Speech: Insurance in the Digital World

Thank you for inviting me to speak to you this afternoon. I believe the focus of this conference – the relationship between cyber, data and technology – is one of the most important challenges and opportunities that we face in the coming months and years.

The Internet and digital technologies have transformed almost every aspect of our lives over the past 20 years. They have brought huge benefits for society, many beyond measure; entertaining us; helping us learn; saving us time and money; keeping us up-to-date; creating new jobs; and bringing us closer together, wherever and whoever we are.

And yet we are only at the cusp of technology realising its true potential: artificial intelligence, machine learning and automation of the means of production are set to change our world faster and more fundamentally than any previous technological revolution.

As someone who comes from a tech background, I find this change both exciting and daunting. It offers great promise for humanity, but also has the potential to bring dark new threats. The question we face as a society, is how to harness the power of new technology for good, to improve the condition of mankind, and to mitigate those threats.

The basic problem is that technology is developing faster than the speed at which society has built new rules to deal with the challenges it creates. As a result, we do not yet have a shared understanding of what is and isn't acceptable online. It is the role of Government to lead the way in closing this gap.

This is the underlying thinking behind the Digital Charter that we will introduce. It will set out a framework for how businesses, individuals and wider society should act in the digital world.

We need to make sure that the digital world is safe and secure and our Internet Safety Strategy Green Paper, published last week, aims to tackle growing online dangers such as cyber-bullying, trolling and underage access to pornography, while continuing to embrace the huge benefits and opportunities the Internet has brought for British citizens.

Another key part of our mission, as set out in the National Cyber Security Strategy published last year, is to make sure that all organisations in the UK, large and small, are effectively managing their cyber risk.

The incidents that we have seen this year, in particular the Wannacry attack which affected parts of the NHS, only reinforce the importance of meeting this challenge.

Government has an important role to support organisations with the right, high quality advice and guidance. The National Cyber Security Centre, known as the NCSC, is designing and producing this advice such as its Small

Business Guide, published on 11 October, which provides SMEs with tips to improve their cyber security quickly, easily and at low cost. This compliments our flagship Cyber Essentials scheme which provides the basic controls all businesses should implement to protect themselves.

We must also underpin this advice with the right mix of regulation and incentives. In 2016 we carried out a review of Cyber Security Regulation and Incentives and published our findings in December last year. The review concluded that reforming our data protection laws and implementing the Security of Network and Information Systems Directive, would help to provide a positive regulatory framework in which to improve the cyber security of UK companies and essential services.

However, it is also important that we recognise within Government that we cannot achieve our ambition of a cyber secure nation working alone. We must work with partners from industry to raise the overall cyber resilience of the UK economy. Cyber insurance has a clear and important role to play in helping us to meet this aim.

The insurance industry is one of the main influencers of business behaviour across our economy. You speak to organisations large and small about the risk profile right across their operations and so are almost uniquely positioned to advise them on the importance of cyber security to the particular nature of their work, amplifying the Government messaging and advice being produced by the NCSC.

For this reason we have been working with the insurance industry for a number of years. The Marsh Report, published in 2015, was a result of close working between the insurance sector and Government and highlighted the potential for the insurance industry to help drive change in cyber behaviours.

DCMS chairs a regular Cyber Insurance Forum attended by the major industry bodies, including the ABI, to discuss the issues facing the cyber insurance industry and how we can support the industry moving forward.

For example, we have been working with colleagues in the Department for International Trade to consider how we can use the considerable expertise of the UK cyber insurance sector to develop export opportunities across the world. However, I know that the most critical challenge the industry faces is around the availability of robust actuarial data on which to accurately price cyber risk.

This is an issue that Government can play its part in resolving and when the General Data Protection Regulation takes effect from May next year organisations will be required, by law, to report details of cyber breaches that result in the loss of personal data to the Information Commissioner.

I understand that conversations are well underway between the insurance industry and the Information Commissioner’s Office around how that information will then be collected and reported to make sure that it is as useful as it can be to insurers for actuarial purposes. We will continue to support the industry in pushing for this while recognising the important role

the Information Commissioner plays as an independent regulator.

We must also, however, recognise that data itself needs to be handled carefully. Data flows are the basis of today's increasingly digitalised economy. All of the new technologies and capabilities that are revolutionising our lives are underpinned by the ability to collect, store, process and share data. To enable this to happen we need the right frameworks in place to allow data to flow while also protecting people's privacy.

To this end we are currently taking a Bill through Parliament to update our data protection laws. The Data Protection Bill will create a regime for a digital age in which an ever increasing amount of data is being processed. It will empower people to take control of their data, and support UK businesses and organisations to understand and comply with the new rules.

In developing the Bill we have worked with the ABI to ensure that the insurance sector strikes the right balance between safeguarding the rights of data subjects and processing data without consent when necessary for carrying on insurance business.

Technological innovations will mean that insurers can monitor their customers' lifestyle with more precision and insurance premiums can be tailored to individual characteristics. If they are deployed with the consent of the customer as part of a contract for providing insurance and lead to lower premiums, that is clearly something to be welcomed.

However, there are many ethical dilemmas around the use of data to support technological advances that we must work together to find solutions to. We have already seen an example of one insurer seeking to build algorithms to review social media profiles and identify higher risk individuals for the purposes of pricing car insurance, based on a person's hobbies and interests.

We have also heard stories that some machine learning algorithms have picked up on certain social biases that exist around language, creating a risk that existing social inequalities and prejudices could be reinforced in new and unpredictable ways as an increasing number of decisions affecting our everyday lives are influenced by artificial intelligence.

And there may also be a more fundamental inequality in that poorer people may be willing to give away their data, and arguably decision making, more freely in return for lower insurance premiums. That would create a potentially discriminatory situation where only the rich can afford privacy and freedom of action.

There will also be questions about liability in an increasingly automated, digital world. If an automated car crashes into a pedestrian in trying to avoid an accident that would potentially injure the occupants of the vehicle, based on what its machine learning tells it to do, who is going to be liable for those injuries and how will the insurance market react if the answers to those liability questions fundamentally change current risk pooling methodologies?

It is, therefore, vital that you in the insurance industry continue to act responsibly and lawfully when dealing with the masses of data now available to you. In our General Election manifesto we committed to setting up a Data Use and Ethics body and we're currently working to deliver on this commitment and considering the priority issues on which it should focus.

Another challenge in a more connected world exists around the proliferation of internet connected devices we have in our homes. We are already working with industry to ensure that security measures are built into internet connected products by design, and I look to you to support this ambition, with insurance as one of the most powerful levers for incentivising industry to take security seriously.

In conclusion, getting this relationship between cyber, data and technology right is about finding the proper balance. The balance between using the potential of the digital revolution as a means of growing our economy and ensuring that the digital economy is built on safe and secure foundations and works for everyone in our society.

It means that when we hear reports of hackings and cyber breaches, we must resist the temptation to build a wall around our data as when data cannot flow, it starves the technologies we now take for granted of their vital fuel. However, it also means making sure that the necessary measures are in place to protect our data and the data of our citizens from attack.

If we can achieve this by working together with our partners across the economy, including the insurance industry, then the UK can continue to forge its path as a leading digital trading nation and an example to the world.