

**International Conference – Computers, Privacy & Data Protection  
16-17 January 2009 – Deburen Brussels, Belgium**

[www.cpdpconferences.org](http://www.cpdpconferences.org)

**Data Protection in a profiled World  
Reform of e-Privacy Regulations in the EU  
Prof Steve Saxby  
17<sup>th</sup> January 2009**

Ladies and gentlemen, I have been asked to limit my intervention to no more than 10 minutes in accordance with the request of the organisers. My main point is that as we enter another round of attempted re-drafts of e-Privacy regulation we really need to reflect on the bigger picture and assess in the months to come the dynamics of the challenges we face in a digital world in regulating privacy in all its dimensions.

The qualified rights have been articulated in the conventions:  
“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence”.

But, in the jurisdictions, the privacy law that we have derives definition from a range of values and objectives and from different sources including both legislative and judge made law. The concept, then, and its regulation mean subtly different things to different people and cultures.

I feel that, in the digital world, we need time for reflection to re-assess the philosophy and define a policy and process to take us forward. We need to recognise that the communications revolution of the past 50 years has dramatically changed the societies in which we live. Only when this is truly understood can we strike out on a path of legal intervention with any clear idea of what we want to do and where we want to go.

Digital technology has created a totally different world for information. The meaning, utilisation and value of information has been turned on its head. We are on a different planet today in terms of creation, mobility and access to information and that process is accelerating all the time.

Just as these developments can erode individual privacy in ways either not recognised or possible before, so too can we enjoy the fruits of these information flows in economic, social and political terms. The challenge for us is how to extract the good and control the bad within these elements.

It seems to me that governments ultimately must strive to achieve that goal. Social responsibility and education can contribute but only regulation can establish acceptable standards of what should be accessible, to whom and on what terms.

We are at a stage now when environmental concerns, the global shock of 9/11 and now the economic downturn, has challenged governments around the world in terms of what to do to secure normality in their societies. We are all now engaged in pondering the question what kind of world we want to live in, while governments are reflecting upon which principles might have to be compromised or even sacrificed for the greater good of the prior need.

The problem is that the advance of technology makes those choices ever more difficult to apply, due to the increased range of considerations that arise. In many instances, too, it is governments themselves that are being criticised for the erosion of privacy interests in favour of what the latter might argue are necessary steps for the public good, taken on grounds of national security, or efficient and cost effective government. The question is whether privacy, efficiency and security can live together without consequential sacrifice of principle, core values or effectiveness.

A good illustration of these dilemmas can be seen from the decision of the ECHR on 4th December 2008 in **S & Marper v UK**. This concerned the storage of data in the UK's National DNA Database. The court ruled that:

“the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences.... fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.”

This view explains extremely well the broader dilemma that I have endeavoured to outline. While it might be beneficial to store everyone's DNA at birth in terms of crime prevention and detection, the question is whether this is a proportionate response to those 'needs' when the privacy risks are so high?

In conclusion, I believe that this requires the European Commission to step back and reflect upon its i2010 agenda. This promotes the digital economy, inclusiveness and quality of life on behalf of all its citizens. Privacy, as an issue, lies in the midst of that agenda. Individuals are looking to government, including the EU, to protect their core expectations, but find it hard to articulate exactly how this might be accomplished and how to reconcile the competing values involved in the regulatory response.

I wonder, therefore, whether the correct way forward is to divide the privacy issue into its constituent parts and assess, one by one, the values, principles and policies that need to be put in place. Within this mix the question is whether there should be room for compromise that identifies where cultural diversity and other important factors permit

flexibility and subsidiarity. After all, Member States are starting from many different positions in this regard. Privacy is a moving concept and the issues it raises will vary according to the context. This needs to be taken into account as the e-privacy agenda unfolds.