups? Does it legitimise the system?

The abolitionist gaze sees creativity, as rendered in our economy, as a thread that weaves through interlocking systems of oppression. It invites us to pull that thread.

The global IP regime is vulnerable for another reason, too. Precisely because it is awkwardly modelled on Early Modern laws related to physical property, IP is full of contradictions and absurdities, which offer intriguing opportunities for transgressive experimentation, radical imagination, and subversive play. Here are a few.

Plots from the abolitionist future

Plot #1: Protest as copyrighted performance

Protest is increasingly criminalised across democracies. During peaceful rallies against climate inaction, racial injustice, police brutality, or war, security services arrest and violently repress protesters, journalists, and human rights monitors. Police commanders send out orders to 'take back the streets', transforming individuals exercising a fundamental democratic right—the right to protest—into criminals.[249] More countries are introducing laws to hold protesters criminally and civilly responsible for property damage that occurs during protests.

Digitalisation has become a crucial component of states' enhanced surveillance and coercive capacity, and they deploy it with little regulation or transparency. Journalists, civil rights advocates, and protesters have documented government use of surveillance, social media monitoring, and other digital tools—warning that it could take years after a protest to learn all of the ways that security forces surveilled organisers. Governments are also coordinating with tech-savvy private security forces who got their start as contractors in the 'war on terror'. The 'overlapping interests of government and industry that use surveillance, policing, and imprisonment as solutions to economic, social, and political problems' is what abolitionists refer to as the prison-industrial complex.[250]

During the Dakota Access Pipeline protests at Standing Rock, for example, leaked documents exposed that state and federal military forces were working alongside a private military contractor, TigerSwan, hired by owners of the pipeline, Energy Transfer Partners.[251] Working with police in at least five states to attack the Indigenous-led movement Water Protector, TigerSwan was using military-style counterterrorism measures and digital surveillance to monitor protesters' movements, including a live video feed from a private Dakota Access security helicopter.

Here is where intellectual property comes in. What if we legally protect the creativity inherent in protest as copyrightable performance art? Protests routinely incorporate performative innovations into their repertoire, from Standing Rock[252] to Mexico[253] to Iraq[254] to the United Kingdom.[255] We know that for communities in resistance, 'the rituals, dances, protocols and songs that characterise these struggles are not merely the cultural ephemera of activism; they are an intimate and constitutive part of Indigenous world-making, a means to coordinate and align the collective imagination so as to facilitate and enrich the cooperation of those involved'.[256] Scholars have long recognised the performativity of protest, studying the use of visualisation and space or arguing that 'choreography, movement and gesture are not peripheral but central to the politics of protest'. What if protestors acknowledge that these key features of protest also have legal rights that can help them challenge the prison-industrial complex?

Imagine if protestors wore the © 'all rights reserved' on their bodies or adorned themselves in barcodes that linked to their copyright terms and conditions, specifying that images and audio could not be used for commercial use, including privately contracted surveillance. Imagine if protesters then demanded in court to know how private security forces were using any recording of their art, visual or audio? Imagine if legal discovery (the pre-trial procedure in which each party can obtain evidence from the other party through requests for documents) then revealed the secret

commercial interests between police departments and private security companies, or between a private mercenary firm and its employer, an oil company. Imagine if these companies then had to compensate protesters for copyright violation, or if courts threw out evidence because companies had obtained it unlawfully with copyright infringement. Copyright law is not going to get protestors out of jail for criminal charges, but it can help to ensure that the prison-industrial complex cannot profit from policing.

How would the creators of a copyright-protected performance by Extinction Rebellion, Black Lives Matter, BP or not BP, #NoDAPL, and countless other fearless activists want to condition the use of their performance? What kinds of legally enforceable exclusions would further the goals of their direct action or community response? Should protestors allow police departments (and the private security companies they increasingly work with) to use video and sound recordings of a scripted performance (i.e. a protest) or of visual art such as graffiti—and any other copyrightable material—without any conditions? What should anyone who seizes or destroys an encampment-as-art installation have to pay in reparations?

We inhabit systems that afford more legal protection to performing outrage at injustice than to claiming justice as a right; systems that value the sanctity of property more than the sanctity of Black and Indigenous lives, more than protecting biodiversity. There is no reliably enforceable international human rights regime, but there is a powerful international legal regime associated with intellectual property. We can radically repurpose this power. We can jailbreak the codes and the legal technology of IP from its intended use.

The possibilities are intriguing. Might we be better able to occupy physical property by occupying intellectual property, refashioning the absurd powers given to intangible property into furthering our ability to hold physical space? Can copyright protection complicate how digital power increasingly oppresses protest or acts of preservation, whether they be about environmental issues or dignified living?

Anyone can participate. Every protestor is a performance artist. For those who already identify as socially engaged artists or artivists, here is an opportunity to rethink the political agency of your art. Can a work of art have direct political agency, not through debates over the righteousness of its political aesthetic or content, but through artists occupying the legal and economic scaffolding that surround it?

Plot#2: Occupy employment contracts with IP morals clauses

Employment contracts are where we, as IP producers, most often hand over our rights. We cede to corporations what legally belongs to us through the IP assignment clause: a contract term that gives our employers full ownership and control to use and commercialise our IP. Given the enormous value of IP to a corporation's bottom line, it is no surprise that corporations have tried to make their claims to employee creativity as broad as possible.

Laws governing employee IP assignment clauses vary by jurisdiction, but common terms require employees to relinquish all moral rights: legal rights that empower creators to object to uses of their work that harm their honour or reputation. Other common terms grant employers ownership of any idea recorded on any piece of corporate property, including an employee's idea for a personal project if they happened to record it on a work laptop.

What would happen if we occupied our IP assignment clauses? What if we organised collectively as IP producers and put conditions on our employers' rights to our IP? One existing legal technology we can use is the morals clause: a contractual term that gives one the right to terminate a contract, or take other remedial action, if the breaching party engages in immoral behaviour. What might co-created abolitionist IP morals clauses stipulate?

What if our employers were no longer able to use our IP in supply chains with forced labour and ecological devastation, or in service to militaries, surveillance, and policing?

IP has tremendous power to disrupt an entire supply chain. An IP dispute has the power to stop goods at the border.[257] If IP producers in one part of the supply chain were to use morals clauses, they could trigger an IP dispute whenever these morals are infringed anywhere across a supply chain in which the IP is used.

Here is an example from Big Tech, whose supply chains have insatiable appetites for cobalt. Cobalt mining is notorious for its human rights abuses, corruption, environmental destruction, and child labour.[258] An IP morals clause used by IP producers across these supply chains—say by the Tech Workers Coalition—could be used to implement proposals made by human rights activists, that 'any company sourcing cobalt from DRC must establish an independent, third-party system of verification that all mineral supply chains are cleansed of exploitation, cruelty, slavery, and child labour. They must invest whatever is needed to ensure decent pay, safe and dignified working conditions, healthcare, education and general wellbeing of the people whose cheap labour they rely on'.[259] If such conditions were embedded into an IP morals clause—capable of crippling cobalt-dependent supply chains by triggering an IP dispute when violated—the entire market power of IP could be used as a carrot and a stick to implement such proposals.

Academics, journalists, artists, and musicians can wield powerful IP morals clauses, too. Publishers depend on paper, ink, and glue, or computers, software, Google, and Amazon to disseminate their copyright-protected works. However, the 'pulp and paper' industry continues to profit from deforestation in the Amazon rainforest,[260] ink manufacturers violate labour rights and dump hazardous waste,[261] and book bindings are not recyclable.[262] Digital publishing, meanwhile, fuels supply chains that routinely dump electronics waste across the Global South.[263] Copyright producers can use IP morals clauses to condition the publication and commercialisation of their works on a publisher's commitment to use state-of-the-art, labour-and-environmental-friendly supply chains. Such conditions can exist alongside open-access licensing terms that enable anyone to freely access copyrighted content, while still prohibiting publishers from delivering open-access content through unethical supply chains.

Through IP morals clauses, can we put *ideas* about abolition, sustainability, or human rights into *practice* across the supply chains in which these ideas are commercialised. We can also harness the power of IP to deepen worker solidarity across supply chains. In the process, we can experiment with IP not as an exclusive *individual* right but as a collective tool. Can we imagine IP unions organised around collective IP morals?

Why open access is not abolitionist

Abolitionist creativity can be at odds with the IP world's most successful countercultural movements, such as the free software movement, the open-source movement, and the Creative Commons movement. Although heterogeneous, and engaged in spirited debates among each other, these movements share a common concern: how does society resolve the mismatch between what digital technology theoretically enables—the opportunity to access, share, and collaborate on creativity at an unprecedented scale and with near-zero marginal cost—and what copyright law restricts?

The answers of open-access movements have succeeded in building an alternative community, culture, and practice in relation to copyright. Through creative messaging and accessible educational resources, these movements have brought copyright into the public sphere and freed it from its arcane scaffolding. Their easy-to-use standard licences allow creators to opt out of the default 'all rights reserved' framework and exercise greater agency without needing to become experts in copyright law. The movements have also made information more accessible to those who cannot afford paywalls, and enabled collective action to create more secure, privacy-conscious software.

Abolitionist creativity builds on the contributions of contemporary open-access movements, but fundamentally shifts the crux of the problem. Open-access movements are centrally concerned with how to share ideas and culture more freely; how to facilitate free speech and free access while sustaining innovation. These concerns are a product of the location and historical moment from which they emerged. In the 1990s, computer scientists and cyberlaw scholars in Europe and the United States who participated in the rise of software and the internet as mass tools (the so-called Information Age) sought to resolve a particular challenge: how to realise the potential and hope of the internet while copyright law grows increasingly restrictive and punitive.

Instead, we begin our analysis by looking at the broader global system in which knowledge and information operate: a settler-colonial system that extracts wealth, knowledge, and culture from economically marginalised communities and inequitably redistributes their economic fruits to the wealthiest and most powerful. This approach is in line with critiques that activists and critical scholars have long made of open-access movements:[264] that the central focus on liberty values ignores concerns about equality; that a romantic notion of the 'public domain' as a neutral landscape where every person can reap its riches ignores its real role in exploiting the labour and bodies of people of colour, women, people from the Global South, and the impoverished.[265] We now know that the 'public domaining' of Indigenous knowledge about local flora and fauna, traditional medicines, folklore, or traditional cultural expressions has enabled Big Pharma to take Indigenous knowledge, transform it into IP, and become the exclusive owner of that knowledge: a phenomenon known as biopiracy.

Abolitionist creativity also disagrees with an ideological belief that runs through some prominent segments of the open-access movements, namely that the system once worked well, but that 'unfortunately, our IP regimes have strayed far from their original purposes'.[266] For the colonised, for Indigenous Peoples whose collective knowledge has been ransacked, for communities forced into oppressive trade agreements (e.g. TRIPS), for the rising number of modern slaves working in global supply chains powered by intangibles,[267] it is hard to see how the IP system ever worked for them—or what decades of reformist attempts inside IP law in the US have accomplished.

For abolitionists, the system is not broken and in need of reform, tweaking, and tinkering. It is working as it was designed to work, as a settler-colonial legal and economic structure. And we are running out of time and of magical thinking waiting for public policy to somehow turn favourable in a corporate-dominated oligarchy.[268]

Open-access movements must also confront an uncomfortable fact: Big Tech is on their side. The conventional wisdom that large corporations always prefer stronger IP regimes to block new competitors, or that zealous enforcement of IP law favours the powerful, is not borne out by the historical record. With the exception of the pharmaceutical industry, monopolists in technology-intensive industries have resisted strong patent protection throughout history: the railway industry in the nineteenth-century, IBM in the computing industry of the 1960s and 1970s, Big Tech today.[269] Google, Facebook (Meta), and Twitter are trying to selectively apply IP enforcement,[270] spending millions of dollars lobbying to ensure as little IP friction as possible inside markets in which they already have dominant market power,[271] to have unfettered control over data and knowledge, to continue to make 'colossal advertising profits from content produced for free by users',[272] and to avoid the dreaded IP dispute.[273]

If the most powerful actors are the real winners in an open-access world, shouldn't we re-evaluate the claim that 'information wants to be free'? If free access means continuing to ignore the pleas of Indigenous communities to stop the biopiracy, cultural expropriation, and 'public domaining' of the colonised, why do we continue to hold it as an absolute value?

Unlike open-access movements, abolitionist creativity recognises that the global economy into which we release our creativity is not a neutral, level playing field. Surrendering or limiting the existing rights to creativity in our current system does nothing to interfere in the structure of oppression. It simply cedes agency to more powerful actors—agency that should be ceded down, not up. Rather than relinquish our rights on behalf of a kind of libertarianism for the Information Age, we should open our eyes to the material ways our creativity enters the economy and reifies structures of digital (and other types of) power.

As our plots for an abolitionist future illustrate, there are intriguing experiments and exercises in recognising and repurposing the power of what is classified as 'intellectual property'. By seizing the means of imaginative production, we can transform creativity into a tool for collective liberation that disrupts and overturns the very regimes of digital power that enclose and exploit it. At the same time, far from reifying the IP system itself, abolitionist creativity highlights its contradictions, shakes its equilibrium, and creates internal crisis. If there is a future for intellectual property, we will discover it, collectively, in our acts of resistance and imagination.

BIOGRAPHIES

Julia Choucair Vizoso is an independent knowledge producer and co-founder of the art collective AbolishIP. She works on environmental and climate justice in the Arab world, teaches courses on political economy, and occasionally translates Arabic literature into English. She holds a PhD in Political Science from Yale University and an MA in Arab Studies/BS in Foreign Service from Georgetown University.

Chris Byrnes is an intellectual property (IP) lawyer, independent scholar, and co-founder of the art collective AbolishIP. He focuses on ethical IP licensing, web3-based IP commoning, and hacking IP to protect biodiversity and empower radical imaginaries. He holds a JD from Georgetown University, an MTS in Religion, Ethics & Politics from Harvard University, and a BA in Physics from Denison University.

Tying up Goliath

Activist strategies for confronting and harnessing digital power

Anastasia Kavada, Tina Askanius, Anne Kaun,
Alice Mattoni, Julie Uldam

The last decade has seen a sweeping change in our perception of social media platforms and their role in social movements. Within the wave of protests in 2011, from the so-called Arab Spring to the Occupy mobilisations, such platforms were often presented as technologies of liberation. Ten years on, however, social media have come to be seen as spaces of surveillance and repression that are captured by capitalism and authoritarian governments. The Edward Snowden revelations in 2013 were a turning point in this regard, when the role of commercial social media platforms in the surveillance of activists was made abundantly clear. Since then, many mainstream social media platforms have been saturated by misinformation and offensive speech. They have often been seized by far-right forces that, under the banner of 'free speech', have used them to ruthlessly attack their opponents. In 2022 we may have seen another turning point in this tale, as this was a year when the power of social media faced intense challenges. The chaotic takeover of Twitter by Elon Musk, the recent losses in the value of Meta (formerly Facebook), and the growing calls to regulate content on these platforms have been accompanied by a modest exodus from social media, and Twitter in particular, and the migration to alternative platforms such as Mastodon, even though this move might be short-lived.

Of course, mainstream social media platforms still hold significant power. They have become important conduits of news and information with research both in the US[274] and the UK showing that platforms like Facebook and YouTube are increasingly spaces where users get their news. The business model of such platforms promotes 'surveillance capitalism', the relentless gathering and selling of data on user behaviour. The companies behind them have also become too big to regulate and control, as they have been steadily acquiring smaller start-ups and adding diverse platforms and applications to their list of products. So, although social media platforms may have offered more opportunities to users to express their voice, they still reinforce the capacity of the powerful to shape public opinion as they have the resources to pay the fees charged by some of these platforms, to conduct black propaganda through bots and fake accounts, and to invest in digital ad campaigns. These platforms also have an ambivalent relationship with repressive regimes around the world, sometimes colluding with them – as the Snowden revelations amply showed – and sometimes providing a channel for dissent that is not controlled by the government, even though it is still shaped by complex geopolitical interests.

Within this landscape, progressive activists need to both challenge and harness the power of social media in an effort to build the world that they'd like to see. But how can social movements do this? And what are the obstacles they face along the way? In this essay, we explore some strategies that activists can use by focusing on the example of the environmental movement, and particularly groups and organisations mobilising against climate breakdown. These are diverse and heterogeneous, ranging from traditional non-government organisations (NGOs) and charities, to more recent groups like Extinction Rebellion (XR), which focus on direct action, to mobilisations associated with Greta Thunberg and the Fridays for Future movement.

Our analysis draws on the work of social movement scholar Dieter Rucht on the strategies that activists adopt when dealing with the tendency of the mainstream media (MSM) to misrepresent, trivialise and marginalise activist causes. In the early 2000s, Rucht observed that, in response, some activists decide to put visibility aside, and abstain from the mainstream press. Others opt to openly blame the mainstream press in an attempt to make them accountable for their biased reporting of protest. Still others choose to bypass the mainstream press by creating alternatives

to cater to their constituencies. Finally, some groups attempt to get good mainstream media coverage by seeking to understand how the media work and by adapting their communication to them. Rucht's framework was named the 'Quadruple A' as each of the four strategies begins with the letter 'A': Abstention, Attack, Alternatives, Adaptation. While Rucht's strategies originally referred to an age of dominance by the mainstream press, they still resonate today when social media platforms, as well as the press, take centre stage in the communication strategies of activist groups.

Since the mainstream media follow a capitalist model, it comes as no surprise that these four strategies echo Erik Olin Wright's (2019) discussion of the four logics that characterise anti-capitalist struggles: smashing, escaping, eroding, and taming capitalism.[275] When activists engage in collective action with the logic of smashing capitalism, they are in tune with communication strategies that revolve around attacking social media platforms. Similarly, when activists promote collective action that would allow people to escape capitalism, they are consistent with the strategy of abstention from social media platforms. When activists develop collective action that does not wholly reject capitalism but, rather, seeks to tame it, we can see a resemblance with the strategy of adaptation. Finally, anti-capitalist struggles that aim to erode capitalism link to activists who are creating alternatives to social media platforms, building and curating spaces of contention that they can manage directly.

Keeping in mind these different anti-capitalist logics and the four strategies that activist groups might employ to address the issue of visibility, we explore how the environmental movement has engaged with social media platforms.

Abstention (Escaping Capitalism)

Strategies of **abstention** involve shunning the mainstream social media completely as a form of both protest towards and protection from their business models and surveillance mechanisms. Deciding not to delegate your group's visibility to the profit logic of social media platforms is liberating. It frees activists from the constant pressure to be visible and produce content on these platforms. It also emancipates activist groups from the opacity that characterises social media algorithms – black boxes whose functioning is difficult, if not impossible, to understand. The strategy of abstention can promote more sustainable ways of maintaining membership beyond Facebook groups or Twitter threads, by developing the group's own media.

It can also protect activists from online attacks and surveillance. As the case of Greta Thunberg has shown, prominent activists can be the targets of scathing attacks on social media that range from trolling to death threats. Being present on social media also renders activist groups vulnerable to surveillance by the authorities. This is particularly dangerous for activists who use tactics of civil disobedience or push the lines of legality.[276] Such groups thus typically engage in face-to-face planning rather than online coordination. Therefore, abstaining from social media platforms is crucial for enhancing the privacy and data integrity of internal organising.

Alongside abstention, some activist groups have also launched campaigns urging people to disconnect from such platforms or to engage in practices of digital or data 'detox'. For instance, Tactical Tech provides a tool kit for creating awareness of the data traces that we leave online

and for developing alternative practices for what they call 'a more confident relationship with technology'.[277] Disconnecting from social media may also be done for environmental reasons. As Tactical Tech notes, digital detox strategies can help in the fight against climate change as digital technologies are now responsible for 3.7% of the world's global carbon emissions, a figure that may increase to 8% by 2025. 'That's currently more than the civil airline industry, and soon it's predicted to surpass the automobile industry, too.'[278] Environmental groups may therefore opt to abstain from social media in order to reduce their e-waste and carbon footprint.

However, 'digital detox' practices are often related to individual lifestyle politics rather than collective efforts to achieve systemic change. Attending digital detox camps or restricting our digital data footprints by using specific browsers and configurations involve individual practices and ways of relating to social media. They may thus have a smaller impact on challenging capitalism and Big Tech than seeking to promote structural change through regulation, for example.

Furthermore, a complete abstention from digital platforms seems virtually impossible, especially for political causes with a transnational character or those aiming to mobilise large numbers of supporters. In a world where visibility on social media has become crucial for expanding a movement's community, abstaining from these platforms means cutting oneself off from a dense network of relationships that has sustained numerous protests around the world over the past decade. The environmental movement is no exception, as evidenced by the extensive use of social media by organisations such as Greenpeace and Extinction Rebellion or movements like Fridays for Future. Instead, and as we note in the sections on the strategies of Adaptation and Alternatives, activist groups often choose to use mainstream platforms for promoting their cause to a broader audience, even if they abstain from using them for internal organising.

Attack (Smashing Capitalism)

Activists and social movements can also **attack** social media platforms and campaign for them to reform their corporate practice or the regulations governing their operation. 'Attack strategies' include anti-trust actions that challenge the size and concentration of social media companies, as well as digital rights campaigns that target the misuse or misappropriation of data by companies and national governments.

There are also many campaigns against disinformation on social media, a problem that is also enormously affecting campaigns on climate change. Large polluters such as oil companies engage in elaborate greenwashing campaigns on social media. False statements regarding climate change have proliferated, often peddled by fake accounts and 'astroturf' campaigns. Climate change denialism is rising on social media platforms, also as a result of the strengthening of far-right accounts and the lack of effective moderation. In February 2022, Reuters reported that Facebook 'failed to flag up half of posts that promote climate change denial'.[279] Research undertaken by Global Witness has found that the Facebook algorithm not only locks climate-sceptic users in echo chambers of climate denialism but also directs them 'to worse information, so that what began on a page full of distract and delay narratives, ended on pages espousing outright climate denial and conspiracy'.[280] On Twitter, the situation seems to have worsened after Elon Musk's takeover, which led to the firing of content management teams, the dismantling of the platform's sustainability arm, and the return of banned users to the platform, some of whom have a significant history of

climate denialism.[281] Consequently, the hashtag #ClimateScam has climbed in the rankings and is 'now regularly the first result that appears when 'climate' is searched on the site'.[282]

Campaigns against disinformation on social media have included the #StopHateForProfit campaign in 2020, in which various civil society groups and organisations called on advertisers to boycott Facebook for this reason. The campaign was initiated by a coalition of activist groups, including the Anti-Defamation League, Free Press, and GLAAD.[283] In February 2020, Avaaz ran a campaign specifically about climate change denialism on YouTube and other platforms, which was based on a detailed report compiled by the organisation.[284] Avaaz called 'on all social media platforms to detox their algorithms by ending the amplification and monetisation of disinformation and hate speech'. It also urged 'regulators to turn this into a legal requirement' and demanded that 'platforms work with independent experts to track and downgrade creators of repeated and deliberate disinformation'.[285] It is worth noting that the group amended the initial text of the petition to remove a 'demand to "deplatform" creators of repeated and deliberate disinformation'.[286] While no reason was given for this amendment, we suspect that it relates to the slippery slope when demands to deplatform individuals or groups peddling disinformation can be turned against progressive actors and used to restrain their voices on social media. Calls to boycott and deplatform should thus be alert to the implications for freedom of speech across the political spectrum. Furthermore, for such actions to be effective, they need backing from prominent activist groups and advertisers so that they are considered sufficiently effective for others to join and are able to draw sufficient news coverage.

Attacks can also occur more directly, such as through hacking. For example, Twitter and Facebook have been targeted by denial-of-service attacks in which computers prevent users from accessing the platform or slow down their use. Such attacks have not always been clearly linked to criticism of the platforms themselves, but to protests against the role of such platforms in giving voice to particular political viewpoints, for instance in relation to Russia's conflicts with neighbouring countries.[287] Yet, 'hacktivism' requires sophisticated technical skills and comes with the risk of arrest and other repercussions. This is probably why there are no recorded cases of environmental hacktivism, even by groups like Extinction Rebellion that focus on disruptive action (at least until their very recent change in strategy) although the group did engage in internal discussions about hacktivism during the pandemic.[288] For the academic Gabriella Coleman, who has conducted extensive research on Anonymous, this may be because there are few overlaps between hardcore hackers and hardcore environmentalists,[289] meaning that the environmental movement lacks the necessary skills and experience to engage in such activism. On the contrary, it is environmental activists who have fallen victim to hacking attacks. For instance, in 2017, environmental groups who ran a climate change campaign against Exxon Mobil received phishing emails by accounts impersonating their colleagues and lawyers, as part of 'a sprawling hacking-for-hire operation that for years has targeted the email accounts of government officials, journalists, banks, environmental activists and other individuals.'[290]

Collective actions that follow a strategy of attack are typically seen as spectacular interventions and so are likely to gain mass media attention. However, media reporting tends to focus on the attack itself, rather than on the message it attempts to convey, making it difficult to gain resonance among the broader public and policymakers. At the same time, attacks that disrupt users' daily use of social media risk generating annoyance, which again may restrict the impact of the message.

Alternatives (Eroding Capitalism)

The strategy of **alternatives** (or eroding capitalism) entails activists building their own social media platforms or digital properties where they can network on social issues and disseminate alternative information to the public. Such platforms operate with different rules: they are often designed by advocates of Free and Open Source Software (FOSS), meaning that the code is open for everyone to use, adapt and change, provided that they are not doing it for commercial reasons. Such platforms also operate with different policies regarding anonymity and privacy, in an effort to guarantee the safety of their users. Examples include the platform N-1 developed by activists in Spain right before the first stage of the Indignados movement in 2011, as well as RiseUp!,[291] Crabgrass,[292] and Occupii, the activist alternative to Facebook created by Occupy Wall Street in 2011. Other examples include video-streaming platforms such as BitChute (previously also Vine or Periscope) or podcast channels hosted outside the dominant commercial platforms to circumvent moderation. Activists may further use platforms like Mastodon, which is now emerging as an alternative to Twitter, that, although not explicitly developed by social movements, still operate in ways that accord with progressive values.

There are also alternatives for instant messaging or email that facilitate more secure internal organising processes for social movements. For instance, Riseup.net, an independent social network based in Seattle, has provided encrypted secure email and mailing-list management services for social movements since its inception in 1999–2000. More recently, platforms such as Signal, Telegram or GroupMe have also been used for coordination, with Telegram in particular facilitating both interpersonal and broadcast communication. Such channels are also used by environmental activists that engage in more disruptive tactics.

Social movements have also created their own platforms to disseminate information about their causes and to report on their mobilisations in an effort to tackle the marginalisation and misinformation peddled by most mainstream news outlets and social media platforms. One example is Unicorn Riot, a non-profit online news collective, which was founded in 2015 by activists who were involved in alternative media around the Occupy movement, the tar sands mobilisations[293], and the Ferguson protests[294]. Unicorn Riot reported from the ground in North Dakota during the #NODAPL or Dakota Access Pipeline Protests in 2016, when different Native American tribes opposed the building of a pipeline carrying crude oil from Dakota to Illinois. Protesters considered the pipeline, which was going to pass through the Indian reservation at Standing Rock, as posing a serious hazard of water pollution. Calling themselves 'water protectors', activists established a protest camp in the area and attempted to stop the building of the pipeline. The mainstream news media provided little news coverage, while prominent investigative journalists, like Amy Goodman, co-founder and presenter of Democracy Now!, were arrested on riot charges.[295] By contrast, Unicorn Riot was able to provide independent coverage of the protests, with journalists staying in the camp and interviewing protesters.[296] The decentralised online platform is therefore a good example of the kind of community media built in the service of social movements and the continued importance of journalism produced from *within activist communities.*

With some notable exceptions, however, efforts to build anti-capitalist alternatives tend to be ephemeral, under-funded and unable to fully replace the services afforded by corporate social media. What these platforms also lack is 'network effects', a term that points to a crucial dynamic

of social networks: that the more members they acquire, the more useful they become, since they can be used to communicate with a wider range of participants. In reality, many alternative platforms are used only by the converted – experienced activists who are already familiar with the mobilisations in question. Hence, by communicating solely within these spaces, activists may effectively remain invisible within a communicative niche.

Adaptation (Taming Capitalism)

The limitations of small-scale alternative platforms often lead activists to use corporate applications like Facebook, Twitter, and Instagram to attract a wider public. Activists thus engage in a strategy of **adaptation,** meaning that they adapt to the rules of corporate platforms, trying to harness their power for increasing their movement's visibility.

Corporate social media platforms have now become key channels for publishing information about climate change. Most major activist groups and movements are using their social media accounts to disseminate information about their cause. Social media have also facilitated the rise of 'green influencers' – environmental activists who command very large followings on social media.[297] Alongside them, we find collectives like EcoTok who report on environmental issues on TikTok.[298] According to the Reuters Institute for the Study of Journalism, such channels are particularly important for users under the age of 35 who 'are often two or three times more likely to say they pay attention to celebrities, social media personalities, or activists for climate change news than people over 35'.[299]

There are also cases where social media channels have enabled marginalised voices to come to the fore. An example is the Digital Smoke Signals Facebook page, founded by the late Native American journalist Myron Dewey, which provided important coverage of the #NODAPL protests. The page was one of the most followed news outlets on the protests and some of its videos amassed more than 2.5 million views.[300] Facebook live was also used to report live from the protests, allowing activists unfiltered and uncensored reporting from the ground. In the years since the Arab Spring, livestreaming has become an important application in the hands of citizen reporters. While in the 2011 wave of mobilisations, livestreaming was provided by smaller start-up companies, by the mid-2010s most major social media platforms, including Instagram and Facebook, started to offer this functionality, thus eclipsing the smaller players in the field.

Strategies of adaptation also include the development of new approaches for engaging with the campaign targets or for demonstrating one's support for a cause, which are tailored to the social media environment. These may include relatively 'effortless' acts, such as adding a banner on your profile picture on social media to show your support for an environmental cause. While such tactics are useful for gaining visibility in a crowded media landscape, they are often derided as 'clicktivism' – a portmanteau term that combines 'click' with 'activism'. Critics point to the limited commitment needed to engage in such activism and its potential to create a misleading sense of effectiveness and connection. Yet this depends on the political context since in more restrictive and authoritarian countries a tweet or a Facebook post can easily land you in prison, or even face a death sentence. 'Clicktivism', in other words, depends on the eye of the beholder.

Strategies of adaptation are also associated with the emergence of new activist tactics such as Twitter storms, whereby users bombard a hashtag with tweets to make it into a trending topic. Hashtag hijacking is a variant of this tactic, where activists seize control of a target's hashtag. Environmental activists have also pioneered the tactic of 'greentrolling' the social media accounts that peddle climate disinformation or engage in 'greenwashing'. 'Greentrolling' is a strategy of adaptation as it is based on adopting 'a form of rebuttal better associated with the Internet's ne'er-do-wells—trolling—infused with voice, verve and mordant humor'.[301] By targeting the social media of large corporations, climate activists gain a wider reach for their messages and attract mainstream media interest. A famous example came in November 2020, when Shell put up a social media poll asking users 'what are you willing to do to reduce emissions?'. The poll received many ironic replies from environmental activists, politicians and ordinary users, including high-profile individuals such as Greta Thunberg and Alexandria Ocasio-Cortez, who used the poll to denounce Shell's role in increasing emissions. [302]

Yet, to pursue strategies of adaptation, activists have to obtain intimate knowledge of how commercial social media platforms operate. This may demand greater professionalisation of activist communications, leading movements to employ social media professionals or to provide training to social media administrators, as well as to develop specific guidelines and protocols.

The adaptation strategy has several risks for progressive activists. It forces them to give up direct management of their visibility spaces as they can exercise very limited control over the materials they publish on commercial platforms or the infrastructure that enables their publication. This makes their visibility particularly fragile: if a social media outlet decides to delete a group's profile, the entire archive of content published up to that point will probably disappear, along with the network of contacts built up through ongoing use of the platform.

Commercial social media platforms are constantly tweaking their algorithms to impede content creators from attracting wider audiences on the basis of organic reach. This allows them to charge creators for reaching their own followers with prices that are sometimes exorbitant for most activist groups. It also creates power asymmetries in activist efforts to counter disinformation. Groups that spread false information on, for instance, the role of polluters in slowing down the adoption of policies on climate change are often financed by these very polluters, capital that enables them to pay for greater reach. Social media are also exploiting the user data created by the activity of social movements on the platform. The more polarising the cause, the more profit it creates for the company as it fuels traffic and user activity. It is thus no surprise that the strategy of adaptation tends to be at odds with core values of left-leaning activist communities, such as their aversion to capitalism. In fact, the use of proprietary platforms is often at the heart of internal conflicts within activist groups, between those who support their use for pragmatic reasons and those who refuse to engage with them.

The corporate surveillance on mainstream social media also feeds into systems of state surveillance. This is the double sword of visibility, where becoming more visible on social media also makes activist groups more vulnerable to the authorities. A key strategy in this respect is to use commercial platforms to promote public events, but keep all internal organising on alternative platforms that have encrypted communication or off digital media altogether by employing the time-worn methods of secret face-to-face meetings. In other words, activist groups need to combine different

strategies and platforms, depending on the tasks they need to accomplish and their associated privacy or need for greater visibility.

Moving forwards: Collaboration, Interconnectivity and Curation

Progressive social movements, and environmental activists in particular, can use different strategies for both challenging and harnessing the power of commercial social media. They can abstain, build alternatives, go on the attack and adapt. Each has advantages and drawbacks in terms of effectiveness and impact, and depends on context. In practice, activists often deploy some or all forms.

In other words, the four types of strategies outlined in Rucht's 'Quadruple A' work better in combination rather than separately. Yet, it is exactly this art of pursuing different strategies simultaneously that is the most formidable. What should be the balance between challenging corporate platforms but at the same time harnessing their power? And can one group do all this alone or should it work in coalition, so that it can specialise in specific strategies?

In this respect, working collaboratively seems to be the way forward. This may take the form of more formal coalitions and umbrella platforms or happen more informally through the development of common themes in campaigns, the exchange of resources, as well as sharing each other's content and creating more densely hyperlinked communication properties. Environmental groups, for example have also begun to work in a more intersectional manner by considering the issues on which they campaign from the perspectives of different stakeholders and by mapping the interlocking systems of power that need to be overcome.[303] Such collaboration and coalition-making need to be reflected more strongly in the digital realm, with greater hyperlinking and interconnectivity among environmental groups, whether via social media accounts on commercial platforms or alternative media outlets. In this respect, studies on video activism around climate justice and social justice movements in the early 2010s showed very weak connections between actors on YouTube.[304] The actions and actors within social justice movements were largely disconnected – or at least they were not coming together in any meaningful way on that particular platform. Thus, as a potential site of resistance YouTube failed to provide a space for sustainable, horizontal, and radical media practices.[305]

This seems to ring even truer today – a decade on and in a context where YouTube is mainly discussed in terms of rabbit holes, radicalisation and disinformation rather than democratic broadcasting, visual evidence and radical eye-witnessing. When there is evidence to suggest that a network of connective actions is in fact materialising, the process is led by anti-democratic and far-right reactionary forces. They have largely succeeded in connecting across party lines and intra-movement differences, building a sizable audience, and forming a coherent web of related channels and content which extend into a larger media ecology of alternative far-right media. They do this through an interlocking series of connective practices including guest appearances on each other's YouTube channels, joint livestreaming, as well as various referencing and hyperlinking practices.

Even when the right have been deplatformed, for example in the wake of The Unite the Right rally in Charlottesville in 2017, far-right groups have migrated to Alt-Tech platforms that are harder to control, including Gab, Parler, Gettr, BitChute, Rumble, PewTube, Odysee, Hatreon and numerous others. These have been designed following the models of Big Tech platforms and mimic their features while also offering anonymity and far fewer restrictions on the level of offensive and harmful material that can be posted.

The far right has been very able to engage on a wide range of platforms at the same time and for different purposes – combining alternative and mainstream – while deliberately adopting a different tone for different platforms with some degree of success. It helps, of course, that in comparison to progressive movements, far-right activists have fewer scruples in using a more offensive, irreverent and populist tone that does well on social media in terms of virality and algorithmic optimisation. The far right is also less reluctant to use commercial and profit-driven platforms, and has found ways of monetising its content by interspersing business strategies with political propaganda techniques.

Far-right activists have thus built an ecosystem of Alt-Tech platforms that has outdistanced progressive alternative media in terms of crowdsourcing and successful fundraising for tech start-ups. Of course, the recent success of the far right has resulted not only from savvy social media strategies, but also from a broader political context that is conducive to its goals. After the repression – and, in some quarters, perceived failure – of the 2011 progressive movements, some of the same anger towards the establishment has been harnessed by reactionary, conservative actors. Far-right activists have thus made the most of the opportunities that come with being in line with broader political currents and particularly the rise in the politics of fear that go along with uncertainty and increasing inequality. Yet, the perfect storm of economic, social and climate crises that we are currently facing is also presenting an opening for radical change on the progressive side of the political spectrum. Developing greater connectivity across groups, issues and digital media properties is paramount within this context.

Apart from hyperlinking and *interconnectivity, consistency and continuity* will also help progressive groups, and the environmental movement in particular, in harnessing digital power. Lasting bonds of collaboration can alleviate the immense efforts of voluntary labour for establishing and running alternative platforms through the development of routines and a repository of knowledge and experience. Such labour is also necessary for attacking commercial social media, which is often based on the painstaking collection of information about the profit-driven logics of Big Tech. Sustained collaboration over a period of time makes this voluntary labour possible as it enables knowledge transfer across different activist groups and generations, gathering insights from past experiences, from what works and what doesn't, and ensuring that these lessons are passed on and combined with new insights for new generations of activism.

As demonstrated by the example of the far right, the curation of digital content is another crucial aspect of interconnectivity and collaboration. Curation refers to the process of finding, selecting, organising, and interlinking suitable messages. It thus helps to create a collaborative network of interconnected actors and communications that provides a rich and consistent message and offers users different entry points to the 'message space' of progressive movements. At its core, curation is all about the cultivation of community, connectivity and participation, a logic that

goes against social media business models which foster individualism and the personalisation of political action.

Obviously, such strategies of collaboration often encounter many obstacles. Doctrinal and ideological differences, however minute they may seem to outsiders, may split progressive movements and increase factionalism. Greater collaboration can pose risks to legitimacy, as groups may be afraid to align more closely with, for instance, a more radical actor, since they can be tainted by association. Or the reason may be more self-interested, as groups may want to retain audiences in their own social media properties rather than sharing them with related actors. The lack of funding and resources for progressive politics may lead to competing for audiences and a lack of connectivity between activist groups online.

Thus, for collaboration to work, activists need to be committed to working together in providing alternatives. Moving ahead, it is this belief in the value of building broader networks of networks that can help activists in harnessing the power of digital media, resisting Big Tech and changing the world.

BIOGRAPHIES

Anastasia Kavada is a Reader in Media and Politics in the School of Media and Communication at the University of Westminster, where she is leading the MA in Media, Campaigning and Social Change. Her research focuses on the links between digital media, social movements, participatory democracy and campaigning for social change.

Tina Askanius is an Associate Professor in Media and Communication Studies at the School of Arts and Communication at Malmö University and affiliated researcher at the Institute for Futures Studies in Stockholm. Her research concerns the interplay between social movements, media technologies and processes of mediation.

Anne Kaun is Professor of Media and Communication Studies at Södertörn University. She is a 2021 Wallenberg Academy fellow and leads several projects exploring the digital welfare state and automated decision-making. In 2023, her co-authored book *Prison Media* will appear with MIT Press.

Alice Mattoni is an Associate Professor in the Department of Political and Social Sciences at the University of Bologna. She researches the relationship between social movements and media, digital and otherwise. She is one of the three co-founders and current editor of the Routledge Series Media and Communication Activism.

Julie Uldam is an Associate Professor at Copenhagen Business School where she leads the project Imagining Digital Power and the Power of Digital Imagination in Business and Society Encounters. Her research explores the role of activism digital media in societal challenges, including the climate crisis and democratic debate.

Endnotes

1 Texas Attorney General et al. (2022) In Re: Google Digital Advertising Antitrust Litigation, available at: https://www.nysd.uscourts.gov/sites/default/files/2022-09/In%20re%20Gogle%20Digital%20Advertising%20Antitrust%20Lirtigation.pdf

2 US DoJ (2020) Justice Department Sues Monopolist Google For Violating Antitrust Laws, Washington DC: Department of Justice, available at: https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws

3 Online advertising can be differentiated between programmatic and contextual advertising; the former represents advertising targeted at individuals on the basis of their interests and preferences, which are inferred from their personal data, while the latter represents advertising attached to webpages that correspond to the advert's contents see Hwang (2020) for more on the implications of this difference.

4 Mirowski, P. and Nik-Khah, E. (2017) The Knowledge We Lost in Information, Oxford: Oxford University Press.

5 Texas Attorney General et al., 2022, p.104)

6 ibid., p.107

7 Birch, K. (2017) What Exactly is Neoliberalism?, The Conversation (2 November), available at: https://theconversation.com/what-exactly-is-neoliberalism-84755

8 Hayek, F. (1945) The Use of Knowledge in Society, available at: https://www.econlib.org/library/Essays/hykKnw.html?chapter_num=1#book-reader

9 Again, see Mirowski and Nik-Khah's book on the history of 'information' in orthodox economics.

10 Amadae, S.M. (2016) Prisoners of Reason, Cambridge: Cambridge University Press.

11 McMillan, J. (2003) Market Design: The Policy Uses of Theory, Stanford Business School: Working Paper No.1781, available at: https://www.gsb.stanford.edu/faculty-research/working-papers/market-design-policy-uses-theory

12 Birch, K. (2020) Automated neoliberalism? The digital organization of markets in technoscientific capitalism, New Formations 100-101: 10-27.

13 Birch, K. and Bronson, K. (2022) Introduction: Big Tech, Science as Culture 31(1): 1-14. There are several books on the rise of Big Tech which are worth reading (and many not worth reading). My suggestions are: Cohen (2019), Doctorow (2020), Foroohar (2019), Lanier (2014), Pasquale (2015), Srnicek (2016), and Zuboff (2019). There are, of course, many more books, articles, etc. worth reading, I simply can't put them in this endnote.

14 I use the term enclaves' rather than 'enclosure' to reflect the fact that digital personal data has to be *made, rather than existing in a raw state ready for anyone to collect and use. So, collection comes to define use in ways that lead to problematic outcomes, as I have discussed in an open access journal article with two colleagues (*Birch et al., 2021).

15 US House of Representatives (2020) Investigation of Competition in Digital Markets, Washington, DC: House of Representatives.

16 Leonard, C. (2022) The Lords of Easy Money, New York: Simon & Schuster.

17 Birch, K., Cochrane, D.T. and Ward, C. (2021) Data as asset? Unpacking the measurement, governance, and valuation of digital personal data by Big Tech, Big Data & Society 8(1): 1-15; Morozov, E. (2022) Critique of Techno-feudal Reason, New Left Review 133/134, 89-126.

18 Viljoen, S., Goldenfein, J. and McGuigan, L. (2021) Design choices: Mechanism design and platform capitalism, Big Data & Society 8(2): 1-13. Algorithmic technologies refer to a range of developments often lumped under umbrella terms like 'artificial intelligence' or 'machine learning'. Rather than go into a debate about to what extent these technologies represent actual 'intelligence' (which I don't think they do), I prefer to refer to them in terms of how they function, which is primarily as algorithms (i.e. they take in inputs and give you outputs based on some internal operation, which can be transparent or opaque). I especially like Meredith Whittaker's (2021) take on these technologies, since it demystifies them: 'we must first recognize that the "advances" in AI celebrated over the past decade were not due to fundamental scientific breakthroughs in AI techniques. They were and are primarily the product of significantly concentrated data and compute resources that reside in the hands of a few large tech corporations'.

19 Collins, G. (2020) Why the infinite scroll is so addictive, available at: https://uxdesign.cc/why-the-infinite-scroll-is-so-addictive-9928367019c5

20 Birch et al., 2021

21 CPRC (2022) Duped by Design: Manipulative Online Design: Dark Patterns in Australia, Melbourne: Consumer Policy Research Centre, available at: https://cprc.org.au/dupedbydesign/

22 See Salomé Viljoen's (2021) great article about this.

23 Borgesius, F.Z. (2020) Price discrimination, algorithmic decision-making, and European non-discrimination law, European Business Law Review 31(3): 401-422

24 Rosenblat, A. and Stark, L. (2016) Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers, The International Journal of Communication 10: 3758-3784.

25 Baker-White, E. (2022) Swiping Right As Much As You Want On Tinder Costs Users Wildly Different Amounts, A Study Found, BuzzFeed News (8 February), available at: https://www.buzzfeednews.com/article/emilybakerwhite/tinder-plus-pricing-study

26 Where I live, in Canada, the federal government has introduced legislation to update data protection and privacy regulations, which have not changed for over 20 years; however, its government's approach to reform is premised on enabling companies to keep collecting and processing our data within a new privacy framework, rather than challenging that collection and use itself (Birch, 2022).

27 Doctorow, C. (2021) End of the Line for Uber, Pluralistic (10 August), available at: https://pluralistic.net/2021/08/10/unter/#bezzle-no-more

28 Roy, R. (2020) Doordash and Pizza Arbitrage, Margins (17 May), available at: https://www.readmargins.com/p/doordash-and-pizza-arbitrage

29 Goldfischer, E. (2022) Scams: The Dark Side of Alternative Accommodations, Hertelier (3 August), available at: https://www.hertelier.com/post/airbnb-booking-com-scams

30 Birch, K. (2020)

31 Posner, E. and Weyl, E.G. (2019) Radical Markets, Princeton: Princeton University Press.

32 Wiley, B. and McDonald, S.M. (2018) What is a Data Trust?, Centre for International Governance Innovation (9 October), available at: https://www.cigionline.org/articles/what-data-trust/

33 Scholz, T. and Calzada, I. (2021) Data Cooperatives for Pandemic Times, Public Seminar (19 April), available at: https://publicseminar.org/essays/data-cooperatives-for-pandemic-times/

34 Zuboff, S. (2019) The Age of Surveillance Capitalism, New York: Public Affairs.

35 Dorsey, J. (2021) 'You don't own "web3." The VCs and their LPs do. It will never escape their incentives. It's ultimately a centralized entity with a different label. Know what you're getting into...'. Twitter.

36 Muoio, D. (2017) The early Uber investor suing Travis Kalanick turned its $12 million investment into $7 billion stake. *Business Insider*. https://www.businessinsider.com/benchmarks-uber-investment-worth-7-billion-2017-8

37 Crunchbase (2022a) Amazon—Funding, Financials, Valuation & Investors. https://www.crunchbase.com/organization/amazon/company_financials

38 Crunchbase (2022b) Query Builder | Google Funding Rounds. https://www.crunchbase.com/search/funding_rounds/field/organization.has_investor.reverse/funding_total/google

39 StartupRanking (2022c) Facebook Funding Rounds | Startup Ranking. https://www.startupranking.com/startup/facebook/funding-rounds

40 Crunchbase (2022d) Airbnb—Funding, Financials, Valuation & Investors. https://www.crunchbase.com/organization/airbnb/company_financials

41 Crunchbase (2022e) Uber—Funding, Financials, Valuation & Investors. https://www.crunchbase.com/organization/uber/company_financials

42 Klinge, T.J., Hendrikse, R., Fernandez, R. and Adriaans, I. (2022) Augmenting digital monopolies: A corporate financialization perspective on the rise of Big Tech. *Competition & Change* 10245294221105572. https://doi.org/10.1177/10245294221105573

43 Summers, L.H. (2016, 15 February) The age of secular stagnation. *Foreign Affairs*. https://www.foreignaffairs.com/articles/united-states/2016-02-15/age-secular-stagnation

44 Bank of England (2022) Quantitative easing. https://www.bankofengland.co.uk/monetary-policy/quantitative-easing

45 Tech Nation (2021) *The future UK tech built—Tech Nation Report 2021*. https://technation.io/report2021/

46 European Commission (2017) A Fair and Efficient Tax System in the European Union for the Digital Single Market. COM/2017/0547 final

47 Tech Nation (2021), op. cit.

48 Teare, G. (2022) Global Venture Funding And Unicorn Creation In 2021 Shattered All Records. Crunchbase News. https://news.crunchbase.com/business/global-vc-funding-unicorns-2021-monthly-recap/

49 Nicholas, T. (2019) *VC: an American history*. Cambridge, MA: Harvard University Press.

50 Uber Technologies Inc. (2019) Form S-1 Registration Statement. https://www.sec.gov/Archives/edgar/data/1543151/000119312519103850/d647752ds1.htm#toc647752_16

51 Davies, H., Goodley, S., Lawrence, F., Lewis, P., O'Carroll, L. and Cutler, S. (2022, 11 July) Uber broke laws, duped police and secretly lobbied governments, leak reveals. *The Guardian*. https://www.theguardian.com/news/2022/jul/10/uber-files-leak-reveals-global-lobbying-campaign

52 Chen, A. (2021) *The cold start problem: How to start and scale network effects*. New York: Harper Business.

53 Horan, H. (2019) Uber's path of destruction. *American Affairs Journal*, 3(2). https://americanaffairsjournal.org/2019/05/ubers-path-of-destruction/

54 Levingston, I. (2022, 15 August) Uber raises prices by about 5% in London to attract more drivers. Bloomberg. https://www.bloomberg.com/news/articles/2022-08-15/uber-raises-prices-by-about-5-in-london-to-attract-more-drivers

55 Agence France-Presse (2018, 25 February) Gobee.bike pulls out of France due to 'mass destruction' of its dockless bike fleet. *The Guardian*.

56 Taylor, A. (2018, 22 March) Bike share oversupply in China: Huge piles of abandoned and broken bicycles. *The Atlantic*. https://www.theatlantic.com/photo/2018/03/bike-share-oversupply-in-china-huge-piles-of-abandoned-and-broken-bicycles/556268/

57 Lunden, I. (2022) Berlin's Gorillas lays off 300, exits four markets. TechCrunch. https://techcrunch.com/2022/05/24/berlins-gorillas-lays-off-300-explores-strategic-options-in-4-countries-as-funds-dry-up-for-its-3b-instant-grocery-play/

58 Lee, R. (2022) Layoffs.fyi. https://layoffs.fyi/

59 Steinschaden, J. (2019) Startups Spend $44b on Google, Facebook and Amazon. Could this be a sign for a new bubble burst? Trending Topics. https://www.trendingtopics.eu/startups-spend-44b-on-google-facebook-and-amazon-could-this-be-a-sign-for-a-new-bubble-burst/

60 Wigglesworth, R. (2021, 23 November) The 'Tesla-financial complex': how carmaker gained influence over the markets. *Financial Times*.

61 Greenfield, P. (2019, 2 October) World's top three asset managers oversee $300bn fossil fuel investments. *The Guardian*. https://www.theguardian.com/environment/2019/oct/12/top-three-asset-managers-fossil-fuel-investments

62 Buller, A. and Braun, B. (2021, 7 September) Under new management: Share ownership and the growth of UK asset manager capitalism (Finance). Common Wealth. https://www.common-wealth.co.uk/reports/under-new-management-share-ownership-and-the-growth-of-uk-asset-manager-capitalism

63 Kruppa, M. and Parkin, B. (2021, 27 July) Tiger Global: the technology investor ruffling Silicon Valley feathers. *Financial Times*. https://www.ft.com/content/54bb342c-230f-4438-a4d7-7cbde010ea1a

64 Muoio, D. (2017) The early Uber investor suing Travis Kalanick turned its $12 million investment into $7 billion stake. *Business Insider*. https://www.businessinsider.com/benchmarks-uber-investment-worth-7-billion-2017-8

65 Scahill, J. and Greenwald, G. (2014.) 'The NSA's Secret Role in the US Assassination Program', *The Intercept* [online], 9 February. Available at: https://theintercept.com/2014/02/10/the-nsas-secret-role/. (Accessed 1 December 2022.)

66 Friedersdorf, J. (2012.) 'How Team Obama Justifies the Killing of a 16-Year-Old American', *The Atlantic [online], 24 October. Available at:* https://www.theatlantic.com/politics/archive/2012/10/how-team-obama-justifies-the-killing-of-a-16-year-old-american/264028/. (Accessed 1 December 2022.)

67 Taylor, A. (2015.) 'The US Keeps Killing Americans in Drone Strikes, Mostly by Accident', *Washington Post [online], 23 April. Available at:* https://www.washingtonpost.com/news/worldviews/wp/2015/04/23/the-u-s-keeps-killing-americans-in-drone-strikes-mostly-by-accident/. (Accessed 1 December 2022.)

68 Tau, B. (2021.) 'Military Intelligence Agency Says It Monitored US Cellphone Movements without Warrant', *Wall Street Journal* [online], 22 January. Available at: https://www.wsj.com/articles/military-intelligence-agency-says-it-monitored-u-s-cellphone-movements-without-warrant-11611350374. (Accessed 28 November 2022.)

69 Heinrich, T. (2002.) 'Cold War Armory: Military Contracting in Silicon Valley', *Enterprise & Society 3(2), 247-284. Available at:* https://www.jstor.org/stable/23699688. (Accessed 25 November 2022.)

70 Kaplan, F. (2016.) 'The Pentagon's Innovation Experiment', *Technology Review [online], 19 December. Available at:* https://www.technologyreview.com/2016/12/19/155246/the-pentagons-innovation-experiment/. (Accessed 15 November 2022.)

71 Kastrenakes, J. (2014.) 'Google Signs 60-Year Lease on NASA Airfield and Hangars', *The Verge* [online], 10 November. Available at: https://www.theverge.com/2014/11/10/7190057/nasa-leases-moffett-airfield-to-google-60-years. (Accessed 20 November 2022.)

72 Myrow, R. (2019.) 'That Giant Structure off 101 once Housed a Flying Aircraft Carrier', *KQED Bay Curious* [podcast], 11 April. Available at: https://www.kqed.org/news/11738379/that-giant-structure-off-101-once-housed-a-flying-aircraft-carrier. (Accessed 21 November 2022.)

73 Kaplan F. (2016.) 'The Pentagon's Innovation Experiment', *Technology Review [online], 19 December. Available at:* https://www.technologyreview.com/2016/12/19/155246/the-pentagons-innovation-experiment/. (Accessed 15 November 2022.)

74 Hempel, J. (2015.) 'DOD Head Aston Carter Enlists Silicon Valley to Transform the Military', *Wired* [online], 18 November. Available at: https://www.wired.com/2015/11/secretary-of-defense-ashton-carter/. (Accessed 19 November 2022.)

75 Ibid.

76 Mehta, A. (2016.) 'Carter Names Three to Innovation Board', *Defense News* [online], 10 June. Available at: https://www.defensenews.com/industry/techwatch/2016/06/10/carter-names-three-to-innovation-board/. (Accessed 18 November 2022.)

77 Mitchell, B. (2018.) 'No Longer an Experiment—DIUx Becomes DIU, Permanent Pentagon Unit', *FedScoop* [online], 9 August. Available at: https://fedscoop.com/diu-permanent-no-longer-an-experiment/. (Accessed 17 November 2022.)

78 Williams, L. (2018.) 'DIUx Gets a Big Boost in FY19 Budget', *FCW* [online], 12 February. Available at: https://fcw.com/acquisition/2018/02/diux-gets-a-big-boost-in-fy19-budget/198959/. (Accessed 22 November 2022).

79 Behrens, J. (2019.) 'FY 20 Budget Request: DOD Science and Technology,' *AIP [online], 28 March. Available at:* https://www.aip.org/fyi/2019/fy20-budget-request-dod-science-and-technology. (Accessed 30 November 2022.)

80 Reinert, J.T. (2013.) 'In-Q-Tel: The Central Intelligence Agency as Venture Capitalist', *Northwestern Journal of International Law & Business* 33(3), 677-709. Available at: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1739&context=njilb. (Accessed 5 January 2023.)

81 Louie, G. (2017.) Quoted in an interview with Ernestine Fu at Stanford University, 8 May. Available at: https://www.youtube.com/watch?v=DfUm0RxXWxI. (Accessed 3 December 2022.)

82 Paletta, D. (2016.) 'The CIA's Venture-Capital Firm, Like Its Sponsor, Operates in the Shadows', *Wall Street Journal [online], 30 August. Available at:* https://www.wsj.com/articles/the-cias-venture-capital-firm-like-its-sponsor-operates-in-the-shadows-1472587352. (Accessed 2 December 2022.)

83 Cook, C.R. (2016.) 'DIUx: Capturing Technological Innovation', *The RAND Blog* [online], 23 November. Available at: https://www.rand.org/blog/2016/11/diux-capturing-technological-innovation.html. (Accessed 1 December 2022.)

84 Schachtman, N. (2010.) 'Google, CIA Invest in "Future" of Web Monitoring', *Wired* [online], July 28. Available at: https://www.wired.com/2010/07/exclusive-google-cia/. (Accessed 3 December 2022.)

85 Levine, Y. (2018.) 'Google Earth: How the Tech Giant is Helping the State Spy on Us', *The Guardian* [online], 20 December. Available at: https://www.theguardian.com/news/2018/dec/20/googles-earth-how-the-tech-giant-is-helping-the-state-spy-on-us. (Accessed 8 December 2022.)

86 Kehualani Goo, S. and A. Klein. (2007.) 'Google Makes Its Pitch to Expand Federal Business', *Washington Post* [online], 28 February. Available at: https://www.washingtonpost.com/archive/business/2007/02/28/google-makes-its-pitch-to-expand-federal-business/7d045b92-a5bb-44eb-bd6e-c85355210caf/. (Accessed 10 December 2022.)

87 Szoldra, P. (2016.) '14 Cutting Edge Firms Funded by the CIA', *Business Insider* [online], 21 September. Available at: https://www.businessinsider.com/companies-funded-by-cia-2016-9. (Accessed 12 December 2022.)

88 Fang, L. (2016.) 'The CIA Is Investing in Firms that Mine Your Tweets and Instagram Photos', *The Intercept* [online], 14 April. Available at: https://theintercept.com/2016/04/14/in-undisclosed-cia-investments-social-media-mining-looms-large/. (Accessed 10 December 2022.)

89 Wang, Maya. (2019.) 'China's Algorithms of Oppression', *Human Rights Watch Report* [online], 1 May. Available at: https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass. (Accessed 15 December 2022.)

90 Work, R.O. (2017). Official US government memorandum, 26 April. Available at https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf. (Accessed 15 December 2022.)

91 Allen, G.C. (2017.) 'Project Maven Brings AI to the Fight against ISIS', *Bulletin of the Atomic Scientists [online], 21 December. Available at:* https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/. (Accessed 13 December 2022.)

92 Ibid.

93 Pellerin, C. (2017.) 'Project Maven to Deploy Computer Algorithms to War Zone by Year's End', *DOD News* [online], 21 July. Available at: https://www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/. (Accessed 12 December 2022.)

94 Conger, K. (2018.) 'The Pentagon's Controversial Drone AI-Imaging Project Extends beyond Google', *Gizmodo* [online], 21 May. Available at: https://gizmodo.com/the-pentagons-controversial-drone-ai-imaging-project-ex-1826046321. (Accessed 20 December 2022.)

95 Statt, N. (2018.) 'Google Reportedly Leaving Project Maven Military AI Program after 2019', *The Verge* [online], 1 June. Available at: https://www.theverge.com/2018/6/1/17418406/google-maven-drone-imagery-ai-contract-expire. (Accessed 21 December 2022.)

96 Conger, K. (2018.) Google Plans Not to Renew Its Contract for Project Maven', *Gizmodo* [online], 1 June. Available at https://gizmodo.com/google-plans-not-to-renew-its-contract-for-project-mave-1826488620.

97 Ibid.

98 Conger, K. (2018.) 'Google Employees Resign in Protest against Pentagon Contract', *Gizmodo* [online], 14 May. Available at: https://gizmodo.com/google-employees-resign-in-protest-against-pentagon-con-1825729300.

99 Ibid.

100 Pichar, S. (2018.) 'AI at Google: Our Principles', *Google Blog* [online], 7 June. Available at: https://blog.google/technology/ai/ai-principles/. (Accessed 10 December 2022.)

101 Fang, L. (2019.) 'Defense Tech Startup Founded by Trump's Most Prominent Silicon Valley Supporters Win Secretive Military AI Contract', *The Intercept* [online], 9 March. Available at: https://theintercept.com/2019/03/09/anduril-industries-project-maven-palmer-luckey/. (Accessed 11 December 2022.)

102 Tech Inquiry (2021.) 'Easy as PAI' [online report], 10 September. Available at: https://techinquiry.org/EasyAsPAI/resources/EasyAsPAI.pdf. (Accessed 30 August 2022.)

103 Kelly, M. (2018.) 'Microsoft Secures $480 Million HoloLens Contract from US Army', *The Verge* [online], 28 November. Available at: https://www.theverge.com/2018/11/28/18116939/microsoft-army-hololens-480-million-contract-magic-leap. (Accessed 29 November 2022.)

104 Lecher, C. (2019.) 'Microsoft Workers' Letter Demands Company Drop Army HoloLens Contract', *The Verge* [online], 22 February. Available at: https://www.theverge.com/2019/2/22/18236116/microsoft-hololens-army-contract-workers-letter. (Accessed 4 December 2022.)

105 Riley, C. and S. Burke (2019.) 'Microsoft CEO Defends US Military Contract That Some Employees Say Crosses a Line', *CNN* [online], 25 February. Available at: https://www.cnn.com/2019/02/25/tech/augmented-reality-microsoft-us-military/index.html. (Accessed 5 December 2022.)

106 Conger, K. (2018.) 'Amazon Workers Demand Jeff Bezos Cancel Face Recognition Contracts with Law Enforcement', *Gizmodo* [online], 21 June. https://gizmodo.com/amazon-workers-demand-jeff-bezos-cancel-face-recognitio-1827037509. (Accessed 10 December 2022.)

107 Leskin, P. (2018.) 'Amazon Employees Are Reportedly Gearing Up to Confront CEO Jeff Bezos at an All-Staff Meeting This Week about Selling Facial Recognition Software to Law Enforcement', *Business Insider* [online], 6 November. Available at: https://www.businessinsider.com/amazon-workers-confront-jeff-bezos-facial-recognition-software-2018-11. (Accessed 3 December 2022.)

108 Keane, T. (2021.) 'Azure Government Top Secret Now Generally Available for US National Security Missions', *Microsoft Azure Blog* [online], 16 August. Available at: https://azure.microsoft.com/en-us/blog/azure-government-top-secret-now-generally-available-for-us-national-security-missions/. (Accessed 29 December 2022.)

109 Oracle (2023.) 'Oracle Cloud for the Defense Department', *Oracle website* [online], n.d. Available at: https://www.oracle.com/industries/government/us-defense/. (Accessed 29 March 2023.)

110 Amazon Web Services. (2018.) 'Amazon Web Services for the Warfighter' [online video], 9 August. Available at: https://www.youtube.com/watch?v=HHbBizyTet4. (Accessed 22 December 2022.)

111 Price, D. dual use

112 O'Mara, M. (2018.) 'Silicon Valley Can't Escape the Business of War', *New York Times* [online], 26 October. Available at: https://www.nytimes.com/2018/10/26/opinion/amazon-bezos-pentagon-hq2.html. (Accessed 22 December 2022.)

113 Tucker, P. (2015.) 'How US Special Forces Uses Google Maps', *Defense One* [online], 7 January. Available at: https://www.defenseone.com/technology/2015/01/how-us-special-forces-uses-google-maps/102396/. (Accessed 20 December 2022.)

114 O'Mara, M. (2018.) 'Silicon Valley Can't Escape the Business of War', *New York Times* [online], 26 October. Available at: https://www.nytimes.com/2018/10/26/opinion/amazon-bezos-pentagon-hq2.html. (Accessed 22 December 2022.)

115 Heinrich, T. (2002.) 'Cold War Armory: Military Contracting in Silicon Valley', *Enterprise & Society 3(2), 247-284. Available at:* https://www.jstor.org/stable/23699688. (Accessed 25 November 2022.)

116 Poulson, J. (2019.) Personal communication, 19 June.

117 We use 'migrant(s)' to refer to people on the move without differentiating between refugees, asylum seekers or economic migrants.

118 Cáceres, G. and Gressier, R. (2021, 14 May) 'Sting operation against migrant caravan arrests working-class migrants as human traffickers', *El Faro*. https://elfaro.net/en/202105/el_salvador/25479/Sting-Operation-against-Migrant-Caravan-Arrests-Working

119 Johnson, R. (2021, 15 January) 'Aplaudo a las autoridades salvadoreñas que están tomando acción contra quienes quieren engañar a los ciudadanos con caravanas y promesas falsas Solo promueven #UnViajeEnVano', Twitter. https://twitter.com/FGR_SV/status/1350133335549501443

120 de Goede, M. and Westermeier, C. (2022) 'Infrastructural geopolitics'. *International Studies Quarterly*, 66(3): 1–12. http://dx.doi.org/10.1093/isq/sqac033.

121 Muñiz, A. (2022) *Borderland Circuitry: Immigration surveillance in the United States and beyond*. Oakland, CA: University of California Press; see also Mijente, Immigrant Defense Project, NIPNLG (2018) 'Who's behind ICE'. https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling-Deportations_v4.pdf

122 This lens also enables us to emphasise the connection to historical antecedents such as physical transit and trade infrastructure 'modernisation' projects, where the link to state violence is indisputable (e.g. railway construction projects and genocide of indigenous peoples in Sonora from 1880 to the 1900s). See Guidotti-Hernández, N. (2011) *Unspeakable Violence: remapping U.S. and Mexican national imaginaries.* Durham, NC & London: Duke University Press. We emphasise that this scale is no departure from the racialised logics that have defined border practices in this region for decades. See Rosas, G. (2006) 'The managed violences of the borderlands: treacherous geographies, policeability, and the politics of race'. *Latino Studies*, 4(4): 401–418. https://doi.org/10.1057/palgrave.lst.8600221

123 See, for example, Shivkumar, G., O'Neil, K. and Nordhaug, L. (2021, 30 August) 'How to bring digital inclusion to the people who need it most'. https://www.weforum.org/agenda/2021/08/4-reasons-you-should-care-about-digital-public-infrastructure/ ('[Digital Public Infrastructure (DPI)] refers to digital solutions that enable basic functions essential for public and private service delivery, i.e. collaboration, commerce, and governance. Think about our existing shared public infrastructure such as roads and education, but online: that's DPI in a nutshell'); Masiero, S. and Arvidsson, V. (2021) 'Degenerative outcomes of digital identity platforms for development'. *Information Systems Journal*, 31(6): 903–928. https://doi.org/10.1111/isj.12351; Massally, K. and Frankenhauser, C. (2022, 3 August) 'The right way to build digital public infrastructure: 5 insights'. https://www.weforum.org/agenda/2022/08/digital-public-infrastructure/

124 Aizeki, M., et al (2021) *Smart Borders or A Humane World*, https://www.tni.org/en/publication/smart-borders-or-a-humane-world

125 Andersson, R. (2018) *Illegality, Inc.: clandestine migration and the business of bordering Europe*. Oakland, CA: University of California Press, Miller, T. (2019), op. cit.; Akkerman, M. (2021) *Border Wars*. Amsterdam: Transnational Institute.

126 Paley, D. (2014) *Drug War Capitalism*. Oakland, CA: AK Press.

127 Miller, T. (2019) *Empire of Borders: The Expansion of the U.S. Border around the World*. London, New York: Verso.

128 Ibid, p. 177

129 Immigrant Defense Project, Mijente, and NIPNLG (2018), 'Who's Behind ICE: The Tech and Data Companies Fueling Deportations'. https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling-Deportations_v4.pdf

130 FOIA request 330020322000471 directed to the National Institute of Migration. https://r3d.mx/wp-content/uploads/Oficios-y-anexos-471.pdf.

131 Watch CBP Intel (2019) 'Central American Caravans and Migration Crisis Flow - Update 32'. U.S. Customs and Border Protection. https://r3d.mx/wp-content/uploads/Central-American-Caravans-and-Migration-Crisis-Flow-Update-32.pdf.

132 Meissner, D., Kerwin, D.M., Chisti, M. and Bergeron, C. (2013) *Immigration Enforcement in The United States: a formidable machinery*. Washington, DC: Migration Policy Institute. https://www.migrationpolicy.org/pubs/enforcementpillars.pdf.

133 Woodward, J. (2005) 'Using biometrics to achieve identity dominance in the Global War on Terrorism'. *Military Review*; see also Jacobsen, A. (2021) *First Platoon: a story of modern war in the age of identity dominance*. New York: Dutton.

134 Angel, A. (2020, 15 December) 'Población en cárceles crece a ritmo récord en 2020: hay 14 mil reos más que al inicio del año', Animal Políitico. https://www.animalpolitico.com/2020/12/poblacion-carceles-crece-record-2020/#:~:text=Mientras%20que%20en%20diciembre%20de,de%20que%20cometieron%20un%20delito

135 Romero, O.A. (2014, 10 February) 'La criminalización de la pobreza y el sistema de justicia penal', Información Sididh. http://centroprodh.org.mx/sididh_2_0_alfa/?p=31418

136 de Goede, M. & Westermeier, C. (2022), op. cit.

137 Woodward, J. (2005) 'Using biometrics to achieve identity dominance in the Global War on Terrorism'. *Military Review*. https://www.rand.org/pubs/reprints/RP1194.html; see also Jacobsen, A. (2021) op. cit.

138 Kwet, M. (2021), 'Digital Colonialism'. https://longreads.tni.org/digital-colonialism-the-evolution-of-us-empire

139 DHS Office of Inspector General (2021) 'CBP Targeted Americans Associated with the 2018–2019 Migrant Caravan'. https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-62-Sep21.pdf

140 LIS and R3D (2023 forthcoming) 'Uso de las tecnologías digitales en los contextos migratorios: necesidades, oportunidades y riesgos para el ejercicio de los derechos humanos de las personas migrantes, defensoras y periodistas'. www.r3d.mx/publicaciones.

141 Open Society Justice Initiative (2019), *Unmaking Americans: insecure citizenship in the United States,* p. 102. https://www.justiceinitiative.org/uploads/e05c542e-0db4-40cc-a3ed-2d73abcfd37f/unmaking-americans-insecure-citizenship-in-the-united-states-report-20190916.pdf

142 Chambers, S., Boyce, G., Launius, S. and Dinsmore, A. (2019) 'Mortality, surveillance and the tertiary "funnel effect" on the U.S.-Mexico border: a geospatial modeling of the geography of deterrence'. J*ournal of Borderlands Studies*, 36(3): 443–468. https://doi.org/10.1080/08865655.2019.157086

143 Muñiz, A. (2022), op. cit.

144 Rosas, G. (2006), op. cit.

145 Jacobsen, A. (2020), op. cit.

146 Guidotti-Hernandez, N. (2011) *Unspeakable Violence: Remapping U.S. and Mexican National Imaginaries*. Durham & London: Duke University Press. Woodward, J. (2005), op. cit.

147 Woodward, J. (2005), op. cit.

148 Muñiz, A. (2022), op. cit.; Rosas, G. (2006), op. cit; Khan, J. (2019) Islands of Sovereignty: Haitian migration and the borders of empire. Chicago: University of Chicago Press.

149 Rosas, G. (2006), op. cit.

150 McCoy, A. (2017) *In the Shadows of the American Century: The Rise and Decline of US Global Power*. Chicago: Haymarket Books.

151 Endnotes: Scheer, S. (2021). Israel signs cloud services deal with Amazon, Google. *Reuters*. [online] 24 May. Available at: https://www.reuters.com/technology/israel-signs-cloud-services-deal-with-amazon-google-2021-05-24/ [Accessed 20 Mar. 2023].

152 Fung, B. (2021). *Amazon Web Services disables cloud accounts linked to NSO Group | CNN Business*. [online] CNN. Available at: https://edition.cnn.com/2021/07/19/tech/amazon-nso-group-pegasus-cloud-accounts/index.html [Accessed 20 Mar. 2023].

153 Middle East Eye. (2021). *Meet Blue Wolf, the app Israel uses to spy on Palestinians in the occupied West Bank*. [online] Available at: https://www.middleeasteye.net/news/israel-whats-blue-wolf-app-soldiers-use-photograph-palestinians.

154 WhoProfits. (2021). *Hewlett Packard Enterprise (HPE)*. [online] Available at: https://www.whoprofits.org/company/hewlett-packard-enterprise-hpe/ [Accessed 20 Mar. 2023].

155 Investigate & Dismantle Apartheid. (2022). *Al Haq issues landmark report 'Israeli Apartheid: Tool of Zionist Settler-Colonialism'*. [online] Available at: https://antiapartheidmovement.net/updates/view/al-haq-issues-landmark-report-israeli-apartheid-tool-of-zionist-settler-colonialism/15 [Accessed 20 Mar. 2023].

156 Amnesty International. (2022). *Israel's apartheid against Palestinians*. [online] Amnesty International. Available at: https://www.amnesty.org/en/latest/campaigns/2022/02/israels-system-of-apartheid/.

157 Stop The Wall. (n.d.). *Digital Walls*. [online] Available at: https://stopthewall.org/digitalwalls/ [Accessed 20 Mar. 2023].

158 Stop The Wall. (n.d.). *Digital Walls*. [online] Available at: https://stopthewall.org/digitalwalls/#militarization [Accessed 20 Mar. 2023].

159 Khan, A. (2021). Hidden Pentagon Records Reveal Patterns of Failure in Deadly Airstrikes. *The New York Times*. [online] 18 Dec. Available at: https://www.nytimes.com/interactive/2021/12/18/us/airstrikes-pentagon-records-civilian-deaths.html.

160 Brewster, T. (2021). *Project Maven: Amazon And Microsoft Scored $50 Million In Pentagon Surveillance Contracts After Google Quit*. [online] Forbes. Available at: https://www.forbes.com/sites/thomasbrewster/2021/09/08/project-maven-amazon-and-microsoft-get-50-million-in-pentagon-drone-surveillance-contracts-after-google/?sh=549483dc6f1e [Accessed 20 Mar. 2023].

161 Strout, N. (2022). *Intelligence agency takes over Project Maven, the Pentagon's signature AI scheme*. [online] C4ISRNet. Available at: https://www.c4isrnet.com/intel-geoint/2022/04/27/intelligence-agency-takes-over-project-maven-the-pentagons-signature-ai-scheme/.

162 Big Tech Sells War. *Big Tech Sells War - How Big Tech Sells War on our Communities*. [online] Available at: https://bigtechsellswar.com/ [Accessed 20 Mar. 2023].

163 Big Tech Sells War. *Big Tech Sells War - How Big Tech Sells War on our Communities*. [online] Available at: https://bigtechsellswar.com/#timelines-home [Accessed 20 Mar. 2023].

164 Nextgov.com. (2021). *NSA Awards Secret $10 Billion Contract to Amazon*. [online] Available at: https://www.nextgov.com/it-modernization/2021/08/nsa-awards-secret-10-billion-contract-amazon/184390/.

165 www.theregister.com. (2022). *$10b US defense cloud contract re-awarded to AWS*. [online] Available at: https://www.theregister.com/2022/04/28/nsa_wands_aws/.

166 Novet, J. (2021). *Microsoft wins U.S. Army contract for augmented reality headsets, worth up to $21.9 billion over 10 years*. [online] CNBC. Available at: https://www.cnbc.com/2021/03/31/microsoft-wins-contract-to-make-modified-hololens-for-us-army.html.

167 Israel Innovation. *Attack is the Best Form of Defense*. [online] Available at: https://innovationisrael.org.il/en/reportchapter/attack-best-form-defense [Accessed 20 Mar. 2023].

168 Mondoweiss. (2014). *Israel surveils and blackmails gay Palestinians to make them informants*. [online] Available at: https://mondoweiss.net/2014/09/blackmails-palestinian-informants/ [Accessed 20 Mar. 2023].

169 Abukhater, J. (2022). *Under Israeli surveillance: Living in dystopia, in Palestine*. [online] www.aljazeera.com. Available at: https://www.aljazeera.com/opinions/2022/4/13/under-israeli-surveillance-living-in-dystopia-in-palestine.

170 Alys Samson Estapé. (2021). *Israel: the model coercive state* and why boycotting it is key to emancipation everywhere [online] Available at: https://longreads.tni.org/stateofpower/israel-the-model-coercive-state [Accessed 20 Mar. 2023].

171 VentureBeat. (2015). *Microsoft confirms it has acquired cloud security platform Adallom*. [online] Available at: https://venturebeat.com/business/microsoft-confirms-it-has-acquired-cloud-security-platform-adallom/ [Accessed 21 Mar. 2023].

172 Lunden, I. (2017). *Microsoft to buy Israeli security firm Hexadite, sources say for $100M*. [online] TechCrunch. Available at: https://techcrunch.com/2017/06/08/microsoft-confirms-its-acquired-hexadite-sources-say-for-100m/?guccounter=2 [Accessed 21 Mar. 2023].

173 Algemeiner, T. (2021). *Unit 81: The Elite Military Unit That Caused a Big Bang in the Israeli Tech Scene - Algemeiner. com*. [online] www.algemeiner.com. Available at: https://www.algemeiner.com/2021/01/08/unit-81-the-elite-military-unit-that-caused-a-big-bang-in-the-israeli-tech-scene/ [Accessed 21 Mar. 2023].

174 Scheer, S. (2022). Google activates Israel's first local cloud region. *Reuters*. [online] 20 Oct. Available at: https://www.reuters.com/technology/google-activates-israels-first-local-cloud-region-2022-10-20/ [Accessed 21 Mar. 2023].

175 notechforice.com. *About | #NoTechForICE*. [online] Available at: https://notechforice.com/about/ [Accessed 21 Mar. 2023].

176 7amleh, the Arab Center for Social Media Development (2021). *#Hashtag Palestine 2021*. [online] Available at: https://7amleh.org/storage/Hashtag%202021%20EN.pdf

177 Statt, N. (2018). *Google reportedly leaving Project Maven military AI program after 2019*. [online] The Verge. Available at: https://www.theverge.com/2018/6/1/17418406/google-maven-drone-imagery-ai-contract-expire.

178 Kantor, J., Weise, K. and Ashford, G. (2021). The Amazon That Customers Don't See. *The New York Times*. [online] 15 Jun. Available at: https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html

179 Couldry, N. & Mejias, U. (2019b) Making data colonialism liveable: How might data's social order be regulated? Internet Policy Review, 8(2). https://doi.org/10.14763/2019.2.1411

180 Viljoen, S. (2021) A relational theory of data governance. The Yale Law Journal, 131(2): 370–781. https://www.yalelawjournal.org/feature/a-relational-theory-of-data-governance

181 Polanyi, K. (1957 [1944]) The Great Transformation: The political and economic origins of our time. Boston, MA: Beacon Press.

182 Fraser, N. (2014) Can society be commodities all the way down? Post-Polanyian reflections on capitalist crisis. Economy and Society, 43(3): 541–558. https://doi.org/10.1080/03085147.2014.898822

183 Bhambra, G. K. (2021) Colonial global economy: Towards a theoretical reorientation of political economy. Review of International Political Economy, 28(2): 307–322. https://doi.org/10.1080/09692290.2020.1830831

184 Ashiagbor, D. (2021) Race and colonialism in the construction of labour markets and precarity. Industrial Law Journal, 50(4): 1–26. https://doi.org/10.1093/indlaw/dwab020

185 Beckert, S. & Rockman, S. (eds.) (2016) Slavery's Capitalism: A new history of American economic development. Philadelphia, PA: University of Pennsylvania Press; Berry, D. R. (2017) The Price for Their Pound of Flesh: The value of the enslaved, from womb to grave, in the building of a nation. Boston, MA: Beacon Press.

186 Fraser (2014).

187 Polanyi (1957), p.54.

188 Ensmenger, N. (2018) The environmental history of computing. Technology and Cutlure, 59(4): S7–S33. https://doi.org/10.1353/tech.2018.0148

189 Mazzucato, M. (2013) The Entrepreneurial State: Debunking public vs. private sector myths. London. Anthem Press.

190 Peters, B. (2016) How Not to Network a Nation: The uneasy history of the Soviet internet. Cambridge, MA: MIT Press.

191 Medina, E. (2011) Cybernetic Revolutionaries: Technology and politics in Allende's Chile. Cambridge, MA: MIT Press.

192 Levine, Y. (2018) Surveillance Valley: The secret military history of the internet. New York: Public Affairs.

193 Staab, P. (2019) Digitaler Kapitalismus. Berlin: Suhrkamp.

194 Crain, M. (2021) Profit over Privacy. How surveillance advertising conquered the internet. Minneapolis, MN: University of Minnesota Press.

195 Levine (2018).

196 Haggart, B. (2018) 'The government's role in constructing the data-driven economy', Center for International Governance Innovation [online]. https://www.cigionline.org/articles/governments-role-constructing-data-driven-economy/

197 Starosielski, N. (2015) The Undersea Network. London: Duke University Press.

198 Tully, J. (2009) A Victorian ecological disaster: Imperialism, the telegraph, and gutta-percha. Journal of World History, 20(4): 559–579. https://www.jstor.org/stable/40542850

199 Blum, A. and Baraka, C. (2022, 10 May) 'Sea change', Rest of World [online]. https://restofworld.org/2022/google-meta-underwater-cables/

200 [Al Jazeera English] (2019) Is Big Tech colonising the internet? | All Hail The Algorithm, YouTube [online]. https://www.youtube.com/watch?v=_fC7acShZkg

201 Global Witness (2022) A deadly decade for land and environmental activists—with a killing every two days [online]. https://www.globalwitness.org/en/press-releases/deadly-decade-land-and-environmental-activists-killing-every-two-days/

202 Ross, C. (2014) The tin frontier: Mining, empire, and environment in Southeast Asia, 1870s—1930s. Environmental History, 19: 454–479. http://dx.doi.org/10.1093/envhis/emu032

203 Friends of the Earth (2012) Mining for smartphones: The true cost of tin [online]. https://www.foe.co.uk/sites/default/files/downloads/tin_mining.pdf; Simpson, C. (2012, 24 August) 'The deadly tin inside your smartphone', Bloomberg [online]. https://www.bloomberg.com/news/articles/2012-08-23/the-deadly-tin-inside-your-smartphone

204 Zhong, R. and Chang Chien, A. (2021, 8 April) 'Drought in Taiwan pits chip makers against farmers', The New York Times [online]. https://www.nytimes.com/2021/04/08/technology/taiwan-drought-tsmc-semiconductors.html

205 Gaydos, E. (2019) In the shadow of big blue: The birthplace of IBM is struggling to live in its shadow. Logic, 9 [online]. https://logicmag.io/nature/in-the-shadow-of-big-blue/

206 Hogan, M. (2015) Data flows and water woes: The Utah data center. Big Data & Society, 2(2). https://doi.org/10.1177/2053951715592429

207 Adjei, A. (2014, 19 April) 'Life in Sodom and Gomorrah: The world's largest digital dump', The Guardian [online]. https://www.theguardian.com/global-development-professionals-network/2014/apr/29/agbogbloshie-accra-ghana-largest-ewaste-dump

208 Bauman, Z. (2004) Wasted Lives: Modernity and its outcasts. Cambridge: Polity.

209 Dwoskin, E., Whlen, J. and Cabato, R. (2019, 25 July) 'Content moderators at YouTube, Facebook and Twitter see the worst of the web—and suffer silently', The Washington Post [online]. https://www.washingtonpost.com/technology/2019/07/25/social-media-companies-are-outsourcing-their-dirty-work-philippines-generation-workers-is-paying-price/; Elliott, V. and Tekendra, P. (2020, 22 July) 'The despair and darkness of people will get to you', Rest of World [online]. https://restofworld.org/2020/facebook-international-content-moderators/

210 Couldry, N. and Mejias, U. (2019a) The Cost of Connection: How data is colonizing human life and appropriating it for capitalism. Stanford, CA: Stanford University Press, p. 5, emphasis original.

211 Ibid., p. 117.

212 Boyd, d. and Crawford, K. (2012) Critical questions for big data. Information, Communication & Society, 15(5): 662– 679. https://doi.org/10.1080/1369118X.2012.678878

213 Cohen, J. E. (2019) Between Truth and Power: The legal constructions of informational capitalism. Oxford: Oxford University Press.

214 Viljoen (2021).

215 Micheli, M., Ponti, M., Craglia, M. and Suman, A. (2020) Emerging models of data governance in the age of datafication, Big Data & Society, 7(2). https://doi.org/10.1177/2053951720948087

216 Sadowski, J., Viljoen, V. and Whittaker, M. (2021) Everyone should decide how their digital data are used—not just tech companies. Nature, 595: 169–171. https://doi.org/10.1038/d41586-021-01812-3

217 Bria, F. (2018) A new deal on data, in McDonnell, J. (ed.) Economics for the many, London: Verso, pp. 164– 171; Hind, D. (2019, 20 September) The British digital cooperative: A new model public sector institution. Common Wealth [online]. https://www.common-wealth.co.uk/reports/the-british-digital-cooperative-a-new-model-public-sector-institution; Delacroix, S. and Lawrence, N. D. (2019) Bottom-up data trusts: Disturbing the 'one size fits all' approach to data governance. International Data Privacy Law, 9(4): 236–252. https://doi.org/10.1093/idpl/ipz014; Sadowski, Viljoen and Whittaker (2021).

218 Beraldo, D. and Milan, S. (2019) From data politics to the contentious politics of data. Big Data & Society, 6(2). https://doi.org/10.1177/2053951719885967

219 Piasna, A. and Zwysten, W. (2022) New wine in old bottles; organizing and collective bargaining in the platform economy. International Journal of Labour Research, 11(1-2): 36-46. [online]. https://www.ilo.org/actrav/international-journal-labour-research/WCMS_856837/lang--en/index.htm; Qadri, R. and Raval, N. (2021) Mutual aid stations. Logic 13 [online]. https://logicmag.io/distribution/mutual-aid-stations/

220 Kwet, M. (2022) The digital tech deal: A socialist framework for the twenty-first century. Race and Class, 63(3): 63–84. https://doi.org/10.1177/03063968211064478

221 Hickel, J. and Kallis, G. (2019) Is green growth possible? New Political Economy, 25(4): 469–486. https://doi.org/10.1080/13563467.2019.1598964

222 Internet Archive (2021) Available at: https://archive.org/details/the-wizard-of-oz-1080p. (Accessed 13 March 2023).

223 'Alan Turing' (2023) *Wikipedia, the Free Encyclopaedia.* Available at: https://en.wikipedia.org/wiki/Alan_Turing (Accessed 13 March 2023).

224 'Hal 9000' (2023) *Wikipedia, the Free Encyclopaedia.* Available at: https://en.wikipedia.org/wiki/HAL_9000 (Accessed 13 March 2023).

225 Página12 (2018) *La inteligencia artificial de Urtubey.* Available at: https://www.pagina12.com.ar/107412-la-inteligencia-artificial-de-urtube (Accessed 13 March 2023)

226 Microsoft News Center LATAM (2017) Microsoft y el gobierno de Salta firman un acuerdo para aplicar la inteligencia artificial en la prevención de los problemas más urgentes. Available at: https://news.microsoft.com/es-xl/microsoft-gobierno-salta-firman-acuerdo-aplicar-la-inteligencia-artificial-la-prevencion-los-problemas-mas-urgentes/ (Accessed 13 March 2023)

227 Perfil (2018) Albino dijo que el preservativo no protege porque "el virus del SIDA atraviesa la porcelana" Available at: https://www.perfil.com/noticias/politica/albino-dijo-que-el-preservativo-no-protege-del-vih-porque-atraviesa-la-porcelana.phtml (Accessed 13 March 2023)

228 Alonso, A. (2018) Microsoft democratiza la IA y los servicios cognitivos, It.sitio, 28 March. Available at: https://www.itsitio.com/es/microsoft-democratiza-la-ia-y-los-servicios-cognitivos/ (Accessed 13 March 2023)

229 'Deep neural networks' (2023) *Wikipedia, the Free Encyclopaedia.* Available at: https://en.wikipedia.org/wiki/Deep_learning#Deep_neural_networks (Accessed 13 March 2023).

230 'Bayesian networks' (2023) *Wikipedia, the Free Encyclopaedia.* Available at: https://en.wikipedia.org/wiki/Bayesian_networks (Accessed 13 March 2023).

231 'Markov chains' (2023) Wikipedia, the Free Encyclopaedia. Available at: https://en.wikipedia.org/wiki/Markov_chains (Accessed 13 March 2023).

232 Brunet, P., Font, T., Rodríguez, J. (2022) Robots asesinos: 18 preguntas y respuestas. Available at: https://centredelas.org/publicacions/robots-asesinos-18-preguntas-y-respuestas/?lang=es (Downloaded 13 March 2023).

233 Eubanks, V. (2018) Automating Inequality; How high-tech tools profile, police and punish the poor. New York: St Martin's Press.

234 Ortiz Freuler, J. and Iglesias, C. (2018) Algoritmos e Inteligencia Artificial en Latinoamérica: Un Estudio de implementaciones por parte de Gobiernos en Argentina y Uruguay. World Wide Web Foundation. Available at: https://webfoundation.org/docs/2018/09/WF_AI-in-LA_Report_Spanish_Screen_AW.pdf (Accessed 13 March 2023)

235 Laboratorio de Inteligencia Artificial Aplicada (2018) Sobre la predicción automática de embarazos adolescentes. Available at: https://liaa.dc.uba.ar/es/sobre-la-prediccion-automatica-de-embarazos-adolescentes/

236 Barron, K., Kung, E., and Proserpio, D. (2020) 'The effect of home-sharing on house prices and rents: Evidence from Airbnb'. *Marketing Science* 40(1):23–47. https://ssrn.com/abstract=3006832

237 Bernardi, M. (2 October 2018) 'The impact of AirBnB on our cities: Gentrification and 'disneyfication' 2.0'. *The Urban Media Lab*. https://labgov.city/theurbanmedialab/the-impact-of-airbnb-on-our-cities-gentrification-and-disneyfication-2-0/

238 Griffith, E. (2020, 10 December) 'Airbnb tops $100 billion on first day of trading'. *The New York Times.* https://www.nytimes.com/2020/12/10/technology/airbnb-tops-100-billion-on-first-day-of-trading-reviving-talk-of-a-bubble.html

239 Airbnb, Inc. (2021, 11 February) 'Annual Report for the fiscal year ended Dec. 31, 2020.' Form 10-K, United States Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1559720/000155972021000010/airbnb-10k.htm

240 Tang, D. (2022, 5 January) 'WIPO: the IP Office of the future'. *World Trademark Review*. https://www.worldtrademarkreview.com/report/special-reports/q4-2021/article/wipo-the-ip-office-of-the-future

241 WIPO. (2017) *World Intellectual Property Report 2017: Intangible capital in global value chains*. Geneva: World Intellectual Property Organization. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_944_2017.pdf

242 WIPO. (2021) *IP for the Good of Everyone: Report of the Director General to the 2021 WIPO Assemblies*. Geneva: World Intellectual Property Organization. https://www.wipo.int/dg-report/2021/en/

243 Patent Progress. 'Too Many Patents'. https://www.patentprogress.org/systemic-problems/too-many-patents/

244 Boyle, J. (2008) *The Public Domain: Enclosing the commons of the mind*. New Haven & London: Yale University Press. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=5385&context=faculty_scholarship

245 Blumberg A. and Sydell L. (2011, 22 July) 'When Patents Attack'. *This American Life* [Podcast]. https://www.npr.org/sections/money/2011/07/26/138576167/when-patents-attack

246 Owles, E. (2017, 22 June) 'The making of Martin Shkreli as "pharma bro"'. *The New York Times*. https://www.nytimes.com/2017/06/22/business/dealbook/martin-shkreli-pharma-bro-drug-prices.html

247 Gilmore, R. W. (2020, 10 June) 'What are we talking about when we talk about "a police-free future"?' MDP150. https://www.mpd150.com/what-are-we-talking-about-when-we-talk-about-a-police-free-future/

248 Duda. J. (2017, 9 November) 'Towards the horizon of abolition: A conversation with Mariame Kaba'. *The Next System Project.* https://thenextsystem.org/learn/stories/towards-horizon-abolition-conversation-mariame-kaba

249 International Network of Civil Liberties Organizations. (2013) '"Take back the streets": Repression and criminalization of protest around the world'. https://www.aclu.org/sites/default/files/field_document/global_protest_suppression_report_inclo.pdf

250 Critical Resistance. 'What is the PIC? What is Abolition?' https://criticalresistance.org/mission-vision/not-so-common-language/

251 Brown, A. (2020, 15 November) 'In the mercenaries' own words: Documents detail TigerSwan infiltration of Standing Rock'. *The Intercept*. https://theintercept.com/2020/11/15/standing-rock-tigerswan-infiltrator-documents/

252 Mural Arts Philadelphia. *Standing Rock: Decolonizing Creative Practice in the Environmental Justice Movement*. [online video]. https://www.youtube.com/watch?v=z5A2Xf5B7Lc

253 Cadena-Roa, J. and Puga, C. (2021) 'Protest and Performativity', in S. Rai, M. Gluhovic, S. Jestrovic and M. Saward (eds.) *The Oxford Handbook of Politics and Performance*. New York: Oxford University Press, pp. 101–116.

254 Reuters. (2019, 4 January) 'Basra youth adopt new tactic for peaceful protest'. https://uk.movies.yahoo.com/basra-youth-adopt-tactic-peaceful-131430647.html

255 Brown, M. (2015, 3 September) 'Activists plan oil protest at British Museum'. *The Guardian.* https://www.theguardian.com/culture/2015/sep/03/art-not-oil-plan-protest-british-museum

256 Haiven, M. (2017) 'Monsters of the Financialized Imagination: From Pokémon to Trump', in N. Buxton and D. Eade (eds.) *State of Power 2017*. Amsterdam: Transnational Institute. http://longreads.tni.org/state-of-power/age-of-monsters/

257 WIPO. (2022) *The Role of Border Measures in IP Enforcement.* Geneva: World Intellectual Property Organization. https://www.wipo.int/meetings/en/details.jsp?meeting_id=72168

258 Kelly, A. (2019, 16 December) 'Apple and Google named in US lawsuit over Congolese child cobalt mining deaths'. *The Guardian.* https://www.theguardian.com/global-development/2019/dec/16/apple-and-google-named-in-us-lawsuit-over-congolese-child-cobalt-mining-deaths

259 Ochab, E. U. (2020, 13 January) 'Are These tech companies complicit in human rights abuses of child cobalt miners in Congo?' Centre de Ressources sur les Entreprises et les Droits de l'Homme. https://www.business-humanrights.org/fr/derni%C3%A8res-actualit%C3%A9s/are-these-tech-companies-complicit-in-human-rights-abuses-of-child-cobalt-miners-in-congo/

260 Vermeer, K. (2020, 21 September) 'Two sides of the same coin: How the pulp and paper industry is profiting from deforestation in the Amazon rainforest'. *Environmental Paper Network.* https://environmentalpaper.org/2020/09/two-sides-of-the-same-coin-how-the-pulp-and-paper-industry-is-profiting-from-deforestation-in-the-amazon-rainforest/

261 China Labor Watch. (2021, 13 December) 'Abuse in the printing supply chain: An investigation into two cartridge manufacturers'. *China Labor Watch.* https://chinalaborwatch.org/zh/abuse-in-the-printing-supply-chain-an-investigation-into-two-cartridge-manufacturers/

262 Ro, C. (2021, 11 February) 'Reducing the environmental toll of paper in the publishing industry'. *Book Riot*. https://bookriot.com/environmental-toll-of-paper-in-publishing/

263 Good Electronics. (2021, 25 March) 'Global South: The dumping ground for the world's electronics waste'. *Good Electronics*. https://goodelectronics.org/topic/health-safety/

264 Vats, A. and Keller, D. A. (2018) 'Critical Race IP'. *Cardozo Arts & Entertainment Law Journal*, 36(3).

https://scholarship.law.pitt.edu/fac_articles/512

265 Chander, A. and Sunder, M. (2004) 'The romance of the public domain'. *California Law Review*, 92:1331. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=562301

266 Electronic Frontier Foundation. 'Creativity and Innovation'. https://www.eff.org/issues/innovation

267 ILO. (2022, 12 September) '50 million people worldwide in modern slavery'. Geneva: International Labour Organization. https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_855019/lang--en/index.htm

268 Gilens, M. and Page, B. (2014, 18 September) 'Testing theories of American politics: Elites, interest groups, and average citizens'. *Perspectives on Politics*, 12(3): 564–581. https://doi.org/10.1017/S1537592714001595

269 Barnett, J. M. (2021) *Innovators, Firms, and Markets: The organizational logic of intellectual property*. New York: Oxford University Press. https://academic.oup.com/book/33492

270 Michel, P. R. (2022, 5 August) 'Big Tech has a patent violation problem'. *Harvard Business Review*. https://hbr.org/2022/08/big-tech-has-a-patent-violation-problem

271 Schiffner, C. (2022, 31 May) 'As tech giants push for IP reform, plaintiffs firms see new momentum for litigation'. *The National Law Journal*. https://www.law.com/nationallawjournal/2022/05/31/as-tech-giants-push-for-ip-reform-plaintiffs-firms-see-new-momentum-for-litigation/

272 Riekeles, G. (2022, 28 June) 'I saw first-hand how US tech giants seduced the EU—and undermined democracy'. *The Guardian*. https://www.theguardian.com/commentisfree/2022/jun/28/i-saw-first-hand-tech-giants-seduced-eu-google-meta

273 Pegoraro, R. (2015, 30 June) 'Why the tech industry hates patent trolls, and you should too'. *Yahoo Tech.* https://finance.yahoo.com/news/why-the-tech-industry-hates-patent-trolls-and-you-121628489339.html

274 https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices/

275 https://www.datadetoxkit.org/en/wellbeing/environment/

276 https://www.reuters.com/business/cop/facebook-climate-change-can-falsehoods-be-reined-2022-02-23/

277 https://www.globalwitness.org/en/campaigns/digital-threats/climate-divide-how-facebooks-algorithm-amplifies-climate-disinformation/

278 https://www.theguardian.com/technology/2022/dec/02/climate-change-denialism-flooding-twitter-scientists

279 https://www.theguardian.com/technology/2022/dec/02/climate-change-denialism-flooding-twitter-scientists

280 https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2021/how-and-why-do-consumers-access-news-social-media ; https://www.freepress.net/sites/default/files/2022-11/stop_toxic_twitter_coalition_open_letter_to_twitter_final.pdf

281 https://secure.avaaz.org/campaign/en/youtube_climate_misinformation/

282 https://secure.avaaz.org/campaign/en/detox_the_algorithm_loc/

283 https://secure.avaaz.org/campaign/en/detox_the_algorithm_loc/

284 https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy ; https://www.live5news.com/story/10860187/hackers-attack-twitter-facebook-also-slows-down/

285 https://techmonitor.ai/technology/cybersecurity/the-return-of-hacktivists

286 https://techmonitor.ai/technology/cybersecurity/the-return-of-hacktivists

287 https://www.nytimes.com/2020/06/09/nyregion/exxon-mobil-hackers-greenpeace.html

288 https://riseup.net/

289 Rucht D. (2004). "'The quadruple 'A': mMedia strategies of protest movements since the 1960s', in." In W.Van De Donk, B. D. Loader, P. G. Nixon and D. Rucht (eds) *Cyberprotest: New media, citizens and social movements*, pp.eds. Van De Donk Wim, Loader Brian D., Nixon Paul G., Rucht Dieter, 25–48. London, England: Routledge.

290 https://techcrunch.com/2016/10/15/multi-media-journalists-face-jail-time-for-reporting-on-north-dakota-pipeline-protest/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGHZ8r3PFUD0h5BYi7TYQ-_-A8TMriPAiEkmwNz0SI6xv_VXjtIRjXOPfQkeQi9NZaotuw4g9LDe5fzkwPoHO7qGa-JtJqcDcPvfmeAs1TvoX40QrO_9HJyE0tullkIgRO3IH5SIGKNUChzcBfk0fGhbZZHs9jmxOp00H60aUANV

291 https://unicornriot.ninja/tag/standing-rock/

292 https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2022/how-people-access-and-think-about-climate-change-news

293 The tar sands mobilisations were protests against the building of pipelines carrying tar-sands in Canada in 2014. Tar sands are low quality oil whose extraction and processing tends to be more environmentally hazardous. In the tar sands mobilisations, environmental groups were joined by First Nations protesters. Idle No More was a key group behind the organisation of protests.

294 The Ferguson protests were a key event in the Black Lives Matter movement. They emerged in Ferguson, Misouri after the killing of Michael Brown by police in August 2014.

295 https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2022/how-people-access-and-think-about-climate-change-news

296 https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2022/how-people-access-and-think-about-climate-change-news

297 Martini, M. (2018) 'Online distant witnessing and live-streaming activism: emerging differences in the activation of networked publics'. *New Media & Society*, 20(11): 4035–4055.

298 Kavada, A. and Specht, D. (2022) 'Environmental movements and digital media', in M. Grasso and M. Guigni (eds) *Routledge Handbook of Environmental Movements*. New York: Routledge.

299 https://www.washingtonpost.com/business/2021/07/30/greentrolling-big-oil-greenwashing/

300 https://www.washingtonpost.com/business/2021/07/30/greentrolling-big-oil-greenwashing/

301 https://juststopoil.org/background/

302 Askanius, T. (2012) *Radical online video: YouTube, video activism and social movement media practices*, Doctoral thesis, Lund Studies in Media and Communication 17, Lund University.

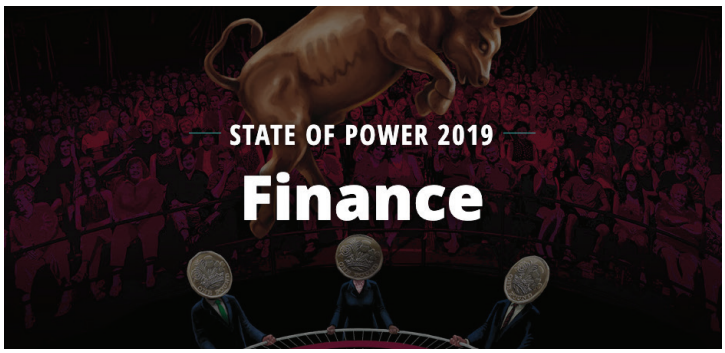
303 Wright, E. O. (2019) *How to be an anti-capitalist in the 21st century.* London: Verso. Books

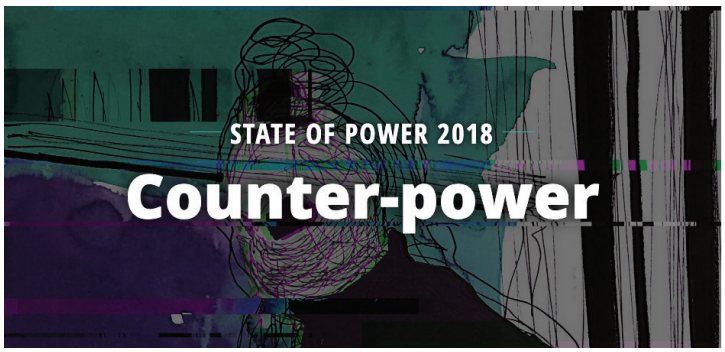
304 Uldam, J. (2018). 'Social media visibility: challenges to activism'. *Media, Culture & Society*, 40(1): 41–58. https://doi.org/10.1177/0163443717704997

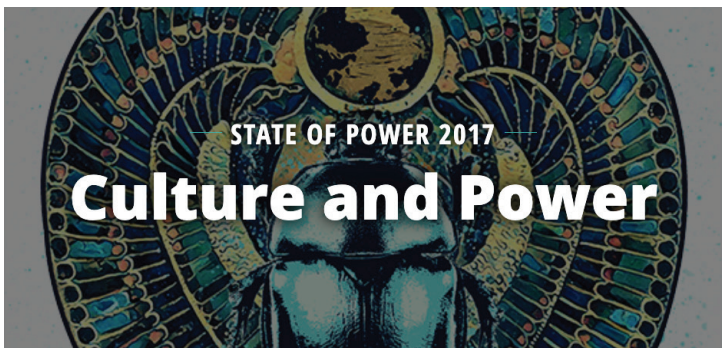
305 https://tacticaltech.org/projects/data-detox-kit/

Previous State of Power editions

tni.org/en/topic/state-of-power







Big Tech has concentrated vast economic power with the collusion of states, which has resulted in expanded surveillance, spiraling disinformation and weakened workers' rights. TNI's 11th flagship State of Power report exposes the actors, the strategies and the implications of this digital power grab, and shares ideas on how movements might bring technology back under popular control.

The Transnational Institute (TNI) is an international research and advocacy institute committed to building a just, democratic and sustainable planet. For more than 40 years, TNI has served as a unique nexus between social movements, engaged scholars and policy makers.

www.TNI.org