[Speech: Matt Hancock's speech to the Leverhulme Centre](#)

It's an enormous pleasure to be invited to speak to the Leverhulme centre about trust and policy in an age of intelligent machines.

A pleasure, yes, and also daunting. After all, the centre exists so you can spend your time thinking of the future of intelligence. I'm sure that starting with a politician isn't the best place to start. At least it means that the only way is up.

I'm glad that you've linked trust and policy in the title.

Because our starting point should be to ask why trust matters in public policy overall.

And the truth is this:

Without trust, public policy is incredibly difficult. At one level, any progressive politician, particularly of the centre right, believes that our task is to unleash the potential of all citizens: to remove barriers where we find them, and to empower and help citizens to make the most of their lives. So the entire mission and purpose of government is founded on a profound trust of people's capability, so a free society is a better society. Trust the people!

This freedom of course has boundaries, to prevent harms, and we must trust that society, through legitimate democratic systems, can find that balance to protect people, and protect our freedom. I will return to this later.

And trust matters on a much more direct, practical level too.

It's hard to see how citizens will back innovation in the public or the private sectors, and won't be prepared to take decisions that enhance the collective good without high levels of trust in others, and especially in those making decisions about them, whether businesses, or public services, or elected officials.

So innovation and progress depend on trust. Good policy improves trust, and trust in turn improves policy.

So far, so ageless.

The next question I want to ask is, how does, and how will, artificial intelligence change this?

I want to ask, how do we best ensure advanced digital technology enhances, rather than undermines, trust, and how can we generate the trust needed to harness advanced digital technology?

In part thanks to technology, we are living in an age of scepticism, in which sources of authority are challenged in a way unprecedented. Rational scepticism is the basis of scientific progress; so how do we harness scepticism to generate, not undermine, trust in a wider sense?

And then I want to ask an even more prosaic question: what role can and should government play to make it happen?

I am glad that these questions are being asked explicitly, now.

As a society, sometimes technology moves ahead of the rules and norms we have — the framework — in which the technology operates. This is particularly true — and particularly tricky — with a general purpose technology like AI, which has the potential to disrupt so many areas.

Like Lord Leverhulme himself, I believe we need to come at the question from a point of optimism about technology.

The prospects of this technology are simply enormous and we all know that the UK is already a word leader. So I look forward to reading the findings of Professor Dame Wendy Hall and Jermoe Pesenti's AI review, which we commissioned to help make sure the UK remains at the cutting edge.

But we mustn't allow optimism to become panglossian.

Digital technology is incredibly powerful, and with great power comes great responsibility.

Just because you could doesn't mean you should.

So we need to do the work now to build the framework, of ethics, norms, rules and regulations, in which digital technology can thrive and innovate safely. Where we balance freedom and that responsibility.

Fortunately, this need to develop freedom in a framework that prevents harm is not new. We've been doing it offline for generations. And we can look to the rich seam of political philosophy to guide us.

Perhaps Burke put it best when he said this:

"of all the loose terms in the world, liberty is the most indefinite. It is not solitary, unconnected, individual, selfish liberty, as if every man was to regulate the whole of his conduct by his own will. The liberty I mean is social freedom. It is that state of things in which liberty is secured by the equality of restraint. A constitution of things in which the liberty of no one man, and no body of men, and no number of men, can find means to trespass on the liberty of any person, or any description of persons, in the society. This kind of liberty is, indeed, but another name for justice; ascertained by wise laws, and secured by well-constructed institutions."

I submit that, online, it is Burke's liberty is what we seek.

Trust has to be part of how AI can develop to benefit society and the economy

now, not an afterthought.

Why is this important?

Senior decision-makers will not let their organisations' data be used for AI if they don't believe the data will be used securely, and if they don't believe AI can help them to deliver better.

Employees will not work well with AI-driven functions if they don't trust that those work better than what they have.

Consumers and citizens won't accept widespread use of AI if they don't see questions of trust properly addressed.

And they will not be enthusiastic if no one explains the benefits.

So this is the right time to raise the questions, and find out where trust needs to be built, and how to build it.

So the next question is, what is the role for Government?

Because digital technology is changing so many aspects of our lives, there is no one simple solution to this challenge.

We are agreed, I think, on some principles.

An important legal one: that what's legal offline, is legal online.

Next, that freedom is precious, but not the freedom to do harm.

That our drive for protection must not undermine the enormous innovative power of technology to improve people's lives.

And that transparency matters, and even when uncomfortable, doesn't just improve trust, but improves outcomes too.

Given these broad principles, I want to talk about three crucial areas where governments can help drive trust in an age of intelligent machines.

First, a solid legal framework

In the UK, we benefit from a good starting point of a strong consensus behind the laws over the digital world, underpinned by the Data Protection Act, overseen by our independent Information Commissioner, who gave a thoughtful and important speech on this topic last week.

We will strengthen that with a new Data Protection Bill in this Parliamentary Session, which will bring the laws up to date for the modern age, introduce new safeguards for citizens, stronger penalties for infringement, and important new features like the right to be forgotten. It will bring the EU's GDPR and Law Enforcement Directive into UK law, ensuring we are prepared for Brexit.

This sort of strong, effective regulatory regime is vital. It must balance

strong privacy protections with the need to allow innovation, and I think the ICO's proposal of a data regulatory "sandbox" approach is very impressive and forward looking. It works in financial regulation and I look forward to seeing it in action here.

But the legal framework is not enough.

Second, we need to look ahead and understand future challenges on the horizon, before they are subject to the law and regulators.

Our Digital Strategy sets out our overall plan, including on skills, infrastructure and cyber security.

And we need to identify and understand the ethical and governance challenges posed by uses of data, now and into the future, where they go beyond current regulation, and then determine how best to identify appropriate rules of the game, establish new norms, and where necessary regulations.

Let's take an example.

Unfair discrimination will still be unfair. Using AI to make some decisions may make those decisions more difficult to unpack. But it won't make fairness less important.

And this is not all about risks: some applications of AI could make it easier to detect unfair biases, including biases in the institutions and processes that we already use to make decisions affecting people.

In terms of governance, it's likely that we will need overarching principles, broadly across different uses of AI in different sectors.

However, that may only get us so far. AI is also likely to generate specific challenges, and need specific answers in different sectors. We have different concerns and different tolerances about fairness in, for instance, retail, finance, and personalised medicine.

We don't yet know how much we will be able to rely on general issues in AI and automation, and how much will be more specific to application areas.

We may find that the solution to many challenges created by application of AI in particular sectors is to make sure that application of the existing sector rules can keep up, with the right tools, rather than that we need completely new rules for AI.

We already have expertise in sector regulators. They may need to develop new skills to look at AI-related cases in their sectors, if the major businesses in their sectors use new data technologies, which many will.

I'm delighted that the Royal Society and the British Academy have done such excellent work, setting out the challenges we face, and proposing a new body or institute that can take a view, talk to the public and provide leadership. It's a very interesting idea similar to that we proposed in the manifesto, and we are considering it carefully.

But it can't all be done for people.

So third, we will need senior decision-makers in business and the public sector to be able to understand and talk about the implications of AI, and represent their use of it to the public, to customers, to employees, and to shareholders, if they are going to use it confidently and effectively. And be trusted to use it.

We will need to encourage individual businesses and organisations across sectors to do more themselves to be responsible and transparent in the ways they are using data, and to understand and manage the risks posed by it as they would any other significant corporate risk.

Businesses are now realising that cyber security is not a niche issue for the IT department, but a boardroom issue for core management.

So too, increasingly for AI.

Business will need clear and transparent governance, accountability and quality assurance around the algorithms they use and processes for understanding and managing risk.

The UK will not grow full AI capability and broad application across sectors, if trust is not built and maintained.

These are not by any means all of the issues we must confront.

Our Digital Charter represents a broad array of changes we seek to bring to harness digital technology for good. We need to work with businesses and build consensus around shared understanding of how technology should be used, and how we act online — balancing freedom and security.

This is what will be set out in a Digital Charter, which will help citizens and businesses understand their freedom and responsibility, allow them to interact safely and securely, promote fairer ways to do business and ethical use of data and technology, and protect intellectual property and value online. Crucially, we can't do this alone.

The issue of who in society is able to earn and build trust, and how they do so, is increasingly complex. Politicians, policy makers and Parliament have a key role to play, but in reality we're not always the only or best placed to earn trust.

So thats a question I want to leave you with today

What do we know now about what drives or harms public trust in the digital age?

Who or what is best placed to take citizens with them on this journey, and how best can governments partner with and enable that to happen?

By strengthening public confidence, and giving greater clarity to business, this will support — and must be done alongside — measures to help the tech

industry to flourish, strengthening the UK's position as one of the world's leading digital economies.

This is our goal: to be a world leader, in allowing innovation within a framework of development that doesn't just provide safety but requires it, and doesn't just allow innovation but nourishes it.

We seek to be the best place in the world to start and grow a digital business and we want the UK to be the safest place to be online.

These two are not in contradiction, but complementary, and I think the prize for the society that answers these questions is to be the best place to seize the enormous opportunities for the benefit of citizens of this amazing, powerful, new technology.

[News story: Royal Navy and Royal Marines train alongside partner naval forces](#)

Around 60 Royal Navy and Royal Marines personnel exercised with their counterparts from other countries during the five-month annual French naval deployment to the Indian Ocean and Far East, including the first ever four-part maritime exercise involving France, Japan, the UK and US.

The two-staged exercise named Forager Deux and Arc 17 took place in the sea and in the skies near to Japan, Guam, and Tinian, with the purpose of enhancing joint operating between the UK and international partners and deepening Defence cooperation.

In addition to UK maritime personnel, the exercise also included two Royal Navy Merlin Mk3 helicopters from the UK's Commando Helicopter Force, which as part of a week-long practice assault moved 330 French, Japanese and American troops to and from Tinian.

UK forces have been on board French assault ship FS Mistral since March as part of the Jeanne d'Arc 2017 French task group, which has visited Singapore, Sri Lanka, Japan, Guam, Australia and Vietnam.

Minister of State for the Armed Forces Mark Lancaster said:

> Working shoulder-to-shoulder with French forces, as well as personnel from other partners' navies, shows the flexibility of our world class Armed Forces.
>
> The Royal Navy and Royal Marines play an important role carrying

out Britain's commitment to international maritime security, as
well as protecting our own shores.

Several instalments of training and Defence Engagement have taken place as
part of this deployment.

This week, UK personnel worked alongside French and Egyptian armed forces
when the Jeanne D'Arc task group arrived in Egypt to take part in Exercise
Cleopatra. The cross-decking exercise, which saw UK Merlins land on the
Egyptian warship ENS Nasser, was the latest in a series of multilateral
amphibious exercises that the UK has taken part in throughout the five month
deployment.

News story: Technology solutions for gestational diabetes: apply for funding

The [Department of Health](#) and [Department for Economy](#) in Northern Ireland are
to invest in new technology solutions that improve the health of women with
gestational diabetes.

Funding of up to £60,000 per project is available for the development of
technologies that can:

- enable diabetic pregnant women to take better control of their health
- increase the effectiveness of interventions
- reduce pressure on health care services, (maternity, neonatal and
  endocrinology services)
- support an ongoing care programme
- improve the lives, well-being and outcomes for maternal and infant
  health
- enable women to lead as normal a life as possible
- reduce the need for travel to specialist clinics

This is a [Small Business Research Initiative](#) (SBRI) competition. It's part of
the GEMS project — 'gestational, type 1 and type 2 diabetes empowering
mothers through mobile technologies'.

- this competition is open now
- the application deadline is 3pm on 25 August 2017
- SBRI is open to any type of organisation
- successful projects will attract 100% funded development contracts
- phase 1 contracts are worth up to £60,000 and last up to 6 months
- if phase 1 testing is successful, organisations may be able to bid for

phase 2 to develop and test their prototypes

[News story: CIC Regulator's voicemail techinal fault](#)

We would like to apologise for any inconvenience caused during this disruption. We ask that all enquiries are sent to cicregulator@companieshouse.gov.uk and we will respond within 24-48 hours.

We are hoping the voicemail service will be back up and running shortly and will keep you updated via this page and [@CICRegulator](#).

[News story: Draft Technical Capability Regulations notified to European Commission following targeted consultation](#)

The Home Office has notified the European Commission of regulations to help make companies maintain the technical capability to respond to warrants and authorisations from law enforcement, security and intelligence agencies.

The Investigatory Powers (Technical Capability) Regulations 2017 do not include any new powers but relate to powers already set out in the Investigatory Powers Act 2016 which enable the Secretary of State to give a "technical capability notice" to a telecommunications operator in relation to interception, communications data or equipment interference.

The purpose of a "technical capability notice" is to ensure that, when a warrant or authorisation is served on or given to an operator, that company has the capability to provide assistance in giving effect to it securely and quickly.

The use of these powers is vital in the fight against terrorism, crime and other national security threats.

Security Minister Ben Wallace said:

Technical advances present ever-evolving opportunities for terrorists, criminals and paedophiles.

These regulations will help make sure that we maintain the capabilities to confront this challenge, subject to strict safeguards.

The regulations do not impose requirements on telecommunications operators, but set out the specific obligations that may be imposed on operators in a "technical capability notice", including those which relate to maintaining the capability to remove encryption in response to a specific warrant or authorisation.

The move comes after a targeted consultation which included hearing views from telecommunications operators that are likely to receive a notice; bodies that hold statutory functions in relation to operators, such as the Investigatory Powers Commissioner; and the Technical Advisory Board.

Following [notification](#) under the Technical Standards Directive, the regulations have been published and there will now be a three month standstill period, during which they can be considered by the European Commission and Member States.

The secondary legislation will be subject to a debate and a vote in both Houses of Parliament before it can come into effect.