

Responsible use of data : Government response to the Committee's fourth report of session 2014-15 : fourth special report of session 2014-15.

Contributors

Great Britain. Parliament. House of Commons. Select Committee on Science and Technology
Stationery Office (Great Britain)

Publication/Creation

London : The Stationery Office Limited, 2015.

Persistent URL

<https://wellcomecollection.org/works/u834p8bk>

License and attribution

You have permission to make copies of this work under an Open Government license.

This licence permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Image source should be attributed as specified in the full catalogue record. If no source is given the image should be attributed to Wellcome Collection.



Wellcome Collection
183 Euston Road
London NW1 2BE UK
T +44 (0)20 7611 8722
E library@wellcomecollection.org
<https://wellcomecollection.org>



House of Commons
Science and Technology
Committee

**Responsible Use of
Data: Government
Response to the
Committee's Fourth
Report of
Session 2014–15**

**Fourth Special Report of
Session 2014–15**

*Ordered by the House of Commons
to be printed 2 March 2015*

HC 1086
Published on 5 March 2015
by authority of the House of Commons
London: The Stationery Office Limited
£5.00

Science and Technology Committee

The Science and Technology Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Government Office for Science and associated public bodies.

Current membership

Andrew Miller (*Labour, Ellesmere Port and Neston*) (*Chair*)
Dan Byles (*Conservative, North Warwickshire*)
Jim Dowd (*Labour, Lewisham West and Penge*)
Mr David Heath (*Liberal Democrat, Somerton and Frome*)
Stephen Metcalfe (*Conservative, South Basildon and East Thurrock*)
Stephen Mosley (*Conservative, City of Chester*)
Pamela Nash (*Labour, Airdrie and Shotts*)
Sarah Newton (*Conservative, Truro and Falmouth*)
Graham Stringer (*Labour, Blackley and Broughton*)
David Tredinnick (*Conservative, Bosworth*)

The following members were also members of the committee during the parliament:

Gavin Barwell (*Conservative, Croydon Central*)
Caroline Dinanage (*Conservative, Gosport*)
Gareth Johnson (*Conservative, Dartford*)
Gregg McClymont (*Labour, Cumbernauld, Kilsyth and Kirkintilloch East*)
Stephen McPartland (*Conservative, Stevenage*)
David Morris (*Conservative, Morecambe and Lunesdale*)
Jonathan Reynolds (*Labour/Co-operative, Stalybridge and Hyde*)
Roger Williams (*Liberal Democrat, Brecon and Radnorshire*)
Hywel Williams (*Plaid Cymru, Arfon*)

Powers

The Committee is one of the departmental Select Committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No.152. These are available on the Internet via www.parliament.uk

Publications

Committee reports are published on the Committee's website at www.parliament.uk/science and by The Stationery Office by Order of the House.

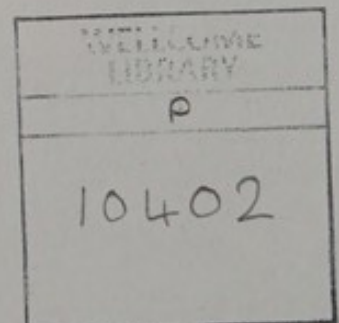
Evidence relating to this report is published on the Committee's website at www.parliament.uk/science.

Committee staff

The current staff of the Committee are: Dr Stephen McGinness (Clerk); Dr Elizabeth Rough (Committee Specialist); Darren Hackett (Senior Committee Assistant); Julie Storey (Committee Assistant); and Nick Davies (Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Science and Technology Committee, Committee Office, 14 Tothill Street, London SW1H 9NB. The telephone number for general inquiries is: 020 7219 2793; the Committee's e-mail address is: scitechcom@parliament.uk.



22502669948

Fourth Special Report

On 28 November 2014 the Science and Technology Committee published its Fourth Report of Session 2014–15, *Responsible Use of Data* [HC 245]. On 17 February 2015 the Committee received a memorandum from the Government which contained a response to the Report. The memorandum is published as Appendix 1 to the Report.

Appendix 1: Government response

Introduction

1. The Government thanks the Committee for its report on responsible use of data, and for its helpful recommendations. As the report recognises, data—including the vast amount that is produced every day through the use of social media—is transforming all aspects of our society. This includes the way companies generate new opportunities and interact with customers, and the nature and provision of public services.

2. The Government's ambition is to make the UK one of the most advanced digital economies in the world. Intelligent use of data will play a crucial role in realising this ambition, and that is why the Government is investing over £450million to develop the UK's data infrastructure, and has been at the forefront in establishing the UK as the world leader in open data. We note that the Worldwide Web Foundation's recently published Open Data Barometer ranks the UK as the most open and transparent nation in a list of 83 countries.

3. As the Committee recognises, protecting the rights of individuals whilst also enabling businesses to use personal information responsibly for innovation and growth is essential if the UK is to realise the full commercial and societal benefits that data can provide. The Government is therefore grateful that the Committee has acknowledged the important steps that HMG has already taken with businesses, regulators and consumer bodies in this area. We agree with the Committee's point on the need to develop this work still further.

4. Responses to specific conclusions and recommendations are provided below.

Skills and Infrastructure

Recommendation 1:

*We have seen repeatedly that the UK is not producing the technically proficient people required to support modern businesses. In our report, *Educating Tomorrow's Engineers*, we concluded that, despite the Government's recognition of the importance of engineering skills, there is a persistent gap in the numbers of engineers required to achieve economic growth. Data science is yet another skills area that urgently needs to be addressed if the UK is to be able to build an economy that can compete on the global stage. It is essential that the Government ensures that data science skills are promoted in educational*

institutions and within organisations that are able to provide data skills development. (Paragraph 21)

5. The Government recognises that the UK must continue to develop the right digital skills, including data science and data analysis skills, to support continued economic growth. We are working with partners in industry and education to ensure that education and training routes are providing the skills needed now and in the future. A number of activities are underway to develop a strong digital and data skills pipeline which include:

- A new and more stretching computing curriculum was launched in schools in September 2014. The new curriculum has a greater focus on computational thinking, preparing and inspiring young people for a range of digital careers, including data science.
- The Government's reform of Apprenticeships is enabling employers to develop apprenticeship standards which reflect the skills they need for particular roles. One of the digital standards being developed is for a data analyst role.
- Government has provided £18.4million of funding for the Tech Partnership—an industrial partnership created to put employers in the driving seat in articulating and addressing their skills needs.

6. These activities are enhanced by a series of new announcements made by the Government in November and December 2014, which include:

- New Degree Apprenticeships that will enable young people to get a full honours degree alongside on-the-job training, ensuring that individuals gain the right mix of technical skills and the ability to apply them in business environments.
- A pilot of new digital skills short courses that will be accredited by business, and will help to set a new benchmark for Further Education provision to fill current skills shortages.
- A National College for Digital Skills which will be a beacon for digital skills provision, driving up standards across the country and ensuring a strong supply of Further Education talent.
- An independent review of computer science degree accreditation to ensure that Computer Science courses are of a high quality and that students are gaining the skills required for the current and future workplace.

7. The Engineering and Physical Sciences Research Council (EPSRC) is also working with UK universities to invest in research and high level skills in data science and data analytics. Its investments to date include:

- The £42million Alan Turing Institute, announced in Budget 2014, which will promote the transfer of knowledge and skills in algorithms and the application of data science. The Institute will form an important part of the UK's big data capability, complementing EPSRC's significant portfolio of computer science, ICT, and mathematical sciences research and training.

- The Research Data Facility at the University of Edinburgh, which is available to all researchers and for collaboration with industry. Users can share data, combine different datasets in new ways to address inter-disciplinary problems, curate and make data widely available, and improve data reusability.
- Eight EPSRC Centres for Doctoral Training specialising in aspects of data, which opened for students in Autumn 2014.

Recommendation 2:

*We repeat our recommendation, from our report, *Educating Tomorrow's Engineers*, that learned societies, professional institutions and trade bodies put an obligation on their members to systematically engage in promoting data science skills through a structured programme of educational engagement. We request that the Government detail to us, in its response to this report, how it intends to ensure that organisations take part in a national effort to promote data science skills within the current and future UK workforce. (Paragraph 22)*

8. The Government is working closely with a range of partners and organisations to promote the importance of digital skills, including data science skills, and to promote the value of digital skills careers for the current and future workforce.

9. As part of the reformed computing curriculum which launched in September 2014, the Department for Education is working with a wide range of private sector organisations to provide teachers with the resources they need to teach the new curriculum in inspiring ways.

10. The Government funded STEM Ambassador Network has over 28,000 volunteers from the private sector who go into schools to encourage young people to enjoy STEM subjects across a range of areas including digital, data science, and technology, and make them aware of the opportunities and possibilities which come from pursuing STEM subjects and careers. The Ambassadors also support teachers in the classroom by explaining current applications of STEM in industry or research.

11. Last year, the Government launched the 'Your Life' campaign where more than 180 organisations have committed to helping pupils towards the right career choices and to better prepare them for the world of work.

12. The Government has provided £18.4million of funding for the Tech Partnership, an industrial partnership which brings together companies from across the economy to work together to address digital skills needs. The Partnership has deliverables which include creating over 2,700 apprenticeships for young people and the provision of careers advice.

Government Use of Data

Recommendation 3:

Real buy-in from members of the public for the use of their data is most likely to be achieved by delivering well-run services, which meet the expectations of customers. There are some excellent examples of administrative services that already exist in the UK, which

demonstrate exactly what the UK should be aiming for: one shining example is paying your road fund license on the DVLA website, an easy-to-use and efficient service. Services such as these provide benefits to both the service provider and customer, providing a trusted platform for the exchange of data and service. care.data is a clear example where this trusted relationship failed to develop. (Paragraph 28)

13. The Government welcomes the Committee's acknowledgement of the improvements that have been made to the delivery of public services by organisations such as the DVLA through the effective use of data, and we agree that the building of trust around government use of citizen data is key to gaining public buy-in to these changes in service provision.

14. There have been, and continue to be, many conversations between government, citizens, business and civil society organisations on how the use of data can provide direct benefits to citizens. There is little disagreement about the possibilities arising from data in offering the right service to the right citizen at the right time. However, it is clear that concerns exist around how that is best achieved. The provision of clear and robust safeguards, including transparency, provide high levels of reassurance in many cases.

15. It is for these reasons that the Government has a Digital Service Standard that all new services must meet. In addition, the creation of a new Government Data Standard that will harmonise the operational approach it takes in the creation and use of data systems was announced in the 2014 Autumn Statement.

Recommendation 4:

Members of the public do not appear to be wholly against the idea of their data being used by Government institutions, but support for data usage is highly dependent upon the context within which the data is collected. The Government should have learned from the experience with care.data and we recommend that the Government develop a privacy impact assessment that should be applied to all policies that collect, retain or process personal data. (Paragraph 29)

16. The Government acknowledges that lessons can be learnt following reaction to the initial proposals to introduce the care.data programme, and action is now being taken to ensure that the national roll out of the programme will only proceed when we are satisfied the process is right.

17. On 7 October 2014, NHS England outlined its pathfinder stage for the care.data programme to work with four Clinical Commissioning Groups (Leeds North, West and South and East, Somerset, West Hampshire, and Blackburn with Darwen) to test, evaluate and refine all aspects of the data collection process of the programme.

18. Alongside this, in November 2014, the Government announced the appointment of Dame Fiona Caldicott as the National Data Guardian on healthcare information sharing.

19. It is now envisaged that information will be collected from GP practices involved in the pathfinder stage in early 2015. However, this collection will only take place once the National Data Guardian is satisfied it is right and safe to do so. Also, the care.data programme will only be rolled out more widely when the pathfinder stage has been

evaluated by the National Data Guardian and the care.data Programme Board to ensure the right approach is being taken.

20. The ICO has published a Code of Practice on conducting Privacy Impact Assessments¹ (PIAs) and encourages Government Departments to conduct PIAs for significant projects that involve the processing of personal data.

21. In addition, as part of the Government's data science programme, we are developing an ethical framework to ensure we maximise the use of the greater amount of available data to create insight that can improve public policy and government operations, in a way that the public would understand and feel comfortable with.

Better information for users of online services

Recommendation 5:

We note that a primary concern of the general public is that it is unable to limit the misuse of personal data by large organisations, but we recognise the work of the ICO in addressing some of these issues. We are attracted to the position of the ICO that big data should play by the same rules as every other form of data processing. It is essential that organisations operate in a transparent manner, allowing public confidence to flourish in light of knowledge about the way that their data is used. The UK is already a leading player on the global stage in using social media data and we are keen for this status to be maintained, but only if that can be achieved while ensuring the personal privacy of UK citizens. (Paragraph 35)

22. The ICO published its report on the data protection issues related to big data in July 2014. The report framed the risks in using personal information in the context of the large scale analytics that characterise big data². The ICO was also the first data protection authority in Europe to publish a report on big data. The importance of transparency, and the innovation needed to enhance the process of providing privacy information to individuals, is highlighted in report. The ICO ran a consultation in relation to the report and the follow up will be published later in 2015. The ICO will continue to work to highlight how existing data protection tools, such as PIAs, can be used by organisations using big data analytics to assess privacy risks.

23. In parallel, a proposed new EU data protection framework is being negotiated in Brussels. The key driver for this new legislation is the unprecedented technological advances and the means and scale by which personal data is used, including the use of social media and big data. The Government is committed to negotiating for proportionate legislation that provides the right conditions for technological innovation and deriving the real benefits of big data, while at the same time providing robust safeguards for the protection of personal data.

24. The Government is taking steps to empower individuals to take responsibility for their personal data when online, as they do when offline, by increasing awareness and self-protection levels. The National Cyber Security Programme-funded Cyber Streetwise

¹ <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

² <https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf>

campaign and website, and Get Safe Online, provide useful sources of information and guidance on a range of topics on protecting personal, sensitive and financial information. These include the use of social media, using strong passwords, updating software and operating systems and running anti-malware programmes, as well as being aware of common scams.

25. The Government is also working with the Digital Economy Council, the British Standards Institution, and consumer organisations to examine the development of a set of standards that UK companies can sign up to that will explain to customers in a clear way how information about them is collected and used.

Recommendation 6:

We are not convinced that users of online services (such as social media platforms) are able to provide informed consent based simply on the provision of terms and conditions documents. We doubt that most people who agree to terms and conditions understand the access rights of third parties to their personal data. The terms and conditions currently favoured by many organisations are lengthy and filled with jargon. The opaque, literary style of such contracts renders them unsuitable for conveying an organisation's intent for processing personal data to users. These documents are drafted for use in American court rooms, and no reasonable person can be expected to understand a document designed for such a niche use. We commend the Information Commissioner's Office for investigating ways to simplify the contents of terms and conditions contracts and ask the Government, in its response to this report, to detail how the public at large will be involved in arriving at more robust mechanisms for achieving truly informed consent from users of online services. Clear communication with the public has been achieved in the past, for example in the use of graphic health warnings on cigarette packets. Effective communication with the public can be achieved again. (Paragraph 49)

26. The Government agrees with the Committee that the terms and conditions in a consumer contract, including website terms and conditions, should be fair, clear and intelligible to the consumer.

27. The Consumer Rights Bill, which is currently going through Parliament, streamlines and clarifies the law on unfair terms in consumer contracts and notices. Consumer groups such as Citizens Advice and Which? have been closely involved with the development of the Bill, which provides that terms must be fair if they are to be binding on the consumer. Provisions in the Bill also cover terms in Online End User Licence Agreements such as 'click-wrap licences' which require consumers to explicitly agree to terms before they can purchase (and then download) digital content.

28. Under the provisions of the Bill, any terms traders use must be in plain, intelligible language and, if written, legible to ensure consumers are aware of the main elements of a contract and are less likely to agree to something that later proves detrimental. There is also a new requirement for the most important terms to be 'prominent' to avoid challenge in court for fairness.

29. The ICO has also published a Code of Practice on Privacy Notices³, and the document sets out the principles organisations should follow when providing privacy notices or information to individuals. The ICO is currently in the process of updating the Code to reflect changes in technology, for example providing privacy notices on devices such as mobile phones and techniques such as in-product notices. A new version will be published for consultation in the first half of 2015.

Recommendation 7:

We consider it vital that companies effectively communicate how they intend to use the data of individuals and that if terms and conditions themselves cannot be made easier to understand, then the destination of data should be explained separately. We recommend that the Government drives the development of a set of information standards that companies can sign up to, committing themselves to explain to customers their plans to use personal data, in clear, concise and simple terms. In its response, the Government should outline who will be responsible for this policy and how it plans to assess the clarity with which companies communicate to customers. Whilst we support the Government in encouraging others to meet high standards, we expect it to lead by example. The Government cannot expect to dictate to others, when its own services, like care.data, have been found to be less than adequate. We request that the Government outline how it plans to audit its own services and what actions it plans to take on services that do not meet a satisfactory level of communication with users about the use of their personal data. (Paragraph 54)

30. The Government considers that consumer awareness and trust in how personal information is used by companies can provide benefits and reassurance to both businesses and citizens.

31. We are therefore working with the Digital Economy Council, the British Standards Institution, and consumer bodies to consider the development of a set of standards that UK companies can sign up to that will explain to customers in clear terms how information about them is collected and used.

32. Within Government, development of this policy is being led by the joint BIS and DCMS Digital Economy Unit, with the work programme being taken forward by a working group of the Digital Economy Council. Discussions on a possible set of standards are on-going, and these will also consider how any new measures should be assessed and monitored.

33. Work in this area is already progressing in some industrial sectors. In summer 2014, through a project delivered jointly by BIS and DECC as part of the midata programme, the largest energy companies committed to developing systems that would allow automated data access between energy suppliers and third parties with their customer's consent.

34. As part of this project the Government, working with business, consumer groups and regulators, has considered what is needed to give consumers confidence that their data is being used fairly, ethically, and for clearly stated purposes, by these third parties. It is expected that a voluntary trust framework that clearly sets out the behavioral and technical

³ https://ico.org.uk/media/for-organisations/documents/1610/privacy_notices_cop.pdf

standards applied to the use of the data by third parties will be established alongside the delivery of automated data access during 2015. This framework should help consumers better understand how their energy data is being accessed and used with their consent.

35. We agree that the Government should also lead by example. Effective communications and transparency will be important aspects of the new Government Data Standard and the associated responsibilities of the new Chief Data Officer, which were announced in the 2014 Autumn Statement.

36. The new Government Data Standard will be enforced across the public sector to ensure a common set of operational practices apply to the use of data, in a manner that is consistent with the relevant legislation.

37. In addition, as the independent Data Protection Authority, the ICO would be responsible for taking action against any services that breach the Data Protection Act.

Regulating the use of personal data

Recommendation 8:

There is a qualitative difference between requesting personal information when registering for a service and requiring that same information. Companies should have a greater responsibility to explain their need to require (and retain) personal information than when they simply request it. We welcome the work of the Information Economy Council and recommend that the Government use that work to provide companies with guidelines to aid organisations in deciding what information they should require and how that, and the subsequent use of the data, might be managed responsibly. We expect the Government, in its response to this inquiry, to outline a draft timetable for when businesses might expect to receive Government endorsed guidelines in this area. (Paragraph 57)

38. The Data Protection Act 1998 and Article 8 of the European Convention on Human Rights impose clear legal limits on how organisations can record, store, alter, use or disclose personal data. Advice is also available to both companies and individuals from the ICO on data protection rights and responsibilities.

39. It is intended that the Government's work with the Digital Economy Council will build on existing data protection legislation, and will be used to provide clear guidance and advice on best practice to companies on the responsible and transparent use of personal information.

40. For any new measures to be effective and of benefit to both consumers and companies, they must be practical, robust, and clear to understand. To ensure these criteria are met, discussions are taking place in February 2015 with the British Standards Institution. It is intended that these discussions will also be used to help develop a proposed timetable and framework for the new guidance.

Recommendation 9:

In our report Malware and cybercrime we noted that the UK Government has a responsibility to protect UK citizens online, in an extension of the protections that are

conferred on citizens in the offline world: a responsibility the Government accepted in its written evidence to this inquiry. As the majority of popular social media platforms are head-quartered in the US, we find it essential that the Government revisit all international agreements, including the US-EU safe harbour, to ensure that they protect UK citizens. We ask that, in its response to us, the Government outlines the international agreements that currently exist where it has ensured that the data of UK citizens will be guarded as well as if it were within UK legal jurisdictions. (Paragraph 64)

41. There are two principal international agreements on data protection that safeguard UK citizens' data. These are:

- The EU Data Protection Directive (1995)—the scope of which covers the processing of personal data by public authorities and private entities. This was transposed by the Data Protection Act 1998.
- The EU Data Protection Framework Decision (DPFD) 2008—which governs the processing of personal data in the law enforcement context.

42. A new EU Data Protection Framework is currently being negotiated in Brussels, which consists of a General Data Protection Regulation and a 'law enforcement' Data Protection Directive. These two proposed measures will repeal and replace the 1995 Directive and the DPFD respectively.

43. In addition, the Council of Europe is currently updating its own data protection rules under Convention 108. This is a broader international agreement which sets out high level principles for this sharing of personal data.

44. In November 2013, the European Commission brought forward a series of recommendations to strengthen the functioning of EU-US Safe Harbour arrangements. These recommendations mainly focus on improving the transparency and accountability of Safe Harbour arrangements, as well as addressing the issue of legal redress for EU citizens in US courts. Dialogue between the EU and the US are ongoing towards making progress on each of these recommendations, and the UK is constructively engaged as part of these discussions.

Recommendation 10:

We consider an internationally recognised kitemark to be the first step in ensuring the responsible use of the data of UK citizens by both social media platforms and other organisations. We are pleased that the Government seems to be working toward this end and recommend that, in its response to this report, it provides a draft timetable for when proposals for a kitemark can be expected. (Paragraph 69)

45. The Government agrees that the use of standards, kitemarks, seals or certification are useful to help consumers make choices between different products and services.

46. The Government is working with the Digital Economy Council, the British Standards Institution, and consumer bodies to consider the development of a set of standards that UK companies can sign up to on the collection and use of personal information. A proposed timetable for this work is expected to result from discussions taking place between these organisations in February 2015.

47. Alongside this work, the ICO are looking to launch a privacy seal programme in 2015. Consultation with industry has indicated significant support for the project. The first stage will be to invite applications from third party providers to apply for endorsement of their privacy seal framework and the ability to award an ICO privacy seal to organisations. Privacy seals are also a proposed component of the EU Data Protection Regulation currently being negotiated. The ICO privacy seal programme will be developed to align with the work of the Digital Economy Council.

Recommendation 11:

We have become increasingly concerned that the benefits of data sharing that might be achieved, in both governance and economic growth, are at risk because the public distrusts the technology and some organisations that provide online services. The Government has been working to provide an identity assurance scheme that would give those in receipt of Government benefits an online presence so that individual citizens can manage their personal details in their transactions with the State. This scheme could be the basis for all UK citizens to have a protected, online identity that could be used, if the Government was willing, for both governance and online commercial activities. (Paragraph 70)

48. GOV.UK Verify is a new way for people to prove their identity when accessing digital services. It is in public beta, and is being implemented incrementally by services across government.

49. At this stage, the Government is prioritising building and scaling a service that works for users of central government services. We are working to make it easier and quicker for people to prove their identity digitally when using digital government services. The approach we are taking is designed not just to meet central government requirements, but to also stimulate a new market of identity services that can be used in the wider public and private sectors in the way the Committee has suggested.

50. GOV.UK Verify operates according to published standards which have been designed to make them usable for services in any sector and in any country.

51. The Cabinet Office is working with industry through the Open Identity Exchange (OIX) to explore possible applications of the service in the private sector and in local public services. Details of some of the projects OIX members are working on are available on the OIX website⁴.

52. In 2015, the identity assurance programme will continue its work to understand the commercial, legal, and operational issues involved in private sector re-use of GOV.UK Verify and related services. The programme will continue to work with partners in government, the wider public sector, and the private sector to develop a shared approach to this issue.

⁴ http://oixuk.org/?page_id=10

Protecting the interests of UK citizens online

Recommendation 12:

We have also seen that the Government's approach to online safety has been piecemeal and conducted tactically to meet immediate needs with little evidence of any horizon scanning. The Government should be considering now how it wants UK citizens to engage with both governmental and commercial online services. It should be seeking to provide a platform for UK citizens to engage those services without unnecessarily risking their personal data and enabling its citizens to make informed choices about what data to share, with whom and for what purpose. Future prosperity will be impacted by how well information flows between government, citizens and business. The Government needs to begin work so that all of its citizens have firm and secure foundations from which to build their online functionality. (Paragraph 71)

53. The Government disagrees that its work has been piecemeal on this issue. The Government Digital Strategy⁵ clearly sets out our vision for how UK citizens should engage with online public services.

54. Supported by the National Cyber Security Programme, the new GOV.UK Verify platform provides a secure way to prove who you are online, and is being rolled out across an increasing number of services including HMRC's PAYE service, Defra's Rural Payments service, and DVLA's View Driving License service.

55. A key objective of the National Cyber Security Strategy is making the UK one of the safest places in the world to do business online, and the Strategy comprehensively sets out our vision for protecting UK businesses and individuals. This is being delivered through the £860million National Cyber Security Programme, and aims to ensure that Internet users are provided with the right information to go online safely and securely, whether interacting with online public services or otherwise.

56. As part of the National Cyber Security Strategy, the Government is working to ensure that consumers are better informed of potential risks when online and what they can do to reduce them, as well as enabling individuals to demand better cyber security in the products and services they buy. The Government is also investing in a number of successful initiatives to help individuals become more aware of cybercrime and how to protect themselves online. These include the multi-media Be Cyberstreetwise campaign launched in January 2014 to measurably improve the cyber confidence and safety of consumers and small businesses, and support for the work of Get Safe Online.

⁵ <https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy>

Faint, illegible text, possibly bleed-through from the reverse side of the page. The text is too light to transcribe accurately.



Distributed by TSO (The Stationery Office) and available from:

Online

www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail

TSO

PO Box 29, Norwich NR3 1GN

General enquiries 0870 600 5522

Order through the Parliamentary Hotline *Lo-call* 0845 7 023474

Fax orders: 0870 600 5533

Email: customer.services@tso.co.uk

Textphone: 0870 240 3701

The Houses of Parliament Shop

12 Bridge Street, Parliament Square

London SW1A 2JX

Telephone orders: 020 7219 3890/General enquiries: 020 7219 3890

Fax orders: 020 7219 3866

Email: shop@parliament.uk

Internet: <http://www.shop.parliament.uk>

TSO@Blackwell and other Accredited Agents

© Parliamentary Copyright House of Commons 2015

*This publication may be reproduced under the terms of the Open Parliament Licence,
which is published at www.parliament.uk/site-information/copyright/*



ISBN 978-0-215-08383-8



9 780215 083838