COUNCIL OF EUROPE CONSEIL DE L'EUROPE
Committee of Ministers
Comité des Ministres

Recommendation CM/Rec(2012)4
of the Committee of Ministers to member States
on the protection of human rights with regard to social networking services

(Adopted by the Committee of Ministers on 4 April 2012
at the 1139th meeting of the Ministers' Deputies)

Social networks as human rights enablers and catalysts for democracy

1. Social networking services are an important part of a growing number of people's daily lives. They are a tool for expression and communication between individuals, and also for direct mass communication or mass communication in aggregate. This complexity gives operators of social networking services or platforms a great potential to promote the exercise and enjoyment of human rights and fundamental freedoms, in particular the freedom to express, to create and to exchange content and ideas, and the freedom of assembly. Social networking services can assist the wider public to receive and impart information.

2. The increasingly prominent role of social networking services and other social media services also offer great possibilities for enhancing the potential for the participation of individuals in political, social and cultural life. The Committee of Ministers has acknowledged the public service value of the Internet in that, together with other information and communication technologies (ICTs), it serves to promote the exercise and enjoyment of human rights and fundamental freedoms for all who use it. As part of the public service value of the Internet, these social networking services can facilitate democracy and social cohesion.

Human rights may be threatened on social networks

3. The right to freedom of expression and information, as well as the right to private life and human dignity may also be threatened on social networking services, which can also shelter discriminatory practices. Threats may, in particular, arise from lack of legal, and procedural, safeguards surrounding processes that can lead to the exclusion of users; inadequate protection of children and young people against harmful content or behaviours; lack of respect for others' rights; lack of privacy-friendly default settings; lack of transparency about the purposes for which personal data are collected and processed.

4. Users of social networking services should respect other people's rights and freedoms. Media literacy is particularly important in the context of social networking services in order to make the users aware of their rights when using these tools, and also help them acquire or reinforce human rights values and develop the behaviour necessary to respect other people's rights and freedoms.

Social networking providers should respect human rights and the rule of law

5. A number of self- and co-regulatory mechanisms have already been set up in some Council of Europe member States in connection with standards for the use of social networking. It is important that procedural safeguards are respected by these mechanisms, in line with the right to be heard and to review or appeal against decisions, including in appropriate cases the right to a fair trial, within a reasonable time, and starting with the presumption of innocence.

6. The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe, recommends that member States, in consultation with private sector actors and civil society, develop and promote coherent strategies to protect and promote respect for human rights with regard to social networking services, in line with the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5, hereinafter referred to as "the European Convention on Human Rights"), especially Article 8 (Right to respect for private and family life), Article 10 (Freedom of expression) and Article 11 (Freedom of assembly and association) and with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), in particular by engaging with social networking providers to carry out the following actions:

− provide an environment for users of social networks that allows them further to exercise their rights and freedoms;

− raise users' awareness, by means of clear and understandable language, of the possible challenges to their human rights and the ways to avoid having a negative impact on other people's rights when using these services;

− protect users from harm without limiting freedom of expression and access to information;

− enhance transparency about data processing, and refraining from illegitimate processing of personal data;

− set up self- and co-regulatory mechanisms where appropriate, in order to contribute to the respect of the objectives set out in the appendix to this recommendation;

− ensure accessibility to their services to people with disabilities, thereby enhancing their integration and full participation in society.

7. Member States should:

− take measures in line with the objectives set out in the appendix to this recommendation;

− bring this recommendation and its appendix to the attention of all relevant public authorities and private sector actors, in particular social networking providers and civil society.

Appendix to Recommendation CM/Rec(2012)4

I. Essential information and measures needed to help users deal with social networks

Context and challenges

1. Social networking services offer the possibility both to receive and to impart information. Users can invite recipients on an individual basis, but in most cases the recipients are a dynamic group of people, sometimes even a "mass" of unknown people (all the members of the social network). In cases where users' profiles are indexed by search engines, there is potentially unlimited access to parts of or all information published on their profiles.

2. It is important for users to be able to feel confident that the information they share will be processed appropriately. They should know whether this information has a public or private character and be aware of the implications that follow from choosing to make information public. In particular, children, especially teenagers, and other categories of vulnerable people, need guidance in order to be able to manage their profiles and understand the impact that the publication of information of a private nature could have, in order to prevent harm to themselves and others.

Action

3. Member States should co-operate with the private sector and civil society with a view to upholding users' right to freedom of expression, in particular by committing themselves, along with social networking providers, to carry out the following actions:

− help users understand the default settings of their profiles. The default setting for users should limit access by third parties to self-selected contacts identified by the user.[1] Users should be able to make an informed decision to grant wider public access to their data, in particular with regard to indexability by external search engines. In this connection, the social networking service should:

− inform users of the consequences of open access (in time and geographically) to their profiles and communications, in particular explaining the differences between private and public communication, and the consequences of making information publicly available, including unrestricted access to, and collection of, data by third parties;

− make it clear to the users – offering accessible tools – that they retain the right to limit access to their data, including the right to remove data from archives and search engine caches;

− offer adequate, refined possibilities of enabling the user to "opt in" in order to consent to wider access by third parties;

− enable users to control their information. This implies that users must be informed about the following: the need to obtain the prior consent of other people before they publish their personal data, including audio and video content, in cases where they have widened access beyond self-selected contacts; how to completely delete their profiles and all data stored about and from them in a social networking service, and how to use a pseudonym. Users should always be able to withdraw consent to the processing of their personal data. Before terminating their account, users should be able to easily and freely move the data they have uploaded to another service or device, in a usable format. Upon termination, all data from and about the users should be permanently eliminated from the storage media of the social networking service. When allowing third party applications to access users' personal data, the services should provide sufficiently multi-layered access to allow users to specifically consent to access to different kinds of data;

− help users make informed choices about their online identity. The practice of using pseudonymous profiles offers both opportunities and challenges for human rights. In its Declaration on Freedom of Communication on the Internet (adopted on 28 May 2003), the Committee of Ministers stressed that "in order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member States should respect the will of users of the Internet not to disclose their identity". The right to use a pseudonym should be guaranteed both from the perspective of free expression and the right to impart and receive information and ideas and from the perspective of the right to private life. In the event that a social networking service requires real identity registration, the publication of that real identity on the Internet should be optional for users. This does not prevent law-enforcement authorities from gaining access to the user's real identity when necessary and subject to appropriate legal safeguards guaranteeing the respect of fundamental rights and freedoms;

− provide users with concise explanations of the terms and conditions of social networking services in a form and language that is geared to, and easily understandable by, the target groups of the social networking services;

− provide users with clear information about the editorial policy of the social networking service provider in respect of how it deals with apparently illegal content and what he considers inappropriate content and behaviour on the network.

4. In addition, member States should:

− foster awareness initiatives for parents, carers and educators to supplement information provided by the social networking service, in particular in respect of much younger children when they participate in social networks.

[1] See Article 29 Data Protection Working Party Opinion 5/2009 on online social networking (12 June 2009); 30th International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy Protection in Social Network Services (Strasbourg, 17 October 2008); International Working Group on data Protection in Telecommunications (IWGDPT) "Rome Memorandum" (Rome, 3-4 March 2008).

II. Protection of children and young people against harmful content and behaviour

Context and challenges

5. Freedom of expression includes the freedom to impart and receive information which may be shocking, disturbing and offensive. Content that is unsuitable for particular age groups may well also be protected under Article 10 of the European Convention on Human Rights, albeit subject to conditions as to its distribution.

6. Social networking services play an increasingly important role in the life of children and young people, as part of the development of their own personality and identity, and as part of their participation in debates and social activities.

7. Against this background, children and young people should be protected because of the inherent vulnerability that their age implies. Parents, carers and educators should play a primary role in working with children and young people to ensure that they use these services in an appropriate manner.

8. While not being required to control, supervise and/or rate all content uploaded by its users, social networking service providers may be required to adopt certain precautionary measures (for example, comparable to "adult content" rules applicable in certain member States) or take diligent action in response to complaints (ex-post moderation).

9. Age verification systems are often referred to as a possible solution for protecting children and young people from content that may be harmful to them. However, at present there is no single technical solution for online age verification that does not infringe on other human rights and/or is not exposed to age falsification.

Action

10. In co-operation with the private sector and civil society, member States should take appropriate measures to ensure children and young people's safety and protect their dignity while also guaranteeing procedural safeguards and the right to freedom of expression and access to information, in particular by engaging with social networking providers to carry out the following actions:

− provide clear information about the kinds of content or content-sharing or conduct that may be contrary to applicable legal provisions;

− develop editorial policies so that relevant content or behaviour can be defined as "inappropriate" in the terms and conditions of use of the social networking service, while ensuring that this approach does not restrict the right to freedom of expression and information in the terms guaranteed by the European Convention on Human Rights;

− set up easily accessible mechanisms for reporting inappropriate or apparently illegal content or behaviour posted on social networks;

− share best practices on ways to prevent cyber-bullying and cyber-grooming. In this connection, age-differentiated access should be treated carefully where age is provided by children and young people themselves. Social networking providers should take diligent action in response to complaints of cyber-bullying and cyber-grooming.

11. In addition, member States should:

− encourage the establishment of transparent co-operation mechanisms for law-enforcement authorities and social networking services. This should include respect for the procedural safeguards required under Article 8, Article 10 and Article 11 of the European Convention on Human Rights;

− ensure respect for Article 10, paragraph 2, of the European Convention on Human Rights. This includes refraining from the general blocking and filtering of offensive or harmful content in a way that would hamper its access by users. In this connection, the Committee of Ministers' Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters

should be implemented with a view to ensuring that any decision to block or delete content is taken in accordance with such principles. Transparent voluntary individual filtering mechanisms are also to be encouraged.

III. Personal data and trust in social networks

Context and challenges

12. Social networking services process large amounts of personal data, including users' profiling data and data on their Internet use. Publishing personal data in a profile can lead to access by third parties, including, amongst others, employers, insurance companies, law enforcement authorities and security services.

13. Social networking services should not process personal data beyond the legitimate and specified purposes for which they have collected it. They should limit processing only to that data which is strictly necessary for the agreed purpose, and for as short a time as possible.

14. Social networking services should seek the informed consent of users if they wish to process new data about them, share their data with other categories of people or companies and/or use their data in ways other than those necessary for the specified purposes they were originally collected for. As stated in Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, users should be informed where their personal data is used in the context of profiling. The user's decision (refusal or consent) should not have any effect on the continued availability of the service to him or her. When allowing third party applications to access users' personal data, the services should provide sufficiently multi-layered access to allow users to specifically consent to different kinds of data being accessed.

Action

15. In co-operation with the private sector and civil society, member States, in addition to the measures stated in section I of this appendix, should take appropriate measures to ensure that users' right to private life is protected, in particular by engaging with social networking providers to carry out the following actions:

− promote best practices for users. This includes default privacy-friendly settings that limit access to contacts selected by users themselves, the application of the most appropriate security measures, informed consent of users before personal data is disseminated, the sharing of personal data with other categories of people or companies and/or the use of their data in other new ways;

− ensure that users are able to effectively exercise their rights by offering, amongst other things, a clear user interface, and sufficiently multi-layered access to allow users to specifically consent to different kinds of data being accessed by third parties;

− ensure that sensitive data have enhanced protection. The use of techniques that may have a significant impact on users' privacy − where for instance processing involves sensitive or biometric data (such as facial recognition) − requires enhanced protection and should not be activated by default;

− ensure that the most appropriate security measures are applied to protect personal data against unlawful access by third parties. This should include measures for the end-to-end encryption of communication between the user and the social networking services website. In the absence of applicable legislation relating to the security of personal data and foreseeing the obligation to report data breaches, social networking services should nevertheless inform their users of breaches, to enable them to take preventive measures, such as changing their password and/or keeping a close eye on their financial transactions (where the providers are in possession of bank or credit card details);

− implement "privacy by design". Social networking services should be encouraged to address data protection needs at the stage of conception of their services or products and continuously assess the privacy impact of changes to existing services with a view to strengthening security and users' control of their personal data;

− protect third parties who are associated with the users of social networks. Non-users of the social network may also be affected by the disclosures of users of social networking services or by use of their data by the social networking service itself. They should have effective means of exercising their rights without having to become a member of the service in question and/or otherwise providing excessive personal data. Social networking service providers should refrain from collecting and processing personal data about non-users, for example e-mail addresses and biometric data (such as photographs). Users should be made aware of the obligations they have towards other individuals and, in particular, that the publication of personal data related to other people should respect the rights of those individuals;

− ensure that processing of personal data stemming from social networks for law enforcement purposes respects Article 8 of the European Convention on Human Rights. Enforcing applicable data protection standards is essential. This includes ensuring that the processing of personal data stemming from the use of social networking services for law enforcement purposes is carried out only within an appropriate legal framework, or following specific orders or instructions from the competent public authority made in accordance with the law;

− provide clear information about applicable law and jurisdiction. Users should be informed as to what law is applicable in the execution of the social networking services and the related processing of their personal data. Provisions contained in the terms and conditions of use or service involving a choice of forums or applicable jurisdictions made for opportunistic or convenience reasons should be regarded as void if there is no reasonable link to the forum or jurisdiction in question; the user's forum or jurisdiction would be preferable in cases where a significant number of users are present in a particular territory;

− ensure that users are aware of the threats to their human rights and able to seek redress when their rights have been adversely affected. Users should be informed about possible risks to their right to private life, not only in the social networking services' core conditions (including when changes are made to general terms of service), but every time such a challenge may arise, for example, when the users make information on their profile available to new (groups of) users or when they install a third party application.

Users should be informed about the processing of their personal data, including the existence of, and means of exercising their rights (such as access, rectification, deletion), in a clear and understandable manner and in language geared to the target audience.

In addition to applicable legal provisions, appropriate complaint handling mechanisms should be guaranteed against abusive behaviour of users, in particular with regard to identity theft.