# TACD

TRANS ATLANTIC CONSUMER DIALOGUE

DIALOGUE TRANSATLANTIQUE DES CONSOMMATEURS

DOC NO: INFOSOC 43-09 DATE ISSUED: MAY 2010

## Resolution on Social Networking

Social networks are a virtual home for hundreds of millions of people. They enable users to interact with each other, to share photos and interests. They make possible that the Internet is no longer simply consumed, but shaped by the individual. However, social networks also pose substantial challenges to users' privacy. Furthermore, marketing is used in highly subtle and covert ways to influence social networking users, in particular children.

Due to the complexity of social networks, most users are not aware of the potential risks in using such platforms and they often do not know how to best protect themselves. At the same time, social networks make it difficult, if not impossible, for individuals to act cautiously on the Internet. In most cases, to access and use social networks individuals must agree that their data can be used for marketing purposes. These one-sided agreements leave users with insufficient control over their personal data. Governments on both sides of the Atlantic have so far failed to take adequate protective measures. For example, the Safer Social Networking Principles for the EU of February 2009 are more of a declaration of intent rather than a set of clear standards in particular regarding privacy aspects – and still lack implementation.

**Recommendations**

**TACD resolves that EU and US governments should:**

1. Enact or revise privacy legislation to:

    a. Forbid making access and the use of a social network contingent on agreement by the user to the use of his or her data for marketing purposes. Users should retain the ownership of data posted online.
    b. Prohibit data about users from being collected, processed and used for marketing purposes without their express and voluntary permission – acquired through an opt-in procedure. No data of another person may be provided without consent.
    c. Require social networks to use effective and state of the art technology and organisational measures to protect confidential personal data against unauthorized use.
    d. Require social networks to regularly inform their users of the measures they can take to protect their data and warn against possible detriment.
    e. Require social networks to take responsibility for all access, abuse and misconduct by third parties to data stored by the social networks.
    f. Limit the personally identifiable information available to social network application providers to those necessary for the purpose of the application. Require application providers to explain to the user what data they want to use, to give details for what purpose the data is needed for and to delete all data immediately after the application is removed and verify to the user that the information has been deleted.
    g. Require social networks to ensure no personally identifiable information is obtained by third party services without user permission.
    h. Require social networks to open their registration procedures for third party authentication providers such as OpenID.
    i. Require social networks to delete or correct user information at any time at the request of the user.

j. Prohibit social networks from targeting via advertisements children under 16 or sites where those under 16 predominate. Invitations must not be issued to those under 13 where age is known.
k. Introduce new rights: the right to be "forgotten" i.e. a right to have one's data deleted for good and the right to data portability i.e. the right to recover and/or to shift from one platform/cloud to another data posted (e.g. photos)

2. Initiate pro-active co-operation between relevant EU and US agencies to achieve better harmonization of regulatory practices and privacy protection. This is particularly important since most of the social networks operate on both sides of the Atlantic. Different regulatory practices create confusion for users and reduce their effectiveness in a global environment.

3. Raise awareness about the potential risks in particular regarding privacy in using social networks and educate the public how individuals can protect their privacy. Also require that these messages are made available on the social network sites (consumer education about privacy).[1]

4. Improve enforcement of existing rules and regulation. The lack of enforcement renders current EU privacy policies ineffective and gives individuals a false sense of security. In the United States, the Children's Online Privacy Protection Act (COPPA) is easily circumvented in practice. COPPA is, for example, not classifying cookies as online information. In the EU, privacy protection authorities lack sufficient resources and the sanctions available are weak.

5. Encourage development of global guidelines for online advertising, sales promotions and direct marketing to children in social networks, starting within the OECD.

6. Commission research and inquiries into today's online marketing system, identifying and assessing the strategies being used on social networks, video channels, online games and virtual worlds.

7. Explicitly prohibit, through regulation, online marketing practices that have been proven, through such research, to have a negative impact on people - and in particular children's - cognitive and emotional development. For example, there should be no digital marketing of food and beverage products that have been identified as contributing to childhood obesity epidemic.

**Social network operators should:**

1. Integrate privacy and security by design. This means that the default settings should ensure maximum privacy for users by minimizing the disclosure of personal information and that the sites should use state of the art measures to prevent attacks and unwanted access to users' profiles.[2] [3]

2. Enable consumers to always remain "masters of their data". For example, if users cancel their membership, the stored data should be completely deleted. In cases in which the user wants to delete data, the social network operator should not put any obstacles in place. This principle also applies for references by users or applications to user profiles: before any content links to a user's profile, the user has to be prompted by default and asked for his/her permission.

3. Prevent the readout of personal data by search engines and third parties by default. Without the user's explicit permission, no data should be available to crawlers.

4. Develop common binding ethical codes for behavioral tracking and advertising online in co-operation with consumer organisations. These should include providing prominent, clear statements that data is being collected for commercial purposes.

---

[1] The EU Safer Social Networking Principles include steps into the right direction but do not pay sufficient attention to privacy issues and set adequate standards.
http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

[2] Recent research by isecLAB has shown that ostensible insensitive information such as group membership may lead to profiling and de-anonymization of users.
http://www.iseclab.org/papers/sonda-TR.pdf

[3] The maximum privacy requirement is already part of the EU's Safer Social Networking Principles' demand, but is not implemented on most of the platforms.

5. Develop industry codes that include detailed provisions for standardized disclosure content, guidelines for easy-to-understand privacy policies, and rules on free offers.

6. Provide tracking-free versions.

**Brief Background**

**Introduction**

The content and choices to be found in the Internet are no longer just "consumed." Thanks to fast Internet access, such services are now used interactively. It is not necessary to program a personal homepage in order to provide information about oneself and communicate with others. The "interactive-web" makes it possible for individuals to actively use and participate in the Internet. Virtual life adds another element to real life.

There are hundreds of social networks on the Internet. Social networks such as nasza-klasa.pl, studiVZ.de, facebook.com, and myspace.com provide a means to exchange information among members. These portals enable users to set up their own personalised profile pages with information such as their resumes, photos, hobbies and contact details and to network with others. They may be topic-oriented (music, cars, animals, health, sports, books, travel) or target group-oriented (college students, schoolchildren or business portals), but nevertheless they are usually open to anyone. On some portals, one can only register after having been invited by another user who is already registered. Most social networking portals are free of charge; some charge a small fee (e.g. so-called premium members at Xing or LinkedIn).

**Figures and Facts**

According to a study by the Universal McCann Agency from July 2009, 62.5 percent of the Internet users worldwide use social networks. The percentage of users has grown rapidly from 2007 when it was 36.2 percent worldwide. 22,729 users from 38 countries were surveyed in this study.[4]

Facebook for example is announcing 211.741.580 users on it's advertisement platform by March 9th 2010 – just from the US and EU member states.
Estimated earnings through social networks supposedly reached 965 million US Dollars in 2007; by 2012 this sum was projected to increase to 2.4 billion but recent figures show that the worlds largest social network provider Facebook only might reach 1 billion in revenues in 2010.[5] [6]

According to an investigation by PricewaterhouseCoopers AG (PwC), in 2008 71 percent of registered social network users participated in multiple networks.[7] Seventy percent of those users said they want to remain members in their most important Internet social networks "forever." Their willingness to pay is rather low and advertising is accepted in preference to membership fees. The acceptance of services paid by advertising is in our view explained by the lack of knowledge about how user data is analysed and how this can have a negative impact on peoples' privacy. Consumers therefore should have choice.

The existing study material and data clearly show the symbiosis between users and platform operators. For the Internet user, membership in at least one social network has gained in social importance. At the same time, these platforms are developing into lucrative sources of income for the advertising industry. Unlike traditional advertising, social networks on the Internet offer a highly efficient opportunity for targeted and personalised advertising. Some of them even use profile information of users for advertising (on) their platform, i.e. Facebook. This very new quality of advertising requires attention on both legislative and executive levels.

---

[4] http://universalmccann.bitecp.com/wave4/Wave4.pdf
[5] http://www.cio.de/markt/uebersichten/845681/;
http://www.focus.de/digital/Internet/studie-Soziale-netzwerke-boomen_aid_299612.html
[6] http://www.insidefacebook.com/2010/03/02/facebook-made-up-to-700-million-in-2009-on-track-towards-1-1-billion-in-2010/
[7] http://www.pwc.de/portal/pub/!ut/p/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLd4p3djUBSZnFG8Q76kfCRIL0vfV9PfJzU_UD9AtyI8odHRUVASpBSEg!/delta/base64xml/L3dJdyEvd0ZNQUFzQUMvNElVRS82X0JfQ0VS?siteArea=49c4e4a420942bcb&content=e51fa203db61223&topNavNode=49c4e4a420942bcb

With the pressure of competition, the social network operators are forced to offer their users incentives - for example in form of features - for the continuing use of their platforms. However, there have been controversies which reflect the immense economic and competitive pressure that the platform operators are under and the fight to keep the users on the platform at any cost. In one scandal, the database of StudiVZ including information on 2 million users was published on peer to peer platforms. The platform lacked even basic security features. Platform operators are increasingly changing the Terms of Use and Privacy Terms to the disadvantage of the user or targeting advertising to members based on their online activities without their permission. Facebook was subjected to public pressure in March 2009 when its new Terms of Service seriously discriminated against its users.

Social networks are also a popular target for hackers and data thieves. There are questions about whether platform operators are devoting sufficient resources to security or whether users are bearing the costs for inadequate protection of their personal data. A study by the Fraunhofer Institute SIT showed that operators of social networks require a significant amount of personal data from their users during registration but offer very little protection from unwanted access to that information.[8] The German pupils network SchülerVZ had to admit that more than hundred thousand and even some ten thousand 'protected' profile data sets were crawled during automated attacks in 2009,[9] one year after the security problem was published by Fraunhofer SIT.

**Challenges posed by social networks**

Although social networks serve as an important instrument for interactive communication and have become part of the cultural norm, they also create many challenges for users.

Data protection

The business models for social networks are based on using the data of registered members in a way that is not always transparent and where no conscious consent for the use has been obtained. That data includes information that has been entered by the users themselves on their profile pages and also clickstream analysis from their activities on the networks and possibly also gathered from other sites on the web. Platform operators use that data to create profiles of their users for target-oriented, personalised advertising. Their Privacy Terms are usually formulated so broadly that consumers do not understand exactly how information about them will be used[10]. It is quite common for the use of the platform to be contingent on agreeing to have one's data used for advertising purposes, whether by the platform operators themselves or by third parties. In some cases, personal profile pages are visible to anyone, not just to so-called friends and acquaintances. Platform operators sometimes offer the ability to restrict access to users' personal information. However, this is often presented as an opt-out. Users' data has sometimes been used for purposes other than that to which they originally agreed. It is also vulnerable to being targeted by identity thieves and hackers.[11]

Furthermore, many Internet users are not aware that the net "doesn't forget" and that in spite of believing that all data is deleted, it is saved in another place and possibly even retrievable on the Internet. Social network services providers have the ability to remove user data from their servers, but some are reluctant to do so.

---

[8] http://www.stern.de/computer-technik/Internet/:Datensicherheit-Netzwerken-Mein-Freund-Datenh%E4ndler/636203.html

[9] http://www.vzbv.de/go/presse/1225/36/102/index.html

[10] A study produced by the Consumer Council of Norway documents that consumers generally do not understand the terms of service that is offered by their favourite social networks, http://www.sintef.no/upload/Konsern/Media/Person%20og%20forbrukervern.pdf

[11] http://www.webnews.de/kommentare/137277/0/Hacker-attackieren-MySpace-Nutzer.html
http://www.stern.de/computer-technik/Internet/:Soziale-Netzwerke-Der-Spion,/641364.html
http://www.pcwelt.de/start/sicherheit/virenticker/news/187901/ein_wurm_geht_auf_myspace_und_facebook_um/
http://www.tecchannel.de/sicherheit/news/1738627/myspace_hack_musiker_seiten_verbreiten_malware/
http://www.abzocknews.de/2008/07/14/studivz-identitatsklau-im-online-netzwerk/
http://www.tagesanzeiger.ch/digital/Internet/Wuermer-Hacker-Betrueger-Facebook-in-Gefahr/story/16501875;
http://www.heise.de/newsticker/Soziale-Netzwerke-im-Visier-der-Kriminellen--/meldung/106173
http://www.call-magazin.de/multimedia/multimedia-nachrichten/steigende-zahl-von-spam-angriffen-auf-soziale-netzwerke_23662.html

Data protection is crucial in all social networking portals. The challenges to traditional privacy concepts, despite all varieties in the different cultural heritages, constitute severe problems to almost all citizens. Children in particular may not understand the consequences of providing their personal information and lack the capacity to agree to its use for marketing or other purposes.[12]

Advertising

Social networking platforms are usually not charitable organisations; they are businesses. They profit from targeted personalised user advertising and have sometimes used information about users' purchases without their knowledge to advertise to other users. During the purchase of a product in an online shop that is linked to the platform, and under the catchword "trustworthy advertising"/"recommendation", all members defined as a friend on the profile page of the buyer are informed about the purchase with the goal of having them purchase the item as well.[13] Many of the Social Network platforms also reveal users' online behavior to so called 'behavioral targeting' companies, analyzing online behavior for marketing purposes.

Application Developers

Application developers are given access to far more user data by social network services than is necessary to provide the application offered.[14] This practice creates a serious and unnecessary privacy risk and violates the principle of least authority, a security design principle that states that an actor should only be given the privileges needed to perform a job. "In other words, an application that doesn't need private information shouldn't be given any."[15] Similar concerns arise with the collection of personally identifiable data by advertisers.

Mobile Applications

Many social network providers offer their clients an application for mobile use. These mobile versions often enable members the ability to upload their phonebooks to the social network platform. The social network providers can store and process that data for their own purposes, even though the individuals to whom the data pertains may not have relationships with the social network providers and never gave their consent. This violates the principle that individuals should have control of their personal data.

Children and minors[16]

Social networking platform operators that mainly direct their services at children and minors are currently not required on principle to follow special regulations in regard to data protection or advertising. This lack of constraints poses the risk that minors and children will be taken advantage of. According to a study by the Institut für Demoskopie (Institute for Opinion Surveys) in Allensbach (IfD) from the year 2008, half of all teenagers between the ages of 14 and 19 are active in an online community.[17] Ofcom research (March 2010) shows that a quarter or children aged 8 -12 are active on social networking sites.

**Insufficient action taken by EU and US governments**

In February 2009 the EU Commission together with a number of providers of social network services published the Safer Social Networking Principles for the EU.[18] The document outlines the principles by which providers of social network services should be guided to minimise potential harm to children and young people, and recommends a range of good practice approaches. Furthermore, in March 2009

[12] According to the report and the data protection in social networks recommendation from the International Working Group on Data Protection in Telecommunications from March 3 – 4, 2008 in Rome (Italy; „Rome memorandum")

[13] http://www.faz.net/s/RubE2C6E0BCC2F04DD787CDC274993E94C1/Doc~E4868361D131740FBA8E380E7C7B3A8DC~ATpl~Ecommon~Scontent.html

[14] http://www.cs.virginia.edu/felt/privacy

[15] Id.

[16] See also TACDs Resolution on Marketing to Children Online (Infosoc 38-09) http://www.tacd.org/index2.php?option=com_docman&task=doc_view&gid=207&Itemid=40

[17] http://www.spiegel.de/netzwelt/web/0,1518,584572,00.html

[18] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

the German Freiwillige Selbstkontrolle Multimedia-Diensteanbieter published a new codex for social network service providers.[19]

While we recognise the EU Commission's attempts to better protect consumers in social networks and the initiatives of industry, codes of conducts and self-regulations alone are insufficient means to address the challenges posed by social networks. In light of the rapid development of new technologies changes to legislation are necessary and enforcement needs to be improved. The first report on the implementation of the Safer Social Networking Principles has shown that almost all providers are even in the light of the modest criteria chosen just partially complying with the SSNP. It is merely a sign of weak criteria definition that 'not compliant' is a rare exception. Instead of making social networking sites safe, the providers even fail to comply with the still low standards they agreed on.[20]Implementing the requirements of this resolution as well as the requirements defined in the Madrid Declaration[21] as of 3rd of November 2009 is a first step towards a more user friendly online environment, making the real and the digital world a place where consumers do not have to fear less about abuse of their data and securing the trust in providers which we believe is the common ground for the economy of the 21st centuries information society markets.

[19] http://www.fsm.de/de/Web_2_0

[20] http://ec.europa.eu/information_society/activities/social_networking/eu_action/implementation_princip/index_en.htm

[21] http://thepublicvoice.org/madrid-declaration/