NETHERLANDS INSTITUTE FOR HUMAN RIGHTS

RECOMMENDATIONS AND PRESS RELEASE
Draft bill of the 20.. Intelligence and Security Services Act to the Prime Minister, the Minister of the Interior and Kingdom Relations, the Minister of Security and Justice and the Minister of Defence in response to the Internet consultation held from 2 July 2015 through 1 August 2015, August 2015

SUMMARY
The most important change to the powers of the intelligence and security services arising from the draft bill is the extension of the power of untargeted interception of telecommunications and other means of data transfer. This entails the intercepting of large amounts of information from an unlimited group of people not suspected of any offence. This may heavily impact the privacy of all Dutch citizens. The proposed provisions on the supervision performed by the security services also affect the right to have effective recourse to remedies.

Violations to the right to privacy are justified only if a clear and precise legal basis exists. This legal basis is also to contain guarantees against misuse. In addition, the necessity and proportionality of the proposed extension of powers are to be demonstrated.
The Institute is of the opinion that the draft bill in its current incarnation has shortcomings as concerns the parts detailed in the below and in this connection makes the following recommendations.

- The necessity
  The necessity of extending the powers of the services has been insufficiently demonstrated, also as various international studies have shown that there are serious doubts to the effectiveness of the large-scale monitoring of telecommunications from a perspective of national security.
  The Institute recommends that the necessity, and in particularly the effectiveness of the proposed extension of powers of interception, be further substantiated.

- Legal basis/foreseeability
  No sufficiently clear and precise legal basis exists. The target criterion of 'in the interests of national security' is insufficiently clear. In addition, the bill does not list the offences that may allow for using the power of interception, nor the categories of people the power of interception may be used against.
  The Institute therefore recommends that the nature of the (imminent) offence that may allow for using the power of interception of telecommunications be detailed and that a description is added of the categories of people the power of interception may be used against.

  The Institute finds that the powers to be created are discussed in highly abstract terms in both the wording of the bill and its explanatory memorandum. This phrasing results in the scope of the practical impact the powers have on privacy not being foreseeable. The technical data exchange facilities currently develop at such a tremendously rapid pace that the legislator cannot, at this point in time, know what forms of data transfer may be or become eligible for interception on the basis of the wording of the bill. This raises questions on the foreseeability of the legal

provisions, effectively rendering a test of the necessity and proportionality of the provision of powers impossible.
The Institute recommends that the nature and the essence of the special powers granted to the services be clarified in at least the explanatory memorandum, using a phrasing that can be understood by those less versed in the jargon of the services as well, and with a view to the means of exchanging data presently in development, so as to have the (potential) scope and impact be more readily comprehensible.

- Prior consent
  The bill provides for the prior consent to be given by a minister instead of by an independent organisation. However, the substance of the bill concerns large-scale data interception operations that may affect large groups of people. The Institute therefore is of the opinion that advance review by the court or an independent organisation would be preferable. Such independent review would provide a better guarantee that the various interests and the decision on the necessity, subsidiarity and proportionality of such an operation are properly considered.
  The Institute recommends that it be laid down by law that each use of the special powers of the services, in particular the targeted and untargeted interception of telecommunications data, be approved in advance by an independent body.

- Lawfulness review by CTIVD
  The minister is not, under the draft bill, obliged to follow the opinions of the Review Committee for the Intelligence and Security Services (CTIVD), the supervisory body for the services. Due to the covert nature of the actions performed by the services, the Institute deems it important that the CTIVD's opinions on the lawfulness of the actions by the services (independently of complaints) are given legally binding force. The Institute considers it incomprehensible that the draft bill and the explanatory memorandum in this connection ignore both the recent developments in ECHR case law and the broader international developments expressed in, *inter alia*, the recommendations and reports of UN and Council of Europe bodies, which are united in their consistent emphasis on the necessity of there being an independent supervisory body entitled to issue binding opinions on the lawfulness of an act outside of complaints procedures as well.
  The Institute recommends that the opinions on lawfulness issued by the CTIVD be made legally binding.

- Position of persons entitled to privilege
  The draft bill lacks a special provision on the use of special powers against persons entitled to privilege, like lawyers and doctors. This is a shortcoming, as the substance of the bill touches on special, vulnerable and dependent situations involving, in addition to the right to privacy, the right to accessible healthcare and the right to confidential communication with a lawyer.
  The necessity to have a guarantee in place ensuring the position of persons entitled to privilege reinforces the Institute's recommendation, provided in the above, to have the services only be allowed to intercept the communications of persons entitled to privilege following permission thereto by the court or by another independent body (as has already been provided in the draft bill with respect to journalists).

PRESS RELEASE - 1 SEPTEMBER 2015

Extension powers of security services out of balance

Should the new Intelligence and Security Services Act be adopted, the government would come to hold much more power over all information in the Netherlands. The bill allows for the untargeted interception of telecommunications by the Dutch security services. This means that the government would be able to listen in on all Dutch citizens. A strong violation of privacy, the Netherlands Institute for Human Rights argues. To make matters worse, the sole body supervising the application of this Act, the CTIVD, is not granted the power to force that same government to halt such interception. Human rights provide guarantees protecting us from violations of our privacy. And exactly those guarantees are lacking in the bill. The Institute therefore calls on the government to as yet embed these guarantees in the bill.

The most important point of criticism directed at the bill is that the security services are entitled to use these powers without requiring the permission of an independent body, like the court. The services only require permission of the minister involved. Sweden, Germany and Belgium do require the services to request permission from an independent body. No reason was provided why this would be impossible in the Netherlands.

Furthermore, the supervisory body, the CTIVD, is not granted enough power. This body is to review whether the actions by the services are lawful. But the minister is not obliged to comply with the CTIVD's opinion. This runs counter to the recommendations of the Dessens Committee, which, at the request of the government, reviewed the legislation currently in force and expressly recommended that the CTIVD's opinion be binding.

Why is the untargeted interception of information a problem?
The bill allows for the interception of large amounts of information of an unlimited group of people not suspected of any offence. This includes practices like tapping e-mails and social media messages. But the bill even goes beyond this. The bill would also allow the interception of all other sorts of digital data traffic. Should this bill enter into force, the security services would also be allowed to tap these new forms of data traffic. The developments in this field proceed at such a rapid pace that the scope and impact on privacy cannot be foreseen.

In brief: the security services are granted more powers, but there is no corresponding increase in supervision. Due to the enormous impact these new powers may have on the privacy of all Dutch citizens, this is unacceptable from a human rights position. Confidence and trust in governments and security services have globally been under pressure ever since the revelations by Edward Snowden showed that intelligence services exceeded their powers. The Dutch security services do not have a completely unblemished record in this connection, either. The bill does not improve public confidence in the performance of the security services. Rather, it only strengthens the mistrust already felt.