



## **“PRIVACY AND TRANSPARENCY: THE RACE TO THE BOTTOM”**

Article for EU Reporter, 9<sup>th</sup> February 2006

I experienced the dreaded ‘identity theft’ two years ago. I checked into a hotel in Brussels owned by a leading American chain. The suave and uniformed gentleman behind the counter swiped my card once and then fluently swiped it again under the counter, while apologising for the delay. Within hours a version of me was happily at Heathrow. By the next day my doppelganger was spending its way across Bangkok. I have a very good bank and this identity theft cost the real me nothing. However when I complained vigorously and repeatedly to the hotel management they showed no interest and denied any culpability by their staff. Such identity theft is a sharp lesson on the limits to personal privacy made possible by technical advances. This invasion does not stop at credit cards and bank details. Those more scientifically literate than I, tell me that a hair taken from my shoulder will give access to my DNA. A similar hair would record with hirsute accuracy all drugs taken during its growth, both legal and illegal. Of course if you have nothing to hide, you have no reason to worry ...

In the late 1990s I made myself unpopular by arguing that privacy would be a bigger issue in the twenty first century than traditional human rights. Now we can see that the exercise of human rights in an age of terror can be subverted by states that have invaded individual privacy. In the USA President Bush is claiming to be above the law as long as the state is at war. He proposes to continue eavesdropping on Americans outside the Congressionally approved system. This is not foreseen as a temporary assertion of the Presidential prerogative as he argues that the “War on Terror” will be a long one. In Europe the state is also back with a vengeance. Information on individuals is to be traded and retained. It is a historical inaccuracy to call this a Fascist state, but it certainly begins to approximate to a police state. Surprisingly for a nation that claims to be concerned about freedom, the British have led the way with a huge concentration of CCTV cameras. The average Londoner can expect to be caught on camera three hundred times a day. I always assumed that such cameras were computer operated and static. However a recent article on the cameras in central London revealed individual operators, who can pan in so closely that they can read a letter over the shoulder of their victim. Of course if you have nothing to hide, you have no reason to worry ...

There is amusement to be had even in the gravest circumstances, so we should maintain our sense of humour. Who would have thought that it would be a British Home Secretary who was the first to use the “Passerelle to K9”. This enabled him to move data retention from Pillar III to Pillar I in order to get round inconvenient national vetoes. Such a joy to see a British government using a federalist device and then claiming it as a triumph for the British Presidency. It is on a par with their other great Presidency triumph of forcing the opening of negotiations with Turkey in the face of European public opinion!

The front page article in EU Reporter on 30<sup>th</sup> January rightly identifies the threat from RFID technology. This, as with all new gadgets, can be used as effectively by organised crime as by governments. The idea that government technology can somehow stay ahead of criminal technology is a charming conceit. It is like assuming that virus protection will always be effective despite the legion of geeks intent on cracking the system. Chip and pin was likewise supposed to increase security, but we are now told that criminals have exploited public confusion to find new scams. I am all in favour of co-ordinated European and global action against identity theft, phishing and the rest. My worry is that we may be entering a new “race to the bottom” in which governments and organised crime leapfrog each other until all our privacy is gone. Of course if we have done nothing wrong, we have no reason to worry ...

No doubt the governments think of themselves as the “Platonic Guardians” of our rights. But who is to guard the guardians? I remember asking Robin Cook, when he appeared in front of the Foreign Affairs Committee during his stint as President in Office, whether it was true that the British had been using their intelligence services to spy on the French and Germans ahead of important Summits. He looked embarrassed and responded with the standard reply that he could not discuss intelligence matters in front of any parliament. Of course if he had done nothing wrong, he had no reason to worry ...

Parliament rightly shone a bright light on the abuse of the Echelon system. The US government was using intercepts of communications from European businesses to advantage American companies. It justified this commercial espionage on the grounds that European companies were probably bribing their customers, whereas American companies were notionally pure. Of course if European companies had done nothing wrong, they had nothing to fear ...

The information society of the twenty first century is forcing companies to learn new and exotic skills. Most corporations have a well-honed Crisis Management process in place. However there must be some puzzled Danish companies currently trying to cope with the backwash from the great cartoon saga. Cheese companies are used to having scientific advisors. Will they now need to employ spiritual advisors with expertise on radical Islamic groups? From another flank companies are now required by campaigning NGOs to observe absolute consistency between what their CEO says in his corporate responsibility declarations and the behaviour of tens of thousands of employees around the world. Of course if they have done nothing wrong, they have nothing to fear ...

The ECPA Annual Conference on 7<sup>th</sup> March has working groups on three related aspects of this jigsaw puzzle. We will be looking at the subject of “Joined up Public Affairs”, examining the relationship between corporate responsibility and the public affairs function. We will look at “Campaigning with Groups in Society” and try to establish what is acceptable and what is appropriate transparency. We will also look at “Building Effective Pan- European Teams”. Indeed we might take the cartoon saga as a good case study in public affairs practice by a radical Islamic group. Abu Laden clearly purveyed one set of pornographic representations of the Prophet around the Middle East in order to stoke the flames of a controversy that had started with illustrations for a children’s book. This was not a case of offence accidentally caused leading to political uproar. The original cartoons had already been published in Egypt, producing no public outcry. The Danes are deserving of more support than they have received from some sections of European society. They have undoubtedly been singled out in order to establish precedents of what may or may not be said by the host community in Europe. I find the earnest soul searching about self-censorship deeply depressing. Self-censorship is the building block which allowed totalitarian states to maintain control over their populations. Of course if Europeans have done nothing wrong, they have no reason to worry ...

Meanwhile in the Berlaymont, good Commissioner Kallas struggles to implement the controversial sections of his ill-structured European Transparency Initiative. He wants the public affairs function to self-regulate, but he does not exclude mandatory regulation if nothing happens. Elsewhere the Commissioner has accepted that total transparency in law-making is impossible as there must be a certain space for private reflection when the Commission is forming policy. Ah yes! What is legitimately private? What are the limits to transparency? Commissioner Kallas’s recent article in the Wall Street Journal ends with the slightly worrying sentence – “Because there is nothing wrong with lobbying, there should be nothing to hide”.

