COUNCIL OF EUROPE CONSEIL DE L'EUROPE

T-PD-BUR(2011) 05 prov en
21 April 2011

BUREAU OF THE CONSULTATIVE COMMITTE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD-BUR)

Draft opinions of the T-PD Bureau on the draft texts prepared by the Committee of Experts on New Media (MC-NM) on social networking

Secretariat document prepared by
the Directorate General of Human Rights ad Legal Affairs

Introduction

1. The Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108) (T-PD) would like to begin by welcoming the work of the Committee of Experts on New Media (MC-NM).

2. The Bureau of the T-PD was asked for its opinion on two draft texts prepared by the MC-NM on social networking services, namely a draft recommendation (document MC-NM (2010)3) and a set of draft guidelines for social networking providers (MC-NM (2010)8).

3. Following an initial exchange of views on these drafts at its 23rd meeting (22-24 March 2010), the Bureau asked its members to send written comments on the texts to the Secretariat to help it with the preparation of its opinion.

4. It should be emphasised that this opinion is that of the Bureau of the T-PD alone and that it would be advisable to consult the T-PD as a whole in view of the scope of the issues raised. It is planned to arrange for a written consultation of the members of the T-PD on the basis of this opinion and the draft texts and to forward the T-PD's views to the Steering Committee on Media and New Communication Services (CDMC) in time for its plenary meeting of 14 and 17 June 2011.

Structure

5. The Bureau of the T-PD would point out firstly that it is not always easy to make the link between the two draft texts (recommendation and guidelines), among other things because the recommendation itself refers to a separate set of appended guidelines.

6. Although it is specified in the guidelines for service providers that they must be "read and understood in connection with … the [draft] recommendation", steps should be taken to ensure that a consistent, exhaustive set of principles are also made available to service providers. For example, the guidelines for service providers do not refer to the indexing of data using external search engines whereas measures enabling users to give their free, specific and informed consent to such indexing, for which systematic and automatic provision must be made, relates first and foremost to service providers. This point could be added after that relating to the automatic limiting of access to data to self-selected "friends"[1].

References

7. The Bureau of the T-PD draws the MN-CM's attention to the texts already adopted on this subject at European and international level, to which reference should be made, at least in the explanatory memorandum on the recommendation, beginning with Convention 108.

8. Particular mention should be made of Opinion 5/2009 on online social networking, adopted on 12 June 2009 by the Article 29 Data Protection Working Party, the Resolution on Privacy Protection in Social Network Services adopted in Strasbourg on 17 October 2008 by the 30th International Conference of Data Protection and Privacy Commissioners and the report on the subject adopted in Rome on 3 and 4 March 2008 by the International Working Group on Data Protection in Telecommunications (IWGDPT) known as the "Rome Memorandum".

Data protection principles

9. Generally speaking, the word "finalité" rather than "objectif" should be used in the French text when referring to the purpose of processing (the word "purpose" is used throughout the English). Examples should also be given of legitimate and illegitimate processing.

10. With regard to the rights of the persons concerned, the Bureau of the T-PD would point first and foremost to the need for all users of social networking services to be given clear and understandable general information in language geared, where necessary, to the target audience. This information should be available in the official language of the various user groups' countries of residence. It must alert users to the

[1] This notion of "friends" does not seem suited to social networks based on professional relationships.

dangers connected with publishing data of any kind and the means at their disposal to restrict access so as to keep certain matters in the private sphere. The information provided must be comprehensive and cover subjects such as the maximum length of time for which data may be kept, means of exercising access rights and conditions for the indexing of data by search engines. Lastly, it must list all of the applicable legislation relating to these issues.

11. It should be emphasised that the rights that users exercise over their personal data are not limited to data deletion (a definition of the user's "profile" will have to be given) and that providers must make it simple to carry out the various functions on offer. The idea of data "portability" and what it implies should figure in the draft. User interfaces should be simple to use and enable users to fully understand the impact of their actions on their personal data (making it clear for example that by using a particular application their entire list of contacts will be used to send direct notifications to these contacts – a process that inevitably entails their prior consent).

12. The Bureau points out that certain categories of vulnerable people other than children may require enhanced protection systems.

13. The Bureau of the T-PD stresses how much caution is required in the use of age verification systems and suggests that it should be recommended that such systems are made to comply with human rights.

14. With regard to the processing of data by third parties and the service provider's obligation to "seek the informed consent of users before their data is … processed" (the word "unknowingly" should be deleted as it is not compatible with the effect of informed consent), it should be specified that the user's decision (refusal or consent) should not have any effect on the continued availability of the service to him or her. There may also be a question as to whether such consent should be obtained before the data are "processed" or before they are forwarded to the third party and whether it is necessary to spell out that the third parties concerned are those "offering the applications". In this connection, the Bureau draws the MC-NM's attention to Recommendation (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, in which it is noted in the preamble that data processing for the purposes of profiling may relate to data stemming from social networks.

15. The indexing of personal data published by search engines should generally be prohibited and made possible only if the person concerned has given his or her free, specific and informed consent.

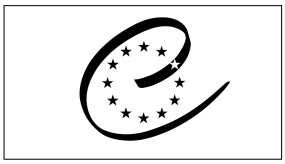
16. Service providers should respect the principle of "data minimisation", in other words limiting processing only to those data which are strictly needed for the purposes agreed to and for as short a period as possible.

17. The call to "apply state of the art security measures" to protect data against unlawful access by third parties is to be welcomed (though it may be preferable to talk instead of the "most appropriate" security measures).

18. In the light of current events, it may be advisable to reiterate under what conditions personal data held by service providers may be used by law enforcement bodies (the police) and what protection mechanisms need to be set up to supervise such use (Recommendation No. R (87) 15 regulating the use of personal data in the police sector.

19. Lastly, provision should be made for the data protection authorities to be called to help set up co- or self-regulatory mechanisms (particularly when drafting instruments such as codes of conduct and reference frameworks).

Appendix 1: Draft Recommendation on measures to protect and promote respect for human rights with regard to social networking services [MC-NM(2010)003_en]



Strasbourg, 12 March 2010

MC-NM(2010)003_en
Français
Pdf

COMMITTEE OF EXPERTS ON NEW MEDIA

(MC-NM)

_____

2nd Meeting
25 – 26 March 2010
Agora Building
Room G 05

_____

Draft
Recommendation on measures to protect and promote respect for human rights with regard to social networking services

_____

1. Social networking services are increasingly becoming an important part of people's daily lives. They are a tool for expression but also for communication between individuals or for mass communication. This complexity gives them 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 communication.

2. Given their increasingly prominent role, social networking services and other social media services also offer great possibilities for enhancing the individual's right to participate in political, social and cultural life. Bearing in mind Recommendation (2007)16 of the Committee of Ministers on the public service value of the Internet which states that the Internet and other ICT services have high public service value in that they serve to promote the exercise and enjoyment of human rights and fundamental freedoms for all who use them, greater efforts could be put into exploring how social networking services and other social media could act as a means to enhancing participation (especially of marginalised groups in society) and contributing to the strengthening of democracy and social cohesion.

3. The right to freedom of expression and information, as well as the right to privacy and human dignity, may also be challenged on social networking services. These challenges may arise, for example, through lack of due process preceding the exclusion of users, insufficient protection of minors against harmful behaviour of others, violation of other people's rights and lack of transparency about the purposes for which personal data is being collected and processed.

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

5. A number of co- and self-regulatory mechanisms have already been set up in some Council of Europe member states. It is important that procedural safeguards are respected by these mechanisms, in line with the human right to a fair trial, within reasonable time, and starting with the presumption of innocence.

6. The Committee of Ministers recommends that member states, in cooperation 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 particular by:

- ensuring users are aware of possible challenges to their human rights on social networking services (in particular their freedom of expression and information and their right to private life and protection of personal data) as well as on how to avoid having a negative impact on other people's rights when using these services;

- protecting users of social networking services from harm by other users while also ensuring all users' right to freedom of expression and access to information;

- encouraging transparency about the kinds of personal data that are being collected and the legitimate purposes for which they are being processed, including further processing by third parties;

- preventing the illegitimate processing of personal data;

- encouraging providers of social networking services to set up co- or self-regulatory mechanisms which are effective, transparent, independent and accountable and which give individuals the right to appeal decisions;

- taking measures with regard to social networking services in line with guidelines set out in the appendix to this recommendation;

- bringing these guidelines to the attention of all relevant private and public sector stakeholders, in particular social networking providers, and civil society.

Appendix – Guidelines

I. Transparency as regards freedom of expression and access to information

1. Social networking services offer the possibility to both receive and 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 (parts of) users' profiles are indexed by search engines there is potentially unlimited access to parts of or all information published on the profile.

2. It is important for participants to feel confident about imparting information and to know whether the information they impart has a public or private character. In particular, children and young people need guidance in order to be able to manage their profile and understand the impact that private and (semi-)public expression can have in order to prevent harm to themselves and others. In cooperation with the private sector and civil society, member states should ensure that the users' right to freedom of expression is guaranteed, in particular by:

- informing users clearly about the difference between private and public communication and the possible consequences of unlimited access (in time and geographically) to their profile and communication;

- providing information about the core conditions of participating in the social networking service in a form and language that is appropriate to, and easily understandable by, the target groups of the social networking site;

- fostering awareness initiatives for parents and teachers to supplement information provided by the social networking service.

II. Appropriate protection of children against harmful content and behaviour

3. Freedom of expression includes the freedom to impart and receive shocking, disturbing and offensive content and/or content that is unsuitable for particular age groups. In some cases however, human dignity and the duty to respect and protect the rights of vulnerable groups may outweigh this right to freedom of expression.

4. Social networking services play an increasingly important role in the life of minors, as part of the development of their own personality and identity and as part of their participation in (semi-) public debate. Similarly, there is a need to protect minors against the inherent vulnerability that their age entails.

5. [Age-verification systems may be one way of protecting children from output that may be harmful to them. However, there is not a single technical solution with regard to online age verification that does not infringe on other human rights and/or does not facilitate age falsification, thus causing greater risks than benefits to the minors involved]. In cooperation with the private sector and civil society, member states should ensure users' safety and protect their human dignity while also guaranteeing procedural safeguards and the right to freedom of expression and access to information, in particular by:

- informing users what content is considered "illegal" according to legal provisions and what content or behaviour is considered "inappropriate" according to the general terms and conditions of the social networking site;

- encouraging law enforcement bodies and social networking sites to establish a transparent basis for cooperation and involve qualified initiatives or hotlines;

- ensuring that users have access to an easy to use mechanism for reporting inappropriate and illegal content or behaviour of other users to the site providers;

- adopting other specific measures to prevent cyber bullying and cyber grooming, such as labelling and age rating of content; [offering age-differentiated access should however be treated carefully, as a best effort that is based on age input provided by the minors themselves];

- ensuring that any decisions to block content should be taken in accordance with Recommendation (2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters and its guidelines;

- guaranteeing that blocking and filtring and in particular nationwide general blocking or filtering measures, are only introduced by the state if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled and avoiding the general blocking of offensive or harmful content for users who are not part of the groups for which a filter has been activated to protect. [Instead, encouraging social networking services to offer adequate voluntary individual filter mechanisms may suffice to protect those groups.]

III. Ensuring users' control over their data

5. Social networking services process large amounts of personal data. It is key that they apply state of the art security measures to protect this data against unlawful access by third parties. Access by third parties may also be gained through third party applications. Social networking services may not process personal data beyond the legitimate and specified purposes for which they have collected the data and should seek the informed consent of users before their data is unknowingly processed by the third parties offering the applications.

6. The default setting for users should be that access is limited to self-selected friends. Users should be able to make an informed decision to grant access to a larger public. The social networking service must offer adequate, refined possibilities to 'opt in' for (consent to) wider access. In case a user wants to widen access to, for example, all users of a social networking service or even globally, through indexability by external search engines, it must be clear - and the appropriate tools must be easily accessible - how they may restrict access again, including removal from archives and search engine caches.

7. Users should be informed about possible challenges to their right to privacy not only in the social networking services' general terms and conditions but every time such a challenge might 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. In particular, children and young people need special guidance in order to be able to manage their profile and understand the risks of changing their privacy settings to a more public profile.

8. The practice of pseudonymous profiles offers both possibilities 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 practice should be encouraged both from the perspective of free expression of information and ideas and from the perspective of the right to privacy. It should however, also be accompanied by an effective control system for inappropriate behaviour like complaint and report mechanisms, moderating, etc.

9. In cooperation with the private sector and civil society, member states should ensure that users' right to private life is protected, in particular by:

- enforcing applicable privacy regulations, especially that social networking services by default limit access to self-selected friends, apply state of the art security measures and have legitimate grounds for the processing of personal data for specific purposes, including further processing by third parties and use for behavioural advertising.

- ensuring transparent information for users about the management of their personal data in a form and language that is appropriate for the target groups of the social networking services;

- ensuring that users are informed about the need to obtain the prior consent of other people before they publish their personal data, including audio and video, in cases where they have widened access beyond self-selected friends;

- guaranteeing that users must be able to completely delete their profile and all data stored about and from them in a social networking site; [this includes tools for parents to manage their children's data];

- encouraging the possibility of pseudonymous profiles.

Appendix 2: Proposal for draft guidelines for social networking providers [MC-NM(2010)008_en]

Strasbourg, 5 October 2010

MC-NM(2010)008_en
Français
Pdf

COMMITTEE OF EXPERTS ON NEW MEDIA

(MC-NM)

2nd Meeting
25 – 26 March 2010
Agora Building
Room G 05

Proposal for draft GUIDELINES FOR SOCIAL NETWORKING PROVIDERS

Social networking services provide a very important platform both for receiving and imparting information. They are therefore an important tool both for realising the human right to free expression as well as the participation in social, cultural, economic [and in some cases even, political] life.

It is important for individuals using social networking services to feel confident about using these tools. They have to be sure that their right to private life will be protected when they use social networking services and that their personal data will not be misused. They also have to understand when the information they post online is no longer private correspondence but has become available to a large public.

It is equally important to recall that the exercise of freedom of expression carries with it duties and responsibilities, in particular as regards the protection of health and morals and the rights of all users. Social network providers are encouraged to ensure that users are protected from harmful content or actions such as cyberbullying.

Social network providers should promote and facilitate users' well-being while respecting fundamental rights, in particular the right to freedom of expression and the right to privacy and secrecy of correspondence.

Social network providers are therefore encouraged to take note of, discuss and make their best efforts to comply with the following guidelines (below). These guidelines should be read and understood in connection with the relevant Council of Europe documents, in particular [draft] Recommendation on measures to protect and promote respect for human rights with regard to social networking services [CMRec…].

- Inform users clearly about the terms of usage in a form and language that is appropriate to and easily understandable by, the target groups of the social networking site (for example, short videos or information in 'plain language').

- Inform users in particular about the difference between private and public communication and the possible consequences of unlimited access (in time and geographically) to their profile and communication.

- If possible, offer or contribute to awareness raising initiatives for users, parents and teachers on the safe use of social networking services.

- Inform the user clearly about what content is considered "illegal" according to legal provisions and what content or behaviour is considered "inappropriate" according to the general terms and conditions of the social networking site.

- Ensure that users have access to an easy to use mechanism for reporting inappropriate and illegal content or behaviour of other users to the site providers.

- Adopt other specific measures to prevent cyber bullying and cyber grooming, such as labelling and age rating of content; [offering age-differentiated access should however be treated carefully, as a best effort based on age input provided by the minors themselves].

- Establish a transparent basis for cooperation with law enforcement bodies and involve qualified initiatives or hotlines.

- Ensure that any decisions to block content are taken in accordance with Recommendation (2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters and its guidelines.

- Ensure, in particular, that self-regulatory mechanisms set up to protect users from illegal and harmful content are effective, transparent, independent and accountable and give individuals the right to appeal decisions to block content.

- Respect applicable privacy regulations, especially limit by default access to self-selected friends, apply state of the art security measures and have legitimate grounds for the processing of personal data for specific purposes, including further processing by third parties and use for behavioural advertising.

- Ensure transparent information for users about the management of their personal data in a form and language that is appropriate for the target groups of the social networking services.

- Ensure that users are informed about the need to obtain the prior consent of other people before they publish their personal data, including audio and video, in cases where they have widened access beyond self-selected friends.

- Make sure that users are able to completely delete their profile and all data stored about and from them in a social networking service [this includes tools for parents to manage their children's data].

- Consider allowing the possibility of pseudonymous profiles.