www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 2 July 2012 T-CY (2012) 16 E

Cybercrime Convention Committee (T-CY)

Opinion of the T-CY

on

Draft Committee of Ministers declaration on risks to fundamental rights stemming from digital tracking and other surveillance technologies [Version CDMSI(2012)002Rev3 (24/05/2012)]

Opinion of the T-CY

on

Draft Committee of Ministers declaration on risks to fundamental rights stemming from digital tracking and other surveillance technologies
[Version CDMSI(2012)002Rev3 (24/05/2012)]

1. The T-CY welcomes the opportunity to express its opinion on the Draft Committee of Ministers declaration on risks to fundamental rights stemming from digital tracking and other surveillance technologies [Version CDMSI(2012)002Rev3 (24/05/2012)] prepared by the Steering Committee on Media and Information Society (CDMSI).

2. The T-CY notes the importance of protecting people and their rights, including their privacy rights.

3. The T-CY underlines that a clear distinction is to be made between intrusion, surveillance and other forms of interference by private sector entities, criminals, and public authorities.

4. The T-CY is of the opinion that the three types of situations must not be confused. Each situation would require different recommendations.

5. In order to clarify the scope of the Declaration, the T-CY, therefore, suggests two options:

a. The declaration could be limited to "the risks to fundamental rights stemming from the private use of digital tracking and other surveillance technologies", and to omit discussion of use by governments and criminals of such methods. The title and the text would then need to be adjusted accordingly (for example, paragraphs 2 and 9 to be deleted, paragraph 13 to specify that the declaration is related to risks of the private use of tracking and surveillance technologies). This option would add clarity and specificity to the Declaration and would support the Declarations of paragraph 13.

b. Alternatively, situations of surveillance and other interference by (i) private sector entities, (ii) criminals and (iii) public authorities (with a further distinction between legitimate use and risks of misuse of powers) should be clearly distinguished, for example, in paragraphs 2 and 9. In paragraph 13, recommendations would then need to be made addressing each specific situation. These could include that all Council of Europe member states, but also other states, fully implement the Budapest Convention on Cybercrime, including Article 15 on conditions and safeguards as well as law enforcement powers permitting the lawful interception of data (Article 21). If this option is followed, the concept of "surveillance" would need to be defined more clearly in order to avoid misunderstandings.

_____

Appendix

Steering Committee on Media and Information Society (CDMSI)

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

CDMSI(2012)002Rev3
24/05/2012

Draft Committee of Ministers declaration on risks to fundamental rights stemming from digital tracking and other surveillance technologies

1. Council of Europe member states have undertaken to secure to everyone within their jurisdiction the rights and freedoms defined in the Convention for the Protection of Human Rights and Fundamental Freedoms (CETS No. 5, hereinafter referred to as the Convention). Having regard to the case law of the European Court of Human Rights, the resulting obligations for member states can be negative, that is to refrain from interference, or positive, involving, inter alia, the protection of individuals from action by private parties which could jeopardize their enjoyment of those rights[1].

2. The right to private life, as provided for in Article 8 of the Convention, is essential for protecting people against misuse of power or authority and for enabling their participation in democratic governance processes. Restrictions of this right can only be justified when it is necessary in a democratic society, in accordance with the law and for one of the limited purposes set out in Article 8, paragraph 2. In some cases, the European Court of Human Rights has ruled that the mere existence of legislation allowing the surveillance of citizens may impinge on their fundamental right to private life[2].

3. A deficit in the protection of private life, and its corollary personal data, can have adverse effects on the enjoyment of other fundamental rights. This is particularly the case as regards freedom of expression, freedom of assembly and association and, in consequence, people's right to participation and deliberation in governance processes. In this latter respect, for people to be able to make genuinely free decisions, they need to feel free from intrusion, surveillance and other forms of interference with their privacy.

4. People nowadays rely on a constantly growing range of both fixed-location and mobile devices which enhance their possibilities to communicate, interact, participate in different

---

1 X and Y v. the Netherlands; Young, James and Webster v. the UK; Plattform Ärste für das Leben v. Austria; Powell and Rayner v.the UK; Costello –Roberts v. the UK; Lopez Ostra v. Spain; August v. the UK; A. v. the UK; Z and Others v. the UK; Calvelli and Ciglio v. Italy; Osman v. the UK; Marcks v. Belgium; Airey v. Ireland; Gaskin v. the UK; Gül v. Switzerland; Ahmut v. the Netherlands; D. v. the UK; Guerra v. Italy; Botta v. Italy; L.C.B v. the UK; Z and others v. the U; S. and Marper v. the UK. Footnote for CDMSI information, to be deleted after consideration and possible approval.

2 Klass and Others v. Germany; Malone v. the UK; Weber and Saravia v. Germany; Halford v. the UK; the Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, etc. Footnote for CDMSI information, to be deleted after consideration and possible approval.

kinds of activities, including those which involve matters of public interest, and manage practical aspects of their everyday life.

5. The use of these devices enables providers to collect, store and process vast amount of users' personal data, including the nature and, in some cases, the content of their communications, the information they accessed or the websites they visited and, in case of mobile devices, their whereabouts and movements. Such data gathering and processing can reveal delicate (e.g. financial data) or sensitive information (e.g. as regards health, political, religious preferences, sexual habits) on the persons concerned. Those devices can therefore provide detailed and intimate portrayals of the individuals using them. Also, data storing in inappropriate conditions constitutes a problem.

6. Reportedly, certain software installed on mobile devices is designed or programmed to collect a wide range of personal data – including sensitive data – related to the use of those devices. Such information can apparently be accessed by or transmitted to third parties without the knowledge of the users and without permitting them to change or adjust the application of the software in their mobile devices. Conscious of the implications for users' right to privacy and protection of personal data, a number of member states' data protection authorities have decided to investigate these cases.

7. Profiles based on the use of new technologies by individuals can be created and used for different purposes, potentially leading to decisions significantly affecting the people concerned even without their knowledge, as highlighted in Recommendation CM/Rec(2010)13 on the protection of personal data in the context of profiling, with clear repercussions on individuals' autonomy and on society as a whole.

8. The development of technologies based on machine-to-machine communication and radio-frequency identification (RFID) raise additional concerns about their impact on fundamental rights and freedoms.

9. The questions stemming from the use of digital tracking technologies can have significant rule of law implications, which require effective safeguards for individuals' rights and freedoms against arbitrary interferences. Similarly, tracking and geolocation can have serious consequences on peoples' right to free movement. Unlawful surveillance activities in cyberspace, whether they concern illegal access, data interception or interference, system surveillance, misuse of devices may have criminal law implications; the Convention on Cybercrime (ECTS 185) is highly relevant in this respect.

10. The practices described above have considerable consequences for the protection of personal data and undermine privacy, which is an essential guarantee of freedom and democracy. A collapse of privacy will have direct consequences for democracy and, ultimately, for society as a whole. The Convention for the protection of individuals with regard to automatic processing of personal data (CETS no 108) is fully applicable in respect of the issues described above.

11. In addition, such practices may pose very specific threats to the rights associated to specific professions, such as journalists as well as other participants in the new communications environment such as bloggers and users as creators of content. The use of certain devices and technologies by journalists and the associated surveillance and tracking could, for example, seriously undermine their right to protection of sources of information which, as highlighted by Recommendation CM R(2000)7 on the right of journalists not to disclose their sources of information, is a basic condition for journalistic

investigative work and for the freedom of the media. Moreover, surveillance and tracking technologies could attract additional threats against the personal safety of journalists.

12. As underlined in the Council of Europe Strategy on Internet Governance for 2012-2015, private sector actors should be encouraged to ensure that their corporate policies and practices respect human rights and fundamental freedoms in all of the countries in which they operate. Concerns in this respect may lead to the introduction of suitable export controls to prevent the misuse of technology in third countries to undermine the freedom, dignity and privacy of Internet users

13. Against this background, the Committee of Ministers:

a. alerts member states to the risks that covert surveillance through the use of user tracking devices entails for the right to private life as a fundamental right and as a pre-condition for the exercise of democratic citizenship and underlines member states' responsibility to ensure that citizens are adequately protected in this context, in particular by ensuring transparency and compliance with legal procedures and providing mechanisms for redress in case of violations of rights;

b. fully supports member states' efforts to address the question of tracking and surveillance technologies and their impact on people's exercise and full enjoyment of fundamental rights and freedoms as well as their impact on society as a whole whilst recognising that digital technologies such as tracking, profiling or geolocation can also be used for legitimate interests for the benefit of users, the economy and society at large;

c. welcomes measures being taken to raise awareness among industry actors and technology developers, and also among users, about the possible impact of these technologies on fundamental rights and freedoms in a democratic society and in this regard encourages the application of principles such as privacy by design;

d. considers that further Council of Europe work on these issues is necessary, in consultation with relevant industry and other actors, including as regards the implications of these technologies for Internet governance, information society media freedom and the protection of journalistic sources, and data protection.