COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION

To the
COUNCIL OF EUROPE COMMITTEE OF EXPERTS ON NEW MEDIA

Regarding
THE RECOMMENDATION AND GUIDELINES TO PROTECT AND PROMOTE HUMAN RIGHTS WITH REGARD TO SOCIAL NETWORKING SERVICES
MC-NM(2010)003_en

The Electronic Frontier Foundation (EFF) is pleased to have the opportunity to submit comments to the Council of Europe Committee of Experts on New Media on the currently available version of the proposal for the Draft Recommendation and Guidelines on measures to protect and promote respect for human rights with regard to social networking services (MC-NM(2010)003_en).

EFF is an international civil society non-governmental organization with more than 14,000 members worldwide, dedicated to the protection of citizens' online civil rights, privacy, and freedom of expression. EFF engages in strategic litigation in the United States and works in a range of international and national policy venues to promote balanced laws that protect human rights, foster innovation and empower consumers. EFF is located in San Francisco, California and has members in 67 countries throughout the world.

EFF commends the Council of Europe for working to protect and promote respect for human rights with regards to social networking services. We agree with many of the basic findings of the recommendations and guidelines which note that social networking services are key tools for "receiving and imparting information." We concur with the statements that individuals "have to be sure that their rights to private life will be protected when they use social networking services and that their personal data will not be misused," and that social network providers should respect "the right to freedom of expression, the right to privacy and secrecy of correspondence." We also recognize that governments might take narrowly tailored

exceptional actions based on the limitations to freedom of expression established in international law, in particular Article 19 of the United Nations International Covenant on Civil and Political Rights and Article 10 of the European Convention on Human Rights.

While we commend the Council of Europe for working to protect and promote respect for human rights by social networks providers, we wish to express caution on some of the provisions as currently drafted and to respectfully provide additional suggestions that can be included.

DRAFT RECOMMENDATION ON MEASURES TO PROTECT AND PROMOTE RESPECT FOR HUMAN RIGHTS WITH REGARD TO SOCIAL NETWORKING SERVICES

We commend the Council of Europe for:

- Recognizing that social networking services "are a tool for expression but also for communication between individuals."
- Recognizing that social networking services "offer great possibilities for enhancing the individual's right to participate in political, social and cultural life."
- Recognizing "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."
- Supporting the Committee of Ministers' recommendation to the Member States to "develop and promote coherent strategies to protect and promote human rights." In particular, "ensuring users are aware of possible challenges to their human rights on social networking services," to encourage "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."

EFF has proposed a "Bill of Privacy Rights for Social Network Users," which stresses that individuals have the right "[t]o see readily who is entitled to access any particular piece of information about themselves," (…) including "government officials, websites, applications, advertisers and advertising networks and services." Moreover, "[w]henever possible, a social network service should give users notice when the government or a private party uses legal or administrative processes to seek information about them, so that users have a meaningful opportunity to respond."[1]

Therefore, we respectfully suggest that the Committee of Ministers recommend member states to take the following actions:

[1] Kurt Opsahl, A Bill of Privacy Rights for Social Network Users, Electronic Frontier Foundation, 2010, available at <http://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users>.

- Adopt strong legal safeguards and due process before disclosure of individuals' data to governmental entities. Government access should be done only upon receipt of a court order, in accordance with international legal norms and instruments relevant to the protection of private life.
- Allow and encourage social networks to notify the person whose social networking records are sought whenever possible. Social networks should agree to a timetable for disclosure to the party requesting data in order to provide a reasonable opportunity for the individual to file an objection with a court before disclosure.
- Foster transparency on the disclosure of citizens' data pursuant to a governmental or private party request. The guidelines should encourage social networks to publicly disclose an accounting of the nature and frequency of governmental and private party requests for access to citizens' data.[2]
- Foster transparency on requests for content removal or the censorship of content. The guidelines should encourage social networking services to publicly disclose the nature and frequency of content removal or requests to censor content, including the justification (e.g., court order, violation of terms of service or other category, if applicable).
- Foster transparency on social networking services' guidelines for law enforcement seeking to request information about users.
- Any government request to get access to users' personal data should include a provision to remunerate a social networking service. This obligation will not only compensate the company for the additional work required to fulfill the request, but will also incentivize governments towards mitigating on the possibility of unlimited requests.

APPENDIX – GUIDELINES FOR SOCIAL NETWORKS PROVIDERS

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

While we agree that the "core conditions" should be written in "a form and language" that is "appropriate to and easily understandable by, the group of social networks sites," we also believe that those terms of services should be accessible in the users' native language since those terms of services condition individuals to the policies' contents upon his or her consent. For example, Facebook's site has been translated in more than 80 languages while the Terms of Services is available only in less than 10 languages.

2. Appropriate protection of children against harmful content and behavior

2.1 Age-verification creates more privacy risks rather than protect privacy

[2] *See* Google Transparency Report, <http://www.google.com/transparencyreport/>.

EFF agrees that age-verification access raises numerous human rights concerns.[3] In particular, the guidelines correctly emphasize that, "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."

Age-verification access intended to protect privacy would, ironically, create more privacy risks. There are already several challenges to protecting privacy against the largely invisible, poorly understood, and continually escalating surveillance of adult's online activities, let alone those of children.[4] A study has identified the unintentional and indirect leakage of personal data via social networking services to third-party aggregation servers. The study also noted that this leakage is also being shared with external online social networking applications, which not only have access to a user's profile information, but also leak a user's social networking identifier to other third parties.[5]

Moreover, age verification processes curtail children's freedom of expression rights, including older children's right to read anonymously. Older children may have ideas that they want to learn that they might not tell their parents about, and leaking more personal information, such as age, will only increase privacy risks for them.[6]

3. Ensuring users' control over their data

3.1 Informed consent

To complement point 5 on the right of users to control their data, EFF "Bill of Privacy Rights for Social Network Users" says:

"Social network services must ask their users' permission before making any change that could share new data about users, share users' data with new categories of people, or use that data in a new way. Changes like this should be "opt-in" by default,

---

[3] *See* Ctr. for Democracy & Tech, Electronic Frontier Foundation, The Progress & Freedom Found., Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule (June 30), <http://www.eff.org/files/coppacomments.pdf>.

[4] *See* Seth Schoen, New Cookie Technologies: Harder to See and Remove, Widely Used to Track You, Electronic Frontier Foundation, September 14, 2009, <https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide>. Peter Eckersley, How Online Tracking Companies Know Most of What You Do Online (and What Social Networks Are Doing to Help Them), Electronic Frontier Foundation, September 21, 2009. https://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks.

[5] *See* Balachander Krishnamurthy, Craig E. Wills, On the Leakage of Personally Identifiable Information Via Online Social Networks, available at <http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf>.

[6] *See* Rebecca Jeschke, Don't Turn COPPA Into Age-Verification Mandate, Electronic Frontier Foundation, July 2, 2010, available at <http://www.eff.org/deeplinks/2010/07/dont-turn-coppa-age-verification-mandate>.

not "opt-out," meaning that users' data is not shared unless a user makes an informed decision to share it. If a social network service is adding some functionality that its users really want, then it should not have to resort to unclear or misleading interfaces to get people to use it."[7]

3.2 Clear user interface

We also ask the Council of Europe to encourage social networks providers to provide a clear user interface that allows users to effectively exercise their rights. Users should have "the right to a clear user interface that allows them to make informed choices about who sees their data and how it is used."[8] Professor Greg Conti has pointed out that a good interface is designed to help users achieve their goals without impediments. However, an "evil" interface is conceived to deceit users into doing things they do not want to.[9] There are many examples of obscure user interfaces, such as Facebook's instant personalization changes and GoogleBuzz which forced Gmail users to share their email contacts and threatened to move private GMail recipients into a public "frequent contacts" list, or Facebook instant personalization changes, are a few examples.[10]

3.3 Transparency on social networking records requests

To address concerns of privacy violations, lack of transparency and public oversight mechanisms on social networking data requests, we respectfully want to repeat our above recommendation:

- Adopt strong legal safeguards and due process before disclosure of individuals' data to governmental entities. Government access should be done only upon receipt of a court order, in accordance with international legal norms and instruments relevant to the protection of private life.
- Allow and encourage social networks to notify the person whose social networking records are sought whenever possible. Social networks should agree to a timetable for disclosure to the party requesting data in order to provide a reasonable opportunity for the individual to file an objection with a court before disclosure.

---

[7] *Supra* note 1

[8] *Supra* note 1.

[9] Professor Greg Conti, Evil Interfaces, Hackers On Planet Earth conference, 2008, <http://wiki.hope.net/TheLastHOPE/Talks#Evil_Interfaces:_Violating_the_User>. *See also*, Tim Jones, Facebook's "Evil Interfaces," Electronic Frontier Foundation, April 29, 2010, available at <http://www.eff.org/deeplinks/2010/04/facebooks-evil-interfaces>.

[10] FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network, March 30, 2011, Federal Trade Commission, available at <http://www.ftc.gov/opa/2011/03/google.shtm>. Kurt Opsahl, How to Opt Out of Facebook's Instant Personalization, Electronic Frontier Foundation, April 22, 2010, available at <http://www.eff.org/deeplinks/2010/04/how-opt-out-facebook-s-instant-personalization>.

- Foster transparency on the disclosure of citizens' data pursuant to a governmental or private party request. The guidelines should encourage social networks to publicly disclose an accounting of the nature and frequency of governmental and private party requests for access to citizens' data.
- Foster transparency on requests for content removal or the censorship of content. The guidelines should encourage social networking services to publicly disclose the nature and frequency of content removal or requests to censor content, including the justification (e.g., court order, violation of terms of service or other category, if applicable).
- Foster transparency on social networking services' guidelines for law enforcement seeking to request information about users.
- Any government request to get access to users' personal data should include a provision to remunerate a social networking service. This obligation will not only compensate the company for the additional work required to fulfill the request, but will also incentivize governments towards mitigating on the possibility of unlimited requests.

3.4 Enable by default site-wide SSL and security breach notification

The guidelines correctly point out the importance for social networking providers to "apply state of the art security measures." We respectfully request the Council of Europe to recommend member states to encourage social network providers to enable site-wide SSL by default to protect users' information and communications from eavesdropping.

In addition to enabling default site-wide SSL, social networking services should inform users and national data protection authorities about any security breach affecting their users.

Security breach notification can be an important tool for helping to ensure online security. For example, during the Tunisian revolution, the Tunisian government launched an attack on activists that stole the usernames and passwords of Tunisians logging in to Google, Yahoo, and Facebook.[11] The Tunisian government then logged in to Tunisians' email and Facebook accounts. During this period of time, EFF urged Facebook, Google, and Yahoo to take concrete steps as quickly as possible to inform and better protect their users against the breach.

3.5 The privacy policies dilemma

The problems with privacy policies are serious. In many cases, the privacy policies of social networking services lack a definition of critical terms or broadly state the purposes of data collection (e.g., "to provide you with a better experience") to allow

[11] Eva Galperin, EFF Calls for Immediate Action to Defend Tunisian Activists Against Government Cyberattacks, Electronic Frontier Foundation, January 11, 2011, available at <https://www.eff.org/deeplinks/2011/01/eff-calls-immediate-action-defend-tunisian>

limitless uses of personal data.[12] Therefore, EFF believes that vague justifications such as providing "a better user experience" tell individuals nothing useful for them to make an informed decision about the use of their personal data.

We agree with guidelines that call for "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." We want to repeat our concerns, however, about the need to provide privacy policies in the user's native language.

3.6 Deletion of profiles

We want to commend the Council of Europe for requesting that social network services "make sure that users are able to completely delete their profile and all data stored about and from them in a social networking service." As we have said in our "Bill of Privacy Rights for Social Networking Users," a user should have the right to delete data or her entire account from a social network service. It should be permanently eliminated from the service's servers. Social network services should not disable access to data while continuing to store or use user's data. The data should be permanently eliminated from the service's servers. Furthermore, if users decide to leave a social network service, they should be able to easily, efficiently and freely take their uploaded information away from that service and move it to a different one in a usable format. This concept is fundamental to promote competition and ensure that users truly maintain control over their information, even if they sever their relationship with a particular service.[13]

3.7 Data Minimization

A social networking service should limit the collection of personal data, including transactional data and location data to the minimum amount necessary to provide services. They should store personal information for the minimum time necessary for the purpose of their operations. A social networking service should effectively obfuscate, aggregate and delete unneeded or unused user personal information about users. They should also maintain written policies addressing those personal data collection and retention minimization policies. Policies should clearly specify the kind of data collected, the period of retention, and avoid the use of general or vague terms that promote the limitless use of data.[14]

Law must provide any restriction on the right to privacy. For a restriction to be permissible, the restrictive measure must be necessary in a democratic society. It is not enough that the restriction serves one of the enumerated legitimate aims; the

---

[12] *See* CDT-EFF, Proposed Smart Grid Privacy Policies and Procedures 5-9 (California Public Utility Commission Rulemaking 08-12-009) (Oct. 15, 2010) (Attached as "Exhibit 1 of 1").
[13] *Supra* note 1.
[14] Electronic Frontier Foundation, Best Practices for Online Service Providers, June 28, 2011, available at <http://www.eff.org/wp/osp>.

restriction must be necessary for reaching the legitimate aim. The restriction must comply with the principle of proportionality; the restriction must be appropriate to achieve its protective function; it must be the least intrusive instrument amongst those that might achieve the desired result; and the restriction must be proportionate to the interest that is to be protected.[15]

Therefore, legal frameworks that compel social networking services to retain personal data, including transactional data and subscription information, may be in violation of Article 17 of the United Nations International Covenant on Civil and Political Rights and the European Convention on Human Rights.[16]

3.8 Freedom of Expression: Anonymity and Pseudonymity

We also commend the Council of Europe for asking a social networking service to "consider allowing the possibility of pseudonymous profiles." In particular, we are pleased to read the "Declaration on freedom of communication on the Internet" which supports anonymity and pseudonymity.[17] In the Declaration, the Committee of Ministers stress 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."

Throughout history, individuals have been writing in anonymous or pseudonymous ways. Anonymous and pseudonymous expression allows individuals to express unpopular opinions, honest observations, and otherwise unheard complaints. Individuals may decide to communicate anonymously or pseudonymously out of

---

[15] Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," p11, available at <http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf>. See also General Comments No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999, available at <http://www.unhchr.ch/tbs/doc.nsf/0/6c76e1b8ee1710e380256824005a10a9?Opendocument>.

[16] Digital Civil Rights in Europe, French Decree Establishes What Data Must Be Retained By Hosting Providers, EDRi-gram - Number 9.5, March 2011, available at <http://edri.org/edrigram/number9.5/data-retention-hosting-france>. *See also* [Norwegian] Protests greet new data storage law, April 5, 2011, available at <http://www.newsinenglish.no/2011/04/05/noisy-protests-greet-data-storage-law/>. *See also*, European Comission Home Affairs, Taking on the Data Retention Directive, available at <http://www.dataretention2010.net/docs.jsp>. *See* Report of The Data Retention Conference, 'Towards The Evaluation Of The Data Retention Directive', Brussels, 14 May 2009, available at <http://www.dataretention2010.net/files/Data_Retention_Directive_conference_14_May_2009_report_final.doc>.

[17] Declaration on freedom of communication on the Internet, available at <https://wcd.coe.int/wcd/ViewDoc.jsp?id=37031>.

concern about political or economic retribution, harassment, or even threats to their lives.

Unfortunately, Facebook's Terms of Service requires Facebook users to provide their real names and information.[18] This practice creates serious risks particularly for dissidents and human rights workers in developing democracies who are compelled to use their real names on Facebook, especially those countries with weaker democracies, and authoritarian regimes.[19] Facebook's real name policy creates a double negative effect: if Facebook's Terms of Service are violated for using a pseudonym, Facebook can disable an individual's account, shutting down a key avenue for political discourse.[20] For example, the administrator of the "We Are All Khaled Said," Facebook page used a pseudonym. The page encouraged its fans to document the Egyptian elections. However, the administrator's Facebook account was deactivated just prior to the elections; the takedown of his account resulted in the temporary takedown of the Facebook page.[21] The Michael Anti case is another example. Michael Anti is the pseudonym of a former journalist, who has used this nickname for more than 10 years. Facebook deactivated his account and cut him off from a network of more than 1,000 contacts who know him as Anti.[22]

3.9 Government Uses of Social Networking Services for Investigations and Beyond

Several news reports have made it clear that governments use social networking services as a tool for investigation.[23] The lack of transparency about how the

---

[18] Facebook, Statement of Rights and Responsibilities, available at <https://www.facebook.com/terms.php>.

[19] Jillian C. York, Policing Content in the Quasi-Public Sphere, Open Net Initiative, page 10, <http://opennet.net/sites/opennet.net/files/PolicingContent.pdf>.

[20] Eva Galperin, EFF Calls for Immediate Action to Defend Tunisian Activists Against Government Cyberattacks, EFF, January 2011, available at <https://www.eff.org/deeplinks/2011/01/eff-calls-immediate-action-defend-tunisian>.

[21] Mike Giglio, Middle East Uprising: Facebook's Secret Role in Egypt, The Daily Beast, February 24, <http://news.yahoo.com/s/dailybeast/20110225/ts_dailybeast/12602_middleeastuprisingfacebooksbackchanneldiplomacy_1>.

[22] Tiny Tran, Activist Michael Anti Furious He Lost Facebook Account--While Zuckerberg's Dog Has Own Page, Huffington Post, August 3, 2011, available at <http://www.huffingtonpost.com/2011/03/08/michael-anti-facebook_n_832771.html>.

[23] *See* Laura Saunders, Is 'Friending' in Your Future? Better Pay Your Taxes First, The Wall Street Journal, Lacrosse Tribune, August 27, 2009, available at <http://online.wsj.com/article/SB125132627009861985.html>. *See also* KJ Lang, Facebook friend turns into Big Brother, November 19, 2009, available at <http://lacrossetribune.com/news/local/article_0ff40f7a-d4d1-11de-afb3-001cc4c002e0.html>.

personal data is collected used, for how long it is kept, and who has access to it make the problem even worse.[24]

EFF, with help from the Samuelson Clinic at the University of California Berkeley Law School, made a series of US Freedom of Information Act (FOIA) requests asking various US law enforcement agencies to disclose documents detailing their use of social networking sites in their investigations.[25] The documents disclosed through this project revealed, among other things, Citizenship and Immigration's surveillance of social networks to investigate citizenship petitions and the DHS's use of a "Social Networking Monitoring Center" to collect and analyze online public communication during President Obama's inauguration. The center monitored social networking sites for "items of interest."[26]

In addition, we have found guidelines revealing how several US social networking services handle requests for user information such as contact information, photos, IP logs, friend networks, buying history, and private messages.[27] The guides we have received through EFF FOIA requests show that social networking sites have struggled to develop consistent, straightforward policies to govern how and when they will provide private user information to law enforcement agencies. The guides also show how those policies have evolved over time.[28] We should emphasize that many of those guidelines are not made available to the public by social networking services. It is worth pointing out that only Craigslist's and Twitter's guides are posted on their websites.

In addition to using this information on social networking sites for law enforcement investigations, the US government has been considering using it for all background checks in security clearances.[29] With just a name, address, date of birth, and social security number, government-hired Internet investigators were able to find "noteworthy" search results for as many as 53% of the 349 study participants. "Noteworthy" information included the proclivity to put personal information

---

[24] *See also,* Electronic Frontier Foundation, Lawsuit Demands Answers About Social-Networking Surveillance, December 1, 2009, available at <https://www.eff.org/press/archives/2009/11/30>.

[25] Electronic Frontier Foundation, FOIA: Social Networking Monitoring Site, available at <https://www.eff.org/foia/social-network-monitoring>

[26] Electronic Frontier Foundation, Lawsuit Demands Answers About Social-Networking Surveillance, December 1, 2009, <https://www.eff.org/press/archives/2009/11/30>.

[27] Jennifer Lynch, Social Media and Law Enforcement: Who Gets What Data and When?, Electronic Frontier Foundation, January 20, 2011, available at <https://www.eff.org/deeplinks/2011/01/social-media-and-law-enforcement-who-gets-what>.

[28] *See* EFF comprehensive spreadsheet that compares how social networking services handle requests for user information such as contact information, photos, IP logs, friend networks, buying history, and private messages, available at <https://www.eff.org/files/EFF_Social_Network_Law_Enforcement_Guides-sprdsht.pdf>.

[29] Electronic Frontier Foundation, FOIA: Office of the Director of National Intelligence, available at <https://www.eff.org/files/20100514_odni_socialnetworking.pdf>.

online, but also included so-called "questionable" material such as disclosure of "underage drinking, profanity, and extreme religious and/or political views on public forums." Social networking sites like MySpace were also included in the background investigations.[30]

These techniques raise questions about the limits and appropriate accountability concerning the ways in which government agencies and law enforcement officials collect and analyze information about individuals online.

4. Conclusion

EFF respectfully asks the Council of Europe to revise its guidelines and recommendation to ensure that social networking services will protect privacy vis-à-vis the government, foster transparency on the disclosure of citizens' data pursuant to a governmental or private party request, foster transparency on requests for content removal or the censorship of content, foster transparency on social networking services' guidelines for law enforcement seeking to request information about users. EFF also asks the Council of Europe to ensure that freedom of expression rights, including the readers' rights to use social networking services anonymously be respected, and not curtailed, by social networking services. The Council of Europe should also ensure appropriate accountability concerning the ways in which government agencies and law enforcement officials collect and analyze information about individuals online. Finally, any government request to get access to users' personal data should include a provision to remunerate a social networking service. This provision will incentivize governments towards mitigating on the possibility of unlimited requests.

EFF would be pleased to answer any questions on these matters.

Thank you for your consideration.

Katitza Rodriguez Pereda
International Rights Director
Electronic Frontier Foundation
katitza@eff.org | https://www.eff.org

[30] Jennifer Lynch, Government Finds Uses for Social Networking Sites Beyond Investigations, Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2010/08/government-finds-uses-social-networking-sites>.