OUR DIGITAL FUTURE

A LABOUR PARTY CONSULTATION

Labour

CONTENTS

Foreword by Ian Russell	**2**
Introduction	**4**
1. Digital Innovation	**8**
2. Harmful Online Content	**13**
3. Personal Data and our Online Lives	**29**
4. Technology and our Public Services	**35**
5. Digital Inclusion	**42**
Conclusion	**48**
Appendix : Introduction to Consultation	**50**

FOREWORD : Ian Russell

Protecting young and vulnerable people from online harms is vital; this really is a matter of life and death. A stocktake of our digital world is long overdue. The internet has changed our connected world in a generation and brought with it many advantages. It is hard for us to remember how we lived our lives just a couple of decades ago. Then, mobile communication by phone was still a novelty for many and social media platforms had yet to be invented. Today's current big tech platforms were born at about the same time as my youngest daughter, Molly. The powerful tech corporations live on, sadly Molly ended her own life in 2017 and I am convinced what she found online helped kill her.

There are far too many people whose lives are detrimentally affected by what they experience online. It is for them, our next generation, that we urgently need to investigate why being mentally healthy seems to have become more elusive and we also need to find better ways to support those who need help. The introduction of the ICO's Age Appropriate Design Code and the proposed Online Harms legislation are just the beginning, a continuing process of review is needed if we are to create a safer online world. A digital consultation to thoroughly investigate all the effects new technology brings is essential if digital tech is to fulfil its intended benefits without the harmful content that is increasingly dominating the platforms.

This Labour Party consultation has the scope and ambition to inform our understanding of our new digital world and guide our future decision making about how to make it a better place. The consultation will help the UK become a world leader for the effective regulation required to make the internet a safer place. Only when we have identified, understood and tamed online harms will modern connected technology fully flourish and bring us all the widespread benefits it promises.

Ian Russell, Founder Molly Rose Foundation

Written August 2020 to launch Our Digital Future consultation.

INTRODUCTION

This is a report on the Labour Party's open consultation entitled Our Digital Future, held between 11 August and 16 October 2020[1]. We wanted to canvas views on one of the biggest issues of our time: namely, how we address the changing role of technology in our society. Our aim was to produce a set of principles to guide Labour's digital policy making, not just for the next election cycle but for the long-term.

In all we received more than 600 submissions from across civil society and industry including but not limited to tech platforms, trade unions, Constituency Labour Parties (CLPs), Labour members, charities, and non-governmental organisations (NGOs).

Policymakers and commentators often talk about the younger generations as "digital natives" but in reality we all must be digital citizens now to fully participate in society - a truth underlined by the challenges of the pandemic. Unfortunately, rather than feeling empowered by the potential of technology, too many people see an erosion of their rights and wellbeing.

Labour is worried about unregulated tech platforms and their overbearing influence on our policymakers and government. While it is easy to sound overly dramatic about these problems, ethical decisions with real world consequences are increasingly being concentrated in the hands of a few senior tech executives with little to no accountability.

Despite the variety of contributors, on certain matters there was a surprising degree of consensus in our consultation. Even tech companies themselves accept that the present regulatory system is highly unsustainable. Gone are the days in which tech companies can be left to govern themselves without

1 See Appendix pg.50

public oversight. There is a new and palpable sense of urgency around the governance of technology.

These responses should embolden the government to make the UK's Online Safety Bill as robust as it needs to be in order to effect real change. But this legislation – which had the potential to be landmark work and to set a new standard for the rest of the world – has been watered down and restricted in its scope.

It is clear from this consultation that many of the internet's problems cannot be solved by the ad hoc actions of individuals or individual companies, but instead require collective solutions. From the submissions, it was also apparent that we need new ways of implementing regulation if we are to keep up with the lightning pace of innovation. It is often said that the clunking machinery of the state struggles to adapt to change but, while there is some truth in this, it is not a reason for doing nothing. On the contrary, it should prompt us to find ways of anticipating and addressing problems before they reach the point of crisis.

This is one of the reasons Labour called for a principles-based framework to online harms, rather than just designating a list of specific harms which will soon be out-of-date. We need robust regulation encompassing the wide range of online harms moving away from the failed self-regulation approach, with effective sanctions that act as a deterrent and an effective regulator.

It might have been possible in the 1990s and 2000s to treat technology policy as a second-tier or isolated concern, but that is no longer an option. Technology is central to almost every political question of our era: how we grow the economy; how we protect our citizens; how we treat each other; how we govern ourselves and; how we allocate government resources and attention.

Labour wants Britain to be the best place to grow up in, to work in, to raise children in and to grow old in. We want empowered citizens who do not merely have access to the internet, but who are equipped with the skills and tools to make the most of technology and who are protected from those who use it to cause harm. To achieve this, we need a robust regulatory framework that protects users and enhances individual and national security.

We want people to have greater control over their online lives, to allow them to reclaim ownership of data currently harvested and monetised by tech platforms. People should also have the right to know how algorithms are used to make decisions on their behalf, through better transparency about the use of AI.

Furthermore, we want the UK to be at the forefront of innovation so that everyone can benefit from the Fourth Industrial Revolution.

In this report we have grouped the problems and potential solutions across five areas:

1. Digital Innovation
2. Harmful Online Content
3. Personal Data and our Online Lives
4. Technology and Our Public Services
5. Digital Inclusion

We recognise from the outset that a consultation of this kind is not a scientific exercise. Though many of the submissions were rooted in empirical research, many were not and did not claim to be. They instead reflected the concerns, anxieties and desires of respondents, who valued the opportunity to be heard.

We were grateful for the diversity of this feedback. It has allowed us to explore the most significant issues to formulate avenues for further enquiry and to lay down principles that can guide the next stages of policy discussion and development.

This report sets out our consultation findings and some thoughts on what might come next. Its purpose is not to prescribe specific policies. Those will come later.

Section 1: DIGITAL INNOVATION

INTRODUCTION

The UK boasts world-leading tech firms, but they are concentrated in our large cities and London in particular. Labour wants every region of the country to have the tools to start, scale and invest in the world-leading digital firms of tomorrow.

The lack of a serious industrial strategy over the last decade has hampered our ability to compete with other countries. Many UK companies are still unable to access the finance or skills they need and are often bought up by foreign companies before they can reach their full potential.

The UK led the First Industrial Revolution, and we can still lead the Fourth Industrial Revolution. But this will require a strategy to promote innovation across the country, while ensuring that it creates good jobs and benefits local communities.

To inform this strategy, we asked respondents: *"How can we promote digital innovation across all of the UK's regions and nations? How can we ensure it generates good, fulfilling jobs for everyone as we build back, better?"*

THE CURRENT SITUATION

Digital is a significant driver of economic growth in the UK. According to the annual TechNation report our tech sector contributes £149 billion to the national economy each year, employing nearly three million people.[2] The Department for International Trade has found that there are now 30 significant technology "clusters" across the country. Five of these clusters – London, Oxford, Cambridge, Manchester, and Bristol – sit in Europe's top 20 cities for tech investment.

[2] https://technation.io/report2020/

In addition to the direct contribution made by the tech sector to our economy, digital provides a number of other run-off benefits for other businesses and organisations. It helps to boost productivity by allowing rapid communications and effective data. It allows businesses to reach new customers at a much lower cost than traditional TV or print advertising, and drive sales in every country in the world.

The Covid-19 pandemic has underscored the need for a robust digital economy. Submissions highlighted three key conditions as particularly important for the pursuit of a first-class innovation economy:

(1) Infrastructure and capital: the raw ingredients that make innovation possible, whether hardware, software, broadband, or funding.

(2) Workforce: the skilled inventors, developers, scientists, and workers who drive digital growth.

(3) Strategy: the choices we make about how we innovate – which will not only define the digital economy, but who we are as a country.

Infrastructure and Capital

The starting point for many submissions was that digital innovation is not cheap or easy. It demands extensive investment – and will continue to do so if the UK is to remain competitive – but submissions told us that at present this investment is overly concentrated in a handful of areas or "clusters". It also requires world-class digital infrastructure, from full-fibre broadband to 5G. Chapter 5 – on the "digital divide" – looks more closely at the state of our digital infrastructure, but submissions were clear that there is much work to be done.

Workforce

Another clear priority in submissions was the need for a skilled workforce. Demand for digital skills in the labour market currently exceeds supply, both of basic computer literacy and specialist IT skills. This gap extends to elite digital talent such as world-leading experts in AI: while the UK trains many top innovators, they too often leave and take their talents to the US . Beyond technical skills, management and critical thinking were also cited as areas where there are shortages.

Strategy

A final theme that emerged from submissions was concern about the nature and purpose of innovation in the UK.

Respondents felt strongly that digital innovation does not follow a predetermined path. It can be shaped and moulded by the conditions in which it evolves. If innovation is driven solely by market pressures, with no regard for social norms, it will potentially produce technologies that are counter-democratic, unethical, or ill-fitted to our national goals – and it has already done so, highlighted in the other sections of this report.

The answer to unbridled market forces is regulation and good governance. However, post-hoc regulation cannot be our only national strategy. The process of innovation itself must be shaped and directed so that it produces technologies which make us safer, happier, and more informed. This, however, can only be done with a clear sense of purpose and strategic thinking from the government, which the majority of respondents felt was currently lacking.

LOOKING TO THE FUTURE

(1) Joined-up thinking on Digital

Currently digital initiatives come from across Government and are often incoherent and disparate. Contributors argued that we should instead seek to ensure public expenditure on digital innovation reflects the national interest and for the common good. We need to develop a strategy for digital which could incorporate the following features:

(1) We should prioritise digital developments with the potential to tackle society's most pressing, significant, and widespread challenges.

(2) We should innovate with the workforce in mind, aiming to provide meaningful employment.

(3) We should seek to make the UK a world centre for ethical innovation.

(2) Build Our Future Workforce

There was broad consensus that we are not prepared for the future of work. Workers must be given every opportunity to train for the jobs of the coming decades.

Many submissions advocated an increase in school-level education, arguing that digital should become more prominent on school curriculums and school resources. A second emphasis was further and higher education. Submissions suggested the Government could encourage colleges and universities to create specialist courses, offering funding incentives for the necessary faculty, students, and infrastructure. Respondents heavily emphasised collaboration between public and private entities in the creation of training schemes, as well as in hiring consortiums for the employment of new trainees. One respondent suggested the provision of additional subsidies for digital training in areas with lower digital proficiency – particularly training in instantly deployable coding languages.

(3) Technological Sovereignty

Respondents felt that once individuals emerge from expert training and education, they must be incentivised to work in the UK, contributing to a home-grown digital economy. The government's failure to invest in this way over the last ten years has led to reliance on high-risk vendors such as Huawei.

Highly successful clusters of innovation can be easily created with just a small number of exceptional researchers, and the greatest advances are often the product of a few minds.

We will need to think creatively to attract and keep these experts here. One submission suggested establishing a new fund, mimicking Canada's Research Chairs programme, with the aim of funding salaries and research for the world's top professors in computer science and artificial intelligence.

Section 2: HARMFUL ONLINE CONTENT

INTRODUCTION

Online platforms such as Facebook, Google, YouTube, Instagram, Twitter and TikTok are now a central part of our lives. Increasingly, they play a vital role in how we access news and information, how and what we spend our money on, how we contribute to public debate and what we do in our spare time. But we have little control over how content is curated by the tech platforms and delivered to us.

To explore what we would like to see from regulation in this area, we asked for responses to the following question: *"What principles should govern our lives online and protect us all against harm? How should they be enforced ?"*

THE CURRENT SITUATION

There is a growing consensus that self-regulation of tech platforms has failed when it comes to protecting users. While for the most part firms have moved to act on the most serious of illegal activity, including child abuse and terrorist recruitment, there is still a long way to go. When it comes to legal but harmful content we believe there is growing support from the public for the tech platforms to be more proactive.

Labour believes that the government's Draft Online Safety Bill (following the Online Harms White Paper) - which is a once-in-a-generation opportunity to tackle these problems - has not gone far enough either in its scope, or in the penalties it introduces. We back a principles-based approach to avoid the legislation only being narrowly focused on tackling existing problems rather than looking forward to those which are yet to emerge.

The government's White Paper, which was published in April 2019, defined "The Problem" as illegal and unacceptable content which is causing concern to users. It then went on to highlight some specific forms of harm including:

- **Terrorist material**
- **Child abuse**
- **Hostile actors and disinformation**
- **Gangs and other criminals**
- **Legal but harmful**

  Other online behaviours or content, even if they may not be illegal in all circumstances, can also cause serious harm. The internet can be used to harass, bully or intimidate, especially people in vulnerable groups or in public life. Young adults or children may be exposed to harmful content that relates, for example, to self-harm or suicide. These experiences can have serious psychological and emotional impact.

There are also emerging challenges about designed addiction to some digital services and excessive screen time.

We are concerned that the government's framing of online harms and online safety is insufficiently dynamic: it assumes that the next ten years will be dominated by the same challenges as the last ten years. There are new harms on the near horizon for instance, problems arising out of computer-generated speech, DeepFakes, and algorithmic discrimination which will require new legal and political thinking.

Any new regulatory regime must be designed to anticipate new challenges, or at least respond flexibly to them, rather than merely reacting to old ones.

Self-Regulation is Broken

As things stand, social media platforms are given a great deal of latitude. They self-regulate and self-regulate poorly. Public opinion now seems to be hardening around a greater role for the government – and not just among critics of Big Tech. Facebook said it welcomed a more active role for the government describing online harms as complex issues that they could not tackle alone. TikTok spoke of the need for a clear framework established by the government and parliament. While the Carnegie UK Trust said the 'move fast and break things' method has had its day.

Similarly, while many respondents highlighted the need for greater digital education and literacy in order to protect people online, few suggested that education alone could provide an adequate solution. The problem is collective, and it must be addressed collectively. Many Labour members asked some variant of the question: we regulate other sectors, including the media – so why not social media?

The draft Online Safety Bill

After a very long wait, the Government finally published the draft Online Safety Bill on 12th May 2021. The White Paper proposals have been watered down in the draft Bill with a much narrower focus. Labour is concerned about that lack of ambition and there is now a real risk that the Bill will fail to urgently and effectively address what was meant to be its core purpose; tackling online harms, including their reach and amplification.

Even the Government's own press release announcing the publication of the Bill admitted that it's proposals would only tackle "some of the worst abuses on social media."

The Bill runs to well over one hundred pages yet it contains no rights and only one principle; a duty of care for adults in respect of illegal content, and children for significant harm. It says something about the place we are in that seeking to prevent criminal content and child abuse online is a step forward.

The Bill introduces financial penalties for platforms that fail to fulfill their duty of care, but having accepted the principle that criminal liability should attach to senior executives/directors for aggravated or egregious breaches of that duty of care in relation to provision of information to Ofcom as the regulator, the Government has then refused to include this for implementation with the rest of the Bill. Labour wants to see that changed. Immediate media reaction honed in on the new measures which focus on protecting freedom of expression including "Duties to protect content of democratic importance" which has a wide scope and "duties to protect journalistic content" where "journalistic content" is self-defined. Yet absent from the draft Bill, are any safeguards to protect our elections and democratic processes in the digital age through fit for purpose regulation addressing the dominant role of social media in election campaigns. More than five years ago, the Law Commission put forward a series of clear recommendations to help secure our democracy for the digital age - the Government has so far failed to introduce any changes.

In this chapter, we set out some of the policy areas where Labour believes the online safety legislation should focus.

What is Illegal and What is Harmful?

A number of submissions wrestled with the distinction between legal and harmful.

In general, it was uncontroversial that online harms form a sliding scale between minimal, on the one hand, and very dangerous on the other. At

some point in this scale, content should be considered so dangerous that the law prohibits it.

With this in mind, respondents expressed a dual concern: both with the way that the government had drawn the distinction between legal and illegal, and the regulatory consequences of that distinction.

First, the government appears to have dodged the difficult question of what content should be treated as illegal and what should be treated as merely harmful. This is the most important question when considering the regulation of online expression, yet the government appears content simply to adopt legal distinctions inherited from the past.

In the past, free speech activists sought to ensure that people were free to express their views without fear of repression. Nowadays, the internet gives everyone a voice, but the resulting cacophony can sometimes mean that few are heard above the clamour. Minority voices can be lost in their entirety. And forms of expression which, in the past, were tolerable, might now need to be prohibited by law – because of their volume and intensity.

Two examples illustrate the point:

1. Disinformation and misinformation

Most so-called "fake news" is perfectly lawful – but it can cause immense harm when amplified using digital technology, to public health and the democratic process. Merely asking, as the government does, "is it legal for platforms to promote and spread misinformation?" is not enough. The question that needs to be asked is: "should it be?"

As Full Fact rightly observed we must not conflate misinformation with ordinary people getting things wrong on the internet. But the bigger question is whether platforms should be allowed, or even incentivised,

to promote such content, or whether the law should encourage them to take steps to reduce its virality and reach. We recognise that many platforms have begun to take such steps. Facebook noted that more than half of its 35,000 staff working on safety and security work in content review. Google stated that it has 10,000 people working on content moderation and removal. But much more needs to be done.

2. Content Harmful to Children

The NSPCC stressed that the regulator must adopt a child-centred and harm-based approach. It must take decisions that balance freedom of expression, but also respond to the very significant potential for harm that comes from algorithmic promotion of harmful content, including suicide and self-harm content. This was echoed by Catch22 following their Online Harms Consultation that gathered insights from young social media users, tech platforms, youth services and experienced youth workers.

In it, over 70% of young people said they had seen specific violent and explicit content online and just under a third (33%) reported seeing harm that occurred offline because of something that happened online. Less than half of respondents reported online harms to the platform containing them and only 27% of young people felt safe all the time.

It is clear that the government has missed an opportunity to do the difficult work of sorting out where the legal line should be drawn between lawful and unlawful content.

The Privatisation of Political Judgment

A second common concern is related to the government's proposal to let platforms decide for themselves which 'lawful' content to host on their

services. At present, the government proposes to let private companies decide “what content and behaviour they deem to be acceptable” and hold them accountable only for how well they enforce their own rules.

This proposal would allow platforms to be the arbiters (within the bounds of the law) of which speech is permitted, and which is prohibited, on their platforms. Given the importance of social media platforms to public deliberation, this is a significant responsibility and one which concerned many respondents to this consultation.

Five problems stood out:

1. **Standards may not be high enough**: No guarantee platforms will adopt community standards that adequately protect people from online harms.
2. **Perverse incentive for weaker standards**: If companies are allowed to set their own community standards and are held to account for their enforcement, as the NSPCC highlighted.
3. **Alternative platforms**: As the Antisemitism Policy Trust (APT) pointed out, there are many “alternative platforms” which exist predominantly to host extreme content. These include platforms such as Gab, BitChute and 4chan which either tolerate or actively encourage content which is legal but harmful. One such platform, Parler, has recently been forced to suspend operations after it was used by domestic terrorists in the US to plan January’s Capitol riot. Other platforms - such as Telegram and Signal - provide encrypted services with legitimate use cases, but there is concern in some quarters that they may be open to exploitation by extreme or malicious users. The draft Online Safety Bill’s scope is limited. Regulation will apply on the basis of the size of the platform (in terms of users) and functionality (essentially, how the platform works). As currently drafted, those “alternative platforms” hosting extreme content would escape regulation.

4. **Not all harms are caused by users**: The platforms themselves sometimes bear responsibility for amplifying disinformation or incentivising radical content. As Demos pointed out in its submission, "Platform design and systems which can amplify online harms are not in scope of a platform's terms of service that focus only on permissible or impermissible user behaviour."
5. **The public should have a say**: The rules and norms that govern sensitive speech online should not be left entirely to the discretion of commercial platforms. We are, as AST put it, in danger of outsourcing our values to individuals and companies in California and elsewhere.

The platforms must be a big part of the solution to online harms. They hold the technical expertise, the resources, and the access to clean up online spaces. But they do not necessarily have the legitimacy to make important decisions about what may or may not be said in a free society and they should not be left to do so without democratic oversight.

The Regulator

The Government has appointed Ofcom as the regulator. Ministers argue Ofcom is a well-established and experienced regulator, recently assuming high profile roles such as regulation of the BBC, and has experience within the communications sector.

But, while respondents did not seek to downplay the experience or credibility of Ofcom, there was concern to ensure that any future regulator has the requisite skills and resources.

Glitch emphasised the need to ensure that investment in the regulator matches "the scale and effect of online harms." It suggested that this funding should come from the service provider and/or those who financially benefit from those services through, for example, targeted online advertising.

Respondents also pointed out that the inherent diversity of social media would require a differentiated response. Google, for instance, emphasised that any system of oversight must recognise the difference between social networks, video sharing platforms and other services primarily designed to help people share content with a broad audience, as against search engines, enterprise services, file storage, communication tools, or other online services, where users have fundamentally different expectations and applications. Different types of content may likewise call for different approaches. Whatever the identity of the regulator, it must be equipped to address this diversity.

Penalties

Ofcom will be able to fine companies which fail in a new duty of care up to £18 million or ten percent of annual global turnover, whichever is higher. It will also have the power to block access to sites.

But the Government has resisted calls for criminal penalties similar to the measures taken to reform the culture in financial services in the wake of the 2008 crash. Instead there is the power to bring a new criminal offence for senior managers which could be introduced two years after the Bill comes in. There was a feeling that sanctions should be robust and that fines are commensurate with the size and wealth of the large platforms. As well as fines and criminal sanctions, AST suggested other penalties such as a public adverse behaviour warning.

Transparency

The Online Harms framework provides for annual transparency reports. However, there was some concern that an annual reporting mechanism was not enough. Full Fact was concerned that only publishing once a year would stop regulation from being effective because of the fast-pace of change

online. They also pointed out that a regulator should not be reliant on the data that internet companies choose to provide.

'Private' Messaging and Online Harm

One difficult issue raised in the consultation is whether private messaging services should be included within the scope of regulation. The issue gives rise not only to technical and enforcement challenges (particularly where such services are encrypted), but to thorny issues of free speech.

5Rights argued that if the aim is to reduce harm, then regulation should look at the nature of the risk rather than the nature of the service.
In reality, a balance must be struck between the reduction of harm on the one hand, and the protection of privacy on the other.

Respondents to this consultation, including 5Rights, argued forcefully that foreseeable risks for children within private messaging platforms must be brought within the scope of government regulation.

Consumer Scams, Frauds, and Unsafe Products

There was concern about the exclusion of scams, frauds, and other commercial misbehaviour from the government's approach to online harms. While the draft bill includes provision for user-generated fraud including romance scams and fake investment opportunities, this excludes the majority of online financial harm and is something Labour will seek to correct.

Nine out of ten UK consumers shopped online last year. As Which? observed, the protections that consumers can expect when they buy through more traditional retail outlets or websites have not kept pace - including safety. Which? testing and investigations found a range of unsafe products for sale on online marketplaces including child car seats that are illegal to use in the

UK; smoke and carbon monoxide (CO) alarms that failed to detect smoke and CO2 during safety testing, and USB chargers that pose a fire or electrocution risk.

However, online marketplaces are not acting consistently to prevent dangerous products from being sold on their platforms. In some cases, the sites remove the exact listings immediately upon notice of the safety issues, but within days identical listings of these unsafe products reappear on the sites. There are also concerns that buyers are not being informed about product recalls or safety issues with items they have purchased.

Which? research showed that many people generally assume that the products they buy online are safe. Only 21% of people were aware that online marketplaces have no legal responsibility for overseeing product safety on their sites. However 70% of online marketplace shoppers think the law needs changing so that these sites are made legally responsible.

Fake reviews were also identified as a growing source of concern. Some fake reviews are generated by humans; others by bots. Online platforms are falling short in detecting, removing, and disincentivising fake reviews. (If platforms consider that 'traffic is traffic', there is little incentive to reduce it.)

Frauds and scams are also a considerable problem. The Carnegie UK Trust cited a statistic from Fraud Action that 85% of losses suffered from frauds and scams in the year to June 2020 were "cyber-enabled". Scams and frauds are, of course, illegal. But very few are prosecuted.

There was support for placing more legal responsibility on platforms for detecting and preventing fraudulent content, and more responsibility for taking quick action to remove it once reported. There was also support for requiring platforms to be clearer about who is responsible for the

“commercial” content on their platforms, not all of which has been moderated.

The European Union’s approach

The European Commission has taken an approach to online harms regulation which is similar to the UK’s in some respects while going further in others. The Digital Services Act, published December 2020, is being billed as the biggest change to European digital regulation in more than twenty years. Like the UK government’s proposed online safety legislation, it will introduce new obligations for online companies to monitor, report and act against instances of harmful content. These obligations will be stronger and more onerous for bigger companies: for example, “very large platforms” will be legally required to share data with authorities and researchers, whereas smaller platforms will not.

Despite these similarities, there are some areas in which the approach of our current government diverges from that of the European Commission. The Digital Services Act lays out more detailed obligations for online companies than the UK’s Draft Online Safety Bill, and will allow for higher fines to be levied against companies that break the rules. While the full scope of the EU Act has not been made clear yet, it seems likely that it will be broader than the UK equivalent, covering additional online harms such as fraud. It will also be accompanied by a Digital Markets Act, which seeks to redress the growing monopoly power of a small handful of digital platforms. This joined-up approach differs from that taken in the UK, where attempts to create a level playing field in the tech sector have been treated as separate to the online harms agenda.

Digital Markets Unit

Labour has welcomed the creation of the Digital Markets Unit (DMU), announced in November 2020 and which was launched in non-statutory

"shadow" form but we are concerned about its powers and resourcing. The unit represents an opportunity to make digital markets work for people but it currently has no powers of enforcement and the Queens Speech did not set out any proposals for powers or for reform of competition law to make it fit for the digital age. This suggests the Unit will not be effective for some time.

LOOKING TO THE FUTURE

The scale of the task ahead remains daunting. Regrettably, the approach in the Draft Online Safety Bill is only a starting point. Even assuming it is not watered down further, it evades some of the most difficult questions and leaves important areas unregulated. It may soon be overtaken by events .

Labour's aim, in the coming years, is to find ways to move past the intellectual and regulatory shortcomings of the government's approach in the following six areas :

(1) Find a Democratic Consensus on the Boundaries of Online Speech

The first task for Labour is to provide answers to the question that the government should have tackled from the start: Are there forms of activity which were lawful in the past, but which should now be made unlawful because of the unique harm they cause online? These could range from (currently lawful) content affecting the wellbeing of children, to (currently lawful) content documenting terrorist activities. The exercise would also cover the algorithms used to amplify content.

Whilst the state should be extremely cautious about criminalising the publication of misinformation per se, it may wish to place legal responsibilities on platforms to prevent the amplification of such misinformation, particularly when it is injurious to public health or the democratic process.

This should be implemented at the systemic level so that the state is not involved in individual content moderation provisions: requiring platforms to put in place adequate systems rather than judging them by individual decisions.

This is not a dry or technical question. Nor can it properly be made by political elites or lawmakers alone. It is a fundamental question in which citizens must have their say.

(2) Minimal Requirements for Community Standards

Unlike the government, Labour believes that for lawful content, platforms should not be left to determine their community standards for themselves. Instead they should be required to meet a baseline of standards, set down in statutory codes of practice. The arguments in favour of a mandatory baseline are powerful:

(a) without such a baseline, there is little accountability on the part of platforms;

(b) the absence of a baseline incentivises platforms to adopt less stringent community standards, to avoid being punished for failing to enforce them;

(c) the government's proposed approach would benefit extremist platforms where the spread of hateful material is their raison d'être;

(d) platform design, just as much as individual contributions, is responsible for the spread of harmful material;

(e) these sorts of issues should arguably be matters of democratic deliberation, and not left to the decisions of commercial actors alone.

We will also look at whether mandatory age verification for certain content should be part of the regulatory response to the threats posed to children online.

(3) Give the Regulator Teeth

Many submissions argued that the Regulator must have "teeth".
They called for it to have:

(a) the expertise needed to address online harms across a host of platforms;

(b) the requisite funding and resources to conduct an immense task properly;

(c) the power to issue fines and sanctions that are meaningful in the context of vast multinational corporations. Meaningful sanctions should include criminal liability as part of changing the culture within tech firms and the demand for social media companies to take responsibility.

(4) Draw up Principles for the Regulation of 'Private' Communications

There are some situations in which it is appropriate for the government to regulate 'private' spaces, either because they are not properly deserving of the term 'private' (such as a closed chat forum) or because the nature of the harm is so serious that it demands it (such as where children are vulnerable to exploitation). At the very least, all platforms should be required to consider, in a formal risk assessment, the threats to child safety posed by their private platforms, including encrypted ones, and publish their findings in a stipulated manner. Even this is unlikely to suffice, however and regulation may need to go further still.

(5) Extend 'online harms' to include scams, frauds, and unsafe products

Online platforms currently have limited responsibility and no legal obligation to protect users against fraudulent and scam content, except and until they are made aware of it. This needs to change. Platforms should be required to take reasonable steps to identify and prevent illegal user-generated content from appearing on their sites. They should carry more legal responsibility for the safety and authenticity of the products sold on their websites (perhaps in

the form of a “due diligence” defence). There should be clear and robust rules about how platforms deal with unsafe or unlawful practices in their marketplaces. There should be greater transparency obligations, so consumers are better able to understand and verify the people from whom they are purchasing. The regulator must be empowered and resourced to take a proactive approach in working with platforms to detect suspect activity.

(6) Plan for Democracy’s Future, Not its Past

The government’s approach misses some of the broader challenges to democracy posed by digital technology. There is a growing body of research which suggests that social media is contributing to a fundamental change in the way we deliberate, by fragmenting society into ‘filter bubbles’ and entrenching political polarisation.

Further, as Reset pointed out in its submission, there is still a critical lack of transparency about how political advertisements are ‘microtargeted’ online. And these are just today’s challenges. As nonhuman systems such as bots become more capable of intervention into the political process – even in crude and blunt ways – we will need to devise systems of regulation that protect democracy itself. We need to anticipate the challenges that come next, rather than fighting the last war.

Section 3: PERSONAL DATA AND OUR ONLINE LIVES

INTRODUCTION

Personal data is central to the information economy. Almost all web services and digital products – from search engines and social networks to online stores and ride-hailing apps – gather personal data and use it for commercial purposes, particularly through advertising.

In recent years privacy concerns have been raised about the extent to which online platforms monitor, control and profit from personal data. With algorithms increasingly using our personal data to make important decisions about how we live and work, we need to protect people from algorithmic bias.

We need greater transparency about how algorithms control and curate the content we see online. And the use of algorithms by employers to control and discipline workers should be examined. High-profile data leaks have also led to pressing questions about the security risks of so much data being gathered by large organisations.

Recent data protection regulation – the EU's General Data Protection Regulation, or GDPR, which is now part of UK law too – is a sign of progress but it is also proving to be insufficient in various ways.

To explore how we can move on, we asked for responses to the following question: *"How can we put people in charge of their online lives? Do we need stricter – or different – rules for how large corporations and public bodies use our personal data?"*

THE CURRENT SITUATION

The use of personal data in the provision of services (both public and private) can support innovation. Many services which we now take for granted require a certain level of tracking in order to function properly.

Responses widely acknowledged these benefits, but they also expressed concerns about the way data is currently used. These concerns largely fell into three categories:

1. **Lack of Knowledge**: the lack of knowledge, understanding and transparency around how individual data is used by corporations.
2. **Lack of Control**: the lack of control individuals have over the ways in which their data is used.
3. **Lack of Trust**: the widespread belief, held by individuals, that tech companies do not always use data in their best interests.

A small minority of responses – from tech sector companies in particular – argued that the use of personal data is only a problem when "demonstrable consumer harm" can be proven. While it is true that individuals can suffer actionable harms at the hands of digital technology (as discussed elsewhere in the report), not every poor practice results in measurable damage to an individual consumer. Widespread surveillance and algorithmic bias are both examples of potential harms which might damage society in quite profound ways – yet not every individual affected will be able to point to a palpable harm caused to them specifically.

(1) Lack of Knowledge

Many submissions highlighted the lack of knowledge that most people have about how their personal data is used by corporations and government. Some submissions put this down to a lack of adequate education – not just about data itself, but more widely about how technology functions and the risks associated with it. Others attributed it to the ways in which technology

companies gather and use data, and the lack of transparency or clear communication about these processes.

Submissions from charities and NGOs made the point that many of the harms associated with personal data use are inherently difficult to understand. The techniques used by technology companies to process data are sophisticated and seemingly harmless information can be used to produce deeply personal insights about an individual. It can therefore be challenging to illustrate to users how their use of digital services can lead to potentially serious breaches of privacy.

(2) Lack of Control

Many submissions also suggested that individuals currently lack sufficient control over what is done with their data. The GDPR was frequently referenced as a good first step, rather than a solution to this problem, with many submissions saying that further reform is needed. For example Data Subject Access Requests (the process that allows individuals to find out what data is held on them by a company or other form of organisation) were specifically cited as being too slow and cumbersome. However, many also considered that the UK's room for manoeuvre would be limited in the long-term, as EU standards are likely to remain the gold standard around the world.

This lack of control is also increasingly felt by many workers with regard to their online working lives and the digital technologies used to monitor and reward them. Recent research by Prospect Union and the TUC[3] has highlighted the use of data collection and surveillance without employees' knowledge or agreement. Prospect is promoting a 'Right to Disconnect' and the TUC recently published its Manifesto "Dignity at work and the AI revolution" which made a number of important proposals.

3 https://www.tuc.org.uk/research-analysis/reports/dignity-work-and-ai-revolution

(3) Lack of Trust

Submissions, including those from tech firms, acknowledged an issue with "trust" – i.e. that users do not always feel that data is used in their best interests – and recognised that this needs to be rectified. Companies noted that a lack of trust might arise from a lack of understanding from users about what data is used for. However, there was little acknowledgement that this lack of understanding stems from their own lack of transparency.

Moreover, individuals demonstrate different levels of trust between different types of institution: one submission cited polling demonstrating that trust is much higher for public institutions and researchers using personal data than it is for multinational companies.

LOOKING TO THE FUTURE

Submissions largely acknowledged that a balance must be struck between the extraordinary benefits to be gained from data analytics, and the privacy trade-offs that come with surrendering personal data. There was an overwhelming sense of frustration that the fruits of data analytics too often flow to large private companies rather than being harnessed for civic ends.

Few responses called for the flow of data to be arrested entirely. But many wanted to see greater social benefits in exchange – and Labour believes this is the principle that should guide our policy-making in this area.

In their submission, Google stressed that both technologies and public attitudes are constantly changing, meaning that uses of data which are considered unacceptable today could be considered acceptable in five years and vice versa. That is not, however, a good guide to future practice. The fact that a practice becomes normalised – for whatever reason – is not necessarily an indicator that it is right for the long term.

(1) Build on the GDPR

There was broad support to re-examine the existing data protection regime – set out in the GDPR – and investigate what can be done to improve it. In particular:

- Can it be made simpler and easier to use for individuals?
- Can any aspect of it be made less onerous for data controllers?
- Can enforcement be improved?
- What kind of education is needed so that ordinary people understand their rights?
- What are people's data rights now and do new rights need established?

(2) Unlock Data for the Public Good

All agreed that we need to do more to unleash data for the public good.

We should investigate ways in which data hoarded by private corporations can better be put to use for the common good, while maintaining the requisite level of confidentiality.

This will require investment in data infrastructure, skills and horizon-scanning – as well as working with industry and trusted third-parties to create an environment where data is shared with trust and confidence.

(3) Explore ways to Rein in the Power of Big Tech

Submissions recognised that the collection of vast amounts of personal data is only one facet of a broader problem: the accumulation of power and wealth in the hands of a shrinking tech industry elite.

There are several ways in which concentrations of power in the tech industry might be reduced. Suggestions we received have included introducing new data portability rules (beyond those in the GDPR) to enable easier movement

between platforms; a new approach to competition regulation, with more aggressive action against companies that abuse market power; new systems of appeal for people subject to adverse algorithmic decisions; reform of IP and/or data protection laws to prevent the long-term hoarding of vast troves of data and potential tax reform, so multinational companies pay what they properly owe.

Section 4: TECHNOLOGY AND OUR PUBLIC SERVICES

INTRODUCTION

Digital technology can be used to make public services better and more available to everyone – from cutting congestion through smart mobility services, to giving citizens more of a say in decision-making. This has started to happen in the UK, but progress has been slow and uneven, both locally and nationally. And we still tend to put existing services online, rather than use technology for exciting new services.

We need to think about how digital technology – from data flows to digital infrastructure – can be used for the public good, both at a local and a national level. To inform our views on this, we asked for submissions on the question: *"How can the government better use tech to work for the public?"*

THE CURRENT SITUATION

The United Kingdom has at times been a leader in digital government. By 2015, our Government Digital Service (GDS) had some notable successes to its name. Notably, it had developed "cleanly designed websites to register to vote, pay car tax, sign up for benefits or register for lasting power of attorney". British software was held up as the gold standard, used by other democracies including New Zealand and Israel.[4]

However, since 2015 the GDS has lost political leadership and direction. Britain has slipped from first to seventh in the United Nations e-Government development index, which measures how well countries use tech to deliver services.[5] Fairly or otherwise, the term "public sector IT project" has become shorthand for inefficiency and incompetence, both on the part of the government and its private sector suppliers.

[4] https://www.economist.com/britain/2020/10/31/the-sad-tale-of-britains-government-digital-service
[5] https://www.economist.com/britain/2020/10/31/the-sad-tale-of-britains-government-digital-service

The Covid-19 crisis offered an opportunity for the government to deploy digital technology in new and vital ways. Instead the government was forced to mothball its own contact-tracing app, while the platform used to manage the test-and-trace system – Excel spreadsheets unfit for the task – inadvertently disregarded more than 15,000 positive cases.

The Labour Party has been concerned for some time about the prospects for digital public services in the UK. Six years ago, we published the report of a consultation entitled "Making Digital Government Work for Everyone", with detailed recommendations on what would need to change to arrest the then-imminent decline in our digital capabilities. Six years on, this report makes for sobering reading. We appear to have made little progress.

When, Where, Why?

A notable theme of submissions was a sense of caution about when, where, and why digital services are appropriate – and when they are not. While respondents agreed that digitalisation can make public services fairer, cheaper and more accessible, they were also clear this is more appropriate for some areas of public service than others.

The services generally considered to be most ripe for digitalisation were those that can be characterised as apolitical or administrative in nature. Services cited in particular included services such as bus timetabling, traffic light operation and waste collection, as well as routine visa renewals and other bureaucratic processes. These services present, in part, technical problems that are (in theory at least) capable of machine analysis and solutions. Some aspects of healthcare, such as the diagnosis of certain illnesses and the monitoring of patient progress, were also mentioned as those which could benefit from digitalisation.

Respondents were less comfortable, however, with algorithms designed to make determinations involving difficult moral choices. This summer saw outcry over the government's use of an algorithm to moderate the grades of students who had been unable to sit public examinations, which produced some results that were plainly unjust. This was one example of a broader trend: the state using algorithms to determine access to important social goods, including welfare payments and housing decisions, in ways that sometimes seem unjust (and are almost always opaque).

Oversight and Accountability

A further concern raised was that without proper oversight and governance, digital technology would only strengthen the hand of government, not the power of the people. If tech is to be used in the provision of important public services, then it ought to be accountable and subject to scrutiny. This is especially important in the use of algorithms and data analytics, which are less transparent than predecessor technologies.

At present, the government's use of digital technology is not unregulated: it is subject to the general law, the GDPR, and the Equality Act. Nevertheless, submissions suggested that the existing legal framework may not suffice. Numerous examples of non-binding guidance regimes have been produced by public and non-governmental bodies, but the guidance in these documents is not always consistent, or well-known by the public. For AI and data analytics alone there are competing sets of principles produced by the GDS, the Information Commissioner's Office, the Department for Culture, Media and Sport, the Centre for Data Ethics and Innovation, the Office for AI and the Alan Turing Institute. Submissions suggested that a "reset" of the oversight and accountability landscape might be needed to address this fragmentation – and that this could involve the strengthening of statutory legislation.

Backdoor Privatisation

A number of respondents raised concerns that digitalisation might be a form of backdoor privatisation, as digital services are often provided by private suppliers. Many of these concerns were prompted by reports of lucrative contracts outsourced to private sector consultants and businesses, with the Test and Trace programme a commonly cited example.

A deeper concern expressed by several respondents was that the UK government had no choice but to use private sector providers, because it was not capable of providing adequate digital services itself. Submissions emphasised the need to build digital skills and capabilities in local and national government, NHS trusts, academy chains and the other public bodies.

Not all respondents were wary of the private sector, with some advocating local procurement as a tool to unlock innovation across the country and others for renewed "challenge-led" collaboration between the public, private and third sectors.

LOOKING TO THE FUTURE

The story of digital government in the United Kingdom - early promise followed by decline – suggests that digital is still seen as an afterthought rather than a central pillar of modern government. When political capital, media attention, funds, or leadership are scarce, digital services are among the first to be left to wither. We need to ensure this does not happen in future, as once momentum is lost, it is costly and hard to regain.

At the same time, there is a significant degree of anxiety about the increasing use of tech in government – at least without clear principles to guide it, or trusted systems of oversight. Tech can improve governance, but it can also

make things worse through undue centralisation, creeping privatisation, lack of transparency, and unaccountability.

Finally, it is clear from this consultation that digital government is about more than making services more efficient, accessible, and affordable. Digital technology can unlock new ways of governing altogether, opening up the potential for policies that would not have been feasible even half a century ago.

Our priorities going forward, as informed by responses to this consultation, are as follows:

(1) Get the Basics Right

Getting the basics right is the swiftest way to build public confidence in digital government. All contributors agreed that online government material should be clear and high-quality, and existing services should be maintained at high levels of functionality. It also means identifying the remaining areas of public services which are ripe for basic digitalisation – areas in which even the minimal use of technology could save considerable time and cost.

(2) Clear Boundaries for Sophisticated Technologies

People deserve some form of control over which public services are subject to automation and other sophisticated forms of digitalisation. Before algorithms are put to use in healthcare, housing, welfare, policing, or other core public services, many submissions argued the government should take stock of public opinion and set out the rationale for using a digital rather than analogue method. How technology is used in government ought to be the subject of democratic debate and choice.

(3) New Safeguards and Oversight Regimes

Most contributors agreed that the power of digital technology must not be unconstrained. For the public to be protected and have faith in the digital systems used to govern them, there must be robust regimes of governance and oversight. Developing these regimes will be a major task.

As such, we will carefully examine the proposals to this effect set out in the recent report of The Committee on Standards in Public Life, Artificial Intelligence and Public Standards.[6] We are also looking closely at the detailed proposal from the Future of Work Institute for an Algorithmic Accountability Act.

(4) Proper Funding, Training and Resources in the Public Sector

Contributors emphasised the importance of investing in the digital capacity of the civil service and other branches of local and national government. There will always be a place for external expertise, but at present public service providers are too dependent on private sector know-how.

Digital competence is not a luxury for a twenty-first century government. It should be seen as a basic element of service provision. We need to train and hire civil servants to do more of the work of digital delivery. And when the government does use private sector providers, it should set procurement requirements to ensure that private companies meet public standards.[7]

(5) A New Tech Regulator?

Many submissions discussed the merits of a new tech regulator. Given the scale of the issues raised by algorithms in both the public and private sectors, there are obvious reasons why a single, powerful regulator for AI

[6] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868284/Web_Version_AI_and_Public_Standards.PDF (paraphrasing and adjusting in places)

[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868284/Web_Version_AI_and_Public_Standards.PDF

might be desirable. It could develop genuine specialism in this area, coordinate the work of sectoral regulators, build public trust, and iron out the inconsistencies across different parts of government and society.

There is more work to be done in sketching out what a new tech regulator would look like. Academics in the United States have begun to do so (one example, for instance, is an "FDA for Algorithms").[8] This is an area in which the United Kingdom could seek to lead.

[8] Tutt, Andrew. 'An FDA for Algorithms' (2016)

Section 5: DIGITAL INCLUSION

INTRODUCTION

Not everyone has equal access to the benefits of digital technology. This section asks: *"How can we ensure that no-one is excluded from this digital revolution? What are the main barriers to digital inclusion and how can we remove them?"*

THE CURRENT SITUATION

When we speak of "digital inclusion", we mean the extent to which individuals have access to the advantages of digital technology. This definition emphasises that digital inclusion is not simply a matter of access to technology itself, but of access to the benefits that the digital world has to offer. Labour believes that, as a matter of course, all citizens of the UK should have a strong minimum level of access to the benefits of digital technology.

Submissions suggested that the obstacles to digital inclusion fall into three main categories:

1. **Lack of access**: to the necessary hardware, software, or connectivity which are needed to reap the benefits of digital technology. Inequality of access is still surprisingly common.
2. **Lack of skills**: that allow us to use technology.
3. **Power imbalances**: that privilege some groups over others, excluding some from the full use of digital technology.

(1) Lack of Access

The most immediate and obvious obstacle to digital inclusion is a lack of access to the technology which makes such inclusion possible. While the use of digital technology is now widespread, many still lack access to the basic hardware required to enter digital spaces. According to BT Group, 9% of

children in the UK have no access to either a desktop, a laptop, or a tablet at home, and 1% of children have no access to a mobile phone either.

Lack of access to the internet, too, is more common than is often realised. Just under 7% of UK households, or 1.95 million, have no internet access at all. Older people are dramatically over-represented in these figures: 90% of those who have never used the internet are over the age of 55. The main reason that people lack internet access is that they believe they don't need it, but other commonly cited factors include a lack of skills and poor broadband performance in certain areas.

(2) Lack of Skills

A lack of skills remains a problem, with the Government estimating that 3.5 to 4 million people (6.8% to 7.9% of the UK adult population) may never be able to gain basic digital capabilities. A majority in this group, too, are elderly, but digital illiteracy also presents disadvantages for those in younger cohorts. According to Which?, around 22% of UK adults are not certain that they could find their bank balance online, in part due to a lack of skills.

For working adults, the most significant threat is ill-preparation for jobs requiring digital proficiency. In particular, many respondents expressed fears that those facing redundancy did not have sufficient opportunity to retrain for digital or digital-adjacent roles. With the adult skills budget cut in half over the last decade, there is now a dearth of suitable digital training available. The Covid-19 pandemic is likely to exacerbate this challenge in two ways: First, by increasing the number of lay-offs; and second, by accelerating the pace of digitalisation, such that the new jobs which do arise are ever more likely to be digitalised.

While for many children and young adults digital skills are second nature, there are also higher expectations on them upon entry to the job market.

According to the CBI, almost half of young people in the UK believe that their education has not prepared them for the world of work and 40% of employers say that they are struggling to fill entry-level jobs.[9] Respondents noted a host of problems with the way we teach digital skills at school, from insufficient digital infrastructure to teachers not properly versed in digital literacy. Others emphasised issues with the curriculum, with "computer work" too often treated as an independent discipline, rather than an integral part of every subject.

(3) Power imbalances

If digital inclusion means the ability to access the best of what the digital world has to offer, access and skills are not enough. Power disparities within digital spaces can have considerable exclusionary effects.

One common manifestation of this is discriminatory product design. Digital products are less often designed with women and minority groups in mind – partly because the tech industry itself is comparatively homogenous. Examples offered by respondents included devices for which the design is unsuited to the needs of disabled groups, sites and products available only in English, and the overwhelming majority of products being primarily marketed towards white men.

Toxic online behaviour was a major concern - particularly hateful, discriminatory, or fraudulent behaviour. This can drive people away from technology, with one survey showing that 19% of 13-15 year old girls have left or significantly reduced use of a social media platform after being harassed online. The problem of toxic online behaviour – and how to tackle it – is discussed at greater length in Chapter 2.

---

9 https://www.standard.co.uk/futurelondon/skills/why-young-people-are-the-key-to-closing-the-digital-skills-gap-ignoring-it-could-cost-uk-economy-a4338956.html

LOOKING TO THE FUTURE

Many respondents offered detailed frameworks for reducing digital exclusion. We take the following away from this section.

(1) A Right to Digital Inclusion

Contributions discussed whether there ought to be a legal right to a minimal level of digital inclusion. This would first mean developing a deeper, more comprehensive, universally recognised baseline for what it means to be digitally included in the UK – something first requiring further public consultation, including those with lived experience of digital exclusion.

(2) A Ministerial Portfolio?

There were some suggestions that including a minister whose portfolio is entirely focused on digital inclusion in the Department of Culture, Media & Sport would push this issue up the political agenda.

(3) The Need for Robust Data

This is an area of public policy in which systematic, timely, and robust data is essential. We need statistics across "key measures, broken down by jurisdiction and by demographic group" (Carnegie UK Trust). We also need to do better at measuring and publishing data concerning the impact of inclusion programmes that already exist.

(4) Be Prepared to Treat Tech as a Public Good

If the market alone is failing to produce or distribute vital technology for marginal groups, then the state must step in. Labour believes that in the twenty-first century having a computer and good internet access should be like having water and electricity.

Ways of making this a reality suggested in submissions included:

- an increase in the number of accessible computers in public libraries, village halls, council offices and job centres.
- the provision of devices and hotspots to students who qualify for free school meals, tying poverty alleviation to the quest for digital inclusivity.
- state support for the recycling of devices, by stimulating consumer engagement, establishing a nationwide collection infrastructure, supporting the wiping and unlocking of devices, and establishing community connection centres in isolated areas.

(5) Broadband is no longer a luxury but a necessity

The Conservatives have a record of bold promises on fast-speed internet but of failing to deliver. While campaigning to lead the Conservative Party, Boris Johnson called Theresa May's government's promise to deliver full-fibre broadband to everyone by 2033 "laughably unambitious". Instead he pledged full fibre to all by 2025 as part of his leadership platform. The Government then downgraded that pledge to universal 'gigabit-capable' broadband to every home in their 2019 manifesto. Then in December 2020 the Chancellor's spending review revealed that only £1.2 billion of the promised £5 billion will be made available up until 2024 to deliver on this. At the beginning of April 2021 Oliver Dowden told the Commons Digital, Culture, Media and Sport (DCMS) Committee that he expects the new target to be met by the telecoms industry delivering 80% coverage by 2025[10].

This constant confusion and flip flopping is detrimental to our economy and social cohesion. Labour believes the essential nature of fast-speed internet access means the government has a duty to make it accessible to everyone – like water or electricity.

[10] https://committees.parliament.uk/publications/5530/documents/54992/default/

(6) A Digital Skills and Diversity Programme

A number of proposals were mooted for school-age development of digital skills, including:

1. Making changes to the curriculum with greater emphasis on skills in data research, analysis, and interpretation.
2. Embedding computer science more deeply in other subjects.
3. Making ICT compulsory at GCSE.

Some respondents were more ambitious, with one suggesting classes in "building video games, learning javascript to animate a website, how to find an open source package, report a bug, check an issue queue, or use Git".

(7) Targeted Programmes for the Elderly

For the elderly cohort – those most likely to be intractably excluded – respondents supported localised training: "Local authorities should provide resources and training to community volunteers and local services, such as libraries, which support older people and others who are digitally excluded to use online services". As a supplement to such training efforts – whether through adult learning classes or community service – many recommend keeping non-digital options easy and available.

(8) A Strategy for Diversifying Tech

There was a great deal of consensus around the need for a more diverse tech industry, and more inclusively-designed tech. The two go hand-in-hand. No single strategy emerged from the submissions, although it was apparent that collaboration would be important – between government, the industry, charities representing under-represented groups, and educational institutions.

CONCLUSION

NEXT STEPS

Labour has a proud history of supporting innovation. In government we have embraced the power of technology to change both the lives of individuals but also the public sphere. We believe that many of those opportunities are now being wasted while the darker elements of the online world are being allowed to flourish by tech companies who lack the incentive to tackle such behaviour.

We launched this wide-ranging consultation to engage with different ideas from across the spectrum from tech innovators, to established platforms, trade unions, the public sector, civil society and Labour members. The contributions we received and the roundtables we held to inform this report have enabled us to begin the work of finding general principles and avenues for further investigation.

The next phase will involve crystallising the ideas and principles in this report into more concrete proposals for change.

We have used this as an opportunity to reflect on how we make policy in the field of digital technology.

Policy for the governance of technology requires the combination of two elements: (1) genuine expertise about the subject-matter, and (2) democratic legitimacy. Few can claim to speak from a position of deep expertise and popular authority. We need to be innovative in the way that we source and combine both.

This consultation yielded contributions of both sorts – from experts and industry groups claiming specialist knowledge, and from a wide range of

stakeholders keen to offer more general perspectives on their concerns and anxieties. But we believe that there is more work to be done. Specifically, we want to hear more from the cutting edge of academic study on these questions, and we want to be able to formulate policy in a more deliberative way.

Labour believes tech can be a force for good but the failure of successive Conservative governments to have a clear vision for all aspects of our digital lives has meant we now have the worst of both worlds; a laissez-faire approach to regulation and a lack of strategy and support for British tech. That failure, to name just one example, has made the process of stripping Huawei from our critical infrastructure much harder because of the lack of home-grown alternatives.

Labour supports tough regulation and accountability for the online space, but it must be accompanied by enthusiastic support for British tech within the right environment for it to compete on the global stage. Only then, through an all-encompassing approach to digital policy with inclusion at its heart, can we ensure Sir Tim Berners-Lee's objective for the world wide web is reality and that it finally is for everyone.

Appendix:

OUR DIGITAL FUTURE: A Labour Party Consultation

Labour believes that technology can change lives for the better – and it already has.

Families separated by oceans are now a video call away. Small businesses sell to customers across the globe. World-class art, cinema and music are live in our living rooms. Personal Protective Equipment is designed professionally and '3D printed' at home. And much of the world's information is now freely accessible to learners of all ages. Digital technology contributes £149 billion to our economy, directly employing nearly three million people and many more indirectly – but its benefits are more than economic.

The events of the last year have moved technology even closer to the heart of our working and domestic lives. The average UK adult now spends around a quarter of their waking life on the internet. The pandemic has highlighted the positive power of digital technology, but it has also brought some of its downsides into focus. Too often those on the wrong side of the "digital divide" have been left without the benefits of technological progress that many take for granted. And there are growing signs that digital technology may be concentrating too much power in the hands of unaccountable bodies – not just government agencies, but large corporations whose decisions increasingly affect our rights, freedoms, and the political system itself. During the pandemic the digital divide has left some children unable to access schooling, directly impacting the life chances of the next generation. We also see employees struggling or unable to adapt to new working practices because they don't have the digital skills. As Sir Tim Berners-Lee famously said of the World Wide Web: "this is for everyone".

Digital is now at the heart of almost every single policy area in one way or another, but it is not really 'for everyone'. Labour believes that we can demand more from our digital technologies – and build a digital future that is safer, fairer and more inclusive. This consultation produces a set of principles to guide Labour digital policy, not just for the next election cycle but for the long-term. We want to create a credible and detailed vision of how our digital future should work. We have set out some initial thoughts with important but deliberately broad questions, under five themes, but to make this a reality we need your help. Thank you for taking part and we look forward to hearing your ideas.

Chi Onwurah, Shadow Minister for Digital,Science & Technology

Jo Stevens, Shadow Secretary of State for Digital, Culture, Media and Sport

Consultation launched August 2020

Labour

0000_20 Reproduced from electronic media, promoted by David Evans, General Secretary, the Labour Party, on behalf of the Labour Party, both at, Southside, 105 Victoria Street, London, SW1E 6QT.