Suggestions for right to privacy-related questions to be included in the list of issues prior to reporting on Germany, Human Rights Committee, 123rd Session

May 2018

Introduction

Privacy International encourages the Committee to seek information from the government of Germany on the impact of communications surveillance on the right to privacy.

In particular, Privacy International is concerned about the following issues:

- Mass surveillance powers in relation to communications of foreign nationals abroad;
- Intelligence sharing with foreign partners;
- Hacking for surveillance.

Mass surveillance powers

The Act for Foreign-Foreign Signals Intelligence Gathering of the Federal Intelligence Service, adopted in 2016,[1] authorizes the Federal Intelligence Service (BND) to gather and process communications of foreign nationals abroad.

Privacy International is concerned by the following aspects of this law:

- Legality - The purposes for such surveillance are very broad, including the undefined "national security" and the over-encompassing "intelligence that is important for foreign and security policy".
- Mass surveillance - Some of the world's largest internet exchange points are situated in Germany, thus making the country a central hub for significant portions of the world's internet traffic. While the Act provides that authorisation for interception against foreigners must be conducted only from *within* Germany's territory, a legislative move which might seem limiting, in actuality in light of Germany's unique geographical position, it authorises the BND to tap these exchange points, which may maximize global surveillance. As noted by the UN Special Rapporteur on the right to privacy, "mass and targeted surveillance of extraterritorial communications between non-German citizens would be effectively authorized in cases where the communication interception is carried out in Germany".[2]

[1] http://dip21.bundestag.de/dip21/btd/18/095/1809529.pdf. The Act (Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes) is in German and there is currently no official English translation. Privacy International notes that its analysis is based on an unofficial translation of the Act.
[2] Report of the UN Special Rapporteur on the right to privacy in the digital age, UN doc. A/71/368, 30 August 2016, paragraph 37.

- Independent authorization and oversight - The law provides for no judicial authorisation of the surveillance measures. Instead the law establishes a three-member administrative committee comprised of two judges and one federal public prosecutor at the Federal Court of Justice. The Panel reviews and may revoke the surveillance directives issued by the Federal Chancellery. As noted by the UN Special Rapporteur on the right to privacy, the panel "is only required to meet four times a year and […] may not have sufficient staff or resources to oversee mass surveillance operations that are, by their very definition, extensive in scope."[3]

Intelligence sharing with foreign partners

The Act for Foreign-Foreign Signals Intelligence Gathering of the Federal Intelligence Service also authorises the BND to gather and process the communications of foreign nationals abroad. Sections 13-15 of the Act set out the general parameters for BND's intelligence cooperation with foreign agencies, including via intelligence sharing. This Act contains important safeguards (e.g. exhaustion of alternative means, cooperation based on written agreement, oversight by the Parliamentary Committee) to govern intelligence sharing. To Privacy International's knowledge, it is the first and only attempt to date by a state to regulate in any detail, via primary legislation, intelligence cooperation through intelligence sharing. However, significant concerns remain:

- Justifications for cooperation: The BND may cooperate with foreign agencies for one of three broadly defined purposes in order to achieve one or more of seven, again broadly defined, objectives. Pursuant to international human rights law, the principle of legality requires that relevant laws must meet certain minimum qualitative requirements of accessibility and foreseeability. Some of the purposes and objectives for cooperation under the Act are so vague (e.g. to handle crises abroad) or open-ended (e.g. in comparable cases) as to arguably violate the principle of legality.

- International Human Rights Law as a guiding framework: Pursuant to the Act, cooperation agreements bind the parties to fundamental rule of law principles but not to international human rights law. Intelligence sharing (and other forms of intelligence cooperation) interfere with fundamental human rights. The Act should therefore clearly state that such cooperative activities shall be governed by international human rights law.

- Circumventing constraints on surveillance: Intelligence sharing may lead to circumstances where states circumvent international or domestic constraints on direct surveillance by relying on their partners to obtain and then share information. The Act does not appear to explicitly prohibit the BND from using sharing arrangements to circumvent such constraints.

- Facilitating serious human rights abuses: The Act does not appear to articulate procedures for assessing whether information shared by the BND with other

[3] Report of the UN Special Rapporteur on the right to privacy in the digital age, UN doc. A/71/368, 30 August 2016, paragraph 37.

agencies may be used to facilitate serious human rights abuses. Similarly, the Act does not appear to articulate procedures for assessing information the BND accesses or receives through sharing, including whether it was obtained in violation of international law or raises reliability concerns.

Hacking for surveillance purposes

Hacking by law enforcement agencies in Germany may be authorised under two legal bases. First, pursuant to the code of criminal procedure to facilitate the interception of communications (section 100a) and to access information from seized devices (sections 94 and 98). Second, pursuant to the Federal Criminal Police Office Act, to covertly access information systems (section 20k).[4]

Privacy International is concerned by the following aspects of the legal regimes governing hacking by law enforcement agencies:[5]

- Legality - because hacking raises such significant privacy and security implications, it must be authorised pursuant to an explicit framework tailored to those implications, rather than through existing surveillance powers, such as those in the code of criminal procedure.
- Necessity and proportionality – while both legal bases provide for judicial authorisation of hacking measures, they do not require the judge to take into account any of the security implications of hacking. This is a significant gap: the exercise of the right to privacy is linked to the security of the devices, networks and services individuals rely on to communicate with each other. Given the significant security risks of hacking, an assessment of those risks is relevant to an assessment of the scope and nature of a hacking measure's interference with the right to privacy.
- Notification – German law requires notification to those whose communications are affected by interception. However, in the case of hacking, notification should also include the affected hardware and software manufacturers and service providers.
- Public reporting – German laws require annual reporting of interception of communications, including through hacking. However, these reporting requirements are not sufficiently specific to allow a review of hacking operations and assess their necessity and proportionality. They do not specifically require reporting on, for example: the method, extent and duration of hacking in applications approving hacking; the number of vulnerabilities exploited; when vulnerabilities were disclosed to companies; whether exploits of vulnerabilities affect systems other than those targeted (and number of non-target systems and users affected by hacking); damage

[4] For an analysis of these powers, see report by LIBE Committee, Germany Country Report (completed with the support of Dr Sven Herpig, Project Director, Transatlantic Cyber Forum, Stiftung Neue Verantwortung; and Rainer Franosch, Senior Public Prosecutor, State of Hesse), available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

[5] For a detailed analysis of the privacy and security considerations that must be included in a human rights assessment of government hacking for surveillance, see Privacy International, Government Hacking and Surveillance, 10 Necessary Safeguards, https://www.privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary.

to systems and data that occurred from hacking and how damage was mitigated or corrected.

Privacy International also notes that the broad surveillance powers contained in the Act for Foreign-Foreign Signals Intelligence Gathering of the Federal Intelligence Service may allow German intelligence agencies to carry out hacking for surveillance for a broad number of purposes and without fundamental safeguards such as judicial authorisation.

List of issues

Based on the above observations, Privacy International proposes the following questions for the List of Issues on Germany:

- How does the Act for Foreign-Foreign Signals Intelligence Gathering of the Federal Intelligence Service comply with the requirements of Article 17 of the ICCPR, in particular by ensuring that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance?
- What safeguards are in place to ensure that intelligence sharing by the German intelligence services comply with Article 17 of ICCPR? How is their effectiveness assessed?
- How is government hacking for surveillance compliant with the ICCPR and in particular how is hacking by German intelligence services regulated and subjected to independent authorization and oversight?