EGE delivers Opinion on security and surveillance to President Barroso

The European Group on Ethics in Science and New Technologies (EGE) has today issued its Opinion on the Ethics of Security and Surveillance Technologies. The Opinion, presented to President Barroso at a handover ceremony on 20 May 2014, examines trends in the development of new security and surveillance technologies. It explores the ethical implications brought by these trends, and advances a set of 16 concrete recommendations for the attention of the EU, member states, and a range of public and private stakeholders.

The Opinion aims to provide a reference point for the European Commission regarding the ethics of security and surveillance measures in an era where rapid advances in telecommunications and computing have enabled the data of billions of citizens around the globe to be tracked and scrutinized on an unprecedented scale.

In the wake of the disclosures by former NSA contractor Edward Snowden, the EGE calls for a renewed public debate on the limits to be placed on security and surveillance technologies, and offers reflection on the far-reaching impact of surveillance on trust, privacy, and civil liberties.

Assessing the governance of security and surveillance, the EGE finds a diverse regulatory framework, in which domains such as telecommunications need to better keep pace with the technological transformation in surveillance capacities. While Europe can genuinely pride itself with some of the strongest privacy protection worldwide, it is still waiting for its revised data protection framework and the national security exception can constitute a form of loophole.

Security and freedom: do we need both? And can we enjoy both without the pursuit of one jeopardising the other? These are two central questions addressed by the Opinion. The Opinion challenges the notion that 'security' and 'freedom' can be traded against one another. While a balance must be struck between competing values when they come into conflict, certain core principles, such as human dignity, cannot be bartered with. The Opinion calls for a more nuanced approach, in which the proportionality and effectiveness of security and surveillance technologies are subject to rigorous assessment, and in which rights are prioritized rather than traded.

At its core, the Opinion contends that an ethical foundation for the use of security and surveillance technologies requires a broader understanding of the security concept, encompassing the human and societal dimensions of security. Security is not simply protection from physical harm, but a means to enable individual and collective flourishing. The Opinion highlights the adverse consequences at stake when security becomes an end in its own right, noting that excessive surveillance in the pursuit of security erodes trust, social cohesion, solidarity and intellectual freedom.

Recommendations

Based on its findings, the Opinion advances 16 recommendations, addressing a wide number of key issues.

- recommendations to improve the application and oversight of technologies with a security function (judicial oversight; a common European understanding of national security; and an EU regulatory framework governing the use of drones);
- recommendations targeting the use of surveillance technologies (including the call for an EU code of conduct for big data analytics; greater transparency in the use of algorithms; and closer scrutiny of EU border surveillance systems);

- recommendations regarding measures designed to re-build trust and improve citizens' control over the management of their data and privacy (including improved data protection enforcement, protection for whistleblowers and measures to improve education and awareness among the public and practitioners).

For further information on the Opinion's recommendations, see overleaf.

Background

The Opinion results from a formal request of President José Manuel Barroso. Its findings and recommendations are the product of an intense series of 12 working meetings (March 2013 – April 2014) and an open roundtable held on 18 September 2013, which drew on the participation of a broad cross-section of European stakeholders, including the scientific community, industry representatives, policymakers, European Institutions representatives, NGOs, and civil society organizations.

The EGE is an independent, multi-disciplinary body supported by the Commission's Bureau of European Policy Advisors (BEPA). It advises the Commission on ethical questions relating to sciences and new technologies. The Opinion is the 28th produced by the EGE and builds on Opinion no. 26 on the ethical implications of Information and Communication Technologies.

For more information

On the EGE and BEPA's work on ethics:
http://ec.europa.eu/bepa/european-group-ethics/index_en.htm

Further information on the recommendations

The EGE has issued 16 recommendations regarding the use of security and surveillance technologies. The following groups and summarises the EGE's recommendations under the four categories of oversight and accountability; data protection and processing; design and development; and public awareness and information.

1. Oversight and accountability

- Member States must ensure that those granted with powers to surveil are ***accountable*** for their actions. Private companies acting on behalf of states must be subject to mechanisms monitoring their compliance with legal and ethical obligations.

- Member States must establish a system of ***judicial oversight*** for surveillance for criminal investigations; individuals should be informed post-hoc and have the possibility to seek judicial redress, in case of unlawful surveillance.

- Member States must vest ***independent oversight authorities*** with powers to monitor the use of public and private surveillance on citizens; collect and publish data on surveillance requests and be systematically consulted in advance of new legislation pertaining to surveillance.

- EU institutions, in conjunction with member states, should find ways to establish a ***common understanding of national security***. Member states should not, in the name of national security, surveil one another for commercial advantage. To preserve trust, member states should establish procedural means to keep one another appropriately informed of extra jurisdictional intelligence activities.

- The increased ***deployment of drone technology*** must be accompanied by the necessary governance and oversight arrangements encompassing: a) common standards and a regulatory framework covering the civilian and commercial use of drones within the EU; b) authorization and oversight by member states of the domestic use of drones; c) increased legal accountability and transparency of the military use of drones.

- The European Commission and Member States should ensure that an effective and comprehensive ***whistleblower protection mechanism*** is established in the public and private sectors.

2. Data protection and data processing

- As regards ***personal data****,* the purpose limitation principle should be the standard for both public and private organisations; data should be anonymised as far as possible; profiling for commercial purposes should be subject to explicit consent.

- The EU should develop a code of conduct for ***big data analytics*** to ensure an ethical basis for the compilation and analysis of large data sets by public and private bodies.

- Underlying ***algorithms*** and their parameters should be made explicit as a mandatory requirement and should be subject to continual examination and validation.

- The European Commission should consider revising the ***e-Privacy Directive*** to ensure new digital interfaces, such as VoIP products, are included within its remit.

- Member States should ensure that **data protection enforcement** at national level by guaranteeing data protection authorities have sufficient legal powers and resources.

3. Design and development of security and surveillance technologies

- ***Privacy Impact Assessment*** procedures must form part of regulatory practice in Member States when new or modified information systems are introduced to the market.

- Public and private organisations should adopt ***privacy-by and privacy-in design*** principles for development of security and surveillance technologies. European values of dignity, freedom and justice should be integrated in the design, development and delivery of such technologies.

- New ***border surveillance systems*** at EU level should only be developed where it is established that existing systems are not sufficient. As this criterion has not been met in the case of the Entry Exit system a moratorium on its introduction is recommended.

4. Public information and awareness

- ***Public awareness of data policies*** must be strengthened by ensuring that public authorities and corporate actors make their policies publicly available. Educational programs, beginning at school, should foster knowledge and debate on security and surveillance technologies.

- A fuller understanding of how European citizens ***conceptualise and value privacy*** should be fostered via EU funding for research examining how citizens consider and cultivate their involvement in issues related to security and surveillance.