German Bundestag **Printed paper 18/843**
18th electoral term 18.03.2014

Motion

tabled by the CDU/CSU, SPD, The Left Party and Alliance 90/The Greens parliamentary groups

Establishment of a committee of inquiry

The Bundestag is requested to adopt the following motion:

A. Establishment

I. A committee of inquiry shall be established.

II. The committee of inquiry is to consist of eight members and the same number of substitute members.

B. Task

The committee of inquiry should – triggered in particular by press coverage following the revelations by Edward Snowden regarding Internet and telecommunications surveillance – clarify for the period from 2001 onwards

I. whether, in what way and on what scale the intelligence services of the "Five Eyes" states (United States of America, United Kingdom, Canada, Australia and New Zealand) collected or are collecting data on communication activities (including content-related, subscriber and traffic data), their content and other data-processing actions (including internet use and stored address directories) from, to and in Germany for data retention or used or are using such data collected by public companies or private third parties and to what extent federal agencies, in particular the Federal Government, intelligence services or the Federal Office for Information Security had knowledge of such practices, were involved in them, combated them or possibly exploited them. To this end, the committee should examine the following specific points:

1. Was data collected and retained, checked and analysed by surveillance programmes of the US intelligence service, the National Security Agency (NSA), and of the British Government Communications Headquarters (GCHQ) or by companies on their behalf (in particular on telecommunications activities, including text messages, Internet use, email correspondence – "C2C", use of social networks and electronic payment transactions) which

also affected communication and data-processing activities from, to and in Germany? Were German nationals residing on the territory of one of the countries cited in point I or in any EU Member State subject to such surveillance? Were such activities carried out by other services of the countries listed under point I? Since when, how and on what scale and, if applicable, on what legal basis did this take place?

2. To what extent were and are diplomatic missions and military sites used or being used to collect data on such communication and data-processing activities and the content thereof?

3. If applicable, which laws at German, European and international level did or do such activities contravene?

4. Do the Federal Government, its subordinate agencies or those they have entrusted with security-relevant tasks (including IT tasks) have indications or affirmative knowledge of the activities cited in points I. or 1. and if so for how long has this been the case? Did they know of, approve, support or order the participation of federal agencies or those they entrusted with security-relevant tasks (including IT tasks) in this?

5. Do the Federal Government, its subordinate agencies or those they have entrusted with security-relevant tasks (including IT tasks) have indications or affirmative knowledge of the activities cited in points I. or 1. against other Member States of the EU or NATO, their population or businesses located there, and if so for how long has this been the case? If so, how was this knowledge viewed and what conclusions were drawn from it?

6. What precautions or measures did federal agencies take or initiate or, as the case may be, should have taken or initiated in order to identify the activities cited in points I. and 1. and their extent and to put a stop to them? In the latter event, up until when and why did this not happen and who bears responsibility for this?

7. Did federal agencies or those entrusted by them with security-relevant tasks (including IT tasks) acquire or use data from the activities cited in points I. or 1. or possibly provide services in kind in exchange? Were federal agencies or those entrusted by them with security-relevant tasks (including IT tasks) part of a systematic mutual or “circular” intelligence exchange, in which the other side receives data or findings which they are not allowed to collect themselves under the laws applicable at the location of the data collection? If so, on what legal basis and for what purpose was or is such data acquired or used? If so, how was it ensured that the information in question can be acquired and used under German law as well? How was it ensured, if applicable, that information was not or is not acquired or used that would not have been allowed to be collected under German law?

8. Were federal agencies or those entrusted by them with security-relevant tasks (including IT tasks) involved in any way in the development or technical implementation or use of programmes such as “PRISM”, “TEMPORA”, “XKeyscore” or other programmes used by the services of the countries listed in point I. or used on their behalf for the activities cited in points I. or 1.? If so, who on the German side was involved, for how long and in what specifically?

9. Did federal agencies or those entrusted by them with security-relevant tasks (including IT tasks) receive, test or use programmes developed by the NSA, GCHQ or other services of the countries listed in point I. themselves or on their behalf and, in doing so, did they also access data records originating from the communication and data-processing activities

stated in points I. or 1.? If so, who on the German side received which programmes, tested or used them for how long and accessed which of the said data records?

10. What knowledge regarding the type and scale of such activities geared against business enterprises located in the Federal Republic of Germany did federal agencies have at what time?

11. Could or should federal agencies possibly already have gained knowledge of such measures at an earlier point in time? If so, which bodies and when?

12. To what extent was the Federal Commissioner for Data Protection and Freedom of Information notified immediately of knowledge and information suited to providing grounds for suspicion that data protection law provisions were being violated? Or, as the case may be, why and due to what circumstances and influences did this not happen?

13. Which IT security concepts has the Federal Government applied in its area of responsibility to secure the organisation and operation of telecommunications and IT structures, files, indexes and administration processes against unauthorised data removal and access by third parties?

14. Have US bodies carried out or initiated telecommunications surveillance, arrests, or targeted killings through the deployment of combat drones on or from German territory? If so, what knowledge did German federal agencies have of this at what time? If applicable, were they involved in the preparation or implementation of such measures in any form whatsoever or did they approve them? If applicable, what action should they have taken in response to such knowledge and what action was actually taken?

15. To what extent did the German Federal Government and its subordinate departments enable US security authorities to take part in the questioning of asylum seekers or to question asylum seekers themselves?

16. What action did the Federal Government and its subordinate departments take and when in order to bring to light, prosecute and end these practices, or if not, why and due to what circumstances and influences did this fail to happen?

17. Was the information the Federal Government provided to the general public on the aforesaid questions correct? Was the information the Federal Government provided to members of parliament or parliamentary institutions on the aforesaid questions correct and comprehensive? Did the Federal Government fulfil all its statutory duties of information towards the Parliamentary Control Panel, the G10 Commission and the Federal Commissioner for Data Protection and Freedom of Information? Was any relevant information withheld from these scrutiny and oversight bodies?;

II. whether and to what extent data on communication activities and the contents thereof (in the form of telecommunication or conversations including their subject matter, such as draft legislation or negotiation strategies) of members of the Federal Government, federal staff and members of the German Bundestag or other constitutional bodies of the Federal Republic of Germany was collected or analysed for intelligence purposes by the intelligence services of the states named in point I. To this end, the committee should examine the following points:

1. Was the data traffic from federal agencies recorded or subject to surveillance by intelligence services of the said countries? Did this also affect German diplomatic missions abroad? If so, since when, how and on what scale?

2. Was telecommunication (telephone conversations, text messages, emails, etc.) or Internet use by members of the Federal Government, federal staff and members of the German Bundestag or other constitutional bodies of the Federal Republic of Germany recorded or analysed by intelligence services of the said states? As of when and on what scale did this happen?

3. If so, why did federal agencies not notice earlier that this type of recording of communication was happening and put an end to it?

4. What strategy did the Federal Government pursue to protect the IT systems of the German Federation from data being accessed or removed without authorisation in the period under inquiry and how has this been further developed?

5. Was the information the Federal Government provided to the general public on the aforesaid questions correct? Was the information the Federal Government provided on the aforesaid questions to members of parliament or parliamentary institutions correct and comprehensive? Has the Federal Government met all its statutory duties of information towards the Parliamentary Control Panel, the G10 Commission and the Federal Commissioner for Data Protection and Freedom of Information? Was any relevant information withheld from these scrutiny and oversight bodies?;

III. whether recommendations to ensure the protection enshrined in the constitution of the right to determine the disclosure and use of one's own personal data, to privacy, to the secrecy of telecommunications and the integrity and confidentiality of IT systems and confidential communication in the state sphere are required. To this end, the committee should clarify the flowing:

1. Are legal and technical changes required to the German system of foreign surveillance carried out by the intelligence services in order to ensure that German authorities comply fully with fundamental and human rights, and if so, which?

2. Are legal and technical changes regarding transmission, receipt and exchange of information with foreign security authorities necessary in order to ensure the Federal Government and all German authorities comply fully with fundamental and human rights, and if so, which?

3. Which measures of a legal, organisational or technical nature can be used to ensure that the guaranteed protection of the confidentiality of electronic communication from, to and in Germany is realised to the fullest extent possible, so that citizens as well as those subject to professional secrecy, those holding the right to refuse testimony and custodians of trade and commercial secrets are protected against electronic communication activities and the content thereof being recorded by foreign intelligence services irrespective of whether there are grounds for suspicion or not?

4. What measures are necessary in order to ensure confidential electronic communication for state bodies as well?

5. Are changes necessary to protect telecommunication and IT security when awarding public contracts in the future?

6. What measures are required to ensure the best possible protection of the privacy of electronic communication at European and international level? The findings of the inquiry by the Civil Liberties, Justice and Home Affairs (LIBE) Committee of the European

Parliament as well as the work at the level of the United Nations should be incorporated into this.

7. What measures are necessary to provide better protection for the population, businesses and public administration against Internet and telecommunications surveillance by foreign authorities?

8. How can the executive, parliamentary, judicial and independent data-protection oversight of the federal security authorities be ensured fully and effectively?

3. What other legal, technical infrastructure and political action must be taken?

Berlin, 18 March 2014

Volker Kauder, Gerda Hasselfeldt and the CDU/CSU parliamentary group
Thomas Oppermann and the SPD parliamentary group
Dr Gregor Gysi and the Left Party parliamentary group
Katrin Göring-Eckardt, Dr Anton Hofreiter and the Alliance 90/The Greens parliamentary group