2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? Response to the National Data Strategy Consultation

2 December 2020

Introduction

Which? welcomes the opportunity to submit a response to the consultation on the Government's National Data Strategy[1]. We welcome the intention to support the UK in building a world-leading data economy. Which? firmly believes that digitisation and the use of data can bring substantial benefits and has great potential for consumers. In looking to secure these benefits, there should be a focus on ensuring that consumers have control of their data and are able to trust the way that data they share is collected and used. A truly world-leading data economy should ensure that people have confidence in the systems that deliver it.

Which? is the UK's consumer champion. As an organisation we're not for profit - a powerful force for good and here to make life simpler, fairer and safer for everyone. We fund our work mainly through member subscriptions. We are not influenced by third parties – we never take advertising and we buy all the products that we test. Which? works in pursuit of its charitable objects for the public benefit.

In Which?'s capacity as the UK's consumer champion, we have chosen to answer those questions which allow us to draw on our experience in consumer protection in the data sphere to present evidence and recommendations that draw on our expertise. We believe that there are other stakeholders and organisations that are well-suited to consult on the other areas of this consultation. Our response therefore will concentrate on questions relevant to consumers, or work Which? has undertaken and published that could bring insights, guidance or recommendations for the National Data Strategy team, going forward.

Overall, Which? is supportive of the National Data Strategy and welcomes a focus on data as a driver for a thriving digital economy; for the wider societal good, as well as for consumers. Consumers, however, are not well considered by the strategy, which focuses on the role of government and the private sector. We believe a **National Data Strategy must be people-centric, and we propose ways in which the government can bring people into the conversation about data to help shape the strategy and its implementation**.

We believe the strategy to be very ambitious and are keen to see an action plan that sets out how it will be achieved. We offer our insights about security - of data on devices and in services, as well as

[1] National Data Strategy Consultation

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

the security of data infrastructure providers - and we caution against over-reliance on dominant infrastructure providers. Our response also discusses our views on strengthening GDPR and details where trade deals could impact UK citizens' data rights, now or in the future. Underpinning our support of the strategy, and any comment we make about improving and strengthening it, **is our desire to support consumers across the UK to get the best possible outcomes from the data opportunity; building consumer trust in data and data-driven services will be of paramount importance in ensuring the strategy is successful.**

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Answers to Consultation Questions

Q1. To what extent do you agree with the following statement: Taken as a whole, the missions and pillars of the National Data Strategy focus on the right priorities. Please explain your answer here, including any areas you think the government should explore in further depth.

1.1 Overall, Which? 'somewhat agrees' with the priorities identified in the National Data Strategy. We welcome the strategy's approach to setting out how the government intends to leverage existing UK strengths to boost the better use of data across businesses, government and civil society, including the opportunities provided to maximise these strengths domestically once the UK has left the EU, and to influence the global approach to data sharing and use.

1.2 The strategy places high value on data, and has placed solid emphasis on government's use of data and the influence that government could - and should - have in the wider world and economy. However, we are disappointed by the lack of reference to people, and specifically to people as consumers.

1.3 It is easy to assume that people are inherently at the core of policy. However, assumptions often need to be clearly defined to preclude misunderstanding as to who the benefits are for when strategies are implemented. **Data is a fundamental aspect of all of our lives, from our home life, work life, engagement with business, government and the national infrastructure; all these aspects must be considered, and they must be considered in relation to people, not just to data.** When data is used to make decisions, provide benefits or steer people towards services, it should be completely clear how the data was collected, used, stored and (where relevant) shared. Transparency on the governance, demonstrating the ethics, and clarity on the benefits and risks, will help to build and instill trust.

1.4 Despite being integral to our lives, data can be an abstract concept. We commend the strategy on its efforts to try and create clear missions, pillars and opportunities for the integration of data. In order to make the intention a reality, people must understand that the value of the data they share is circular; that data sharing will benefit them in some way. It is here that we feel the strategy could be improved.

1.5 Part of this will rely on us all understanding and acknowledging that data is rarely, if ever, one thing. It is rarely about one person, one product, one group; it is agile and complex. The way data is used can change its value and utility. Data is not an unknown, intangible entity and yet that is how it is often seen or referred to.

1.6 We would like to see an improved approach to how data is referred to and considered within government. This is of particular relevance to wider societal understanding of data: what data is, what value it has, what benefits and risks can occur from understanding or misunderstanding data. Arguably, this will occur naturally as we all level-up on our understanding and data literacy, but it is critical that government sets the scene. Not all data is the same; its use can differ, as can its value, depending on context. **It is vital that there**

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

be an improvement in how data is spoken about in order that consumers understand what data is being referred to, collected, stored, shared etc., for what purpose, why and for how long. Personal data, for example, can mean many different things: identifying data, special category data, behavioural data, open data and so on. Assigning all data the same value is unhelpful and will not improve understanding or progress towards next steps, particularly around the four pillars.

1.7 For Which?, consumer-centric data principles must be the foundation of systems and initiatives in order to achieve the desired benefits for businesses, the economy and society as a whole. We feel that consideration of the systems and processes that make data useful are not well developed in the strategy.

1.8 Engagement with people will be key to developing a robust strategy and defining policies that work for all stakeholders. A two-way dialogue is essential in ensuring the work done to date can be developed in such a way that it serves the needs of citizens and consumers in the UK. **We are concerned that the strategy does not include two way engagement with the public** and make suggestions for how Which? might support a National Data Conversation in responses to further questions.

1.9 Furthermore, we raise concern that data is described wholly positively in the National Data Strategy. We appreciate this enthusiasm, but any strategy that talks solely of benefits, without consideration of risks is, in itself, a risky one. It also means that **emphasis on benefits - without accepting and being clear and honest about the risks - can be misleading for consumers and businesses alike**.

1.10 We welcome the hugely ambitious nature of the strategy, but are conscious that this ambition will likely take many years to implement. Thinking long term, rather than short term, is to be welcomed. However, we would like to see an action plan with tangible objectives.

1.11 The approach taken of outlining pillars, missions and opportunities has provided some structure to your thinking. This has been helpful as an outline for the strategy document but, moving forward, we would like to see that thinking established into a clear timeline and a specific action plan, outlining which elements of the strategy are urgent and which are longer term plans.

1.12 With time in mind, we would stress that pillar one (data foundations) and pillar three (availability), will be top priorities for government, as will addressing the siloed and legacy nature of existing government data and data systems. These concerns should be undertaken as a matter of urgency. Making this a priority action will establish a long overdue, and much needed, foundation on which government can build, enabling the more dynamic and long term plans to flourish.

1.13 We would emphasise that pillar four (responsibility) should be actioned in terms of maintaining existing data protection laws, including the General Data Protection Regulation (GDPR), and using them as a foundation on which to build. There is no need to rewrite the rule-book,as has been suggested in a written statement made by the Prime Minister earlier in

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

2020, stating that the UK will be seeking to '*develop separate and independent policies*'[2] post-Brexit. There is the potential that such an approach of scrapping - or moving away from - the existing data protection regulations would cause unnecessary disruption and cost to business, at a time when the country faces multiple other challenges.

1.14 In terms of a strategy that is fit for the whole of the UK, Which? is keen to understand any regional or national considerations. We welcome that the government '*is committed to working with the devolved administrations to align activity on advanced data, digital and R&D skills to support vibrant career pathways and to attract talent*'; yet the strategy pays little attention to any regional differences. Specific markets may operate in different ways within the nations (for example public transport) and devolved administrations (or regulators) may collect their own data (for example food hygiene enforcement). We would welcome the government's response to how any regional or national issues would be considered to ensure all UK consumers can enjoy a thriving, data-driven economy.

Q9. Beyond existing Smart Data plans, what, if any, further work do you think should be done to ensure that consumers' data is put to work for them?

9.1 In order to realise the transformative potential of data, consumers must be at the heart of any new initiatives. **Creating an environment where data is appropriately usable, accessible and available across the economy will only fuel growth if consumers are willing to engage**. Consumer concerns must be addressed and initiatives must be designed to instil trust in data usage and participation in the data economy. This is particularly relevant for Smart Data, as its focus is on citizens asking their providers to share data with third parties. However, it extends to all initiatives that seek to put control back into the hands of consumers.

9.2 Which? believes that, for consumer's data to truly work for them, consumers should be in control of data about them and aware of how that data is used. Yet research has shown that 7 in 10 consumers don't believe they currently have control over how the data is collected and used by companies, whilst **57% do not feel that businesses are open and transparent about the collection and use.**[3]

9.3 *Control, Alt or Delete?*[4] research by Which? also found that consumers who can be identified as **vulnerable are more concerned than the rest of the population about the tangible impact that the sharing of their data could have.** This includes concern that irrelevant data could be 'used against them', for example stigmatising them based on health conditions such that they will be charged a higher price for a product or service. This is something that greater data availability or portability alone will not mitigate; these concerns require targeted action based on understanding how to prevent specific harm, with this subsequently being built into initiatives. This demonstrates that much work is to be done

[2] Written Statement, the Prime Minister, Hansard 2020

[3] Which? ' Consumers and their Data' research review 2018

[4] Which? 'Control, Alt, Delete' Research

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

before consumers' data can be put to work for them. **Which? wants to see consumers be given greater and more meaningful transparency, information and control over how data about them is collected, retained, shared and used.**

9.4 We would extend this beyond the private sector to the public sector also. If the intention is to use consumers' personally identifiable and behavioural data to identify services that public sector organisations feel are suitable to a consumer, such an approach should be completely transparent. Furthermore, it should not be presumed to be beneficial without communication and consent from the individuals and groups involved. **Public sector organisations should ensure that collection and use of data is clear, transparent and necessary**, and that the individual or group is informed throughout of how the data they share will be used and how they can control onward travel of data to third parties. Alternatively, they should be clear on how access can be granted to data for a controlled period of time (to enable a service to function or assist the consumer), as opposed to the requirement for them to share the data in perpetuity. We emphasise these examples in particular to support the intention to create a fairer society for all.

9.5 We welcome the aspiration of a fairer society for all, but note that fairness is subjective. What is fair to one person or group may be inherently unfair to others. This is an area that warrants wider conversation. However, as a starting point we would welcome the use of non-personal or aggregated anonymised data to help steer policy and decision-making to improve society as a whole. We would expect to see clear explanations to consumers about the use of non-personal data, to improve literacy about how different types of data are used for different purposes. We would also expect to see information informing people if personal data is to be used, how they are protected, as far as possible, from re-identification using techniques such as anonymisation or synthetic data or aggregated data sets. Which? research has found that consumers who feel that their data has been used transparently are more accepting of its use[5].

9.6 If there is an intention to use consumers' personal data and/or behavioural or inferred data, it will be vital that there is a 'two way street' of communication between the individual and the business or organisational stakeholders.

9.7 There is general understanding and acceptance that personally identifiable data about us is used for public and private sector services, but there is not wide understanding or awareness of how inferred data about us is used. Which? found examples of how inferred data is used during our research on collection of data for targeted advertising[6]. We understand the reasoning and the perceived value of collecting consumers' behavioural data, but the collection of such data - in such broad, intrusive and hidden ways - is completely unique. Never before have people's inner thoughts been captured in a way that is so invisible and insidious. Whilst the value of benefit may seem to outweigh these concerns - particularly if the intention is to 'improve' people's lives - the ethics and morality of such an approach are questionable. With this in mind, **we expect to see full transparency of what is**

[5] Which? (forthcoming, 2021) *'Are you still following me?'*

[6] Which? 'Are you following me?'

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

planned, with a clear ethical process undertaken, which brings consumers into the conversation so that trust can be determined rather than presumed.

9.8 In circumstances in which consumers' data is to be used to make inferences about them, it may be that greater control should be given by default. For example, use could be on an opt in basis, with no detriment or loss of basic service to the consumer should they choose not to participate. In such circumstances, a requirement to opt in would maximise consumer protection, which is important given that consumer engagement with privacy settings and controls is especially low at sign-up. It should be noted that our research on data use for targeted advertising shows that consumers prefer to opt-in to targeted advertising rather than have to opt-out[7]. An opt in also creates an incentive for businesses to persuade consumers to share their data, creating competitive pressure that can drive innovation as well as a mechanism for commercial gains from data use to be shared with consumers. This is likely to be particularly valuable in digital markets dominated by large platforms. Hence, we support the government's creation of a Digital Markets Unit with the ability to set a code of conduct for platforms designated with Strategic Market Status.

9.9 Data portability and smart services are becoming more prevalent. Ensuring that consumers have access to the 'insights' and 'inferences' organisations create about them based on behavioural data, will be as critical as the existing right to receive the personal and special category data that has been shared with a service. This is a process we would expect to be explored further around the opportunities and risks for data portability and the intention to explore personal data mobility for competition and innovation.

9.10 Whilst there are many positives from the collection and use of consumers' personal data, we raise caution over the intention in the Strategy to use profiling technologies. Such technologies are often perceived as a panacea to societal problems which people should willingly accept as a benefit. But profiling people can create unforeseen vulnerabilities or harms; for example removing people's right to anonymity in certain complex situations based on their jobs or personal circumstances, or identifying and categorising people whose situations may be fluid and whose 'vulnerability' may be temporary. Profiling, and the use of profiling data to build machine learning tools and algorithms, can risk embedding bias or exclusion and undermining trust and fairness for citizens and consumers alike.

9.11 **Which? has found that consumers feel disempowered around how data about them is used**. For example, consumers find third party sharing a fundamental concern[8]. Furthermore, they are often unaware of the extent to which their data is shared with third-parties and when informed about it do not feel that it is transparent or that it offers them control.[9] These are critical areas which are still balanced in favour of the companies as opposed to the consumer.

[7] Which? (2020), *Are you following me?*

[8] Ibid Which? 'Consumers and their Data' research review 2018

[9] Which? (2018) Control, Alt or Delete

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

9.12 The connected world is, for most of us, an integral part of our day to day lives. People treat their online engagement with the similar decision and choice making skills as they do in the offline world. Decisions are made based on the moment in time, levels of trust, the context in which they are undertaking a search or purchase. Decisions based on convenience or recommendations (two of the often cited reasons for a consumer to share data with an organisation) are only one part of a much more complex picture. Consumers have wider reasons for wanting to share or not share data, and their decisions should be based on clear, transparent information about the responsibilities of the service provider. Furthermore, consent messaging and communication must make clear how consumers' data will be used, the benefits this can provide and the protections that will be in place. Communications must additionally take account of - and address - vulnerable consumers' fears about their data (or information pertaining to their vulnerable status) being used to discriminate against them.

9.13 We would encourage the National Data Strategy team to look at the 'Choice Requirement'[10] highlighted by the Competition and Markets Authority and the 'Fairness by Design'[11] duty which seeks to develop as a code of practice the requirement for services to be designed in a way that does not make consumer control over data overly complex, time consuming or incoherent. Whilst these are currently focused on digital advertising there may be a need for the key principles of fairness, transparency and choice to be considered in a broader context when data collection, storage and use may be opaque. Whilst there is plenty of work and exploration to be undertaken to make consumers' data work better for them, we would encourage wider engagement around data portability and personal data mobility as outlined in the Furman Review, as part of public engagement on data more generally. Ensuring that consumers can really benefit from the data about them, and others, that they share will rely on exploring the portability of input data, observed data and inferred data.

9.14 Which? has experience of designing and delivering public engagements with consumers[12]. **We recommend creating a 'National Data Conversation' with consumers.** In this way, the National Data Strategy team and wider stakeholders would hear consumers' expectations, understanding, wants, needs and concerns about how data about them will be used, for what purpose, and with what benefits and risks across all the areas outlined. This would place people at the heart of the National Data Strategy.

9.15 In order to ensure that any initiatives stemming from the National Data Strategy lead to consumers' data truly working for them, their needs must be considered throughout the different development stages. Consumer dialogue and stakeholder engagement are needed to garner the insights into why and how consumers feel their data is not working for them. It is necessary to facilitate meaningful public engagement at the early stages of development, in order to ensure that the right transparency frameworks are identified and designed, the necessary privacy considerations are made, and other barriers to consumer trust and engagement are addressed.

[10] Which? submission to the Digital Markets Taskforce July 2020

[11] Ibid Digital Markets Taskforce

[12] A recent example was the Which? National Trade Conversation

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Q10. How can the UK's data protection framework remain fit for purpose in an increasingly digital and data driven age?

10.1 The UK's Data Protection Act 2018 (DPA 2018) is an excellent foundation on which the UK can build. As with any piece of legislation, there are areas which can be improved and also be expanded and built upon as technologies change. But the foundation of the data protection rights afforded to consumers and citizens alike, through the inclusion of the GDPR into the Act, is one Which? and consumers want to see retained, post-Brexit.

10.2 One of the benefits of the GDPR is that it establishes a duty for organisations to report to the Information Commissioner's Office (ICO) if they have suffered a data breach, along with those affected if the breach is likely to have a high risk of adversely affecting individuals' rights and freedoms. Which? has informed consumers about several large-scale major breaches since the introduction of the legislation[13]. While it has been beneficial for consumers to be aware that a business or organisation has experienced a breach, the opportunity for consumers to seek redress for the very real harm they can experience following a breach of data is an area of the GDPR that needs to be strengthened.

Adequate Redress

10.3 **A critical element to ensuring that the UK's data protection framework remains fit for purpose in an increasingly digital and data-driven age is to build consumer trust in their data rights through access to adequate redress.** Access to adequate redress is a necessary consumer right in the data space. Which? believes there is a compelling need for better provisions.

10.4 In September, 2020 Which? responded to the government's call for views and evidence, 'Review of Representative Action Provisions, Section 189 Data Protection Act 2018'. Our response highlighted elements of the current redress mechanism (in force under the current representative action provisions) that pose a challenge for consumers[14]. Which? continues to seek the implementation of Article 80(2) GDPR and the measures that would allow not-for-profit organisations to bring representative actions on behalf of consumers, on an opt-out basis.

10.5 The current 'opt-in' system is not working to adequately serve consumers who suffer at the hands of data breaches and business practices that contravene data protection principles. This is evidenced by the low uptake of the current provisions, a fact highlighted by the government in the policy paper for the call for views and evidence[15]. A fundamental reason for this is that the current model presupposes that affected consumers are aware that their data has been breached. Furthermore, it presupposes that consumers are aware of their right

[13] https://www.which.co.uk/news/tag/data-breach/

[14] Which? Response to Call for Views and Evidence on Representative Action Provisions DPA 2018

[15] Policy Paper, Call for views and evidence - Review of Representative Action Provisions, Section 189 Data Protection Act 2018

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

to appoint a representative body, and see the value in expending time on such an appointment in circumstances where the individual harm suffered may seem relatively small -even though it may have had a much greater collective impact. Consumers often know less than businesses and organisations about how their data may be used, and by whom, and the associated consequences. We consider it unrealistic to assume knowledge of probabilities of all possible outcomes and for consumers to be able to evaluate these against each other in deciding whether or not to take action. Not-for-profit representative bodies are generally better informed, due to greater available resources and the smaller opportunity cost for them to investigate.

10.6 **More needs to be done to hold businesses to account when they do not adequately protect consumers' data or engage in business practices which contravene the data protection principles**. More also needs to be done to incentivise them to improve their data processing practices. Facilitating redress through an opt-out mechanism that allows not-for-profit organisations to bring collective redress actions on behalf of consumers would be a complementary method to incentivising good practice, alongside existing measures.

10.7 One clear, fundamental legal change to improve enforcement is to bring stronger powers to not-for-profit organisations to tackle systemic issues relating to lack of redress.

Q12. We have identified five broad areas of work as part of our mission for enabling better use of data across government: **quality, availability and access - standards and assurance - capability, leadership and culture - accountability and productivity - ethics and public trust. We want to hear your views on any actions you think will have the biggest impact for transforming government's use of data.**

12.1 Which? believes that better use of data across government will rely on getting the foundations right; and this will take time. The intention to improve data sharing and access across government are admirable and we welcome the broad scope outlined in this document. However, understanding the details of the foundational plans will be critical.

12.2 The five areas outlined all make logical sense. Understanding that each government department works differently and identifying which parts of government are still working on legacy systems will likely be the first step.

12.3 We would encourage the government to make better use of Application Programming Interfaces (APIs), and to mandate APIs as the data sharing standard across government. Implementing APIs would allow data to be interoperable and easily consumed by interoperating government services. Progress in the implementation of APIs for sharing government data will also support and accelerate commercial innovation, as private companies will more easily be able to leverage government data in the delivery of services to support the public.

12.4 Advancements in this area will improve access to data in order to encourage and invigorate innovation, both inside and outside government.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

12.5 The strategy places emphasis on data interoperability and data mobility. Interoperability and mobility, considered individually or together, are not a 'silver bullet' for organisations, or for users. Whilst we agree that public sector data should be interoperable so that it can be used by other systems, we caution against a requirement for private companies to make all data available in such a way. As we have stressed, not all data is the same. Whilst there may be sense in specifying interoperability requirements for certain types of data, we cannot envisage a one-size-fits-all approach being the optimal solution. Furthermore, interoperability and the ability to move data is only useful when there are systems which can consume and use data to drive new innovative services. A focus on data without due attention to services cannot succeed. We would, therefore, urge the government to consider how to support the development of new services that leverage data, as well as focusing on the nature and format of the data itself.

Q14. What responsibilities and requirements should be placed on virtual or physical data infrastructure service providers to provide data security, continuity and resilience of service supply?

14.1 We welcome a focus on security in the strategy. However, this focus is on the security of data infrastructure providers, and does not consider the security of data services. Security plays an important role in the uptake and usefulness of any data service. We would like to take this chance to offer our views on the required security measures for digital services more generally (not limited to data infrastructure providers).

14.2 Robust data security is of critical importance when it comes to protecting consumer rights, instilling trust and encouraging consumers to participate in any initiatives underpinned by data sharing or data access. Consumer fears about misuse of the data they share, inadequate security measures and business practices that put personal data at risk (and lead to data breaches) must all be addressed and used to build responsibilities and requirements into data infrastructure.

14.3 In Which?'s Consumer Insight Tracker, we ask consumers about their worries on a quarterly basis, with November 2020 being the source of our most recent data. 68% of consumers asked said they were worried about the security of the data they share. **Consumers express greater concern about data security than any other issue that we track, including food prices (56%), housing costs (50%), fuel prices (48%) or Brexit (55%)[16].** Initiatives such as making data interoperable, improving availability and portability can only be effective if there are adequate safeguards and security measures, and consumers have trust in these.

14.4 In Which?'s 2020 investigation looking at the human cost of data breaches, consumers expressed worry at the data they have shared being 'out there' following data breaches[17].

[16] Data from the November wave of Which?'s Consumer Insight tracker, conducted by Yonder Ltd. on behalf of Which? from 18th-20th November 2020. A sample of 2,094 consumers was surveyed and weighted to be nationally representative according to a range of demographic characteristics.

[17] The Human Cost of Data Breaches

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

These worries are not unfounded. Data breaches, recovered passwords, phishing and common attacks feed into each other, creating ever-increasing public and private repositories of known email addresses, passwords, and compromised accounts used by scammers.

14.5 Consumers are exposed to considerable harm through data breaches, inadequate security measures that place personal data at risk, and data processing practices that violate data protection principles. Thus, more needs to be done to hold data controllers to account when they do not adequately protect consumers' data and incentivise them to improve their practices and security measures.

14.6 In September 2020, Which? published an investigation which exposed hundreds of serious data security vulnerabilities on major travel firm websites[18]. In June 2020, working in collaboration with security experts, 6point6, Which? assessed the security of websites operated by 98 travel industry companies, including airlines, tour operators, hotel chains, cruise lines and booking sites. Which? did not just look at the main website of each firm, but also related domains and subdomains – including promotional sites and employee login portals.

14.7 Any vulnerability in these websites could be an opportunity for a malicious hacker to target users and their data. We did not engage in complex hacking to find this information, but rather used publicly available, lawful online tools that anyone can access. Certain businesses in the travel industry have already had their details - and those of their customers - stolen in major data breaches, yet our experts found dozens of critical hacking risks on their websites.

Q15. Demand for external data storage and processing services is growing. In order to maintain high standards of security and resilience for the infrastructure on which data use relies, what should be the respective roles of government, data service providers, their supply chain and their clients?

15.1 If it is to be leveraged for societal good or for the good of individuals and consumers, data needs to be stored securely in robust systems that can scale to allow for the demands of future uses of data, and that are continually secured against evolving threats.. As such, scalable cloud services are a necessary part of a data strategy. We welcome government consideration of the role of infrastructure providers since the requirements for robust cloud services mean that the market for such services is contracting. However, security and resilience are not the only areas that should be considered when it comes to data infrastructure. **Market dominance is a key issue in data infrastructure, and one the government should consider carefully.**

15.2 Infrastructure providers that host much of the world's data are very powerful. Indeed, more than half (58%) of the world's data resides on servers owned by just three companies[19]. The market share of the top 3 providers is as follows: Amazon Web Services (AWS) hosts 32%,

[18] Can Travel Websites Keep Your Personal Data Secure?

[19] AWS vs Azure vs Google Cloud Market Share 2020: What the Latest Data Shows

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Microsoft Azure hosts 19%, and Google Cloud hosts 7% of the world's data. While AWS offers a low cost, robust and scalable solution to businesses, startups and organisations, the concentration of data (including much of the UK government's data on AWS[20]), raises concerns that this will be an uncompetitive market, resulting in excessively high prices and low quality. We note that AWS made up 12.1% of Amazon's revenue for Q3 2020, but 57% of its operating income[21]. The National Data Strategy makes no mention of how it might address a lack of competition in cloud storage and we are concerned that this may prove short-sighted.

15.3 'Cloud Neutrality' is a key concern given the market power of these three US-based cloud platforms. How can data infrastructure providers ensure that data held on their systems will be delivered fairly and, indeed, neutrally? Which? welcomes comment from the government on whether it recognises a need to ensure cloud neutrality, and how it might go about doing so to ensure fair access to so much of the UK's data. Cloud neutrality should be defined as 'the principle that requires data infrastructure providers to treat all data equally and without discrimination'.

15.4 Provisions for protecting 'Net Neutrality' should also be present in a National Data Strategy. There are certain potential risks to Net Neutrality that present themselves in trade deal negotiations. The UK and the EU have strong provisions on net neutrality - recently expanded by the Court of Justice of the EU (CJEU) to include banning the provision of consumers with commercial services under 'zero tariffs'[22],[23]. However, in the USA, for example, net neutrality rules have been relaxed in recent years. Net neutrality (often referred to as 'open internet') is the principle that requires that all Internet Service Providers (ISPs)[24] treat all communications equally and without discrimination.

15.5 In the UK and EU, blocking, throttling, and discrimination of internet traffic by ISPs is forbidden. This principle ensures that ISPs cannot restrict or dictate consumers' access to services of their choice on their devices. Under this principle, consumers are guaranteed that all the connections, access to services and internet speeds to access these services are treated equally, and that internet service providers cannot restrict access to them.

15.6 The measures introduced in trade deals to promote net neutrality and an open internet are not always up to the high standards that currently exist in the UK and EU. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), for

[20] AWS scoops three-year cloud deal with UK government

[21] AWS vs Azure vs Google Cloud Market Share 2020: What the Latest Data Shows

[22] Zero tariff or zero rating is the practice of telcos providing preferential access to certain applications and services without any data restrictions, whilst slowing down data speeds for other available applications and services once consumers have used up their data allowances.

[23] https://www.pinsentmasons.com/out-law/news/cjeu-applies-net-neutrality-rules-against-zero-rating

[24] Internet Service Providers, often referred as ISPs, are companies that enable consumers to access the interconnected networks of the internet.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

example, contains a clause that does not fully deliver on net neutrality[25]. Both the United States-Mexico-Canada Agreement (USMCA) and CPTPP include some basic commitments to keep an open internet, but '*subject to reasonable network management*'. The provisions in both trade deals are almost identical and vague, leaving a lot of space for interpretation[26].

15.7 Clauses on net neutrality will not necessarily cause any immediate harm to UK consumers, but the inclusion of weaker or vague provisions in new UK trade deals could help facilitate low-quality regulation that could set a ceiling for consumer rights in this area going forward. The UK must, therefore, maintain its position on net neutrality in trade negotiations.

Q16. What are the most important risk factors in managing the security and resilience of the infrastructure on which data use relies? For example, the physical security of sites, the geographic location where data is stored, the diversity and actors in the market and supply chains, or other factors.

16.1 While we appreciate a focus on security, infrastructure is only one part of a complex environment required to deliver positive outcomes for citizens and consumers through better use of data. **We would welcome more of a focus on devices and products that either generate or collect data and *their* security and resilience.** Without these services or devices there often is no data, so they are vital to consider as part of a comprehensive data strategy. We urge the government to retain the data protection principles of GDPR as the foundation of data protection in the UK, and implement measures to give consumers access to adequate redress mechanisms.

16.2 Which? undertakes research and testing of the security of connected/smart/IoT products on the market in order to better inform consumers of the risks to their personal security, as well as ways they can mitigate such risks. This work involves testing the security of devices and the diverse range of actors in the market and supply chain. Whilst our immediate concern is educating consumers on the risks to them, and how best they can protect themselves and their families, some of the risks and vulnerabilities we find and highlight can extend beyond individuals to groups, and to wider networks, if not contained. Our testing of consumer products should, therefore, be considered as a wider societal issue, not just an issue for the market or for consumers alone.

16.3 An example of the work Which? has done in relation to highlighting the most important risk facts in relation to connected smart products can be found in our most recent paper on the security of Smart Doorbells[27]. We point you to this investigation as a clear example of the ongoing problems and risks in the consumer market of connected products, which leave consumers' data and personal safety open to risk and harm, due to:

- unnecessary and excessive data collection
- unbranded products being sold online

[25] Article 14.10: Principle of Access to and Use of the Internet for Electronic Commerce, CPTPP.

[26] Trade In Services Agreement: Goodbye privacy, hello censorship

[27] The Smart Video Doorbells Letting Hackers Into Your Home, Which?, November 2020.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

- products with no password protection or clear guidance for the consumer on how to change a generic password
- poor or non-existent encryption of data flow
- failure to provide security updates to older, but still used, devices.

These are problems which extend across the Smart Product market, including: toys[28], baby monitors[29] and mobile phones[30], to name a few.

16.4 When it comes to the security of products, Which? welcomed publication of the government's Secure By Design agenda in 2018. We are also supportive of the commitment to introduce new legislation to improve security of IoT consumer devices, as a much needed first step, as was outlined in the subsequent Code of Practice for Consumer IoT Security. For further detail on our thinking and recommendations to the Code of Practice, please refer to our submission to the call for views[31].

16.5 The issue of security extends beyond hardware and software. In October 2020, Red Maple Technologies prepared a private research report for Which?, delving into what happens to consumer's personal data exposed in a data breach and painting a clearer image of what additional risks consumers are then exposed to. The research uncovered extensive information detailing how security vulnerabilities and breached data can expose consumers to further attacks and scams. No personal data was processed on behalf of Which? during this research.

16.6 A data breach of a company typically leaks personal information that includes the email addresses of account holders, as well as other personal information. It is rare for breaches to include passwords in a usable form (plaintext passwords), since industry standard protections for secure password storage (password hashing) are almost ubiquitous. However, given a dump of protected passwords, it is normally possible to recover a proportion of the passwords into their readable (plaintext) form, using password recovery (cracking) techniques that typically require lots of computation and lists of dictionary words and example passwords. Lists of email addresses are used, in conjunction with confirmed and possible passwords, to mount attacks such as phishing, brute-forcing, and credential stuffing.

16.7 Phishing involves sending emails containing malicious content to target addresses. Of late, this most often consists of a link to a malicious website designed to trick the victim into entering their credentials (username/email address and password). Brute-forcing and credential stuffing are both ways of trying to break into online accounts by testing lots of combinations of possible usernames and passwords. Brute forcing involves trying systematically generated passwords, whereas credential stuffing involves trying known passwords.

---

[28] Safety alert: see how easy it is for almost anyone to hack your child's connected toys, Which?, 2017

[29] Could My Baby Monitor Get Hacked?, Which, October 2020

[30] Void Android: More than one billion Android devices at risk of hacking attacks, Which, March 2020

[31] Secure by Design - Which? Response to Call for Views

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

16.8 The sheer scale of such continuous attacks is detailed by Akamai, a global content delivery network, cybersecurity and cloud service company which provides web and Internet security services. From July 2018 through to June 2020, Akamai observed 100 billion credential stuffing attacks across all industries[32].

16.9 While at one time hackers used to focus predominantly on gaining access to systems and data, the focus now is often solely on stealing credentials. This may be to sell them into the large market for credentials, to use them in further attacks, or both. The use of stolen account credentials is the most common action in large surveys of data breaches[33].

16.10 The market for stolen credentials is well established; it largely relies on the Dark Web for hiding the identity of the buyers and sellers, and cryptocurrencies (like BitCoin) for anonymous transactions. The Dark Web is a parallel version of the Internet that can be accessed by anyone using specific applications. These applications provide encryption and anonymisation of the users' traffic and their location. There are a lot of anecdotal examples of such transactions, which range in price from a few dollars for small numbers of accounts, to hundreds or thousands of dollars for large sets of credentials.

16.11 In its research for Which?, Red Maple Technologies safely captured screenshots of Dark Web sites that are either open or require simple registration to access, without any sharing of data or purchases. These screenshots showed large data dumps for sale on sites aimed at selling stolen data. Data dumps of various sizes were presented, each of which affected over a million customers, with prices for the dumps ranging from $200 to $10,000. We have seen the human cost of credentials falling into the wrong hands - consumers suffer real harm as a result of breaches and inadequate business practices.

16.12 Inadequate data security measures and protections, data breaches, recovered passwords, phishing and common attacks all feed into each other. They create ever-increasing public and private repositories of known email addresses, passwords, and compromised accounts that put consumers at risk and lead to consumer detriment.

16.13 Consumers are exposed to considerable harms through data breaches and inadequate security measures that put personal data at risk, as well as data processing practices that violate data protection principles. Therefore, more needs to be done to hold data controllers to account when they do not adequately protect consumers' data, and incentivise them to improve their practices through mandatory security requirements and responsibilities.

16.14 While we are wholly supportive of the approach to data breaches, in terms of fines and potential criminal records outlined in the GDPR, our research (discussed in question 14, above) demonstrates that some companies remain dismissive at best, and ignorant at worst, about their responsibilities towards data security of consumers data.

[32] Akami

[33] Verizon Data Breach Investigations Report 2020

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

16.15 In light of this research, **we urge the government to firstly retain the data protection principles of GDPR as the foundation of data protection in the UK, and implement measures to strengthen gaps in enforcement and transparency.**

16.16 Secondly, we urge the government to implement measures to give consumers access to adequate redress mechanisms[34]. The government has the power to facilitate better redress by implementing Article 80(2) GDPR in its current review of the Data Protection Act 2018. This would allow not-for-profit organisations, such as Which?, to bring collective redress actions on behalf of consumers on an 'opt-out' basis, without those consumers each having to bring – or appoint a representative body to bring - an individual case against the company involved. A properly implemented redress system would ensure that consumers could trust that harm suffered as a result of data breaches would be remedied, and would simultaneously act as an incentive for companies to improve their data handling processes.

Q17. Do you agree that the government should play a greater role in ensuring that data does not negatively contribute to carbon usage? Please explain your answer. If applicable, please indicate how the government can effectively ensure that data does not negatively contribute to carbon usage.

17.1 Which? strongly agrees. We expect to see both the government and the private sector implement sustainable systems and offer transparency regarding the impact of data on the environment.

Q18. How can the UK improve on current international transfer mechanisms, while ensuring that the personal data of UK citizens is appropriately safeguarded?

International data availability

18.1 International data availability has become a critical element to international trade. The UK is developing its trade policy for the first time in over 40 years and digital trade will be a key focus of its trade negotiations. This will present opportunities for the government to ensure that there are effective and efficient mechanisms to transfer personal data from the UK, allowing both consumers and businesses to benefit from digital trade. However, it is critical that robust safeguards are in place to protect and allow consumers to retain control of the data they share about themselves and others. Removing barriers to data flows, personal data transfers and supporting data availability in other countries must not come at the cost of the data protection principles that currently operate in the UK under GDPR and the Data Protection Act 2018.

18.2 Consumers worry about data they share and also about the data protection framework in the UK being affected by trade negotiations in the name of international data availability to underpin digital trade. Which?'s National Trade Conversation has opened up trade issues directly to consumers around the country, giving them the opportunity to say what matters most to them - from digital trade to food standards. These public dialogues, held in five regions of the country and involving people from all walks of life, have provided a unique

[34] Which? Response to Call for Views and Evidence on Representative Action Provisions DPA 2018

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

insight into consumers' expectations around a range of issues, including digital trade. People were receptive to the economic benefits that could come from enhanced digital trade, but expected the government to ensure effective consumer protection. **Maintaining the UK's strong data protection provisions was one of the main priorities for participants.**

18.3 In Which?'s National Trade conversation, consumers were shown government objectives for digital trade. They perceived the opportunities for businesses and the economy to make the trade of goods and the transfer of services easier and faster. However, they were widely concerned about the potential implications for the protection of consumer data and online rights in order to facilitate the free flows of data needed to enable smoother digital trade. The majority view was that a weakening of the GDPR regime, which contains elements that can be improved upon, would remove the minimum protections consumers need against hidden, and growing, online harms[35]. Defining the right digital trade terms has the potential to reap great benefits for the UK, given its strength in exporting services, but necessitates addressing consumer concerns and looking at both protections and rights when data crosses borders.

18.4 The continued success of e-commerce depends on the active engagement of consumers and willingness to share data, which is dependent on their trust. Developing international data transfer mechanisms to underpin digital trade comes with opportunities as well as risks. It is important to consumers that the government strikes the right balance.

International free flows of data and data localisation: opportunity and risk

18.5 Data is an essential asset for digital trade. If it can flow across borders it has a higher potential for providing a more varied marketplace, offering more meaningful services and products for consumers. Free trade agreements have the possibility of further enabling such data flows, and international data availability, by limiting data localisation.

18.6 Data localisation is the requirement for companies to use, or to locate, their computing facilities within a country's territory as a condition of doing business in that country. Data localisation is often deemed a protectionist measure. Data localisation requirements can take different forms, such as businesses having to physically store data on servers in the country the data is collected or requirements surrounding the processing of that data within the country. This is associated with greater costs, due to the IT infrastructure and stringent security measures required. As a result, the banning of data localisation is sometimes sought to enable free flows of data.

18.7 Free flow of data is the unrestricted movement of data across borders and IT systems. Opportunities in digital trade are closely connected with data and its global reach. For example, the same product or service can be bought by consumers across different countries. Digital trade has the potential to provide consumers with more choice when it comes to accessing existing products from other jurisdictions, as well as access to new products and services, and could potentially lower prices.

[35] Which? (2020) National Trade Conversation

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

18.8 Cross-border data flows can facilitate better organisation and delivery of services and goods. For example, businesses can use cross-border data flows to track international shipments of goods using Internet of Things (IoT) services, as goods travel from the factory through to transport and delivery, and then to consumers. This means that consumers could have better access to accurate tracking of orders. Better tracking of goods also reduces the potential for theft or waste. By utilising cross-border data flows, companies could develop more accurate risk management predictions (e.g. for car and life insurance), personalise product offerings, provide cheaper services (via cutting costs on not having local data centres), and even provide better protection from financial crime and money laundering.

18.9 The UK regime for data protection provides high standards for privacy that could be at risk from the measures to promote cross-border data flows in trade deals. This is an important issue for consumers as purchases move online and data-gathering digital technology becomes embedded in all kinds of everyday goods, from fridges to vacuum cleaners. Without strong data protection measures, consumers' data could potentially be collected, retained, used and shared in ways that they did not consent to or expect.

18.10 In this light, free flows of data and banning of data localisation also represent a risk in trade deals. Measures to promote cross-border data flows could make it harder to control the transfers of personal data of UK consumers to countries with lower protections. These measures could clash with the current UK regime of data protection under GDPR, risking existing data flows with the EU and an adequacy decision after the Brexit transition period.

18.11 The government has stated its intention to seek an EU adequacy decision from the European Commission that establishes that a country, territory or a specific sector (eg public sector or certain businesses) must ensure an adequate level of data protection. This would mean that data transfers in this context would continue to be treated as transfers within the EU, without the need to make any extra arrangements. This would, in turn, ensure that UK consumers and businesses enjoy continuity of the high levels of data protection currently in place, alongside the additional benefits of continued digital trade without interruption post the Brexit transition period. References to data protection without extensive detail made in Free Trade Agreements could still be detrimental to UK consumers, if the language used introduces flexibility into the well-regulated UK system, by promoting interoperability between GDPR and weaker international rules for data transfers.

18.12 The text of the US-Mexico-Canada (USMCA) agreement, the most relevant deal for the US's likely approach to a trade deal with the UK, allows for voluntary undertakings by companies relating to privacy to be equally as valid as regulation. This is also the approach taken in The Comprehensive and Progressive Trans Pacific Partnership (CPTPP), to which the UK would like to become a signatory. References to adoption of international data protection laws can initially sound positive. However, recent deals, including the USMCA, have linked them to international guidance, such as that developed by the OECD. This is more limited than current UK data protection rules and would result in lower privacy protection for UK consumers than is currently in place.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

18.13 The data protection clauses in those agreements would not force the UK to replace the GDPR with a lower regime altogether, or stop it from adopting a more stringent regime. However, these texts would blur the lines between strong and weak privacy regimes with the aim of interoperability. The UK must, therefore, ensure that trade deals do not undermine the current level of data protection that consumers can expect in the UK under the GDPR.

18.14 Consumers should be able to exert full control over their personal data (how it is collected), how it is used and whether it is shared in domestic and international contexts. Critically, negotiations surrounding digital trade should be transparent, and multi-stakeholder dialogue should be encouraged both nationally and internationally. Negotiating proposals and consolidated texts should be made publically available so that consumers know what is being negotiated on their behalf.

Limiting business accountability

18.15 Measures designed to prevent disclosure of source code, and to give stronger intellectual property protections to businesses (such as preventing forced technology transfers in exchange for market access) could reduce the transparency and accountability of technical systems that are also, increasingly, being used in many decision systems that use consumer data and affect consumer's lives. This includes things such as credit, financial data, court sentencing or migration status. There is a risk that companies could have greater powers to use algorithms to make unfair, deceptive or discriminatory decisions, such as presenting different prices to some consumers, or even a different service offer altogether.

18.16 Unrestricted data flows to countries that have weaker provisions on data protection would expose UK consumers to a market on personal data that gives businesses disproportionate powers over consumers through information asymmetries. This, combined with measures in trade deals preventing the disclosure of source codes, could be problematic. There are growing concerns about the use of algorithms in many decision systems that affect the lives of citizens and consumers.

18.17 The US negotiating objectives for a deal with the UK, however, include an aim to '*establish rules to prevent governments from mandating the disclosure of computer source code or algorithms*'[36]. The USMCA also specifically prohibits the requirement to transfer algorithms expressed in source code, as a condition. The CPTPP, which the UK has said it would like to become a signatory to, rules out the ability of regulators to require source code of software from businesses as a condition of the import, distribution, sale or use of the software - or products - containing it, for example.

18.18 Companies can use algorithms to make unfair, deceptive or discriminatory decisions. Pricing decisions could take advantage of consumers' vulnerabilities. In addition to pricing and marketing, profiling data services can also be used for political campaigning and to subvert the democratic process providing the basic foundation for consumer rights. In the USA, for example, data brokers search public records from schools, courts or police (as these do not have privacy restrictions in the USA) and buy commercial databases, such as magazine

[36] US, UK Negotiating Objectives

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

subscribers. These companies work with social media platforms to further profile individuals. Digital trade agreements can include some public policy exceptions for courts and regulators to access technical systems, but these may not be sufficient to protect consumers in commercial settings.

Developments in digital trade negotiations relating to international data transfers

18.19 The UK-Japan Comprehensive Economic Partnership Agreement (CEPA) was agreed, in principle, on Friday 11 September 2020. CEPA was then officially signed on Friday 23 October 2020, pending ratification. This is the UK's first major trade deal as an independent trading nation.

18.20 Japan has an EU adequacy decision under the GDPR and is also a signatory to the free flow of data provisions in CPTPP, of which it is a leading member. Japan has been advocating for digital trade liberalisation and is a chief proponent of the ban on disclosure of source code and proprietary algorithms, having been at the forefront to introduce such measures at the World Trade Organisation.

18.21 The UK-Japan Agreement, CEPA differs from the EU-Japan EPA in how it deals with cross-border data flows. The Agreement includes a general binding commitment not to '*prohibit or restrict the cross-border transfer of information by electronic means*', with privacy as a legitimate public policy exception. However, the privacy exception allows for challenge. The inclusion of such provisions raises some concern as it not only affects cross-border data flows between the UK and Japan, but could also have implications for how UK consumers' personal data is then shared with other countries that Japan has agreements with. It would also appear to put the possibility of an EU adequacy decision at risk. It is essential that this agreement, and future agreements, do not inhibit the UK's ability to ensure appropriate consumer protection.

Q19. What are your views on future UK data adequacy arrangements (e.g. which countries are priorities) and how can the UK work with stakeholders to ensure the best possible outcome for the UK?

19.1 Which? welcomes the government's intention to seek EU 'data adequacy' to maintain the free flow of personal data from the EEA, alongside its intention to pursue UK 'data adequacy' with global partners. This will both promote the free flow of data to and from the UK and ensure it will be properly protected.

19.2 The UK is deciding its trade approach with multiple countries at once. As such, this approach introduces risks and opportunities relating to digital trade and international data transfers for UK consumers. These risks and opportunities will change depending not only on the content but also the order that any trade agreements and data adequacy decisions are made.

19.3 As an example, if the EU considers the UK for a data adequacy decision it would need to consider what mechanisms are in place for further transfers of data to countries with lower protections. The EU would seek to prevent the UK from becoming a "data laundering" haven,

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

where European citizens' personal data could end up in low protection jurisdictions due to agreements the UK has already entered into with other countries, such as the US.

19.4 The lack of an adequacy decision would disrupt the continuity of data flows between the UK and EU. This could mean that access to goods and services currently enjoyed by UK consumers is disrupted. It could also lead to greater divergence from GDPR principles in the UK's continued digital trade negotiations with other countries, thereby leading to a lowering of data protection for UK consumers. **It is critical that consumers do not see a lowering of standards and a loss of current levels of protection when it comes to personal data as a result of the UK's future data adequacy arrangements**.

19.5 Furthermore, a data adequacy decision from the EU will enable the continuation of the GDPR for business. We note, and welcome, the government's intention to ensure that we have a '*data regime that is neither unnecessarily complex nor vague*' and agree that businesses '*need certainty to thrive*'. Adequacy and maintaining continuation of the GDPR will enable businesses to continue to work within a framework they are familiar with, and upon which improvements can be made. The GDPR was a complex regulatory change for many businesses, such that the desire to change to another regulatory process is likely to be unappealing (particularly as the current regime is not even three years old).

19.6 In reference to the lifting of compliance burdens, we would expect to see clarity on what the government is thinking, to understand what areas of compliance are perceived as burdensome and to whom.

For further information please contact Katie Lips, Head of Digital & Scams Policy, Which? at katie.lips@which.co.uk