Steering Committee on
Media and Information Society
(CDMSI)

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

CDMSI(2012)002Rev6
30/10/2012

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

1. The propensity to interfere with the right to private life has significantly increased as a result of rapid technological development and legal frameworks which are slow to adapt.

2. Data processing in the information society which is carried out without the necessary safeguards and security can raise major human rights related concerns. Legislation allowing broad surveillance of citizens can be found contrary to the right to respect of private life. These capabilities and practices can have a chilling effect on citizen participation in social, cultural and political life and, in the longer term, could have damaging effects on democracy. They can also undermine the confidentiality rights associated to certain professions, such as the protection of journalists' sources, or even threaten the safety of the persons concerned. More generally, they can endanger the exercise of freedom of expression and the right to receive and impart information protected under Article 10 of the European Convention on Human Rights.

3. In this connection, it is recalled that, in accordance with Article 8 of the European Convention on Human Rights, Council of Europe member states have undertaken to secure to everyone within their jurisdiction the right to respect of private and family life, home and correspondence. Restrictions to 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, of the Convention.

4. As a corollary to the Convention and relevant case law of the European Court of Human Rights, member states have negative obligations, that is, to refrain from interference with fundamental rights, and positive obligations, that is to actively protect these rights. This includes the protection of individuals from action by non-state actors.

5. People nowadays rely on a growing range of both fixed-location and mobile electronic devices which enhance their possibilities to communicate, participate and manage their everyday lives. However, a growing number of these devices are equipped with software that are capable of collecting and storing data, including personal data (e.g. keystrokes that reveal passwords) and private information such as user generated content, websites visited, and geographical locations that potentially allow tracking and surveillance of people. This data can reveal delicate and/or sensitive personal information (such as

financial, health, political, religious preferences,sexual habits) which can be aggregated to provide detailed and intimate profiles of them.

6. Tracking and surveillance technologies can be used in the pursuit of legitimate interests, for example to develop new services, improve user experience or facilitate network management, as well as law enforcement. On the other hand, they may also be used for unlawful purposes that lead to illegal access, data interception or interference, system surveillance, and misuse of devices or other forms of malpractice; for example, geo-location tracking could be used to stalk women and make them more vulnerable to gender-related abuse and violence.

7. In all cases, the modalities for processing personal data should comply with relevant Council of Europe standards. This implies ensuring that law enforcement's own tracking and surveillance measures respect the human rights safeguards referred to in Article 15 of the Budapest Convention on Cybercrime (CETS No. 185). It also concerns strict respect for the limits, requirements and safeguards set out in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) as well as regard for other instruments such as Recommendation CM/Rec(2010)13 on the protection of personal data in the context of profiling.

8. Against this background, the Committee of Ministers:

alerts member states to the risks of digital tracking and other surveillance technologies for human rights, democracy and the rule of law and recalls the need to guarantee their legitimate use which benefits individuals, the economy, society at large, and the needs of law enforcement;

encourages member states to bear these risks in mind in their bilateral discussions with third countries, and, where necessary, consider the introduction of suitable export controls to prevent the misuse of technology to undermine those standards;

welcomes steps taken by data protection authorities in some member states to raise awareness of the implications of tracking and surveillance technologies and to investigate these practices to ensure compliance with the provisions of Convention 108 and their national legislations;

draws attention to the criminal law implications of unlawful surveillance and tracking activities in cyberspace and the relevance of the Budapest Convention in combating cybercrime;

welcomes measures taken by both state and non-state actors to raise awareness among users, and, a fortiori, within the private sector and among technology developers about the potential impact of the use of such technologies on human rights and the steps which can be taken at the design stage to minimise the risks of interferences with these rights and freedoms (e.g. 'privacy by design' and 'privacy by default');

recalls the Council of Europe Internet Governance Strategy 2012-2015 which includes a number of action lines relevant to the challenges identified in this Declaration and looks forward to concrete outcomes stemming from the work of the competent Council of Europe bodies.