Seizing the means of computation

How popular movements can topple Big Tech monopolies
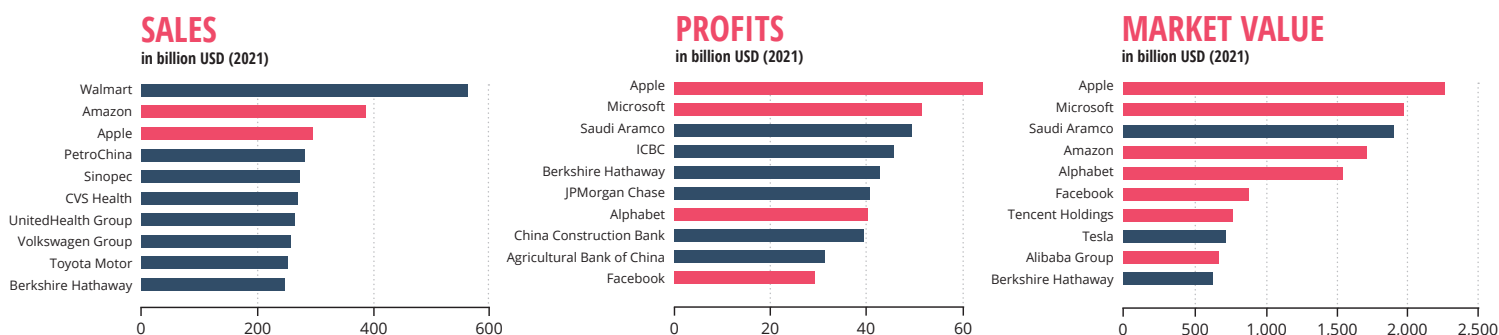
Interview with Cory Doctorow

STATE OF POWER 2023

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

SALES
in billion USD (2021)

Company	
Walmart	
Amazon	
Apple	
PetroChina	
Sinopec	
CVS Health	
UnitedHealth Group	
Volkswagen Group	
Toyota Motor	
Berkshire Hathaway	

0 — 200 — 400 — 600

PROFITS
in billion USD (2021)

Company	
Apple	
Microsoft	
Saudi Aramco	
ICBC	
Berkshire Hathaway	
JPMorgan Chase	
Alphabet	
China Construction Bank	
Agricultural Bank of China	
Facebook	

0 — 20 — 40 — 60

MARKET VALUE
in billion USD (2021)

Company	
Apple	
Microsoft	
Saudi Aramco	
Amazon	
Alphabet	
Facebook	
Tencent Holdings	
Tesla	
Alibaba Group	
Berkshire Hathaway	

0 — 500 — 1,000 — 1,500 — 2,000 — 2,500

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
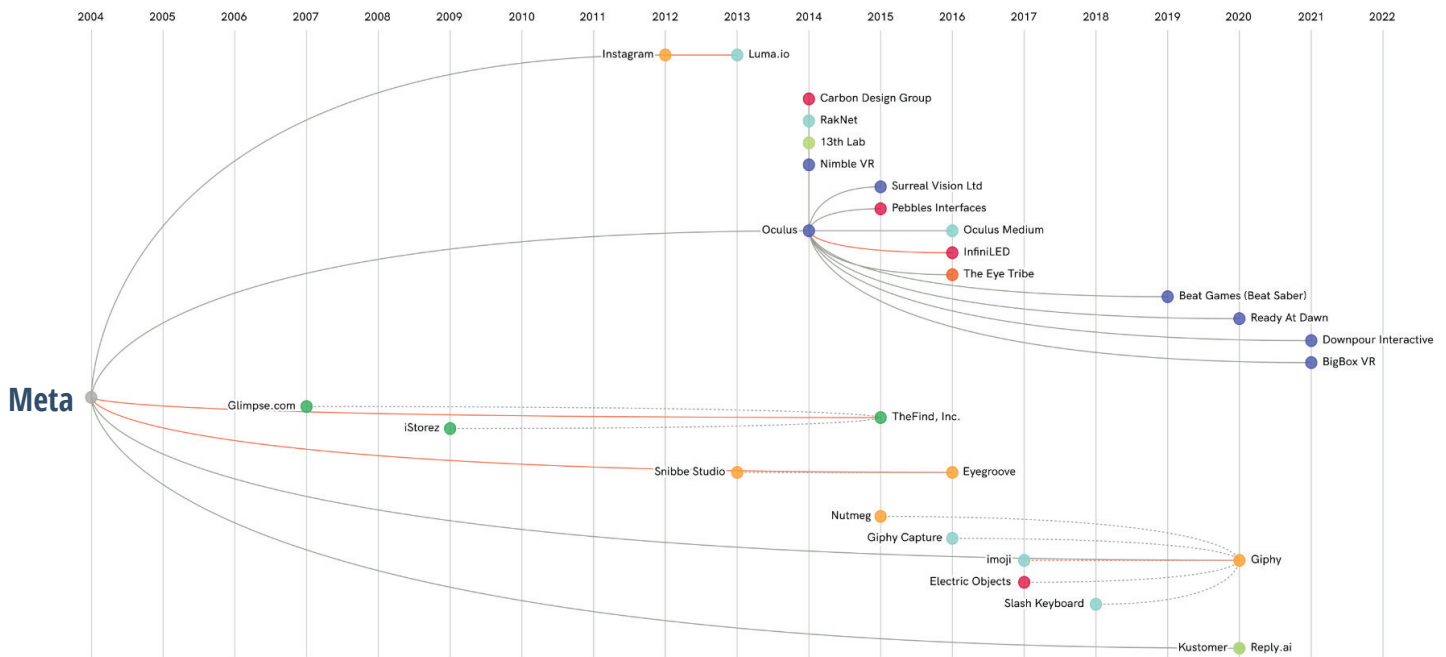
Source: gafam.theglassroom.org

> *"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.