Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Resolution 1986 (2014)[1]
Final version

Improving user protection and security in cyberspace

Parliamentary Assembly

1. The Parliamentary Assembly is concerned that the further development and exploitation of cyberspace is still taking place without adequate protection of the rights and interests of the weakest stakeholder in this process: the individual user.

2. Users of online services have been alarmed by numerous intrusions into their personal data and correspondence by public authorities, commercial companies and also private individuals. Widely publicised examples have been the interception of communication and the screening of user data by national security services in Europe and the United States, the professional data mining of online social networks, the commercial profiling of users by online service providers through Internet access data and geo-localisation data, as well as the large-scale hacking into user accounts and passwords for fraudulent purposes.

3. The Assembly regrets that these attacks on the security and integrity of online and mobile communication services have deeply undermined the trust of users in Internet services. Therefore, it calls on all member and observer States to immediately launch, in co-operation with the Internet and online industry, a global initiative for improving user protection and security in cyberspace. The Internet has no national borders; we must therefore act together in order to ensure respect for universal human rights, as well as for national law and sovereignty. The objective must be an internationally agreed legal framework with appropriate enforcement mechanisms, including protection for whistle-blowers who disclose violations.

4. The Assembly therefore welcomes the Resolution on the right to privacy in the digital age, adopted by the United Nations General Assembly on 18 December 2013. The Assembly concurs that the same rights which people have offline must also be protected online, in particular the right to privacy as expressed in its Resolution 1843 (2011) on the protection of privacy and personal data on the Internet and online media.

5. Welcoming the Montevideo Statement on the Future of Internet Cooperation of 7 October 2013, the Assembly agrees that the globalisation of the Internet Corporation for Assigned Names and Numbers (ICANN) and its Internet Assigned Numbers Authority (IANA) must be accelerated, towards an environment in which all stakeholders, including governments, participate on an equal footing. Associations of users and citizens should be represented on this new body. Global governance of the Internet is to be improved. An international charter on the global principles and objectives of the Internet is to be drawn up. It will, in particular, ensure respect for personal data, including biological data, as well as respect for human rights. This process should be supported by the Council of Europe at the level of the European Union and the United Nations in order to guarantee the independence of critical Internet infrastructure from individual governments.

6. The Assembly recommends that all member and observer States ensure the effective implementation of the following principles:

6.1. everyone's private life, correspondence and personal data must be protected online; users shall always have the possibility to withdraw data, content and information; interception, surveillance, profiling or storage of user data by public authorities, commercial entities or private persons is only

1. *Assembly debate* on 9 April 2014 (14th Sitting) (see Doc. 13451, report of the Committee on Culture, Science, Education and Media, rapporteur: Mr Axel E. Fischer; and Doc. 13481, opinion of the Committee on Legal Affairs and Human Rights, rapporteur: Mr Arcadio Díaz Tejera). *Text adopted by the Assembly* on 9 April 2014 (14th Sitting).
See also Recommendation 2041 (2014).

permissible where allowed by law in accordance with Article 8 of the European Convention on Human Rights (ETS No. 5); member States have a positive obligation to ensure adequate legal protection against the interception, surveillance, profiling and storage of user data; personal data archives must be subject to precautionary measures to protect them from data theft and fraud;

6.2. collection, storage and processing of so-called metadata (data that describes other data, for example information on senders, recipients, timing, key words, movements or contacts) shall be subject, in principle, to the same rules as the collection, storage and processing of any other personal data;

6.3. producers of access devices and online service providers should automatically apply encryption and conditional access technologies as well as tools against online viruses and automatic signs ("cookies"); the duration of the latter should be time-limited; special protection should be afforded by providers of wireless access points ("hotspots") as well as for personal data produced through the "Internet of things"; ISO (International Organization for Standardization) standards should be developed in this respect; it is necessary to provide Internet users with transparent and accessible information about security measures and mechanisms applied;

6.4. criminal activities on or through online services must be combated effectively by the competent State authorities in accordance with Article 8 of the European Convention on Human Rights; law-abiding users have the right to remain anonymous, while law-infringing users must be identifiable and criminals must be identifiable by law-enforcement bodies subject to the legal safeguards required under the European Convention on Human Rights; in order to combat online identity theft, there should be provision for the use of real identification, either by electronic signature, using authentication tools or by a trusted third party;

6.5. hotlines or other online help systems for children and people with special needs should be established by public authorities and online service providers, in particular as regards cyber-mobbing and online child abuse;

6.6. the protection of property must be respected online; online service providers should offer the possibility to attach electronic signatures or apply electronic authentication tools to online content and services; providers of "cloud computing" services should automatically apply special protection measures for property stored with them, including conditional access tools and regular back-up filing;

6.7. providers of cloud computing services must not lower their users' rights and protection by delocalising their "data cloud" outside the jurisdiction applicable to their company; the legal and fiscal system applicable to online services should be that of the end consumer, and the consumer rights that apply should be those that are most favourable between the country of origin and the country of service;

6.8. member States should set up an adequate regulatory framework for online gambling services, irrespective of whether such gambling services are offered by public or private companies; online gambling services registered in one country, which are accessible for, and targeted at, users in another country, should fall under the jurisdiction of the latter;

6.9. commercial or institutional service providers must have the legal obligation to inform their users of their name, legal seat and legal representative or director as well as their policies concerning user protection and security, in particular as regards their protection of a user's private life, correspondence, personal data and property;

6.10. users of online services must be adequately informed of their rights by their service providers, irrespective of whether such services are provided by a public authority or a private entity; the waiver of any rights by users in favour of service providers must require the prior, informed and express consent of those users;

6.11. users of online services must have an effective legal remedy before a national authority against violations of their rights, having regard to Articles 6 and 13 of the European Convention on Human Rights as well as Article 2 of the United Nations International Covenant on Civil and Political Rights;

6.12. commercial or institutional service providers should offer their users the possibility to submit complaints and settle disputes voluntarily out of court, for instance through national or European consumer protection centres or bodies for online dispute resolution, and an easily accessible ombudsman with an obligation to respond should be appointed by each Internet service provider or their national association;

6.13. the secrecy of employees' private correspondence through their employer's communication devices is protected by Article 8 of the European Convention on Human Rights; employment contracts should prohibit any interference in accordance with Committee of Ministers Recommendation No. R (89) 2 on the protection of personal data used for employment purposes.

7. Governments and service providers should undertake an ambitious plan to educate users in security operations.

8. The Assembly calls on the European Internet Services Providers Association (EuroISPA) and its national members to draw up a common code of conduct in view of the above basic principles on user protection and Internet user security in cyberspace. Internet service providers and law-enforcement authorities should have a legal framework for practical co-operation against attacks on the rights and the security of users of the Internet and online media.

9. The Assembly invites the United Nations High Commissioner for Human Rights to co-operate with the Council of Europe and to refer to this resolution, as well as Resolution 1843 (2011) on the protection of privacy and personal data on the Internet and online media, when preparing her report on the protection and promotion of the right to privacy for the United Nations Human Rights Council and the 69th session of the United Nations General Assembly in 2014-2015.

10. The Assembly invites the Multistakeholder Advisory Group preparing the next United Nations Internet Governance Forum (Istanbul, 2-5 September 2014) to pay particular attention to questions regarding Internet user protection and security in cyberspace, in particular the human right to protection of privacy and personal data.

11. The Assembly invites the International Telecommunications Union to draw up global technical standards on the integrity, security and secrecy of online and mobile communications, which are based on Article 17 of the United Nations International Covenant on Civil and Political Rights, taking into account the provisions of relevant regional treaties.