DEMOS

GOOD FOUNDATIONS

WHY DEMOCRACIES SHOULD CARE ABOUT THE WIRING OF THE INTERNET

JOSH SMITH
CIARAN CUMMINS
ALEX KRASODOMSKI-JONES

MARCH 2021

This project was supported by:

GCHQ

Published by Demos March 2021
© Demos. Some rights reserved.
15 Whitehall, London, SW1A 2DD
T: 020 3878 3955
hello@demos.co.uk
www.demos.co.uk

CONTENTS

EXECUTIVE SUMMARY

The design and policing of online spaces bears directly on many of the most important problems faced by democracies today. Many proposed solutions, however, barely skim the surface of the Internet as a technology. Unseen beneath growing public debates around privacy, misinformation and online harms lie layer upon layer of infrastructure and code, sending the messages which make up the visible parts of the Internet. These layers are governed by technical protocols, changes to which affect the complex human societies which exist online. Those aiming to build a better web cannot afford to ignore the foundations upon which it is built.

Protocols, and the Internet more broadly, are developed and governed by a handful of acronym-friendly groups - the IETF, the ITU, the IGF - among others. Many operate on the principles of 'multistakeholderism' - a form of democratic governance which helps groups of organisations to work on common problems, spreading power and decision-making out across stakeholders. This ideal is worth protecting, and it will require concerted effort from their members to do so - as well as to defend these groups from capture by the powerful, and from closing themselves off to outside ideas.

Technology companies and states both wield outsized influence over the Internet. Their power is exerted both over the organisations which develop protocols, and over how and whether their recommendations are implemented. Those able to control a country's communications infrastructure, or change the settings in web browsers used by millions, can unilaterally affect the protocols used by customers and citizens, changing the types of data sent by their computers and the actors to which that data is sent - often without their knowledge.

In this paper, we examine two examples of protocols which may represent the next evolution of the Internet: New IP, developed by China's Huawei, and DNS over HTTPS (or 'DoH'), developed and championed, among others, by the Mozilla Foundation and Cloudflare. For each, we discuss the significant effects which these changes could have on the human and social layers of the Internet. We also take a hard look at the 'multistakeholderist' groups shaping the rules of the Internet.

The relationships between governments, civil society, the groups who govern and develop protocols, and the technology companies who often employ their members are critical in the battle to build a better web. Where motives can be aligned, alignment should be found. Where they cannot, those without the power to implement protocols must be empowered to interpret and challenge the decisions of those who can. To do this, it is crucial that policymakers, citizen groups and technologists are able to find common ground. With this paper, we hope to contribute to this.

INTRODUCTION

HOW CAN STATES AND CIVIL SOCIETY MAKE THE INTERNET BETTER?

Across the Western world, the period of unfettered growth and development online is coming to an end as governments begin to roll out legal and regulatory regimes. These changes, in the eyes of regulators, legislators, the media and the public, have been spurred by scandal. People from across these groups looked at the Internet, and decided they weren't happy with what they saw.

The public attention paid to the Internet's content layer - the thin, visible crust that sits on top of dozens of layers of technology and infrastructure - might well be distracting us from where change actually takes place. What if the battles for a good web, fought at present across those parts of the web we can see, are doomed to be lost on the bits we can't?

This is not to say that those arguing for a new settlement over the web have been fighting the wrong battle. The content layer - Facebook, WhatsApp, Google, 4Chan and the billions of online spaces and applications that comprise it - is worthy of attention. Decisions made around how the Internet allows people to represent themselves and exchange information affects the lives of billions. But we must not lose sight of the foundational layers that make up the Internet. These layers are governed by a set of standards far more precise and effective than we have been able to apply at the content level: Internet protocols - a set of conventions governing the transmission of data.

These protocols detail best practice for those who run the infrastructure underpinning the web, and are under constant review. There are a number of reasons why they might change. Some changes are motivated by a wish to solve difficult problems, by engineers optimising for faster or more stable data transfer. Other changes have been made by corporations interested in improving their services to boost profits or consolidate market power, or states wishing to control the information accessible to their citizens. As we will see, changes propelled by these motives are often presented as a way to increase speed, improve the user experience, or to make people safer.

While many of these proposed changes are discussed the public domain, many are couched in impenetrably technical language and inscrutable to those affected. Representatives tasked with navigating the social impacts caused by these changes - let alone end users - are too often unable to judge what the impact of new proposals might be; to see how they will affect the balance of online power between citizens, governments and technology companies. This must change. Just as policymakers, the public and civil society should care about how these spaces are governed at the content level, those who want to protect or improve the web need to be able to go deeper.

This paper explains what protocols are: how they work, why they matter and how they are governed. It explores the implications of this approach, and urges a closer relationship between the architects of Internet protocols and those responsible for the publics they affect. This is not to say the public need to understand the intricacies of routing protocols or HTTPS - indeed, the web has to a great extent succeeded because it allows the uninterested not to care about these things. However, we need to get better at discussing the social impact of technical changes. To do this, those who want to solve human problems on the Internet need to account for the changing technology which underpins it, and those who are interested in the technology cannot ignore the human impact of their decisions.

WHAT ARE PROTOCOLS?

In order to make the case for the importance of protocols to online life, it helps to understand a few long-standing architectural features of the Internet. Two of these are the Internet's layered design, and the 'end-to-end principle', each of which we touch on below. These are not full technical descriptions, but aim to provide some fundamental points.

INDEPENDENCE BY DESIGN - THE LAYERS OF THE INTERNET

The Internet is made up of separate but interconnected layers of technology, each of which can be changed without impacting the rest of the stack.

The Internet can be separated into distinct conceptual layers, each of which does a different job. At the top sits the application layer. This is the visible, functional part of the Internet, composed of programs which fetch and display videos and email, control what gets onto your Facebook feed and conduct the million other tasks to which online data can be turned. At the bottom is the layer of physical matter which carries Internet traffic - miles of copper wire, glass fibre and air that carries wireless transmissions.

There are a few models for what happens between these upper and lower layers - how the electrical impulses carried by wires are translated to applications. Some models have seven layers in total, others four - it depends who's telling the story. For our purposes, the detail here is besides the point, and for our purposes we will refer to this middle section as the 'transport layer'.[1] Its job is to make sure the data which makes up the application layer gets to the right place, and can be understood when they arrive.

Crucial to the success of the Internet has been the fact that these layers are designed to talk to each other through standardised interfaces, but otherwise work independently. If I am writing code on the application layer - designing, say, a website which allows people to share videos - I don't need to know whether my users will access my site by copper wire or through WiFi. Their videos will upload either way.

This layered design has significant benefits. It has allowed a diverse group of people to improve the Internet by working on the problems which hold their interest - whether that's designing accessible websites or the best way of shining a laser down a hair-like strand of glass - without their choices and innovations disrupting the layers above them. The Internet owes much to the work of engineers and other interested parties informally repurposing existing systems for new uses, and contributing new code where functionality was missing.

The problem with this neat technical separation lies in the layer above the applications: it lies with us. The very topmost layer of the Internet, of any technology, is unruly, chaotic, and refuses to be confined: unlike tweaks to the efficiency of network cables, problems in the social and content layers - the human layers - influence, and are affected by, everything else in the stack.

[1] For a deep drive into one of these models, chapter 4 of Jonathan Zittrain's book The Future of the Internet (And How to Stop it) provides a good overview. See Zittrain, J. The Future Of The Internet And How To Stop It. Yale University Press, 2008. Available at http://yupnet.org/zittrain/ [accessed 15 March 2021]

EFFORT AT THE EDGES

By design, processing happens at each end of Internet messaging, rather than in the middle. This makes centralised control and oversight more difficult.

Many of the protocols which make up the transport layer of the Internet have stood the test of time. TCP/IP - a pair of protocols which, in a nutshell, ensure that the messages which make up the Internet can be i) properly addressed on sending and ii) assembled and understood once they've reached their destination - was first proposed back in 1974. While tweaks and improvements have been made to these protocols, their fundamentals have remained unchanged since their inception. Together, they still underpin the majority of Internet traffic: in 2010, 85% of Internet communication took place over TCP/IP.[2] However, as we explore below, new protocols are arising to take their place.

The flexibility of these protocols has enabled the Internet to keep delivering packets through an explosive expansion of users - and uses - over the last 50 years. It has also influenced the ways in which the network is designed and used. One impactful decision made by Vint Cerf and Bob Kahn, the engineers who first proposed the protocol, is the much-cited 'end-to-end' principle. This essentially states that the difficult tasks involved in packaging up and addressing a message, and in processing them once they've arrived (along with other services) should happen at each end of the network, rather than being the job of the machines which route the messages. In Cerf's design, the Internet has smart edges - computers, phones and servers - and a simple middle - routers whose only job is to pass messages efficiently from one point to another.

This design makes the Internet more difficult - though not impossible - to control centrally, at least at the network level. (Recent events such as the effective removal of the social media site Parler from the web suggest that other forms of central control - especially from groups of companies with effective monopolies over distributed web hosting - are still very much possible.) Since TCP/IP packets are designed to be routed in the same way whatever data they contain, and don't require any knowledge of who is at each end of the package beyond an IP address, it's theoretically impossible for systems using this protocol to treat different types of communications differently - for instance, for Internet service providers (ISPs) to charge customers more for gaming than for accessing Wikipedia.

THE EROSION OF END-TO-END

Over time, states and corporations have found ways to better oversee what information is being shared over the Internet, but these techniques are implemented in spite of the protocols as they were designed.

That, at least, is the theory. In practice, those machines in the middle of the network - including ISPs, corporate networks, and the companies who build applications - have developed a variety of methods to filter, censor and shape the traffic which passes through them. As the Internet Society pointed out in 2004, these shifts have often been prompted by external forces, as "corporate network administrators and governmental officials have become increasingly demanding of opportunities to interpose between two parties in an end-to-end conversation".[3]

This is also driven by consumers, as we, in the age of remote working, demand ever more complex tasks of our Internet connections, as well as safety features such as parental filtering. The UK's 2017 Digital Economy Act made it legal for ISPs to block packets arriving from certain websites, as long as this is mentioned in their terms of service. Many have followed suit, maintaining their own, often broad, lists of blocked sites.[4] This represents a move of services away from the ends of the network, and into the centre.

Much of this filtering is accomplished by ISPs during a process called 'DNS resolution' - essentially the process by which the web address that a browser has requested (e.g. 'www.demos.co.uk') is translated to the actual 'IP address' of the computer which hosts that webpage (172.67.171.247).[5] This translation is often provided by an ISP, or by services recommended by an ISP, allowing them to refuse to translate certain requests. Blocking sites in this way is one of the tools used by the Chinese state to erect its 'Great Firewall'.[6]

[2] Qian, Lei & Carpenter, B. A flow-based performance analysis of TCP and TCP applications. IEEE, 2012, pp.41-45. Available at https://ieeexplore.ieee.org/document/6506531 [accessed 15 March 2021]

[3] Kempf, J. Autein, R. IAB. RFC 3724: The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture. IETF, 2004. Accessible at https://tools.ietf.org/html/rfc3724. [Accessed 15th March 2021]

[4] See the Digital Economy Act 2017, section 104, retrieved from https://www.legislation.gov.uk/ukpga/2017/30/section/104/enacted. An excellent explainer of UK content filtering is provided by the Open Rights Group, Content Filtering by UK ISPs. ORG wiki, last updated 2019. Available at https://wiki.openrightsgroup.org/wiki/Content_filtering_by_UK_ISPs [accessed 15th March 2021]

[5] For a clear explanation of how DNS works in practice, see Clark L. Cartoon intro to DNS over HTTPS. Mozilla hacks, 2018. Available at https://hacks.mozilla.org/2018/05/a-cartoon-intro-to-dns-over-https/ [accessed 15th March 2021]

[6] See the anonymously submitted paper Towards a Comprehensive Picture of the Great Firewall's DNS Censorship. Unix conference, 2014. Available at https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf [accessed 15th March 2021]

Restricting access to content through DNS is also used to combat the distribution of images of child sexual exploitation and abuse (CSEA). The Internet Watch Foundation shares a list of known CSEA websites with the UK Internet industry, which are then universally blocked. By the IWF's own admission, this blocking is only part of an effective response: a "short-term disruption tactic which can help protect Internet users from stumbling across these images, whilst processes to have them removed are instigated" - but it is an important tool in tackling what remains an intransigent and severe online harm.[7]

CHANGING THE TOOLS

New protocols put forward by interested states and corporations could change the way the Internet transmits data. These changes will have human consequences.

While the fundamental ideas behind TCP/IP have been in place from the early 1980s, the protocols which govern how data is sent online are constantly being tinkered with, improved and adjusted. Crucially, there is no central authority which enforces the application of these changes. Internet protocols are contingent; they are suggestions rather than laws, and whether they are used and how they are implemented is at the discretion of those running and using the network. If I chose to address an envelope with, say, your current latitude and longitude, rather than your postal address, Royal Mail is unlikely to be able to deliver it - but one can imagine a reality where a competing provider might.

This advisory nature impacts the Internet in a couple of important ways. First, it ensures that change is incremental, and moves from working state to working state. For a protocol to be successful, it must be adopted in the 'real world' by bodies which will be directly harmed by, and thus resistant to, changes which damage their ability to operate. Second, it means that any company or state which controls a sufficient amount of the web's infrastructure has a huge amount of power to decide which protocols that infrastructure uses, and to convince others to follow suit. Below, we examine modern protocols developed by two such powerful groups - states and technology providers - and discuss the ways in which they might affect the awkward human layer of the Internet.

State protocols: New IP

In May 2020, Huawei - a company over which the Chinese state exercises significant control - released a short article, setting out the vision behind what the company called the "New IP Initiative", part of what the company calls the "next evolution of Internet technologies".[8] The article argues that, to support emerging technologies - namechecking the exciting prospects of holographic communication and autonomous driving - the Internet needs a top-to-bottom redesign, led by Huawei.

The Huawei article is not a technical specification, and little is currently known about exactly how "New IP" would work. However, it hints at a few indicative changes. For instance, Huawei states that New IP would enable "semantic addressing", allowing packets to be addressed using an identifier of flexible length, which would tell the network more about the precise endpoint it's serving. Huawei argues that this could be used to help better route different kinds of requests; but an ID of indefinite length could also be expanded to identify a unique connection, phone or person - easily linked into China's existing and extensive systems of personal identification and surveillance.

Huawei explicitly states that this new initiative, and the protocols introduced under it, is not designed to change Internet governance or increase Chinese control. However, it is not clear that their argument for New IP's necessity holds water. Indeed, many solutions to the problems which Huawei cites to justify a new approach, such as 'IP address spoofing', already exist. In a response to the company's article, the Internet Society points out that:

> *"it is [also] important to understand the difference between defining a capability in a standard and deploying it in operational networks. For example, methods for authenticating users connecting to the Internet and detecting and preventing IP address spoofing have been defined in RFCs and available on equipment for years, but aren't necessarily deployed in all networks.[9]"*

[7] IWF. URL List Policy . Available at https://www.iwf.org.uk/become-a-member/services-for-members/url-list/url-list-policy [accessed 15th March 2021]

[8] Huawei's ownership and governance are unclear - the company itself protests that it is "not owned or controlled by, nor affiliated with the government", but the company is not publicly traded - given existing Chinese legislation requiring companies to share data with the state on request, we believe the above formulation stands. A useful overview of this is given in the New York Times: Raymond Z. Who Owns Huawei? The Company Tried to Explain. It Got Complicated. New York Times, 2019. Available at https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html [accessed 15th March 2021]. Huawei's New IP paper can be found here: https://www.huawei.com/uk/industry-insights/innovation/new-ip

[9] Sharp, H, Kolkman, O, Discussion Paper: An analysis of the "New IP" proposal to the ITU-T, [Internet Society, April 2020] Available at https://www.Internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/ [accessed 15th March 2021]. 'RFC' stands for "Request for Comments", the name given to publications by bodies associated with the Internet Society.

Some of the other issues which Huawei claims as dealbreakers, such as the need for interoperability between multiple new types of device, are problems which the Internet already has an excellent historical track record of solving, having evolved from a system connecting a handful of military supercomputers to one which allows billions of devices - from phones to games consoles and smart light bulbs - to chatter away to one another.

The Internet Society protests that Huawei's proposal duplicates work already underway and is likely to result in "multiple non-interoperable networks," causing the precise problem it claims to solve.[10] A separate question to whether it will work, however, is what this state-led approach might mean for the Internet. Since protocols are advisory, anyone uneasy at China's approach should in theory be free not to support New IP, and there will be barriers to adoption of a system which doesn't work better than the status quo. In practice, and since China has form in blocking access to services which don't align with its objectives, companies who do not adopt or support New IP may find they lose access to a billion-strong market, putting them at a serious commercial disadvantage.

To increase this pressure, and as pointed out in the Financial Times, China is producing this protocol with the International Telecommunications Union (ITU), a body whose recommendations "legitimise new technologies and systems in the eyes of certain governments — particularly those in the developing world who don't participate in other Internet bodies. Ultimately, they give a commercial edge to the companies who have built the tech they are based upon". States may not be able to insist that their technologies are used outside their borders, but can exert diplomatic pressure on others to do so.

Industry protocols: DNS over HTTPS

Arguably, the entities which currently exercise the most power over the development of new protocols are technology companies. This isn't surprising - after all, they employ a large proportion of the engineers with the skills and interest needed to effectively improve the Internet. They also have a clear commercial interest, not only in being able to improve their services, but also in consolidating the power they already wield as controllers of much of the web's infrastructure.

An example of a new protocol developed by a tech company is 'DoH' - for 'DNS over HTTPS'. In a nutshell, this encrypts DNS requests made by your browser - again, requests for the IP address (172.67.171.247) belonging to a given website (www.demos.co.uk). The machines which handle these requests are called 'resolvers', and by default these are often run or recommended by your ISP - though browsers can be configured to use an alternative.

With traditional DNS, these requests are made in the open. Resolvers, as well as other parties in the network, can see the address of the computer making the request in the first place, and which site is being requested. DoH changes this by encrypting these requests, meaning only your computer and the resolver can see which site you're asking for.[11] This protocol was initially defined in 2018 by the Internet Engineering Task Force, or IETF - a global group of engineers who are influential in setting Internet standards, and who we discuss in detail in our section on governance below. DoH has since been developed and championed by the US tech company Cloudflare and the Mozilla Foundation, responsible for the Firefox web browser. In February 2020, Mozilla began switching Firefox traffic in the US to use DoH by default, and Firefox users worldwide can configure their browser to use the protocol.[12]

There are good reasons to want to encrypt DNS requests. Two key reasons cited by Mozilla are privacy and increased control over data.[13] Under the protocol no one except the resolver can read your request, including your ISP. This prevents bad actors from being able to see which sites you are visiting, reducing the possibility that your request will be redirected away from its intended recipient, or data on your browsing habits used for commercial gain.

By bypassing ISPs, however, a number of safeguards currently provided at this level become moot. At present, UK ISPs' ability to block requests at the DNS level allows them to comply with court orders to block specific sites, as well as allowing for parental control over browsing. It also allows them to play a role in blocking dangerous content - filtering out malware, for example, or blocking sites which host child sexual exploitation material. Consumers switching to DoH to gain 'increased security' will lose these safeguards, potentially without realising that they are no longer in place. Additionally, while it's true that these changes will prevent local ISPs

[10] Sharp, H, Kolkman, O, Discussion Paper: An analysis of the "New IP" proposal to the ITU-T, [Internet Society, April 2020] Available at https://www.Internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/ [accessed 15th March 2021]. 'RFC' stands for "Request for Comments", the name given to publications by bodies associated with the Internet Society.

[11] This is explained in more detail in Lin Clark's excellent 2018 article "A Cartoon intro to DNS over HTTPS" https://hacks.mozilla.org/2018/05/a-cartoon-intro-to-dns-over-https/

[12] See Deckelmann S., Firefox continues push to bring DNS over HTTPS by default for US users, [Mozilla, 2020] Available at https://blog.mozilla.org/blog/2020/02/25/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users/ [accessed 15th March 2021]

[13] Mozilla, Firefox DNS-over-HTTPS [Mozilla] Available at https://support.mozilla.org/en-US/kb/firefox-dns-over-https [accessed 15th March 2021]

from gaining value from browsing data, it risks promoting a massive concentration of value in the few resolvers who currently support DoH, and - given that the largest resolvers are currently US based - eliminates the ability of UK regulators to impose limits on their use of data.

To some extent, these problems may be issues of implementation, to be smoothed out as use becomes more widespread. As a presentation from BT put it in 2019, "DoH as a protocol has good privacy and security intentions" but "may create ISP implementation issues and unintended consequences across the ecosystem".[14] In fairness, Mozilla is working to mitigate some of these consequences, insisting, for example, that partners providing DoH to Firefox users are contractually obliged to restrict the commercial benefit they can gain from browsing data, and are prohibited from selling it.[15]

What makes DoH notable here is that it represents a significant transfer of power away from national courts and ISPs, and towards the very companies, such as Google, Cloudflare and Mozilla, who are building and implementing it. It employs features which will increase user privacy, but which are likely in the short term to affect the ability of end users and the UK legal system to reduce the harms which people are exposed to online. Just as liberal democratic societies should not blindly accept China's promises that New IP is the only way to save the Internet, we should also be wary of protocols proposed by powerful tech companies which would improve networking in a way which further consolidates power in their hands.

To act as a counterbalance to this power, it is crucial that a wide variety of groups, including those concerned with reducing harm online, are able to contribute meaningfully to discussions around Internet governance, and develop workable alternatives or modifications. We examine the routes into this engagement below.

[14] BT, A UK ISP view on DNS over HTTPS, [BT, 2019] Available at https://www.icann.org/sites/default/files/packages/ids-2019/08-fidler-icann-dns-symposium-a-uk-isp-view-on-doh-issue-11may19-en.pdf [accessed 15th March 2021]
[15] You can read this contract here: Security / DOH-resolver-policy, [Mozilla wiki, last modified 2020] Available at https://wiki.mozilla.org/Security/DOH-resolver-policy [accessed 15th March 2021]

WHO GOVERNS PROTOCOLS?

WHO GOVERNS PROTOCOLS?

The governance of protocols is carried out by an array of institutions, each with varying rules and membership.

At a glance, Internet protocols are designed, adopted and governed as follows: first, technical experts propose and debate protocols alongside civil society, academia, supranational and state representatives and firms, in various fora and institutions around the globe. These are then offered up as suggestions for how to proceed, with those who control systems deciding if and how they are adopted, based on commercial and political interests, and user and technical preference.

The institutions that have historically been responsible for setting Internet standards vary in function. Some exist solely for this reason whereas others - such as the International Telecommunications Union (ITU) and the International Organisation for Standardisation (ISO) - also address standard-setting more broadly. On the next page, we give a rundown of some of the key actors, though these are just the tip of the iceberg when it comes to governance of Internet protocols - numerous other entities exist to cater to various aspects of their design, governance and adoption.

HOW ARE PROTOCOLS GOVERNED?

Internet protocol governance exemplifies 'multistakeholderism', wherein states, companies, civil society and others attempt to balance their differing interests and no group - in theory - has complete power.

The inherent precariousness of protocol governance is encapsulated neatly by MIT's Alex Galloway: "Protocol is a technique for achieving voluntary regulation within a contingent environment".[16] In reality - and as the varying forms of governance highlighted in the table above suggest - governance of protocols is a varied and contested process: an attempt to balance a multitude of interests.

To achieve this balance, protocol governance has generally adopted the approach of 'multistakeholderism'. This is a form of governance not exclusive to, but exemplified by, the Internet. As Laura DeNardis and Mark Raymond explain, it can be defined as:

> *"[...] two or more classes of actors [e.g. states, businesses, and civil society] engaged in a common governance enterprise concerning issues they regard as public in nature [e.g. the distribution of IP addresses], and characterized by polyarchic authority relations [i.e. where power and authority is spread across many actors] constituted by procedural rules".*[17]

[16] Galloway, A. Protocol: How Control Exists After Decentralization. MIT Press, 2004, p.7. Emphases added.

[17] Raymond, M., Denardis, L. Multi-stakeholderism: Anatomy of an Inchoate Global Institution. Cambridge University Press, 2015 p.2.

TABLE 1.
KEY ACTORS IN SETTING INTERNET STANDARDS

	The Internet Engineering Task Force (IETF)	The World Wide Web Consortium (W3C)	Internet Assigned Numbers Authority (IANA)	The International Telecommunications Union (ITU)	Internet Governance Forum (IGF
Founded	1986	1994	1976	1865	2006
Key Responsibility	Actual technical development of many protocols. Can only recommend these rather than require their adoption.	Specifically develops standards for the World Wide Web.	Coordinates unique identifiers set out in protocols, including IP addresses (which are assigned to each device connected to the Internet)	Responsible for various global communications coordinations, including some protocol setting, e.g. in mobile Internet networks.	A forum for international, multistakeholder discussion of Internet policy. Meets annually and does not have any binding outcomes.
Membership	Open to all: anyone allowed to participate either online or in one of its multiple annual meetings.	Open to all, though generally held by organisations rather than individuals.	Complex. Public Technical Identifiers (PTI), which carries out the operations of IANA, is a non-profit with no members, only a board of directors. PTI is an affiliate of the Internet Corporation for Assigned Names and Numbers (ICANN), which is open to all.	Open to invited organisations. Individuals cannot be members. Members include 193 states and over 700 universities and private sector entities.	Attended by individuals and organisations; open to accredited members of two other UN initiatives (the World Summit on the Information Society and the Economic and Social Council) and open to registration from others.

	The Internet Engineering Task Force (IETF)	The World Wide Web Consortium (W3C)	Internet Assigned Numbers Authority (IANA)	The International Telecommunications Union (ITU)	Internet Governance Forum (IGF
Overall control	Ostensibly internally **democratic:** run at the highest level through member- nominated directors. Operations are supported by the Internet Society (ISOC), a global nonprofit.	Executive: administered via a joint agreement between MIT, ERCIM (a research consortium), Keio University and Beihang University. A team of full-time staff are led by a Director and CEO.	Governmental: initially run under the auspices of the US Government and ICANN, IANA was transitioned to purely being run by ICANN (functioning as an NGO) in 2016.	Intergovernmental: the ITU is a specialised agency of the United Nations.	Intergovernmental: the UN Secretary-General appoints the Multistakeholder Advisory Group (MAG), who determine the IGF's proceedings. The MAG's members represent states, firms, civil society, academia, and technical communities, across all five UN regional groups.
Worth noting:	Members are not technically representatives of their employers, though many work for technology companies and these are also major financial supporters of the IETF.	While public participation is encouraged, the bulk of its work is carried out by member-only groups.	Distributes authority among various stakeholder committees, who have varying powers.	Non-state members have to pay a membership fee, and are not entitled to the same participatory and approval powers as state representatives.	Nation-level IGFs exist which aim at multistakeholder representation like the global IGF. The UK IGF (founded 2009) secretariat is provided by Nominet, the UK national domain name registry.

These rules include how membership is determined, how decision-making capacities are distributed across members, and standards for members when evaluating one another's proposals.[18] The diverse membership of governing bodies - including states, intergovernmental organisations, companies and civil society - and the varying relations of power and authority between them, mean that these rules "remain in flux".[19] As a result, multistakeholder governance cannot straightforwardly or consistently be described as either fully democratic or fully hierarchical.[20] As a form of governance by actors who may represent commercial, civil society or citizen interests, it does not straightforwardly or consistently overlap with the more traditional models of governance: corporate shareholder, not-for-profit stakeholder or state-representative. Multistakeholderism also crucially departs from traditional multilateral governance: it includes stakeholders who are not just states.

Power within these bodies is often flexible. Some allow a degree of multistakeholder input and influence, whilst retaining overriding authority for certain stakeholders. The ITU, which is leading the charge on developing China's New IP, reserves more voting rights for state members: even when ITU multistakeholder working groups have made recommendations, often, state members are the ones who have the final say. Other groups embrace the tensions of multistakeholderism: they seek only a degree of consensus in their decisions and make explicitly non-binding commitments. These include the IGF and IETF, whose recommendations are designed to influence the decisions of policymakers and the actual deployers of protocols - primarily tech companies - respectively. Indeed, the IETF embodies this ethos to their core, famously favouring "rough consensus and running code" over other forms of governance. Pete Resnick wrote in a 2014 'Request for Comments' (RFC) (the publicly documented archive of IETF (and ISOC) consensus):

> *"[...] our credo is that we don't let a single individual dictate decisions (a king or president), nor should decisions be made by a vote, nor do we want decisions to be made in a vacuum without practical experience. Instead, we strive to make our decisions by the consent of all participants, though allowing for some dissent (rough consensus), and to have the actual products of engineering (running code) trump theoretical designs."*[21]

Even for bodies concerned with the technicalities of protocols, a sharp line between 'mere' design of protocols and actual governance over their adoption can't always be straightforwardly maintained. A distinction between governance and design can exist where an institutional context maintains that formally - for example, where an executive and legislature have different formal powers in relation to the creation and enforcement of law. But informal powers go beyond this in practice, allowing the lines between designing proposals, deciding upon them and governing their use, to blur.

Leaving aside potential commercial or state influence upon members, as independent experts protocol designers still play a considerable role in affecting what is subsequently governed in other fora and adopted in the market.[22] In the case of the IETF, members "choose to create" the technology that they do with a shared set of values in mind.[23] As such, they exercise a knowing degree of control over the direction of protocols and maintain preferences about this.[24] Moreover, given the IETF's technical inaccessibility, whatever their values, they have a de facto power to shape protocols in a way that others do not, and exercise this with less public oversight than other expert bodies might be held to. "Rough consensus" is still a form of decision-making and one with real consequences: though these decisions aren't binding, given these designers' technical vantage points (and the potential for state and/or commercial support behind them), their decisions are unlikely to be completely overlooked in practice.

[18] Raymond, M., Denardis, L. Multi-stakeholderism: Anatomy of an Inchoate Global Institution. Cambridge University Press, 2015 p. 19.

[19] Raymond, M., Denardis, L. Multi-stakeholderism, p.2.

[20] Raymond, M., Denardis, L. Multi-stakeholderism, p.1. For a useful discussion of this topic: Chenou, J. 'Is Internet Governance a democratic process? Multistakeholderism and transnational elites'. ECPR General Conference, 2011. Available at: http://www.media-ucn.co.uk/Seminar%20Readings/Soc%20M077/Reading%20for%2017th%20March/net%20govt.pdf. [Accessed 5 January 2021]

[21] Resnick, P. 'RFC 7282 - On Consensus and Humming in the IETF'. IETF, 2014, p.2. Available at: https://tools.ietf.org/html/rfc7282 [Accessed 5 January 2021]

[22] For an insightful study of this as it plays out in the IETF see: Weyrauch, D., Winzen, T. Internet Fragmentation, Political Structuring, and Organizational Concentration in Transnational Engineering Networks. Global Policy. Vol. 12, issue 8, 19 October 2020, pp.51-65. Available at: www.onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12873 [Accessed 12 March 2021]

[23] Alvestrand, H. RFC 3935 - A Mission Statement for the IETF. IETF, 2004, p.4. Available at: https://tools.ietf.org/html/rfc3935. [Accessed 12 March 2021]

[24] Cath, C. 'The Technology We Choose to Create: Human Rights Advocacy in the Internet Engineering Task Force'. GigaNet Symposium, 2 November 2020, p.9. Available at: https://www.giga-net.org/2020symposiumPaper/Cath.pdf?_t=1602675821 [Accessed 5 January 2021]

EVALUATING MULTISTAKEHOLDERISM

Though multistakeholderism is rejected by some for being too democratic, even democrats face a challenge to ensure its ideals are genuinely realised.

The degree to which you think multistakeholderism is a good idea will depend on your view of the basic ethos behind it. It is essentially democratic, calling for input and influence from a wide range of actors. As such, in the eyes of those who oppose the deference to stakeholders besides, for example, the state, multistakeholderism carries an inherent weakness.

A multistakeholderist approach, however, doesn't automatically imply that decisions are made by the breadth of a group's membership. The questions of how much input is required to make a decision, and from which stakeholders, are explicitly left open by the approach. In practice, this can lead to weaknesses, if this open-endedness is not addressed through the clear setting of procedural rules - or if rules are set out but not followed. These weaknesses can include a lack of clarity over what counts as 'sufficient' multistakeholder input; unequal representation or scope of participation across stakeholders; an inability to reach consensus; exclusivity and unwillingness to listen to different views; and too slow a pace of decision-making.[25] Groups can also hold particular power over - or even effectively capture - organisations, exerting undue influence over the development or adoption of recommendations. This risk is present particularly where actual power imbalances go unchecked and 'multistakeholderism' becomes mere rhetoric.

> *"Let not the ideals of democracy in multistakeholderism be reduced to shadowboxing – where emerging hierarchies are denied and those that wield power escape with no accountability"*[26]
>
> – Anita Gurumurthy

All these issues impact the ability of multistakeholder processes to have binding impact and to be perceived as legitimate.[27] As the range of stakeholders who engage increases and the complexity of the issues faced grows, many of these issues may be further exacerbated.[28]

Ultimately, these weaknesses are allowed to manifest if multistakeholderism as a democratic ideal is allowed to become a "static" political fiction, as Jeanette Hofmann calls it.[29] Hofmann is not suggesting it is a problem for multistakeholderism that it relies on a potentially romanticised vision - the problem arises when we abandon or cease to tolerate any critical reflection.[30] For multistakeholderism to remain responsive to challenges in practice, its scrutiny must remain dynamic.[31]

Encouragingly, some of its best manifestations in Internet protocol governance are fora with lively cultures of debate, with the IETF a prime example. One way to improve multistakeholderism in the IETF could be for it to retain a focus on scrutiny of its multistakeholder shortcomings, such as its linguistic, financial, and cultural accessibility, lack of sufficiently broad demographic representation, and lack of dialogue with civil society to improve social and ethical considerations in the design of protocols.[32, 33, 34] Inattention to these and other potential threats to democratic aims - particularly capture of the governance processes by powerful stakeholders, promoting outcomes that unfairly benefit their interests over others - will result in the degradation of multistakeholder protocol governance in practice.

Alongside its commitment to multistakeholderism, the IETF also places a deal of importance on its members being informed about the issues they're engaged with, with practitioner knowledge sought out and prized. This speaks to the need for competence in the highly technical context in which they work. Grand plans such as New IP, quite aside from any wider political concerns, needlessly upend the reliable process of building upon understanding gained through practice. Other features, such as open membership and public records at the IETF and national and regional extensions of the IGF, are strengths of certain Internet protocol

[25] Spuy, A. What if we all governed the Internet? Advancing multistakeholder participation in Internet governance. UNESCO Publishing, 2017, p.30. Available at: https://en.unesco.org/sites/default/files/what_if_we_all_governed_Internet_en.pdf. [Accessed 19 January 2021]

[26] Gurumurthy, A. Statement at the closing ceremony of WSIS plus 10 review. IT for Change, 2013. Available at: https://itforchange.net/sites/default/files/ITfC/WSIS%20+%2010%20closing%20statement%20by%20Anita%20G.pdf. [Accessed 12 March 2021]

[27] Gurumurthy, A. Statement at the closing ceremony of WSIS plus 10 review. IT for Change, 2013. Available at: https://itforchange.net/sites/default/files/ITfC/WSIS%20+%2010%20closing%20statement%20by%20Anita%20G.pdf. [Accessed 12 March 2021]

[28] Gurumurthy, A. Statement at the closing ceremony of WSIS plus 10 review. IT for Change, 2013. Available at: https://itforchange.net/sites/default/files/ITfC/WSIS%20+%2010%20closing%20statement%20by%20Anita%20G.pdf. [Accessed 12 March 2021]

[29] Hofmann, J. Multi-stakeholderism in Internet governance: putting a fiction into practice. Journal of Cyber Policy, 2016, p.44.

[30] Hofmann, J. Multi-stakeholderism in Internet governance, p.44.

[31] Hofmann, J. Multi-stakeholderism in Internet governance, p.44.

[32] Raymond, M., Denardis, L. Multi-stakeholderism: Anatomy of an Inchoate Global Institution. Cambridge University Press, 2015. p.14.

[33] Cath, C., Floridi, L. The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights. 2017. p.458.

[34] Cath, C., Floridi, L. The Design of the Internet's Architecture, p.453.

multistakeholder initiatives. They are testament to the way in which challenges in multistakeholder governance ought to be viewed not as inherent weaknesses, but rather as barriers to be creatively surmounted in an effort to move closer to the democratic ideal of multistakeholderism.

MULTISTAKEHOLDERISM: THE WORST FORM OF PROTOCOL GOVERNANCE, EXCEPT FOR ALL THE OTHERS

To retain and improve existing multistakeholder governance of protocols, we need an alliance between states that reject autocratic alternatives

Alternatives to multistakeholderism in protocol governance mean a ceding of control to fewer stakeholders. Support for this comes primarily from states, which can be split further into two groups. One group endorses what DeNardis and Raymond call the 'Shanghai Cooperation Organisation' view, which is held by China and Russia in particular. This is characterised by a minimisation or complete rejection of consultation with non-state stakeholders, and an emphasis on 'cyber sovereignty': "states' desires to extend the traditional concept of sovereignty to apply to all aspects of the Internet within their own borders".[35] This is seen by critics as a path to fragmentation of the global Internet as we know it.[36]

Another group is composed primarily of postcolonial states (DeNardis and Raymond refer to it as the 'Group of 77' view, in reference to the United Nations' developing country coalition) which favour greater state sovereignty, but not necessarily at the dismissal of other stakeholder input. This is in part because of their greater representation and existing voting rights in older multilateral institutions like the ITU, compared to newer institutions such as the IETF where they have less representation and wield less influence.[37]

For those who believe the best vision for the Internet is one in which it allows democracy to be protected and furthered, multistakeholderism remains preferable as a model for how governance of Internet protocols ought to be carried out. Diplomatically, campaigning against the Shanghai Cooperation Organisation view whilst addressing the legitimate concerns of the Group of 77 is essential to ensuring it remains the globally preferred model. The Group of 77 includes states which have been termed by Morgus et al. as the "digital deciders" - the trajectory of the Internet will be decided "just as much, if not more, on domestic developments in a group of undecided states".[38]

A fruitful starting point for diplomacy here comes from Lindsay Gorman, who suggests that the touted 'D10' club of democracies (the G7 plus South Korea, India, and Australia) should "in coordination with the private sector, conduct ongoing monitoring and assessment of the proceedings of international standards bodies".[39] This highlights the need to create a coordinated, allied approach to international support for promoting and improving the democratic credentials of Internet protocols' design. And Britain's advocacy of D10 in particular would have additional diplomatic benefits, beyond just consideration of the Internet, particularly given Brexit tensions.[40]

However, crucially the move should be to build up inclusion quickly beyond these 10 initial members. This is not only in line with the strategic consideration of the argument from Morgus et al. above, but more importantly, acknowledges the not unfounded potential perception that this is an effort to simply reinforce Western hegemony. This will require working to accommodate the postcolonial dimensions of Internet governance, such as asymmetries of control between the Global North and South of the latter's citizens' data and underrepresentation in bodies such as the IETF.[41] The inclusion of civil society is essential in this process, to ensure that 'assessment' by states and the private sector of international standards bodies doesn't support their interests to the detriment of other stakeholders.

[35] Raymond, M., Denardis, L. Multi-stakeholderism: Anatomy of an Inchoate Global Institution. Cambridge University Press, 2015. p.19.

[36] Sherman, J. Huawei's Global Advancement of Alternative Internet Protocols. Jamestown Foundation, 6 December 2020. Available at: https://jamestown.org/program/huaweis-global-advancement-of-alternative-Internet-protocols/ [Accessed 5 January 2021]

[37] Sherman, J. Huawei's Global Advancement of Alternative Internet Protocols, pp 19-20.

[38] Morgus, R., Woolbright, J., Sherman, J. The Digital Deciders. New America, 23 October 2018. Available at: https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/. [Accessed 5 January 2021]

[39] Gorman, L.P., A Future Internet For Democracies: Contesting China's Dominance in 5G, 6G, and the Internet-of-Everything. Alliance for Securing Democracy, 2020, p.4. Available at: https://securingdemocracy.gmfus.org/future-Internet/ [Accessed 11 January 2021]

[40] Brattberg, E., Judah, B. Forget the G-7. Foreign Policy, 10 June 2020. Available at: https://foreignpolicy.com/2020/06/10/g7-d10-democracy-trump-europe/ [Accessed 11 January 2021]

[41] Hicks, J. 'Digital Colonialism': why some countries want to take control of their people's data from Big Tech'. The Conversation, 26 September 2019. Available at: https://theconversation.com/digital-colonialism-why-some-countries-want-to-take-control-of-their-peoples-data-from-big-tech-123048 [Accessed 11 January 2021]

RECOMMENDATIONS

At a time when the spotlight is on issues such as health misinformation and online extremism, it is understandable that a topic concerned with the deep, technical underpinnings of the Internet would be out of the public eye. Yet the risks are of existential interest to all aspects of our online lives. There is, simply put, no good web without this good foundation. To ensure a liberal democratic future for Internet protocol governance, therefore, we make the following recommendations:

FOR THE UK GOVERNMENT

- We support the Government's recent commitment to protect "an accessible and interoperable global internet for future generations" through various means including support for multistakeholderism and greater diversity in standards bodies, as well as centering of the issue in the G7.[42] In addition, the Government should build on existing protocol governance presence, such as at the ITU, IGF and ICANN Governmental Advisory Committee. The previous Senior Policy Advisor on Internet Governance to the Department for Culture, Media and Sport, Mark Carvell, stressed the importance of bringing public policy priorities further into the design of Internet standards and his successor should be encouraged and supported in doing so.[43] This could include approaching the Internet Architecture Board about the creation of a dedicated UK government IETF liaison.
- The D10 collection of democracies (the G7 plus South Korea, India, and Australia) should be established with the inclusion of civil society, with a mandate to promote democratic credentials in Internet protocols' design alongside brokering discussion on the topic with 'Digital Decider' states. Technical government staff from the D10 should attend IETF stakeholder meetings.
- Liberal protocols need people who understand how to write them. To ensure protocol development is open to those besides corporations and states, it's crucial that as wide a range of people as possible have the freedom and tools to develop and experiment. The government should continue to focus on increasing broadband access and quality for all, and invest in building digital skills at an early age.

FOR INTERNET PROTOCOL MULTISTAKEHOLDER BODIES

- Ensure your commitment to multistakeholderism remains under scrutiny, to address issues such as lack of diversity and linguistic and financial barriers to participation. Experiment with innovative methods of multistakeholder engagement that may assist in reducing barriers to participation.[44]
- Formally institute your outreach efforts with stakeholders where they do not yet exist, and commit to regular external assessments of multistakeholder engagement standards.
- Discourage the siloing of integration of wider stakeholder input to protocol design, such as has occurred in attempts to promote consideration of human rights considerations in the IETF's routine work.[45]

[42] *Global Britain in a competitive age*. The Integrated Review of Security, Defence, Development and Foreign Policy. HM Government, 2021, pp.56-57. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/969402/The_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf [Accessed 16 March 2021]

[43] EuroDIG. Should public policy priorities and requirements be included when designing Internet standards? EuroDIG, 11 June 2020. Available at: https://eurodigwiki.org/wiki/Talk:Should_public_policy_priorities_and_requirements_be_included_when_designing_Internet_standards%3F_%E2%80%93_WS_05_2020 [Accessed 20 January 2021]

[44] For discussion of innovation in participation in such fora, see: Cogburn, D. Enabling effective multi-stakeholder participation in global Internet governance through accessible cyber-infrastructure. *Routledge Handbook of Internet Politics*, Chadwick, A. and Howard, P. (eds.). Routledge, 2009.

[45] Cath, C. The Technology We Choose to Create: Human Rights Advocacy in the Internet Engineering Task Force. GigaNet Symposium, 2 November 2020, p.9. Available at: https://www.giga-net.org/2020symposiumPaper/Cath.pdf?_t=1602675821 [Accessed 5 January 2021]. This is of particular importance given a recent further such attempt to address issues of equality. See: Font, F., Moore, K. 'Diversity and Inclusiveness in the IETF'. IETF, 2021. Available at: https://datatracker.ietf.org/doc/draft-gont-diversity-analysis/ [Accessed 16 March 2021]

FOR TECHNOLOGY COMPANIES

- Technology companies developing protocols, both within and independently of the IETF, should integrate both internal and public discussions around the likely social impact of changes throughout the design process. Externally, this could include convening workshops with civil society groups and accepting Select Committee invitations. Internally, companies should focus on increasing the diversity of staff and empower those tasked with developing and upholding ethical guidelines.

FOR THE PRESS

- The relative lack of journalistic coverage of protocol governance diminishes public understanding and scrutiny of the topic. Best practice should be developed and disseminated on how more journalists can engage.[46]

[46] For example, see: Cath, C., Oever, N.T., O'Maley, D. 'Media Development in the Digital Age'. CIMA, March 2017. Available at: https://www.cima.ned.org/wp-content/uploads/2017/03/CIMA-Internet-Governance_150ppi-for-web_REV.pdf [Accessed 5 January 2021]

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

CONTENTS