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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Resolution 2045 (2015)[1]
Provisional version

Mass surveillance

Parliamentary Assembly

1. The Parliamentary Assembly is deeply concerned about mass surveillance practices disclosed since June 2013 by journalists to whom a former United States national security insider, Mr Edward Snowden, had entrusted a large amount of top secret data establishing the existence of mass surveillance and large-scale intrusion practices hitherto unknown to the general public and even to most political decision-makers.

2. The information disclosed so far in the Snowden files has triggered a massive, worldwide debate about mass surveillance by the United States and other countries' intelligence services and the potential lack of adequate legal regulation and technical protection at the national and international level, and/or its effective enforcement.

3. The disclosures have provided compelling evidence of the existence of far-reaching, technologically advanced systems put in place by United States intelligence services and their partners in certain Council of Europe member States to collect, store and analyse communication data, including content, location and other metadata, on a massive scale, as well as targeted surveillance measures encompassing numerous people against whom there is no ground for suspicion of any wrongdoing.

4. The surveillance practices disclosed so far endanger fundamental human rights, including the rights to privacy (Article 8 of the European Convention on Human Rights (ETS No. 5)), freedom of information and expression (Article 10) and the rights to a fair trial (Article 6) and freedom of religion (Article 9) – especially when privileged communications of lawyers and religious ministers are intercepted and when digital evidence is manipulated. These rights are cornerstones of democracy. Their infringement without adequate judicial control also jeopardises the rule of law.

5. The Assembly about also deeply worried about threats to Internet security by the practice of certain intelligence agencies, disclosed in the Snowden files, of seeking out systematically, using and even creating "back doors" and other weaknesses in security standards and implementation, which could easily be exploited also by terrorists and cyberterrorists or other criminals.

6. It is also worried about the collection of massive amounts of personal data by private businesses and the risk that these data may be accessed and used for unlawful purposes by State or non-State actors. In this connection, it should be underlined that private businesses should respect human rights pursuant to the Resolution 17.4 on human rights and transnational corporations and other business enterprises, adopted by the United Nations in June 2011.

7. The Assembly unequivocally condemns the extensive use of secret laws and regulations, applied by secret courts using secret interpretations of the applicable rules, as this practice undermines public confidence in the judicial oversight mechanisms.

1. *Assembly debate* on 21 April 2015 (12th Sitting) (see Doc. 13734, report of the Committee on Legal Affairs and Human Rights, rapporteur: Mr Pieter Omtzigt; and Doc. 13748, opinion of the Committee on Culture, Science, Education and Media, rapporteur: Sir Roger Gale). *Text adopted by the Assembly* on 21 April 2015 (12th Sitting).
See also Recommendation 2067 (2015).

8. The consequences of mass surveillance tools such as those developed by the United States and allied services falling into the hands of authoritarian regimes would be catastrophic. In times of crisis, it is not impossible for executive power to fall into the hands of extremist politicians, even in established democracies. High-technology surveillance tools are already in use in a number of authoritarian regimes and are used to track down opponents and to suppress freedom of information and expression. In this regard, the Assembly is deeply concerned about recent legislative changes in the Russian Federation which offer opportunities for enhanced mass surveillance through social networks and Internet services.

9. In several countries, a massive "Surveillance-Industrial Complex" has evolved, fostered by the culture of secrecy surrounding surveillance operations, their highly technical character and the fact that both the seriousness of alleged threats and the need for specific counter-measures and their costs and benefits are difficult to assess for political and budgetary decision-makers without relying on input from interested groups themselves. These powerful structures risk escaping democratic control and accountability and they threaten the free and open character of our societies.

10. The Assembly notes that the law in most States provides some protection for the privacy of their own citizens, but not of foreigners. The Snowden files have shown that the United States National Security Agency (NSA) and their foreign partners, in particular among the "Five Eyes" partners (Australia, Canada, New Zealand, the United Kingdom and the United States) circumvent national restrictions by exchanging data on each other's citizens.

11. The Assembly recognises the need for effective, targeted surveillance of suspected terrorists and other organised criminal groups. Such targeted surveillance can be an effective tool for law enforcement and crime prevention. At the same time, it notes that, according to independent reviews carried out in the United States, mass surveillance does not appear to have contributed to the prevention of terrorist attacks, contrary to earlier assertions made by senior intelligence officials. Instead, resources that might prevent attacks are diverted to mass surveillance, leaving potentially dangerous persons free to act.

12. The Assembly also recognises the need for transatlantic co-operation in the fight against terrorism and other forms of organised crime. It considers that such co-operation must be based on mutual trust founded on international agreements, respect for human rights and the rule of law. This trust has been severely damaged by the mass surveillance practices revealed in the Snowden files.

13. In order to rebuild trust among the transatlantic partners, among the member States of the Council of Europe and also between citizens and their own governments, a legal framework must be put in place at the national and international level which ensures the protection of human rights, especially the protection of the right to privacy. An effective tool for the enforcement of such a legal and technical framework, besides enhanced judicial and parliamentary scrutiny, is credible protection extended to whistle-blowers who expose violations.

14. The reluctance of the competent United States authorities and their European counterparts to contribute to the clarification of the facts, including their refusal to attend hearings organised by the Assembly and the European Parliament, as well as the harsh treatment of whistle-blower Edward Snowden, does not contribute to restoring mutual trust and public confidence.

15. The Assembly welcomes initiatives within the US Congress to review existing legislation in order to minimise abuses, as well as the German Bundestag's decision to set up a committee of inquiry into the repercussions of the NSA affair in Germany. It calls on the Bundestag committee to carry out its tasks of holding to account the executive and seeking the truth without regard to party-political considerations and encourages other parliaments to embark on similar inquiries.

16. Recalling the findings of the report on the Democratic Oversight of the Security Services adopted by the European Commission for Democracy through Law (Venice Commission) in 2015, the Assembly emphasises that parliaments should play a major role in monitoring, scrutinising and controlling national security services and armed forces in order to ensure respect for human rights, the rule of law and democratic accountability, as well as international law. The sub-contracting of security or intelligence operations to private firms should be the exception and must not reduce democratic oversight of such operations.

17. The Assembly welcomes the thorough investigation carried out by the European Parliament leading to the adoption, on 12 March 2014, of a comprehensive resolution on the NSA affair and its repercussions for Euro-Atlantic relations. In particular, the Assembly strongly endorses:

17.1. the invitation addressed to the Secretary General of the Council of Europe by the European Parliament to use his powers under Article 52 of the European Convention on Human Rights to request information on the manner in which States Parties implement relevant provisions of the Convention;

17.2. the European Parliament's call to promote the wide use of encryption and resist any attempts to weaken encryption and other Internet safety standards, not only in the interest of privacy, but also in the interest of threats against national security posed by rogue States, terrorists, cyberterrorists and ordinary criminals.

18. The Assembly invites the European Union to accelerate its work towards finalising the General Data Protection Regulation and the Passenger Name Record (PNR) system, to conclude international co-operation agreements based on the Schengen Information System and to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

19. The Assembly therefore urges the Council of Europe member and observer States to:

19.1. ensure that national law allows the collection and analysis of personal data (including so-called metadata) only with the consent of the person concerned or following a court order granted on the basis of reasonable suspicion of the target being involved in criminal activity; unlawful data collection and treatment should be penalised in the same way as the violation of the traditional confidentiality of correspondence; the creation of "back doors" or any other techniques to weaken or circumvent security measures or exploit their existing weaknesses should be strictly prohibited; all institutions and businesses holding personal data should be required to apply the most effective security measures available;

19.2. ensure, in order to enforce such a legal framework, that their intelligence services are subject to adequate judicial and/or parliamentary control mechanisms. National control mechanisms must have sufficient access to information and expertise and the power to review international co-operation without regard to the originator control principle, on a mutual basis;

19.3. provide for credible, effective protection for whistle-blowers exposing unlawful surveillance activities, including asylum, as far as possible under national law, for whistle-blowers threatened by retaliation in their home countries, provided their disclosures qualify for protection under the principles advocated by the Assembly;

19.4. agree on a multilateral "intelligence codex" for their intelligence services, which lays down rules governing co-operation for the purposes of the fight against terrorism and organised crime. The codex should include a mutual engagement to apply to the surveillance of each other's nationals and residents the same rules as those applied to their own, and to share data obtained through lawful surveillance measures solely for the purposes for which they were collected. The use of surveillance measures for political, economic or diplomatic purposes among participating States should be banned. Participation should be open to all States which implement a legal framework at national level corresponding to the specifications enumerated in paragraphs 19.1 to 19.3;

19.5. promote the further development of user-friendly (automatic) data protection techniques capable of countering mass surveillance and any other threats to Internet security, including those posed by non-State actors;

19.6. refrain from exporting advanced surveillance technology to authoritarian regimes.

20. The Assembly also invites the competent bodies of the European Union to make use of all the instruments at their disposal, such as the Convention for the Protection of individuals with regard to Automatic Processing of Personal Data, to promote the privacy of all Europeans in their relations with their counterparts in the United States, in particular in negotiating or implementing the Transatlantic Trade and Investment Partnership (TTIP), the Safe Harbour decision, the Terrorist Financing Tracking Program (TFTP) and the Passenger Name Records (PNR) agreement.