COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

CommDH/Speech(2011)1
English only

Conference on "Social Networks" organised by the Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information marking Data Protection Day 2011

Budapest, 27 January 2011

Speech by Thomas Hammarberg
Council of Europe Commissioner for Human Rights

Ladies and Gentlemen, it is a great pleasure to be with you here in Budapest today as we consider the important and timely question of how human rights protection and other forms of regulation can be applied to the phenomenon of social networking. I will be talking mostly about Facebook, the largest social network in the field – but I trust that my comments can also be relevant more generally.

Imagine, for a moment, if Facebook were a nation State: it would be the third most populous in the world, behind only China and India, with 600 million registered "inhabitants" (or at least, "passport-holders") according to the latest figures. None of our individual States in Europe is close to this size. Indeed, at some point in 2011, probably sooner rather later, Facebook's ever-growing membership is most likely to reach in excess of 800 million people, thus overtaking the size of the entire population of the territory covered by the Council of Europe.

The fact that Facebook is not a nation State, but rather a Social Network, of course gives rise to delicate questions regarding "constitutional order" and, for our purposes, the extent to which Europe's recognised framework for the protection of human rights can be applied to supervise its activities.

In my opinion, there must be two clear points of reference at the outset of our discussion on Social Networks – both of which already appear to be reflected in Facebook's recent dialogue with European authorities, at the EU and national levels.

First: it should be clear that an online social network's activities cannot be adequately regulated alone by the laws of the country in which its headquarters is based (in reality, the United States). Rather, at least insofar as its European usership is concerned, every social network should be properly subject to European law and regulations.

Second, and particularly relevant for this conference: we should study in closer detail the impact of social networking on human rights – in particular, on the individual right to privacy, which constitutes an integral element of the right to respect for private life under Article 8 of the European Convention on Human Rights, the ECHR.

Specifically, we must be alert to the consequences that social networks might have for the special, subsidiary right we refer to as “data protection”.

Data protection is most commonly understood in terms of limits, or regulations, on the extent to which the State can intrude into our private lives, and supervision of the ways in which the authorities process our personal data. When I last published an Issue Paper on the subject of data protection, in December 2008, I highlighted the trend of ever-increasing mass surveillance – employing tools ranging from CCTV to “spyware” – and warned of the unacceptable actions to which this trend is prone to lead in an age of ever more robust counter-terrorist measures. At that time, I made the observation that “we are rapidly becoming a ‘Surveillance Society’”.

Today, in light of the seemingly irreversible growth of Facebook and other similar social networking portals, the context of data protection appears to be evolving, and entering entirely new areas. I therefore wish to take the opportunity to update my observation, and point out that we are also rapidly becoming a ‘Networked Society’.

In contrast to State-led surveillance, our instinctive reaction is to regard social networking as user-driven, and therefore unlikely to incur unwanted infringements on our privacy. But I think I would characterise our relative collective comfort in this regard as a false sense of security.

To understand *why* our right to privacy, and specifically “data protection”, might be in jeopardy, we may consider the public comments of Facebook’s founder, Mark Zuckerberg. His ambition, he has declared, is “to build the greatest communications company in the world”; he has also stated that privacy is “no longer a contemporary concept” for people in the 21st century.

It is obvious that self-declared motivations such as profit and pre-eminence will not automatically accommodate built-in data protection – no matter how much one believes in the “self-regulation” potential of “interactive communities”.

Rather, wherever there emerges such a vast and growing repository of personal data, all of it in digital form, and whenever the operators of this repository are intent on putting the data towards ever wider-ranging and more novel purposes, human rights implications will inevitably arise.

Indeed, data protection more broadly concerns the extent of control over individuals’ data exerted by any data controller. Whether in the hands of a State or non-State actor; our data must be guarded from improper acquisition, collection, storage, transfer or use.

There was a case recently in Germany, where Hamburg’s privacy commissioner argued that Facebook’s unsolicited approaches to non-users using the “Friend Finder” program were infringing on the right to privacy. Facebook’s resolution of this matter has reemphasised, I might add, the vital importance of independent and impartial data protection authorities in overseeing social networking practices – and I think our host at this Conference, Hungary’s Commissioner Jori, is a good example in this regard.

The reality of this “information age”, however, is that all of us, more often than we might imagine, are “data subjects” for Social Networks. Irrespective of whether we have “opted in” to any social networking portal, our data – including personal details, e-mail addresses, telephone numbers, logs of our contacts and chats, as well as photographs

and videos of ourselves, our families and our associates, to name just a few aspects – are subject to extensive "dataveillance". "Dataveillance" means our data is being monitored, archived, searched and analysed, shared and used… on an ongoing basis.

As we consider, especially at this conference, by whom and towards what ends such "dataveillance" is being undertaken… we may well arrive at more questions than answers. Indexing by search engines, as well as targeted advertising by application developers and online merchants, are just two of the known manifestations of "dataveillance" by third parties. It remains to be seen whether other forms of "profiling" may also be able to take place via social networks, including the more objectionable practices I highlighted when discussing law enforcement and counterterrorism actions.

I believe that this uncertainty surrounding the nature and scope of potential "dataveillance" activities via Social Networks in itself underlines the need for strong data protection.

As a matter of principle, for all of us in Europe, privacy must remain paramount. Indeed, the further our understanding of the need for privacy evolves, the longer the underlying concept endures.

It falls to our national and international authorities to ensure that our individual rights to privacy and data protection are not sacrificed to social networks, but rather reinforced to meet the range of new challenges these networks present.

And so it is that in this year – the year of its 30th Anniversary – the Council of Europe Convention for Protection of Personal Data, Convention 108, will also undergo a process of "modernisation", based on wide-ranging consultations, which will also take account of the main EC directive and EU practices in the area, as well as the case law of the European Court of Human Rights and the European Court of Justice.

It should always be remembered that the Council of Europe's human rights instruments are essentially principle-based and technology-neutral. Thus, while Convention 108 was the first international data protection convention of its kind in 1981, it remains just as relevant to the wide embrace of social networking today as it has been to all the other challenges to privacy that have gone before.

Perhaps it is fitting to end by stating my belief that our human rights instruments – much like our Facebook profiles – should not be too quickly deleted or scrapped simply because times have changed, but rather should be judiciously "updated" when necessary to reflect the most recent developments.

Thank you, and may I wish you constructive discussions, as well as some "social networking" of your own, over the course of the next two days.