



Ministry of JUSTICE

**Lord Chancellor and Secretary of State for Justice
Rt. Hon Kenneth Clarke MP**

Data protection 26th May

Mr Chairman, ladies and gentlemen, thank you for that introduction. Thank you very much to the British Chamber of Commerce in Belgium for their hospitality. I'm glad in your introduction, Mr. Chairman, you didn't dwell at hugely excessive length and detail about what I have to admit is becoming my somewhat veteran career. I was actually sitting there listening for some slip that would occur at some stage. And it's probably rather relevant to a gathering on data protection, because not all the data about me is entirely accurate, and one or two myths just persist. Don't worry, it's an absolutely tiny matter, but there is somewhere on some website, I think Wikipedia, I'm described as having an interest in classic cars. Now, I like classic cars, you know, you show me one, I'm quite happy, I'm very keen on motor racing. But the result of chairmen introducing me in that way quite frequently, and people noting this well-known interest that I have in classic cars, and I get deluged with catalogues magazines all kinds of things are sent to me. So one day I shall find who is putting this on to their particular website just to improve to a tiny degree the accuracy of the data about me.

Because I am here to talk about data protection today, and I again entirely agree with your introduction. The reason that I've come for this unfortunately rather brief visit to Brussels to make the speech is that this is a subject that is now heavily on the agenda here – there is going to be a lot of debate - we are moving forward over the next year and this is an ideal venue, thanks to your kind invitation, to make a general speech about the approach and then of course to have a discussion, to have questions and answers afterwards about any aspect that interests people in the audience. This is becoming a higher profile debate, particularly in Brussels and in many Member States.

So let me begin by setting out my stall, laying my cards on the table and saying that I stand before you as a strong proponent of data protection, and the personal liberties

aspects of all this. I think I can certainly claim to be a member of a party which was vigorously opposing the authoritarian extremes of the last Government, and I was quite a vociferous defender of civil liberties and individual freedom against some of the controlling measures that the last government tried to bring before Parliament. My party, now that it's in office and the coalition with the liberals, is now steadily undoing some of the damage on that front which I think the last government did.

The inclusion of over 1 million unconvicted people on our national DNA database, without safeguards, the attempt to introduce compulsory ID cards, which some in the last government were quite obsessed with, the fingerprinting of children in schools without parental consent: these were wrong – and the present government is putting them right. The country is under new management in that respect.

That is symbolised, I think, in the introduction into Parliament of a major bill to improve people's freedoms. The key measure in this bill, which the Deputy Prime Minister, Nick Clegg, is leading on, but carries the entire coalition with him, is:

- stronger independence for the UK's Information Commissioner,
- safeguards against the misuse of Counter-Terrorism stop and search powers,
- further regulation of CCTV, and
- reform of our scheme governing the vetting and barring of ex-offenders and those working with children and vulnerable adults.

So we have had first-hand experience in the United Kingdom of how all too easy it is for a perfectly democratic Government to move into a kind of authoritarianism which stifles democracy and of course, if taken too far, provides succour to our enemies. And the new government is certainly going to guard against this risk.

But we must also guard against regulations or reactions which just invert this old order, that become obsessed with privacy or data protection without recognising the harm that also results to citizens from failure to share information, as well as from careless stewardship of data. Detailed prescription will not in itself make our citizens safer, or more free, in this complex, modern world.

It is obvious to us all that today's society is very different to that of thirty years ago, indeed quite different, in some ways, even from ten or twenty years ago, technologically.

Individuals move easily across borders where there was once barbed wire fences and a wall; we can now earn a qualification in one Member State that we expect to be recognised in another; we can move as freely between Barcelona and Brussels as we can between London and Liverpool – whether we're going to work or whether we're on holiday.

And wherever I am, in this European space, I want to be confident that my privacy, my safety **and** my freedom are strongly protected.

I want my personal information to be safe and secure, and not exposed unnecessarily either to criminals or to the overly intrusive mechanisms of any State.

Equally, I want to be sure that my details are shared where it's to my advantage that they should be shared where I can directly and practically benefit in my daily life.

- I want insurance and credit if I need it;
- I want any doctor to have access to my medical history before he starts poking about with me if I'm seeking his assistance;
- I want to be confident that I am not sharing my flight abroad on an aeroplane with a terrorist passenger alongside me.

All those require some pooling of information.

So the obvious challenge we are going to have to face as we discuss all these measures over the next few months, is the challenge of having a system of rules that are subtle and grounded enough to protect those three crucial rights, all of them: privacy, safety, **and** freedom - in the context of the accelerated technological advances of the modern world.

No-one can second-guess the future, particularly with the extraordinary pace of technological change which, I assure you, is utterly beyond me personally. So the watchword for me in relation to the regulation and politics of data protection is flexibility. Fortunately, we do have some long-standing experience of some tried and tested guidelines.

Almost thirty years ago, the United Kingdom was one of the first countries in the world to introduce a data protection law: a fact of which I think we British can be proud.

We knew then that it was important to set boundaries around the use of personal data, and we agreed a set of principles – the use of personal data had to be fair; lawful; accurate; secure; and the data itself should not be kept for longer than was necessary.

The Coalition Government of which I am a member today stands by the thinking which underpins this approach.

These principles have, in my opinion at least, enduring relevance. Their strength lies in their very generality, in the fact that they don't seek to address a specific technological or political issue of the day, but they are judgements can be applied in different contexts.

If it can be shown that those basic principles are not adequate and leave gaps or weaknesses in protection, then by all means we should revisit them. But I don't see the need for a radical rewrite of all our Data Protection rules or a readdressing of the principles that we have steadily pursued over the years, in the absence of any evidence that we need dramatic change.

I am in favour of modernising data protection law. But we know actually what it is we are trying to protect by way of principle as we do so.

In respect of the international transfer of data by businesses, for example, I agree with respondents to the United Kingdom's own consultation that we should consider moving from a system which restricts information based on national standards of data protection, to a system based on the standard of data protection of the particular company involved – far more relevant to modern methods of business.

So I don't doubt that we in Europe need to make improvements to the current data protection regime. And that's the spirit in which I've been following the Commission's plans to review data protection rules. It has set out a number of principles to guide its thinking.

My view is that while the Commission's principles provide a good starting point, they are not likely to be the end solution to this problem. Security and strong data protection rights are certainly greatly to be desired. But I believe we need to focus more on the broader landscape, and respect the fact that different nations will need different nuance.

This is why we should agree on the broad approach but not lose the point by arguing endlessly over the details.

What's ultimately at stake in this debate is a larger point about how the European Union should work on Justice and Home Affairs matters generally.

The European Union is of course a collection of Member States bound by Treaty and it is always going to be so.

We've come together in a quite unique union, to form a single market because it benefits us economically, and politically because the Union gives us greater opportunities, a safer world to live in, and greater influence on the world stage.

But I always have believed that the only realistic way to make progress with the European vision is to realise that the nation is the fundamental building block, because the population of the different Member States will not respond to any other approach. And we do, in this particular area, have a whole lot of separate national systems, legal jurisdictions and procedures. But being a diverse community has never, in my opinion, stopped us being a close community. What we do have to build on is the things that we do share: the same underlying values: belief in democracy, certain rights, and the rule of law.

The EU has achieved a great deal in Justice and Home Affairs, with tangible benefits to citizens including measures on international crime and terrorism.

So the key question in respect of data protection isn't: Do we have common goals in details? Do we share a set of values? I am sure I am right in saying we can take all this as read. Instead, it's how exactly do we go about doing it?

My view is that the correct approach is one that recognises shared values but rejects a prescriptive one-size-fits-all way of delivering them. We each have constitutional and cultural identities to which we are attached – the EU should not be challenging them.

I also make a rather wild comparison with the very idealistic proponents of Esperanto. There obviously in one world always has been a problem of a multi-lingual world. I don't think it was ever going to be solved by inventing and adding an additional one on a universal basis. And that approach has never actually worked. One thing we don't want is an additional tongue. We just need to improve our ability to understand each others' languages better.

There's also a legal analogy. What matters in Europe, surely, is values, not just adding to the processes without thinking where you're going. So on data protection, let us keep the broad principles of the existing Directive and better understand the 27 laws we all in our nation states have, rather than setting out to create in detail an additional 28th radically different, and artificial new set of laws.

More broadly, let's learn to understand each other's legal systems better, not rewrite our respective statutes and codes from scratch.

So against that background, let me just turn to the detail of what we know so far of the proposals put forward by the Commission.

Many of the issues under discussion are complex and their effects potentially wide-reaching.

The 'right to be forgotten' sounds a simple idea. But you don't need to think about it for long to see it poses all kind of difficulties.

Other voices than mine have raised concerns over its ability to impinge on free speech, and to censor information which has been legitimately circulated in the public domain.

More broadly I worry about the impact on business and the public.

A whole range of vital services that consumers rely upon critically depend, in turn, on the availability of data.

Without reasonably portable health records for example, it's hard to see how medical services can operate sensibly. Without appropriately regulated data on credit histories, then loans and mortgages might in future be very limitedly available – and might even only be available to the very wealthy.

And then there's the question of how a right to be forgotten could ever work in practice, given that we live in a digital era where information is easily replicated in seconds by customers who voluntarily share data. All told, I'm rather worried that this principle would risk setting up what is an unachievable standard and create public expectations that could only be dashed.

The Commission has also spoken of plans to revise radically the data protection rules in the area of law enforcement. Again I caution be careful what you wish for.

Europeans know as well as anyone that the threat of terrorism is a real one, not just some illusion.

The security and wellbeing of our citizens is rightly the critical concern of any government. If we are to be successful in protecting the safety of our peoples against very sophisticated enemies, then we need to be nimble in using information properly and technology to detect, disrupt and prosecute those who would do us harm.

As I said earlier, harm can arise to the citizen where information is not being properly shared, by people he is entitled to assume are sharing it, as well as when it is shared carelessly, so our regime has both to protect the use of data, but also to enable the use of data for a proper purpose.

This isn't some theoretical point. There are documented cases of the importance of what might be called 'data availability'.

It was the use of Passenger Name Record data that enabled the identification of the terrorist facilitator at the heart of the Mumbai attacks.

The retention of communications data has also helped to identify individuals who orchestrated the influx of high grade heroin from Afghanistan to the UK.

Recently, in Britain the call data of a mobile phone helped to locate the whereabouts of a missing 14 year old girl who had a history of self-harm.

So, we must ensure that any revision to the data protection regime bears these cases in mind.

That's why the UK also views with caution the Commission's apparent intention to revise the whole Data Retention Directive. We agree with the large majority of other Member States who also think that it makes no sense to collect PNR information on flights to and from third countries without also collecting the same information on flights between EU Member States.

We can't provide the protection we all wish to see without working with our non-EU partners, given the threats we face are global in nature. We should continue to engage closely with the United States on Passenger Name Records and data protection - it is absolutely crucial to improving US and EU security. And we will be positively negligent if we fail to take advantage of the improved security that we can give to passengers by properly pooling protected data that we both have.

A final area of concern raised by the Commission is the question of 'extra-territoriality' – which appears to be putting forward the idea that European standards should apply to any firm processing EU citizens' data anywhere in the world.

Now it's fine to aspire to a global dimension to data protection in this way – especially with the emergence of Cloud Computing - a technology of which I must admit, I have limited knowledge myself, so don't press me with questions on Cloud Computing. But I do think, as a lawyer, it's wrong to view the extension of the application of European Union law on a global scale as some simple and unquestioned process.

If we expect the EU regime to protect the data of EU citizens regardless of location, then it wouldn't be unreasonable to expect Australians, Japanese and citizens from other countries working in the European Union to import their own legislative rights with them. I see little sign that the Commission has thought about this sufficiently yet? And how on earth are you going to enforce EU protection on a global basis?

And what kind of reciprocity are we going to be engaging in with the other nation states outside the Union. So I've highlighted a few areas today – and there are more I could raise – be it data breach notification or the regulation of data controllers. Across all of them, I have no problem with asking whether the current regime is adequate, and I certainly don't doubt the good intentions of the Commission.

But my fear is that on many of these issues good intentions need to be thought through and, taken too simplistically forward, good intentions could prove counter-productive.

Rather than improving privacy, safety and freedom, there is a real risk that some of these ideas might accidentally undermine them. A preoccupation with imposing a single, inflexible, codified data protection regime on the whole of the European Union, regardless of the different cultures and different legal systems, carries with it serious risks.

I'm not saying - the old political cliché - "if it ain't broke, don't fix it". Technology has moved on.

I *am* saying we may well be talking about doing a good service or test on a well-loved old car, rather than writing off the vehicle altogether and trying to buy a flashy but impractical new one.

I'm optimistic that there's a common sense solution on this. If we actually look at what citizens really want to see us provide in any solution, and keep an eye on what citizens want us to provide, we can make good progress. And our experience in the United Kingdom and most of the other Member States is that security, and freedom, and privacy are all possible, and that all our citizens want to see all three.

I have never agreed with those who have to say that we somehow have to choose between being safe on the one hand, or being free on the other. Or between my security on the one hand, or my freedom on the other. I want both, most people I know want all three. And it's a false choice, a dangerous one, and I hope we have a sensible and flexible regime across Europe that protects all three values.

Thank you very much.

ENDS