DEMOS

STATES, CORPORATIONS, INDIVIDUALS AND MACHINES

ALEX KRASODOMSKI-JONES

MARCH 2021

This project was supported by:

Published by Demos March 2021

15 Whitehall, London, SW1A 2DD
T: 020 3878 3955
hello@demos.co.uk
www.demos.co.uk

CONTENTS

EXECUTIVE SUMMARY

Without a principled vision for the web, our democratic traditions, values, government and society risk falling behind authoritarian states, technopolistic industry giants and autonomous technology in the race to reshape the most important international political, cultural and social space in existence.

The web was born from circumstance: a US project, then a Western project, then a global one. An academic project with military origins built first by digital visionaries before power passed to the web giants with whom our lives are now totally intertwined. This origin story is retold in the principles that underpin the web as we know it.

Those principles are now in question. At first, it was authoritarian regimes that were wary. Now, the world over, governments are vying for change. The future of the open Internet is in doubt, and no cohesive settlement has been found.

The balances of power between states and corporations, corporations and citizens, and the social contract between states and their citizens is in constant flux online. Powerful technologies – artificial intelligence and trustless technology – presents a fourth pressure, with our lives governed by machine, not man.

This short paper explores proposed settlements on the balance of power and what they mean for the future of the web. It highlights the ways state, corporate, individual and machine power might help or hinder the democratic project, and the balance of powers proposed by competing conceptions of government. The paper demands we reset our vision for liberal democracy in a digital age at this juncture, to win over our publics to a vision of something better, and to secure that vision in collaboration with our friends and partners.

WHERE WE ARE, AND HOW WE GOT HERE

Technology is political. No technology could claim greater political importance than that which underpins the Internet. Technology is not created or deployed in a vacuum: it is inherently political, with political, social and cultural contexts shaping what technology is built, how it is designed, and to what ends it is used.

To understand how we have got where we are, we can peel back the layers of information and take a closer look at the technology that ferries it all around. These are the web's protocols, an intimidating-sounding name used to describe the rules for how information is communicated.

We have offline protocols of communication. We might shake hands, for instance, or kiss each other on the cheek (once in Peru, twice in Croatia, three times in Belgium) to say hello. Examining these habits can tell us something about a society, just as looking at those protocols online can tell us something about the principles of the Internet as it stands.

The Internet Protocol Suite (IPS), often referred to as TCP/IP (Transmission Control Protocol/Internet Protocol) after its two most well-known protocols, bears the political and cultural scars of its genesis. The web's origin story is one of squabbles and conflict over its design: over the level of central control possible, over the scale of military and government involvement, and over who should reap its rewards.[1,2] Paul Baran's early projects building resilient global communication at RAND were set against a backdrop of the Cold War, and the eventual ARPANET that emerged in the 1960s was built by academics and funded with military money. States, companies and institutions vied for power while the network's growth accelerated. Corporations then struck gold. Soon after the dot com bubble burst, Google, then Facebook and others discovered metadata-targeted advertising, to date the optimal business model for making money through this technology. It took fewer than twenty years for their applications to form a new bedrock for global business, culture, society and politics.

The larger it got the more deeply embedded the protocols, principles and norms on which it was built were buried. They reshaped the world.

This network's protocols support a "dumb, trusting middle" with "smart, anonymous hosts on the edges".[3] IP itself neither cares nor can control what information is sent across it, not who sends or receives that information. It is trusting. It expects good behaviour, with limited recourse for when people break customs or rules, or abuse it. End users are empowered, anonymous to most participants, and free to join as they wish: scalability is prioritised over any centralised control. In her history of TCP/IP, Rebekah Larsen tells the story of Vint Cerf's switch: one of the fathers of the web had an on/off button for the entire network used to force through updates to the original ARPANET. We are a long way away from that kind of control now.

Anonymous, free, open, trusting, decentralised and resistant to central control: these are the founding principles of the web as written in the technology that knits it together.

1 Larsen, R. *The Political Nature of TCP/IP*, Momentum (2012), p. 27
2 Such as the battle between TCP and the Open Systems Interconnection protocol.
3 Larsen, R. *The Political Nature of TCP/IP*, Momentum (2012), p. 47

How comfortably these principles sit with states and citizens is in constant flux. For some people, at some moments, some are welcome. A Silicon Valley entrepreneur during the dot com bubble or a sympathetic onlooker during the 2011 Arab spring might have celebrated what they saw the Internet as enabling, but so might a scammer or terrorist recruiter. A dictator wary of their citizens' freedom of speech, freedom of press or freedom of association may have been more worried. So might parents concerned about their children's browsing habits or security officials facing new forms of information warfare and digitally-enabled crime.

These concerns define the struggle for the future of the web. It is being fought in shareholder meetings and across front pages, in impenetrable tech roundtables and in the homes of each and every Internet user, in every arena of government activity: investment, war, trade, regulation, security-provision and so on.

One compelling narrative is found in Wendy Hall and Kieron O'Hara's seminal Four Internets paper, which tells the stories of these perspectives.[4] It describes Silicon Valley's Open Internet, the grandchild of the early web where technology and profit drive innovation and principles of freedom and unfettered access remain, albeit caveated by commercial imperatives. Under this model, the state comes second to corporations and technology in determining the rules of the game.

By contrast, "Beijing's Authoritarian Internet" is ideologically positioned as a tool of surveillance and control. States like China are fed up of the "dumb, trusting middle" that acts as a bulwark against government surveillance - benign or otherwise. Private corporations are extensions of the state. Chinese web giants answer to the government, not the other way around.

Alongside these monoliths lie visions that run the gamut of political ideologies: liberty absolutists, for instance, who demand the removal of even existing regulation or protocols deemed anti-competitive. This vision for the web is embodied in Four Internets by Republicans in DC but perhaps is also found in the more visionary crypto-anarchist and alt-tech world hell-bent on maximising individual liberty over responsibility.

Against this backdrop of warring visions, a new power is rising: self-determining technology – tech that automates decisions, or even writes its own rules. We are not at the singularity quite yet.[5] Nevertheless, governments and corporations are wholeheartedly backing machines in making decisions in government and business, from cancer screenings to exam results, from the news I should read to the stuff I should buy, making decisions outside of standards of access, transparency or redress. The spread of end-to-end encryption applications has placed a further technological barrier between users' communications and third-party oversight. Advocates of public blockchain technology have suggested it can replace the need for a traditional institution like a bank or a government department. A user puts faith in the technology, not in government or society or a corporation. Wherever we see governments, society or corporations struggling with technology, it may be time to stop and question whether it is the technology itself that is challenging their power.

The principles of the web as it has been developed have been confusing to liberal democracies. Some are welcome: an expectation of civility – some might say naïve – can be found in both liberal democracies and in the architects of the web's foundations. Rights to privacy, freedoms of speech and of association are founding principles of liberal democracies, and we celebrated the sight of smartphones in Tahrir square.

Other principles have become cause for concern. Democracies turn on a social contract, a trust in government, and the web has repeatedly tested the limits of states' power to have their way. The "dumb middle" and subsequent privacy-boosting technologies such as the uptake of encryption challenge the state's ability to carry out one of its fundamental duties, namely the preservation of its citizens' security, alongside simultaneous concerns about the exploitation of citizens' privacy by technology companies often outside their geographic jurisdictions.[6]

Taken together, we identify four forces able to shape the Internet going forward, four powers to whom we must assign responsibility for digital life. These powers are states, corporations, individuals and machines.

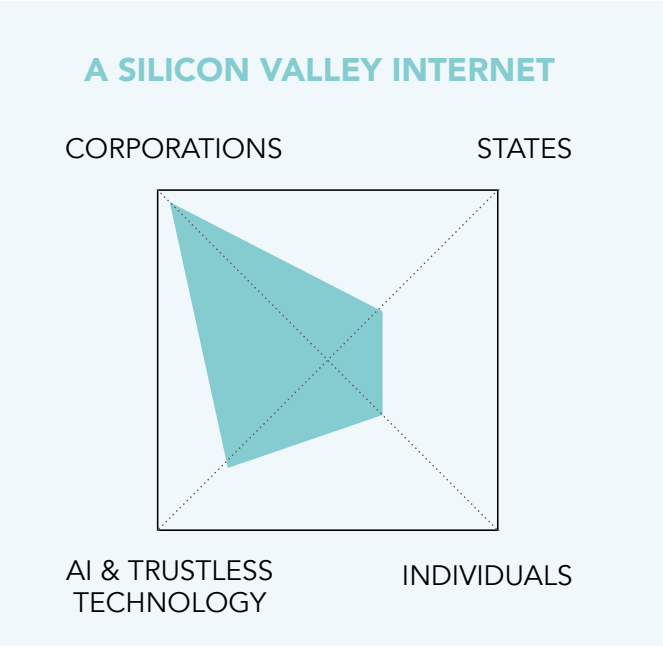
4 Four Internets: The Geopolitics of Digital Governance, K. O'Hara & W. Hall, CIGI (2018)

5 See, for instance: https://en.wikipedia.org/wiki/Technological_singularity

6 Vint Cerf himself admitted the only thing preventing earlier adoption of encryption standards online was military security classification of the required technology. See, for instance: https://www.youtube.com/watch?v=17GtmwyvmWE&feature=share&t=23m1s

STATES, CORPORATIONS, INDIVIDUALS AND MACHINES

Four powers will be responsible for the shape and quality of the Internet: states, corporations, individuals and machines: AI and trustless technology.



A sketch of power balances under one model, the technocentric, corporate Silicon Valley model

State control of the Internet can take many forms, but in this picture includes efforts to regulate and control the shape of the web by national governments and international cooperation. Under a democracy, it is the rule of law and its enforcement.[7] What that looks like in China is very different to what it might look like in Europe, or under a UN or other international treaty, but in all aspects it involves subjecting the Internet and its underlying technology to rules drawn up by governments.

Corporate control is different. Here, companies write the rules. Whether it is the speed or breadth of content moderation policies or the nature of the content that filters through to each user, the rules and mechanisms governing those processes are defined in boardrooms before legislatures. The relationship between state and corporate control is complicated. In some cases, states may devolve rulemaking to companies on the grounds that these are private entities who have the right to set their own standards. In others, governments may simply lack the power or jurisdiction to compel or coerce a platform into changing, either because a platform is unwilling or because the platform simply cannot carry out whatever it is being asked of it. The ongoing fight over copyright content is a useful example of this: some platforms are unwilling to remove copyrighted content, while others lack the technology to detect and remove it quickly enough. In both cases, the state's power is secondary.

Individual power foregrounds citizens' responsibility and ability to meaningfully understand, influence and control the online world around them. The informal agreements written into the protocols of the early Internet are clues that its early architects put a high premium on the freedom and power of its users. Giving power to users to better manage their personal data and cultivate the spaces they use online is core to this. Ensuring people have power

7 In countries where rule of law is itself compromised or alien, it is simply the state's ability to wield ultimate power.

and autonomy online has not been a priority of the corporatized Internet as we know it with its economic model of targeted advertising so dependent on data extraction and a compliant user base. Protection from harm and equality of opportunity are at best lines on a balance sheet.

Finally, machine power, or more accurately: artificial intelligence and trustless technology like encryption, blockchain and cryptocurrencies. Although these technologies are all different, they share a commonality: they move decision-making out of the hands of humans, and trust machines to do a better job. An AI can diagnose cancer, a bitcoin can be bought or sold or traded, and a deed transferred on a blockchain all without needing oversight of a central authority.

In the past few years we have already seen the growing power of these technologies to shape our lives, and their existence implies decisions outside of any corporate or state view. The maths behind end-to-end encryption is public knowledge, theoretically open for anyone to use. But its use creates channels that are less accessible to states, corporations, or other individuals, and throws up new dilemmas around power and policing. The San Bernardino case in 2014 saw a short-lived dilemma in which an iPhone's encryption could or would not be lifted by the state or by Apple.[8]

Blockchain technology is frequently touted as an exercise in removing state and corporate control from a system: Bitcoin needs no central bank. Artificial intelligences, even those nominally in the hands of states or corporations, are frequently so complicated that their decisions cannot be simply explained, computed or reverse-engineered. Citizens already cede decision-making control to algorithms every day, when shopping or navigating, and governments around the world are increasingly turning to algorithms to make decisions. States and corporations may believe that AI is little more than an extension of their own rule-making power, but this is myopia. First come the AIs that civil servants and marketing executives do not understand but deploy anyway. Second come AIs so complicated that even their creators cannot fathom quite how they work. Thirdly, and finally, come future AIs powerful enough to write their own rules and carry out government activities more effectively than any human organisation and are consequently resistant to oversight, accountability or explanation.

Machine power is not a spectre: even in 2021, billions of people are subjected to decisions made by artificial intelligences. Ignoring this power and failing to regulate its use would be a mistake, and early efforts to this end include ongoing work on ethical AI and ethical use of AI, as well as in protests against the use of AI in recidivism management, policing and education.

The lines are blurred. Corporations can and do dissuade government oversight by handing power to inscrutable AIs or implementing end-to-end encryption in a dangerous attempt to reduce liability, while states may incubate compliant corporate players like Sina Weibo or WeChat in China. Nevertheless, these four types of power offer us useful pivots around which to imagine a future Internet.

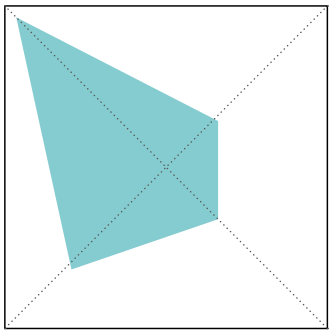
8 See, for instance: https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute

WHERE SHOULD POWER LIE?

FIVE MODELS FOR A DIGITAL FUTURE

A SILICON VALLEY INTERNET

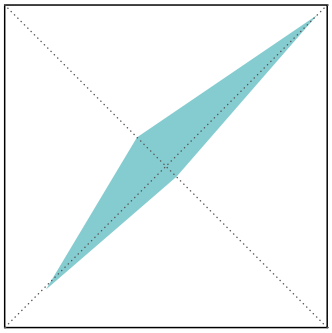
CORPORATIONS STATES



AI & TRUSTLESS TECHNOLOGY INDIVIDUALS

AN AUTOCRATIC INTERNET

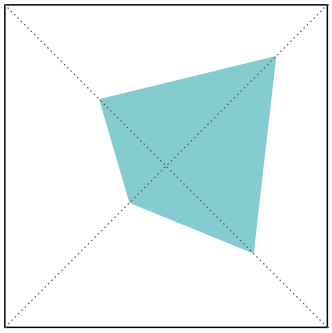
CORPORATIONS STATES



AI & TRUSTLESS TECHNOLOGY INDIVIDUALS

AN EU INTERNET

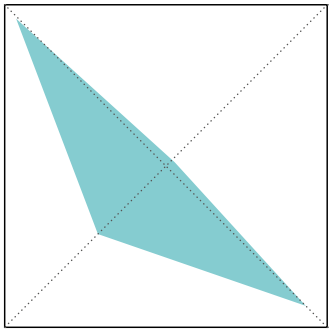
CORPORATIONS STATES



AI & TRUSTLESS TECHNOLOGY INDIVIDUALS

A LIBERTARIAN INTERNET

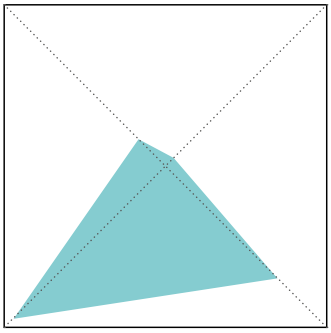
CORPORATIONS STATES



AI & TRUSTLESS TECHNOLOGY INDIVIDUALS

A MACHINE INTERNET

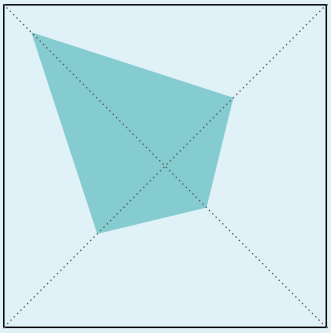
CORPORATIONS STATES



AI & TRUSTLESS TECHNOLOGY INDIVIDUALS

UK IN 2021

CORPORATIONS STATES

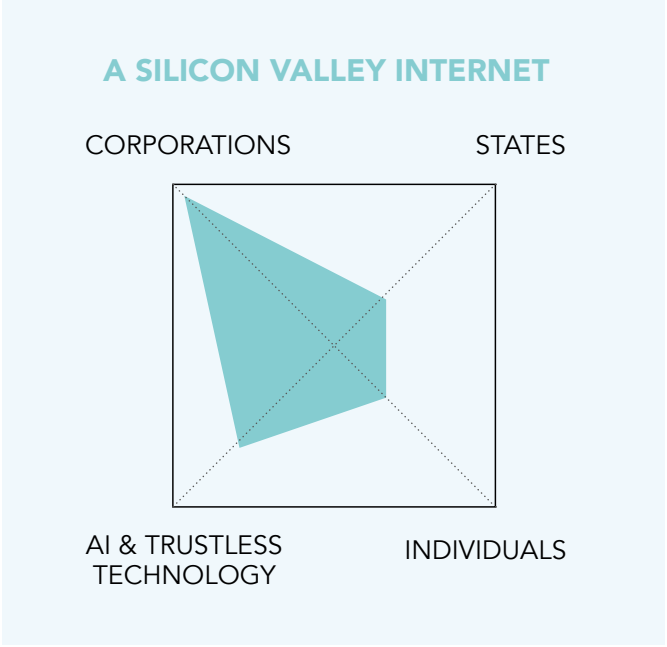


AI & TRUSTLESS TECHNOLOGY INDIVIDUALS

THE SHAPE OF THINGS TO COME

These diagrams are caricatures, but show how different the competing visions for the Internet might look. Each presents its own set of threats and opportunities.

THE CORPORATE INTERNET



The corporate Internet is the closest to the Western world's status quo. Under this model, it is the major international corporations that wield the greatest influence in determining the shape, cultures and rules online: whether Facebook, Amazon or Google and its subsidiary YouTube. Outside of a narrow band of illegal content, the limits of free expression are determined in Silicon Valley boardrooms or across the constellation of smaller platforms sustained by advertising revenue, the mechanics of which are frequently provided by Google, Amazon or Facebook.

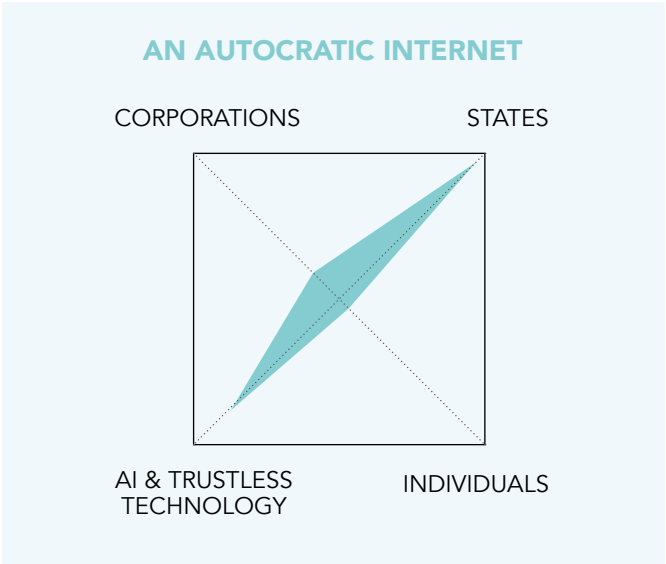
Tension exists between the infrastructure providers and the applications that run on them, but under this model tension is resolved through the private sector. The expansion of Tesla's Starlink programme as a corporate-owned, international provider of Internet access is a useful indicator of what is to come, with corporations bypassing state-imposed infrastructural limits on their activity.

The relationship between platform and state is a one-sided negotiation. Regulation moves slowly, is continually contested, and application of the law is frustrated by a lack of transparency and meaningful ways to measure or survey what is happening on one of these platforms at any one time. Government data access and collection is feeble when compared to the powers of the platforms. Individual users fare even more poorly: the services offered are extraordinary and nominally free, but are exchanged on terms that utterly disempower their users. Redress, control or engagement on platforms is little more than a veneer concealing this asymmetry-by-design.

Technology plays a key role here. Encryption frustrates oversight, and is deployed as much to protect market share through security as it is to create distance between the platform and the content circulating on it.[9] AI and algorithmic curation is the only feasible route to managing spaces this large and to maximise data capture and advertising revenue, and the functionality of these algorithms is opaque, their decisions broadly unchallengeable. The army of devices sourcing data to fuel these platforms continues to grow: this is another area likely worth some scrutiny.

9 See, for instance: https://twitter.com/ashk4n/status/1339340068775870465

THE AUTOCRATIC INTERNET



The shape of the online world evolving in China and under its growing sphere of influence in the developing world stands in contrast to the technopoly of the corporate Internet we are familiar with in the West. Here, the state calls all the shots, and platform technology is an extension of the government's power rather than a thorn in its side. Power invested in individuals is minimal.

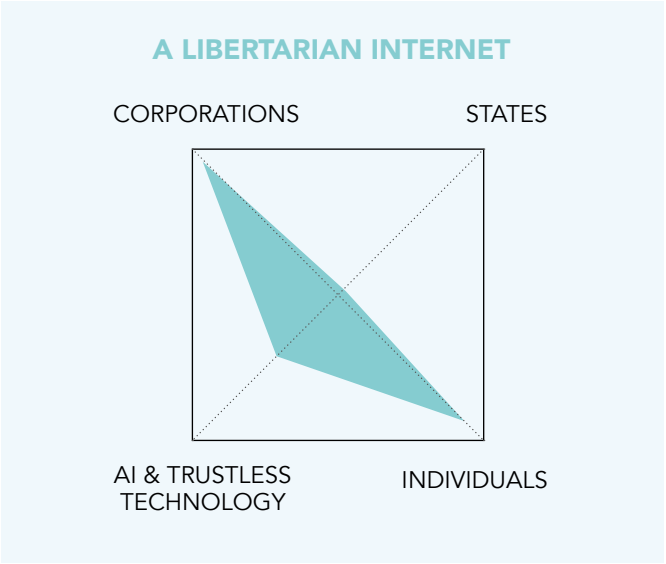
Protocols and infrastructure are state-centric and centre state sovereignty. At their most sophisticated, they include hard limits to the boundaries of the web, like the Internet found in North Korea. At their crudest, they are an on/off switch.

Individuals' rights remain limited. Under this model data access by government is facilitated by platforms, and enormous, joined-up data on Internet users underpin surveillance, social score systems and experimental technology. The subjugation of Uighurs in China country is facilitated by technology above all else.[10]

This same data unlocks the full potential of state-aligned artificial intelligences, themselves a further extension of state power in as far as their outputs and operations remain knowable and intelligible. Citizens' rights of redress are negligible, regardless of whether a decision is made by an AI or the state, and that difference will become increasingly blurry.

Harnessing machines into the service of the surveillance panopticon means stamping out some technology as much as encouraging others. China's 2020 encryption law introduces a tiered approach to encryption which critics describe as tantamount to the ban on end-to-end encryption for everyone but the ruling party.[11] Cryptographic applications like Tor, Telegram, WhatsApp, Mastodon or Virtual Private Networks (VPNs) are banned in the country.

A LIBERTARIAN INTERNET



The US position on the future of the Internet is often associated with ideas and ambitions of the web giants that call it home. But there is division in the country, and a competing vision for the soul of the web: DC's commercial Internet, an Internet prioritising private actors from platform to infrastructure provision, a market free from any regulation whatsoever. Freedom of expression in this model is interpreted as freedom from state intervention, rather than state-guaranteed equality of opportunity.

Under this model, there should be nothing stopping an individual from creating, accessing or participating in digital services online, and individuals take responsibility for their behaviour under terms set and enforced by other individuals. Protecting one's privacy or rights online falls to the individual: their ability or capacity to, or the services they choose to use. Limits on freedom, such as legal codes of speech or expression, are anathema here, as are rules demanding equality of opportunity.

Under this property-based model, corporations have no expectation of providing anything save from what their customers might want. Internet Service Providers (ISPs) should have the power to maximise their profits, and long-standing web principles like net neutrality stand in the way of this. Under this model, there is no expectation of public good or openness in platforms, nor is interoperability between sites and services necessarily supported.

10 How China Uses High-Tech Surveillance to Subdue Minorities, C. Buckley & P. Mozur, New York Times (2019)

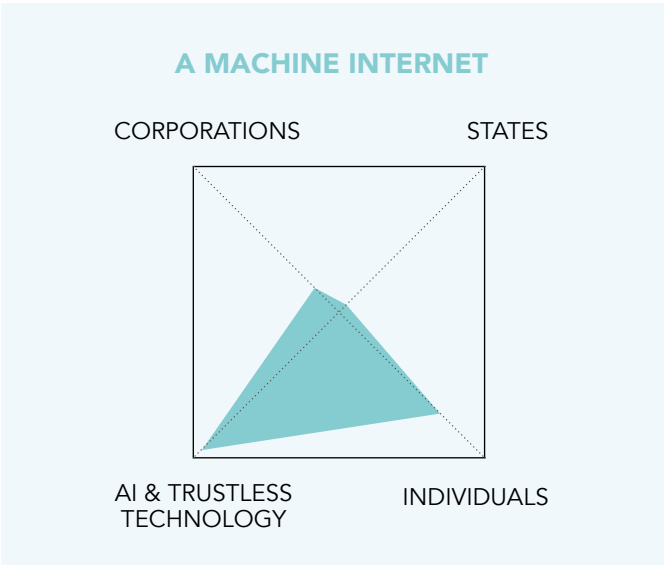
11 Dickinson, S. China's New Cryptography Law: Still No Place to Hide. Available at https://www.chinalawblog.com/2019/11/chinas-new-cryptography-law-still-no-place-to-hide.html [Last accessed March 2021]

This runs contrary to the hopes of early Internet pioneers, for whom the web should be a single, connected information space. Instead, the Internet is balkanized into profit-driven "walled gardens".

Power here is shared by corporations and their customers, free from state oversight. It is a model invoked by those who reject government intervention at a more microscopic level. Pressure on major platforms to reduce online harms has led to the proliferation of so-called 'free speech havens', alternative technology platforms like Parler and Gab that tend to cater to extremist political positions nominally banned by the Silicon Valley giants' terms of use, though the weakness of these alternatives has been brought to light in the latter part of 2020 as they are harried out of the mainstream. Under the Libertarian Internet model, these spaces are promoted: there is a market for them, and so they ought to be allowed to satisfy that market. Pressure on service providers to censor these spaces will accelerate their growth and distribution.

Trustless technology under this model becomes just another product feature. If customers demand security, there should be no barriers to implementing powerful encryption to your service if that is the route to maximising your customer base and outcompeting competitor services.

A MACHINE INTERNET



To improbable but important futures, we propose a fourth framework: A machine Internet where politics, society and culture is governed by rules set by artificial intelligences and code.

In this conception, the technology itself sets and enforces the rules: at first at the behest of a state or corporation, but eventually outside of any corporate or state interest. This is the vision of the Internet furthest from our current one, but the growth in machine-enabled decision-making and the continuing growth of crypto assets make a world where code is law worth exploring.

Governance by AI is on the rise. Sufficiently powerful AIs will be employed to make decisions about increasing parts of our lives, beginning with the routes we take to work, through our ability to access credit or buy a house, and eventually culminating in AI-enabled law enforcement, national security, and provision of public services.

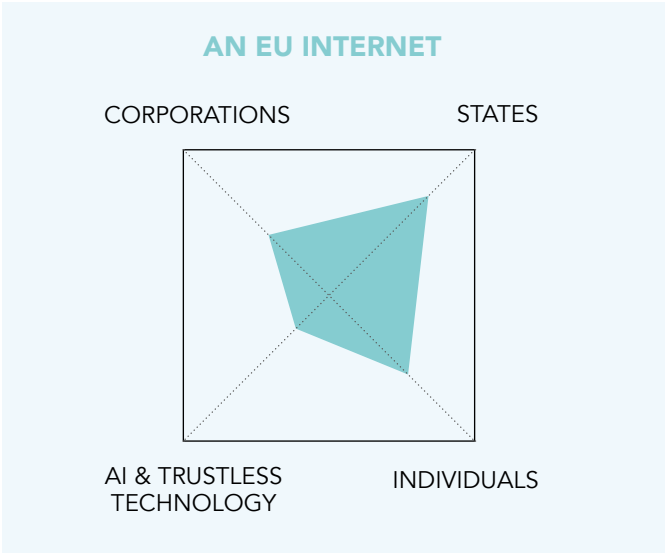
Challenging decisions made by algorithms is already difficult given the level of technical expertise required. Computational decision-making has already been shown to be more effective than human decision-making in some domains - in diagnosing health conditions, for instance, or in identifying fraud. Under a machine internet, AI systems are expected to replicate the functions of government more effectively and efficiently, eventually replacing them piece by piece. This has clear and unresolved ramifications for questions of democratic choice and political representation. Biased, opaque algorithms fail any democratic test.

Again, this is not science-fiction. Every day, billions of people globally are subjected to decisions made by machines that they do not understand nor have any power over or expectation of redress. Every day, governments come face-to-face with technology that limits their power.

Uptake in cryptocurrencies like Bitcoin has tended to be driven by speculation, but the use of cryptocurrencies is seen as a route towards providing financial services to people not able to trust corporate or central authorities. New, so-called permissionless systems, digital autonomous organisations (DAOs), smart contracts and so on are all built to allow the transfer of money and commercial cooperation among users entirely without third-party involvement or oversight, be that corporate or state.[12] The architects behind these systems imagine a world where digital technology replaces nation states entirely by enabling individuals to cooperate through technology alone.

12 A useful list of example DAOs can be found at https://hackernoon.com/what-is-a-dao-c7e84aa1bd69

THE EU INTERNET: A LIBERAL DEMOCRATIC INTERNET?



This model - Hall and O'Hara's Bourgeois Internet - is best described as the state fighting back. It may also be the closest governments around the world have got to a liberal democratic web. Digital regulation led by the EU and its member states is reactive, and driven by attempts to remedy perceived harms and threats enabled by the corporate Internet. Although increasingly couched in proactive language, EU regulation has primarily been remedial. General Data Protection Regulation (GDPR), the Google Spain vs AEPD case, the NetzDG laws in Germany and most recently the EU's Digital Services Act (DSA) are useful examples of states taking steps to curb the behaviour or design of (primarily US) technology platforms.

A vision is now emerging for what this Bourgeois Internet might look like. In this imagination, state power is deployed as the key defence of citizens' rights and liberties, and citizens are expected to put faith and trust in national and international institutions. It places a heavy emphasis on the role of citizens, trusting them, in return, to act with civility and tolerance. Data rights are better protected, with a trajectory towards greater citizen control over the use and value of the data they produce.

Untrammelled machine power presents a threat to state hegemony, and this is as apparent in the Bourgeois Internet as anywhere else. The EU has led the pack in calling for ethical standards for artificial intelligence, recognising the increasing use of this form of decision-making. Civil society organisations are vocal in calling for algorithmic transparency, rights of redress, and for caution in the implementation of AI-enhanced technologies like facial recognition. While the roll-out of trustless technology has been tolerated, laws around the advertising and provision of cryptocurrency services have been implemented. The debate over privacy-enhancing technologies like end-to-end encryption continues to demand a settlement: a dilemma between safety and security on the one hand and rights to privacy, to freedom of expression and commercial questions on the other.

THE LIBERAL DEMOCRATIC INTERNET

Assigning power to states, corporations, individuals and machines all present both threats and opportunities to liberal democratic development. Navigating these ambiguities and dilemmas won't be easy, and time is short. The moment for celebrating the web as a powerful tool in projecting liberal values is over: it was never inevitable, never the end of History. Managing speech and information in a liberal democratic society is a painstaking exercise in slow-moving regulation, care and caution. Timidity and patience is easily exploited in the fast-moving world of technology.

The mission for liberal democracies, and that of the Good Web Project, will be to identify the technologies, design principles and governance that ensure a balance of powers commensurate with liberal democratic values. The breadth and depth of the challenge is formidable.

There is work to do across every layer of the technology stack that makes up the web, and at the level of individuals' rights and liberties up to scales as grand as international security and sovereignty.

In the sections below, we map these dilemmas, identifying the threats and opportunities across three broad areas: the digital citizen, the digital commons, and security and sovereignty. For each, we identify where liberal democracies ought to step up their defence and support, and where the threats from corporate, state, individual or machine power require particular vigilance.

DIGITAL CITIZENSHIP

The defence and promotion of citizens' rights and liberties online, and their active participation in online life, is the foundational challenge facing liberal democracies as they look to reshape the online world.

It is barely an exaggeration to describe the democratic disempowerment of the average user online as the Internet's greatest tragedy. In most Western countries, the active participation of citizens in political and civic life has been utterly subsumed to the prerogatives of monopoly platforms and the economic model that underpins their design. The average Internet user has no power to reshape or cultivate the spaces they live in, limited as they are by arbitrary, confusing or inconsistent terms of use and platform enforcement. The ability to choose those that govern us is a core tenet of liberal democracy, but online users have no right nor route to contest the decisions made by higher powers under the default platform model. "Within this framework," writes Giovanni De Gregorio, "the lack of any users' rights or remedy leads online platforms to exercise the same discretion of an absolute power over its community."[13] Shoshana Zuboff calls these "the social relations of a pre-modern absolutist authority".[14] Others have called the platform model feudalistic or Hobbesian: a system under which you give up your rights in exchange for products and services.[15] Whatever it is, the current situation does not sit comfortably with our conception of citizens in a democracy.

Defence of citizen rights and responsibilities by states, along the lines of a traditional social contract, has been frustrated by corporate power in liberal democracies, and was never a prospect under authoritarian regimes. The COVID-19 pandemic has shone a light on the dangers presented by the digital world when state power is unfettered: AI-driven cameras, data capture and analytics, and facial recognition software ensure citizens are carefully monitored, and infractions against a law or directive are significantly more likely to be detected.[16]

The rule of law itself has been weakened: enforcement is harmed by patchy capability, out-of-date legislation, limited access to evidence and weak international coordination. Moreover, the online boundaries of acceptable behaviour are shaped by terms and conditions long before law and its enforcement.

Finally, the rise of machine-enabled decision-making presents new threats to traditional conceptions of citizen power. Already, trustless technology like end-to-end encryption has by design rewritten the rules on human rights: at once a boon and a risk to rights to privacy and security, and cryptographic technology has extended new powers to a select group of technologically-savvy individuals.

Code becomes law. Our lawmakers are first engineers, then artificial intelligences. The routes to political and social participation and the rights and freedoms of participants will be defined not through human oversight, but by the technology itself, ushering in new questions for how humans can wield power in a world of machines.

Bringing these forces instead to the defence of the rights of citizens and to the service of citizen empowerment is paramount. Ensuring corporate power is checked by law and government power is an essential first step to ensure citizens' rights are defended, and that citizens are able to comprehend,

13 De Gregorio, G. *Democratising Online Content Moderation: A Constitutional Framework*, Computer Law and Security Review (April 2020)
14 Zuboff, S. *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization* (2015) p. 83
15 Schneier, B. *Data and Goliath* (2015) p. 58.
16 Yang, Y. and Zhu, J. Coronavirus brings China's surveillance state out of the shadow, *Reuters* (2020)

affect and challenge the spaces they live in online. While web giants may be the target now, the same questions must be applied to machine power in the future, ensuring algorithms and artificial intelligences operate along lines consistent with liberal democratic principles. Strengthening the power of communities online is an essential step, and the Internet is made up of thousands of examples of how to do this effectively.

The reward of a properly balanced system will be the practical application of these powers in the service of citizen empowerment. State power, and the rule of law, should protect citizens against corporate misdemeanour, and ensure that citizen rights, responsibilities and liberties are enabled by digital design. Corporations, properly empowered, will develop competing models for online life, providing citizens with genuine choices over where they live their online lives, and bring liberal democratic technologies to new audiences around the world. Citizens properly empowered to take responsibility for their online lives will find routes towards a meaningful digital civic society, forming and cultivating new communities and relationships on the terms of their choosing. Trustless technology can be deployed to protect rights and liberties in environments where autocratic states and corporations abuse their power. Blockchain technology has already been used to protect rights to property in places where that right is less than guaranteed.[17, 18] Carefully designed artificial intelligences may well increase citizen capability to live full and free lives through improvements to decision-making, information access and new models of work and social support. The ethical use of AI has frequently been touted as an area where liberal democracies may have an edge.[19]

CASE STUDY: FACIAL RECOGNITION

Without sufficient power for citizens, technology can be all too easily weaponised by states and corporations against individuals and communities. The use of digital surveillance by the Chinese government to perpetrate atrocities against the Uighur people in Xinjiang has long been recorded.[20] Recently it was revealed that the company Huawei had been involved in testing AI facial recognition technologies to identify people's ethnicities which could send a 'Uighur alarm' to the police if a member of the minority group was identified.[21]

And the wielding of power by corporations abetting state oppression is a global concern. Some corporations have tried to distance themselves: law enforcements' use of facial recognition systems in the USA known to have severe gender and racial biases, Amazon, Microsoft and IBM ceased sales of their facial recognition technologies to law enforcement.[22, 23]

The use of various facial recognition systems by law enforcement and private companies has been the subject of lawsuits from South Wales[24] to Illinois.[25]

We are in a situation where state power - and state repression - can be amplified on a huge scale through the use of unaccountable technologies: where we rely on the goodwill or reputation of companies, or, where they exist, cumbersome legal processes to constrain abuses. A liberal democratic settlement cannot be content with always playing catch-up to the relentless pace of technology being developed and adopted, with democratic oversight only ever, if ever, an afterthought.

17 D. Daniel & C. Speranza, The Role of Blockchain in Documenting Land Users' Rights: The Canonical Case of Farmers in the Vernacular Land Market, Frontiers in Blockchain (2020). Found at: https://www.frontiersin.org/articles/10.3389/fbloc.2020.00019/full

18 L. Tombs, Could blockchain be the future of the property market?, HM Land Registry Blog (2019). Found at https://hmlandregistry.blog.gov.uk/2019/05/24/could-blockchain-be-the-future-of-the-property-market/

19 EU Ethics guidelines for trustworthy AI. (2019) Found at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

20 Byler, D. China's hi-tech war on its Muslim minority, *Guardian* (2019)

21 Dou, E. and Harwell, D. Huawei worked on several surveillance systems promoted to identify ethnicity, documents show, *Washington Post* (2020)

22 Devich-Cyril, M. Defund Facial Recognition, *The Atlantic* (2020)

23 Statt, N. Amazon bans police from using its facial recognition technology for the next year, *The Verge* (2020)

24 Rees, J. Facial recognition use by South Wales Police ruled unlawful, *BBC Online* (2020)

25 Statt, N. ACLU sues facial recognition firm Clearview AI, calling it a 'nightmare scenario' for privacy, *The Verge* (2020)

A DIGITAL COMMONS

We entered the 21st century with a series of assumptions about what makes for a 'democratic' information and media space and supported a full, free and fair public debate: freedom of expression; pluralism; the metaphor of a marketplace of ideas. But online spaces have frequently failed to meet these ideals, and pose a new challenge to the coherence of those original principles.

The common analogy is that of the shopping centre or mall: spaces that feel like public spaces in the offline world, but have their own rules, drawn up in private, and enforced by private security. The centralisation and homogenisation of digital public space by a handful of US companies has left the design, the cultural norms and the shape of the public discourse enabled by media in the hands of corporate power. The design imperatives behind these spaces are clear: maximising shareholder values requires a panopticon of data collection and the prioritisation of attention-grabbing content. These spaces are at once rigidly controlled in defence of those powerful or wealthy enough to maximise their share of voice, and simultaneously exploitable by actors savvy enough to do so. Public service media increasingly resembles a model dependent on charity.

Machines play an integral dual role in maintaining this control. They serve to maintain the enormous private commons represented by social media platforms. Complicated algorithms prioritise content for profit, clunky algorithms censor speech and information automatically, personalisation algorithms segment and tailor information to the point where two citizens might live in utterly divergent realities.

Democratic states remain firmly on the back foot. As major funders of platform advertising, states have found a route to make the most of this new world order without meaningfully challenging its principles, and attempts to preserve the principles of public space have been limited to reactive regulations targeting online harms. Solutions are not easy, and well- meaning attempts at digital regulation have often succumbed to an authoritarian vocabulary of take- downs, blocks, bans and censorship.

Authoritarian states, by contrast, have made the most of the digitisation of public space, either by piggy-backing on the surveillance machine or by exploiting its weaknesses within their borders and without.

Individual power in shaping public spaces is incredibly limited when the world is one great shopping centre. Creating or maintaining public space on the Internet is a thankless task for those not able to monetise it. The handful of people able to sustain an online presence as a commentator, journalist, public figure or talking head do so sharecropping through Premium Snapchats, on Amazon's Twitch or Google's YouTube.

Redrawing the public sphere must be a critical priority for democracies, and a liberal democratic Internet requires change at all four corners of the sketches above.

Corporate provision of public space, usually expanded under the proviso of connecting the world, could act as a powerful arena for the projection of democratic values. But new models for sustaining public space and the voices within it are vital. Regulation in favour of alternative models of public media and the restoration and preservation of funding models outside of advertising revenue are vital routes towards ensuring media is plural, responsible and sustainable.

Unaccountable and opaque machine power cannot be entrusted with the governance of the digital commons. Where space is necessarily maintained by algorithms, changing their design and boosting

their transparency should build a technologically-enabled public sphere where machines are deployed in defence of minority voices and the preservation of a free and open media. Technology like encryption and decentralised networks can serve as a further line of defence for the public sphere in the face of those who would look to see it controlled or shut down, though there is a bargain here: the less power lying in the hands of states or corporations, the greater the risk to and responsibility on individuals in shaping their experiences online.

Empowered citizens are custodians and participants in the digital commons. With the right incentives, a liberal democratic Internet will see the transformation of its users from digital serfs to digital citizens, empowered to shape and contribute to a healthy and vibrant public sphere.

CASE STUDY: THE SECTION 230 CONUNDRUM

One of the apparent oddities about the 2020 US Election was how President Trump and President-Elect Biden could come from such different positions on what the online world should look like, and both arrive at the same conclusion: that Section 230, which protects internet companies from liability for content hosted on their platforms, needed to be reformed.[26] Trump's longstanding (unevidenced) complaint against the big tech companies has been that, in taking action against hate speech and extremism on their platforms, they 'censor' conservative and right-wing voices.[27] Biden has said, conversely, that the proliferation of misinformation and disinformation online is cause for reconsidering of the protections.[28]

What is clear is that without a common vision of what it is to be a good public space online (no misinformation? no censorship?) approaches to addressing the power imbalance in public spaces online will be piecemeal and inconsistent. And the ownership of these spaces by private companies who operate without oversight or significant transparency means that these kinds of contradictory conclusions are likely, as government fights to get back power from corporations however it can: whether or not it actually succeeds in enfranchising citizens.

26 Siripurapu, A. Trump and Section 230: What to Know, *Council on Foreign Relations* (2020)
27 Darcy, O. Trump says right-wing voices are being censored. The data says something else, *CNN Business* (2020)
28 Kelly, M. Joe Biden wants to revoke Section 230, *The Verge* (2020)

SECURITY AND GEOPOLITICS

Over the past five years, the cold war online turned hot. Battles over digital sovereignty began with domestic developments, with nation states like Russia and China pressing for greater control over the web within their borders. The Internet has become a vector for international geopolitical aims, too: both through the weaponisation of open, online spaces and the deployment of disinformation, and through the race to deploy digital infrastructure around the world. Running concurrently with these grander plans, cybercrime is the fastest growing threat to citizens: from scams and identity theft to extremist recruitment and the marketing of child sexual exploitation online. Liberal democracies have been slow to respond to these threats.

Corporate power, embodied in the policy and resilience teams inside the major platforms, has been exposed. Platforms were asleep at the wheel: either unaware of the ways their platforms were being exploited, unable to counter it, or choosing to ignore it.

Individuals have been reduced to cannon fodder. Forced into the front line by platforms hell-bent on connectivity and growth and lacking digital literacy, they have been easy prey for groups and individuals looking to exploit them. Education initiatives and fact-checkers were orders of magnitude too weak to be viable tools of self-defence. Fraud and cybercrime is thought to affect one in three Americans.[29]

The state's ability to protect its citizens has been called into question time and again as our lives move online, with encrypted devices and communication platforms and adding a further barrier to law enforcement tasked with tackling digitally-enabled harm. As noted above, technology that is resistant to centralised control and oversight inevitably limits the power of central state or corporate authority.

Nation states relying on reactive regulation as a tool to combat the influence of platforms have also been slow, powerless to defend the new information landscape and its haphazard Silicon Valley custodians against foreign actors. A lackadaisical approach to infrastructural development has seen countries reliant on infrastructural imports from authoritarian regimes in their own backyards. There is a vacuum in competitive infrastructural offerings in the international market when compared with the scale and ambition of China's Belt and Road Initiative, for instance. As we enter the age of the Internet of Things, there continue to be questions about the security implications of the devices being sold to millions.

International cyber supremacy will be dictated in major part by machine power. In the hands of states and corporations, this means the development of artificial intelligence. As noted in Four Internets, the ability by authoritarian regimes to bypass concerns over data privacy and amass enormous, connected datasets on which to train AI may give them an advantage in developing superior products. Chinese-owned apps like TikTok are already finding Western audiences while Silicon Valley applications are banned or neutered within Chinese borders.

Democracies need to define a liberal doctrine of security and sovereignty, one that recognises the threats caused by information operations and cyberattacks, foreign and domestic, as well as online crime, but also guarantees freedoms and the free flow of information across borders.

Empowering states and multilateral institutions to secure and defend an open Internet is a vital step in reasserting sovereignty in the online world. This requires change and improvement to the network architecture of the web, both to reinforce the

29 Carr, H. et al, The Great Cyber Surrender: How police and governments abandon cybercrime victims, *Demos* (2020)

open Internet in the face of protocols designed to balkanize it and to ensure that liberal democratic principles continue to be reflected in the underlying technology. Improved transparency of digital standards bodies and involvement by multilateral institutions must be mainstreamed. Where corporate monopolies are identified as a weakness in national and international security, those weaknesses must be addressed, ensuring global corporations are a vanguard of liberal democratic values instead of undermining them.

Further, states must move beyond authoritarian vocabulary of take- downs, blocks, bans and censorship as the default for thinking about the Internet, and stop jealously peering over the fence at the apparent successes of authoritarian regimes in stamping out speech they do not like online. Illegal content demands zero tolerance, but enforcement of the law is only one small part of the picture here. Instead, a liberal democratic approach to policing and online security must be introduced, ensuring security services are able to protect citizens while doing so in a way that is proportionate and with oversight. Boosting national security will turn on an empowered, literate society and civil society protected by security services working under the rule of law, but able to work nonetheless.

Democratic State- and corporate-sponsored infrastructural growth is vital, including the export and promotion of infrastructure that bolsters the open web around the globe. Handing over the standards and roll-out of digital infrastructure to compromised providers and authoritarian regimes is unacceptable.

CASE STUDY: INTERNET SHUTDOWNS

Governments across the world are taking it as their sovereign right to take action against the open web: at the extreme, through internet shutdowns, more-or-less sincerely to protect national security, law and order, or prevent online harms.[30, 31] However, shutdowns have been described as 'collective punishment'[32] of those affected, And these shutdowns affect not only fundamental freedoms of information and expression, but have significant negative economic and health effects.[33] Internet restrictions going on for months in Myanmar have been criticised in particular in 2020 for blocking access to essential information about the Covid-19 pandemic.

Without clear global standards and commitments to what internet access should be, and when restrictions are legitimate or illegitimate: dealing with problems across platforms by states is leading to citizens' rights being eroded, rather than protected - and their ability to speak out about it curtailed.

30 Shastry, V. Asia's Internet Shutdowns Threaten the Right to Digital Access, *Chatham House* (2020)
31 Johri, N. India's internet shutdowns function like 'invisibility cloaks', *Deutsche Welle* (2020)
32 Johri, N. India's internet shutdowns function like 'invisibility cloaks', *Deutsche Welle* (2020
33 Roth, K. Shutting Down the Internet to Shut Up Critics, *Human Rights Watch* (2020)

CONCLUSION

It is a cliché to describe liberal democracy as a balancing act, but here we are again. Four forces will be responsible for the shape of the future Internet. State power, corporate power, individual power and the power of machines all require harnessing in the name of liberal democracy. Correcting the balance of powers is the challenge facing liberal democracies. The examples presented here show that moving too far in any one direction will undermine the project as a whole, and policy that ignores the importance of one of these powers will be insufficient.

There is evidence of failure wherever you look. The harms and failings of the web in its current iterations are well-documented. We speak about the victories of the Internet less often these days, but this is a question of evidence too. In moving to a proactive vision of a liberal democratic Internet, we must celebrate and support the voices, designers and architects of the best of the web, and ensure we hold all parts of the Internet to the standards of its success stories. There are lessons to be learned from Wikipedia, from StackOverflow, and from the legions of virtual communities that are thriving below the headlines.

There are also lessons to be learned from the web giants. They have rightfully come under fire over the past few years for their failings, but they have contributed more than anyone to opening the Internet up to the world. Brought to the defence of liberal democracy, they may again be perceived as a vanguard of liberal democratic values around the world.

It is state and individual power where the most urgent questions must be answered. The internet will be the place where democracy is redefined in the 21st century, but doing so will require a radical improvement in state and multilateral governance of the online world and its underpinning technology. Ensuring individuals are able to exercise their rights online is a vital check on both state and corporate overreach.

The trilemma of states, individuals and the private sector is, however, not fit for the future. The accelerating development of machine power, from artificial intelligence to permissionless technology, will itself challenge all three for future hegemony. Given the pace at which questions of global governance move, it is of crucial importance that steps taken reflect the growing influence of machines in our social, economic and political lives.

More than ever now, we need a vehicle to unite liberal democracies in advancing and advocating their own vision of the web. While authoritarian powers are increasingly coherent in promoting their vision, democracies are currently fractured, with fundamental differences in approach in North America, Europe and Asia. Yet there are underlying values and interests that unite us and must be articulated.

Without evidence for what works online, and without a principled vision for the internet, our democratic traditions, government and society will fall behind authoritarian states, industry giants and powerful technology in the race to reshape the most important international political, cultural and social space in existence. We must not focus on what we don't want, and forget about what we do.

Licence to publish

Demos – Licence to Publish
The work (as defined below) is provided under the terms of this licence ('licence'). The work is protected by copyright and/or other applicable law. Any use of the work other than as authorized under this licence is prohibited. By exercising any rights to the work provided here, you accept and agree to be bound by the terms of this licence. Demos grants you the rights contained here in consideration of your acceptance of such terms and conditions.

1 Definitions
a 'Collective Work' means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this Licence.
b 'Derivative Work' means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this Licence.
c 'Licensor' means the individual or entity that offers the Work under the terms of this Licence.
d 'Original Author' means the individual or entity who created the Work.
e 'Work' means the copyrightable work of authorship offered under the terms of this Licence.
f 'You' means an individual or entity exercising rights under this Licence who has not previously violated the terms of this Licence with respect to the Work, or who has received express permission from Demos to exercise rights under this Licence despite a previous violation.

2 Fair Use Rights
Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3 Licence Grant
Subject to the terms and conditions of this Licence, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:
a to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;
b to distribute copies or phono-records of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works; The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4 Restrictions
The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:
a You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this Licence, and You must include a copy of, or the Uniform Resource Identifier for, this Licence with every copy or phono-record of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this Licence or the recipients' exercise of the rights granted hereunder. You may not sublicence the Work. You must keep intact all notices that refer to this Licence and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this Licence Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this Licence. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.

b You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.
c If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works, you must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5 Representations, Warranties and Disclaimer
a By offering the Work for public release under this Licence, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:
i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder
and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;
ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.
b Except as expressly stated in this licence or otherwise agreed in writing or required by applicable law, the work is licenced on an 'as is' basis, without warranties of any kind, either express or implied including, without limitation, any warranties regarding the contents or accuracy of the work.

6 Limitation on Liability
Except to the extent required by applicable law, and except for damages arising from liability to a third party resulting from breach of the warranties in section 5, in no event will licensor be liable to you on any legal theory for any special, incidental, consequential, punitive or exemplary damages arising out of this licence or the use of the work, even if licensor has been advised of the possibility of such damages.

7 Termination
a This Licence and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this Licence. Individuals or entities who have received Collective Works from You under this Licence, however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this Licence.
b Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this Licence (or any other licence that has been, or is required to be, granted under the terms of this Licence), and this Licence will continue in full force and effect unless terminated as stated above.

8 Miscellaneous
a Each time You distribute or publicly digitally perform the Work or a Collective Work, Demos offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this Licence.
b If any provision of this Licence is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Licence, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.
c No term or provision of this Licence shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.
d This Licence constitutes the entire agreement between the parties with respect to the Work licenced here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This Licence may not be modified without the mutual written agreement of Demos and You.

DEMOS

Demos is a champion of people, ideas and democracy. We bring people together. We bridge divides. We listen and we understand. We are practical about the problems we face, but endlessly optimistic and ambitious about our capacity, together, to overcome them.

At a crossroads in Britain's history, we need ideas for renewal, reconnection and the restoration of hope. Challenges from populism to climate change remain unsolved, and a technological revolution dawns, but the centre of politics has been intellectually paralysed. Demos will change that. We can counter the impossible promises of the political extremes, and challenge despair – by bringing to life an aspirational narrative about the future of Britain that is rooted in the hopes and ambitions of people from across our country.

Demos is an independent, educational charity, registered in England and Wales. (Charity Registration no. 1042046)

Find out more at **www.demos.co.uk**

DEMOS

PUBLISHED BY DEMOS MARCH 2021

15 WHITEHALL, LONDON, SW1A 2DD
T: 020 3878 3955
HELLO@DEMOS.CO.UK
WWW.DEMOS.CO.UK