

MASS SURVEILLANCE

Who is watching
the watchers?

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

MASS SURVEILLANCE

Who is watching
the watchers?

French edition:
*Surveillance de masse –
Quel contrôle démocratique ?*
ISBN 978-92-871-8103-9

*The opinions expressed in this work
are the responsibility of the authors
and do not necessarily reflect the official
policy of the Council of Europe.*

All rights reserved. No part of this
publication may be translated,
reproduced or transmitted, in any form
or by any means, electronic (CD-Rom,
Internet, etc.) or mechanical, including
photocopying, recording or any
information storage or retrieval system,
without prior permission in writing from
the Directorate of Communications
(F-67075 Strasbourg Cedex
or publishing@coe.int).

Cover design: Documents
and Publications Production
Department (SPDP),
Council of Europe
Photo: © iStock
Layout: Jouve, Paris

Council of Europe Publishing
F-67075 Strasbourg Cedex
<http://book.coe.int>

ISBN 978-92-871-8104-6
© Council of Europe, April 2016
Printed at the Council of Europe

Two Council of Europe bodies, the
Parliamentary Assembly and the
European Commission for Democracy
through Law (known as the Venice
Commission), work together to
define and uphold the Organisation's
fundamental values – human rights,
the rule of law and democracy – more
effectively.

The Parliamentary Assembly holds
debates on major issues of topical
concern in Europe. The Venice
Commission provides the benefit of its
legal expertise.

The "Points of view – Points of law"
collection is designed to bring together,
in a single volume on a single topic, the
Parliamentary Assembly's position and
the Venice Commission's opinions. Each
volume will serve as a reference work
on the political and legal aspects
of a topical issue.

Contents

PART 1 – MASS SURVEILLANCE – REPORT OF THE PARLIAMENTARY ASSEMBLY	5
I. Summary	5
II. Adopted texts	6
III. Explanatory memorandum	10
PART 2 – THE DEMOCRATIC OVERSIGHT OF SIGNALS INTELLIGENCE AGENCIES	55
Executive summary	55
I. Introduction	60
II. The scope of the present study – definitions	61
III. Is there a need for (improved) democratic control?	62
IV. Jurisdiction	69
V. Accountability – constitutional and organisational contexts	70
VI. Accountability for security activities and the case law of the European Court of Human Rights	76
VII. Internal and governmental controls as part of overall accountability systems	84
VIII. Parliamentary accountability	85
IX. Judicial review and authorisation	87
X. Accountability to expert bodies	91
XI. Complaints mechanisms	92
XII. Concluding remarks	93
GLOSSARY	95

Part 1

Mass surveillance – Report of the Parliamentary Assembly

Doc. 13734 of 18 March 2015¹

Rapporteur: Mr Pieter Omtzigt, Netherlands, EPP-CD²

I. SUMMARY

The Committee on Legal Affairs and Human Rights is deeply concerned about mass surveillance and large-scale intrusion practices disclosed since June 2013 by Mr Edward Snowden. 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 huge scale. In several countries, a massive “surveillance-industrial complex” has evolved, which risks escaping democratic control and accountability and threatens the free and open character of our societies.

The surveillance practices disclosed endanger fundamental human rights, including the rights to privacy (Article 8 of the European Convention on Human Rights – ETS No. 5, “the Convention” or ECHR), freedom of information and expression (Article 10), and the rights to a fair trial (Article 6) and freedom of religion (Article 9). The committee is also deeply worried about threats to Internet security by the practice of certain intelligence agencies of seeking out systematically, using and even creating “back doors” and other weaknesses in security standards and implementation, which could easily also be exploited by terrorists and cyberterrorists or other criminals.

-
1. Presentation and discussion of the report on 21 April 2015 during the second part of the 2015 session of the Parliamentary Assembly of the Council of Europe (PACE) (12th sitting).
 2. Group of the European People's Party.

The committee also recognises the need for transatlantic co-operation in the fight against terrorism and other forms of organised crime but it considers that such co-operation must be based on mutual trust and respect for human rights and the rule of law. In order to rebuild trust, a legal and technical framework must be put in place at the national and international level which ensures the protection of human rights, especially that which secures 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.

II. ADOPTED TEXTS

A. Resolution 2045 (2015)³

1. The Parliamentary Assembly is deeply concerned about the mass surveillance practices that have been disclosed since June 2013 by journalists to whom a former United States National Security Agency (NSA) contractor, 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, world-wide debate about mass surveillance by the intelligence services of the United States and other countries and the potential lack of adequate legal regulation and technical protection at national and international levels, and/or their 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), a fair trial (Article 6) and freedom of religion (Article 9) – especially when confidential communications with 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 is deeply worried about threats to Internet security by the practices 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 that could easily be exploited by terrorists and cyberterrorists or other criminals.

3. Text adopted by the Parliamentary Assembly on 21 April 2015 (12th sitting).

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 context, 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 Human Rights Council 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.

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 nature 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 the interested groups themselves. There is a risk that these powerful structures could escape democratic control and accountability and threaten the free and open nature 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 that of foreigners. The Snowden files have shown that the United States NSA and its 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 levels 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 political considerations and encourages other parliaments to embark on similar inquiries.

16. Recalling the findings of the report on the democratic oversight of 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 hamper the 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 transatlantic 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 the 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 their national laws only allow for the collection and analysis of personal data (including so-called metadata) 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 processing 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. Those responsible for 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 credible, effective protection, including asylum, for whistle-blowers who expose unlawful surveillance activities and for those threatened by retaliation in their home countries, as far as possible under national law, 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 the same rules to the surveillance of their own nationals and residents, 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 in participating States should be banned. Adherence to this codex should be open to all States which implement a national legal framework 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 to promote the privacy of all Europeans, for example the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 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 Finance Tracking Program (TFTP) and the Passenger Name Record (PNR) agreement.

B. Recommendation 2067 (2015)⁴

1. The Parliamentary Assembly refers to its Resolution 2045 (2015) on mass surveillance and invites the Committee of Ministers to make use of the tools at its disposal to uphold the fundamental right to privacy in all member and observer States of the Council of Europe.

2. In particular, the Assembly invites the Committee of Ministers to consider:

2.1. addressing a recommendation to member States on ensuring the protection of privacy in the digital age and Internet safety in the light of the threats posed by the newly disclosed mass surveillance techniques (see Resolution 2045 (2015), paragraphs 19.1 to 19.3);

2.2. further exploring Internet security issues related to mass surveillance and intrusion practices, in particular with regard to the human rights and fundamental freedoms of Internet users;

2.3. launching an initiative aimed at negotiating an “intelligence codex” addressed to the intelligence services of all participating States, which lays down rules governing co-operation in the fight against terrorism and organised crime (see Resolution 2045 (2015), paragraph 19.4);

2.4. strengthening co-operation with the competent bodies of the European Union involved in negotiating trade and data protection issues with the United States and other third countries, with a view to bringing to bear the principles laid down in the European Convention on Human Rights (ETS No. 5) in the interest of all member States of the Council of Europe.

III. EXPLANATORY MEMORANDUM

By Mr Omtzigt, rapporteur

Our freedom is built on what others do not know of our existences (Aleksandr Solzhenitsyn)

1. Introduction and procedure

1. Since June 2013, disclosures by journalists to whom Mr Edward Snowden, a former employee of the CIA and of a private contractor working for the United States NSA, had entrusted a large amount of top secret data concerning mass surveillance carried out by the NSA and others have triggered a massive public debate on privacy in the Internet age. The extent of mass surveillance programmes conducted all around the world by the NSA and other countries’ intelligence agencies is stunning. The disclosures have confirmed the need for the Council of Europe to encourage its member and observer states to reassess their own surveillance programmes, assess loopholes in such programmes which enable the targeting of their own citizens by foreign services, and consider possible redress, including through legislative means, international agreements and the promotion of mass encryption. This is a matter

4. Text adopted by the Parliamentary Assembly on 21 April 2015 (12th sitting).