PRIVACY INTERNATIONAL

Minimum safeguards on intelligence sharing required under international human rights law

A report to the UN Counter-Terrorism Committee Executive Directorate

November 2018

Contents

Introduction

Faced with the transnational dimension of terrorist-related activities, United Nations Security Council resolutions have emphasized the need for international cooperation in information-sharing, both for the purposes of collecting intelligence and judicial assistance[1].

Privacy International recognises the importance and benefit of intelligence sharing in the context of preventing and investigating terrorism or other genuine, serious threats to national security[2]. The organisation is concerned, however, that unregulated, unfettered and unwarranted intelligence sharing poses substantive risks to human rights and to the democratic rule of law.

Privacy International's research and comprehensive 2018 report shows that most countries around the world lack domestic legislation governing intelligence sharing, that most intelligence sharing agreements are secret and that independent oversight of intelligence sharing is inadequate[3].

UN Security Council resolutions recognize the need to ensure that measures taken to combat terrorism, including intelligence sharing, must comply with international human rights law. However, they give no indication of the safeguards necessary to ensure such compliance.

Privacy International believes that there is an urgent need to provide guidance to states, particularly in light of the fact that the counter-terrorism measures envisaged in UN Security Council resolution 2396 (2017) were adopted under Chapter VII of the UN Charter.

In the following sections, Privacy International identifies some minimum safeguards that states must introduce in order to ensure their intelligence sharing laws and practices are compliant with applicable international human law. The briefing focusses mainly on states' obligation to respect and protect the right to privacy as enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17

1 See, in particular, UN Security Council resolutions S/RES/1373 (2001), 2322 (2016) and 2396 (2017).

2 Privacy International is a non-governmental organization, which is dedicated to protecting the right to privacy around the world. Privacy International is committed to ensuring that government surveillance complies with the rule of law and the international human rights framework. As part of this commitment, Privacy International researches and investigates government surveillance to raise public awareness about technologies and laws that place privacy at risk.

3 Privacy International, 'Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards' (April 2018). Available at: https://privacyinternational.org/report/1741/secret-global-surveillance-networks-intelligence-sharing-between-governments-and-need

of the International Covenant on Civil and Political Rights[4].

Privacy International encourages the UN Security Council Counter-Terrorism Committee Executive Directorate (CTED) to consider these safeguards in their assessment of states' measures on intelligence sharing and their compliance with the UN Security Council resolutions.

1. Legality

• Intelligence sharing must be prescribed by law and limited to that strictly and demonstrably necessary to achieve a legitimate aim. That law must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the intrusion.

In most countries around the world, governments share intelligence in a legal vacuum. The report of the UN High Commissioner for Human Rights on the right to privacy in the digital age starkly notes that "with very few exceptions, legislation has failed to place intelligence-sharing on a proper statutory footing, compliant with the principle of legality under international human rights law."[5]

International human rights law provides that any interference with the right to privacy, including intelligence sharing, must be in accordance with the law[6]. At the heart of the principle of legality is the important premise that placing "intrusive surveillance regimes on a statutory footing" subjects them to "public and parliamentary debate". Legality is also closely tied to the concept of "arbitrary interference", the idea being that the exercise of a secret power carries the inherent risk of its arbitrary application[8].

The meaning of "law" implies certain minimum qualitative requirements. The

4 Privacy International is mindful that intelligence sharing may facilitate a range of other serious human rights abuses as well as violations of international humanitarian law.

5 UN High Commissioner for Human Rights, Report on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018), paragraph 21.

6 See Article 17(1), International Covenant on Civil and Political Rights ("ICCPR") ("No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence"); Article 11, American Convention on Human Rights ("ACHR") ("2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence […]. 3. Everyone has the right to the protection of the law against such interference"); Article 8(2), European Convention of Human Rights ("ECHR") ("There shall be no interference by a public authority with the exercise of [the right to respect for private and family life] except such as is in accordance with the law").

7 Report of the UN Special Rapporteur on Counter-Terrorism, UN Doc. A/HRC/34/61, 21 Feb. 2017, para. 36.

8 See UN Human Rights Committee, General Comment No. 16, supra, at para. 4 (noting that "the expression 'arbitrary interference' can also extend to interference provided for under the law" and that "[t]he introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims, and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances"). See also, Malone v. United Kingdom, European Court of Human Rights, App. No. 8691/79, 2 Aug. 1984, para. 67 ("Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident.").

meaning of "law" implies certain minimum qualitative requirements. The UN Human Rights Committee has elaborated on the meaning of "law" as follows: "[A] norm, to be characterized as a 'law,' must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public [...] Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not."[9]

The UN General Assembly has recognized the application of the principle of legality to the surveillance context, resolving that the "surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory."[10]

The European Court of Human Rights has elaborated on the "minimum safeguards that should be set out in statute law in order to avoid abuses of power" where the state conducts surveillance:

> "[1] the nature of the offences which may give rise to a [ ] [surveillance] order; [2] a definition of the categories of people liable to [be subject to surveillance]; [3] a limit on the duration of [surveillance]; [4] the procedure to be followed for examining, using and storing the data obtained; [5] the precautions to be taken when communicating the data to other parties; and [6] the circumstances in which recordings may or must be erased or the tapes destroyed."[11]

Similarly, the Inter-American Court of Human Rights held that surveillance measures "must be based on a law that must be precise." The Court further observed that the law must "indicate the corresponding clear and detailed rules, such as the circumstances in which this [surveillance] measure can be adopted, the persons authorized to request it, to order it and to carry it out, and the procedure to be followed."[12]

Notably, these safeguards must apply also in the context of intelligence sharing. The European Court of Human Rights has recently confirmed this requirement in the

9 UN Human Rights Committee, General Comment No. 34 (Article 19 ICCPR), 12 Sept. 2011, para. 25. The requirements of accessibility and foreseeability are also reflected in the jurisprudence of the European Court of Human Rights ("ECtHR"): "Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a law unless it is formulated with sufficient precision to enable the citizen to regulate his conduct; he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail." (Sunday Times v. United Kingdom, European Court of Human Rights, App. No. 6538/74, 26 Apr. 1979, para. 49.)

10 UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc. A/RES/71/199, 19 Dec. 2016.

11 Weber & Saravia v. Germany, European Court of Human Rights, App. No. 54934/00, 29 June 2006, para. 95.

12 Escher et al. v. Brazil, Inter-American Court of Human Rights, Case 12.353, 2 Mar. 2006, para. 131.

judgment of Big Brother Watch and others v. UK. In the judgment, the Court indicates that the interference to privacy resulting from obtaining information through intelligence sharing is equivalent to the interference resulting from if it had obtained that information through its direct surveillance. The Court stated that:

> "As with any regime which provides for the acquisition of surveillance material, the regime for the obtaining of such material from foreign Governments must be 'in accordance with the law'; in other words, it must have some basis in domestic law, it must be accessible to the person concerned and it must be foreseeable as to its effects. Furthermore, it must be proportionate to the legitimate aim pursued, and there must exist adequate and effective safeguards against abuse. In particular, the procedures for supervising the ordering and implementation of the measures in question must be such as to keep the 'interference' to what is 'necessary in a democratic society'."[14]

• Intelligence sharing must not be used to circumvent international or domestic legal constraints – including effective safeguards and oversight – that regularly apply to direct surveillance conducted by the State.

Cross-border access to data may lead to a "revolving door" situation, whereby States circumvent international and domestic constraints on accessing data by relying on authorities in other states to acquire and then share such data. An example of a common constraint is domestic restrictions on a State's ability to conduct surveillance on its own citizens[15]. It is not clear, for instance, how this constraint might meaningfully apply where a State accesses or receives data acquired in bulk by another State. States may also explicitly use intelligence sharing arrangements to obtain information they could not otherwise acquire through direct surveillance, such as that relating to their own citizens.

Independent human rights mechanisms have expressed concerns about the risk that States may be participating in such practices. The UN High Commissioner for Human Rights has noted how "governments across the globe routinely share intelligence on individuals outside any legal framework and without adequate oversight. Intelligence-sharing poses the serious risk that a State may use this approach to circumvent domestic legal constraints by relying on others to obtain and then share information."[16]

13 Big Brother Watch and others v. The United Kingdom, European Court of Human Rights, Application nos. 58170/13, 62322/14, 24960/15, 13 September 2018.

14 Big Brother Watch and others, *supra*, para. 422.

15 See Council of Europe Commissioner for Human Rights, Positions on Counter-Terrorism and Human Rights Protection, p. 11 (5 June 2015) (noting that "the principle of making data available to other authorities should not be used to circumvent European and national constitutional data-protection standards"). For further reading see European Commission for Democracy through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, Study No. 719/2013 CDL-AD(2015)006, para. 11 (7 Apr. 2015).

16 Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/39/29, supra, para. 21.

The European Court of Human Rights has also recognised that:

> "if Contracting States were to enjoy an unfettered discretion to request either the interception of communications or the conveyance of intercepted communications from non-Contracting States, they could easily circumvent their obligations under the Convention. Consequently, the circumstances in which intercept material can be requested from foreign intelligence services must also be set out in domestic law in order to avoid abuses of power. […] they [the circumstances] must nevertheless be circumscribed sufficiently to prevent – insofar as possible – States from using this power to circumvent either domestic law or their Convention obligations."[17]

Similarly, the Council of Europe Commissioner for Human Rights has noted that: "the principle of making data available to other authorities should not be used to circumvent European and national constitutional data-protection standards."[18]

2. Independent authorisation

- **Intelligence sharing must be authorised by an independent authority, preferably judicial.**

Privacy International's research has found no State that requires an independent oversight body to authorise decisions to share intelligence, either at a general level or in specific circumstances. In fact, in most cases, the process to authorise intelligence sharing appears to bypass any independent authority.[19]

International human rights bodies have emphasized prior independent authorisation – preferably judicial – as a key mechanism for "ensur[ing] the effectiveness and independence of a monitoring system for surveillance activities".[20]

Independent authorization should apply also to intelligence sharing, as noted by the UN High Commissioner for Human Rights. The UN Human Rights Committee has further recognised the importance of prior independent authorization in the context of intelligence sharing, indicating that "robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities" should include "providing for judicial involvement in the authorisation of such measures in all cases".[22]

17 Big Brother Watch and others, supra, para. 424.

18 Council of Europe Commissioner for Human Rights, Positions on Counter-Terrorism and Human Rights Protection, p. 11 (5 June 2015).

19 See Privacy International, 'Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards' (April 2018), *supra.*

20 UN Human Rights Committee, Concluding Observations on the Fifth Periodic Report of France, UN Doc. CCPR/C/FRA/CO/5, 17 Aug. 2015, para. 12.

21 UN High Commissioner for Human Rights' report on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018), *supra*, para. 39.

22 UN Human Rights Committee, Seventh Periodic Report of the United Kingdom, *supra*, at para. 24.

3. Effective oversight

• Independent intelligence oversight mechanisms should be able to exercise their powers with respect to intelligence sharing activities.

Intelligence sharing poses a number of challenges to oversight mechanisms. In particular, many intelligence sharing arrangements prohibit the disclosure of information shared between agencies to third parties, which may include oversight mechanisms, without the prior consent of the state from which the information originated. This prohibition is typically referred to as the "third party rule" or the "originator control principle". Such a requirement that oversight bodies seek the consent of a foreign intelligence agency to access information is fundamentally detrimental to oversight.

Oversight mechanisms in States acquiring as well as accessing or receiving the data is fundamental to ensure accountability and prevent abuses. Human rights bodies have repeatedly emphasised the importance of and called for effective oversight of intelligence sharing arrangements.

The European Court of Human Rights has noted that:

> "The governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question and which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures."[23]

The UN Human Rights Committee has repeatedly recommended to put in place "effective and independent oversight mechanisms over intelligence- sharing of personal data"[24].

Similarly, the Council of Europe Commissioner for Human Rights has recommended that intelligence oversight bodies be mandated to scrutinise the human rights compliance of security service co-operation with foreign bodies, including co-operation through the exchange of information, joint operations and the provision of equipment and training[25].

23 Szabó and Vissy v. Hungary, European Court of Human Rights, App. No. 37138/14, 12 Jan. 2016, para. 78.

24 UN Human Rights Committee, Seventh Periodic Report of Sweden, supra, at paras. 36-37; see also UN Human Rights Committee, Concluding Observations on the Initial Report of Pakistan, *supra*, at para. 35; UN Human Rights Committee, Seventh Periodic Report of the United Kingdom, *supra*, at para. 24; UN Human Rights Committee, Sixth Periodic Report of Canada, *supra*, at para. 10.

25 Commissioner for Human Rights, Council of Europe, Issue Paper on Democratic and Effective Oversight of National and Security Services, Commissioner's Recommendations (May 2015).

• Whenever intelligence sharing is done via a bilateral or multilateral arrangement (i.e. an international treaty, agreement, Memorandum of Understanding, etc.) those must be transparent and legally binding agreements subject to the international and domestic procedures governing such agreements.

• Independent oversight bodies must have access to intelligence sharing agreements and must have the power and capacity to consider all relevant policies and activities related to intelligence sharing.

Intelligence sharing is often regulated by arrangements which vary in scope, formality and detail. They are typically confidential and not subject to public scrutiny, often taking the form of secret memoranda of understanding directly between the relevant ministries or agencies.

Such agreements may expressly state that they are not to be construed as legally binding instruments according to international law. By doing so, the agreements can circumvent the requirement of ratification under the constitutional procedures and/or domestic laws of each member State.

Their secrecy poses a significant challenge to independent oversight bodies. As noted by the UN Special Rapporteur on counter-terrorism and human rights:

> "intelligence-sharing arrangements tend to be, more often than not, exempted from the supervision of an independent authority. Oversight bodies are typically not informed of the conclusion of intelligence-sharing agreements and therefore unlikely to review the compatibility of such agreements with domestic and international law. Due to limitations justified by state sovereignty, they have very little or no oversight over the use of information shared with foreign agencies. Moreover, they are limited in their powers to seek or verify information about the means and methods of collection, retention and processing of information shared by another State, particularly as intelligence- sharing arrangements regularly prohibit the disclosure of such information to third parties."[26]

Independent oversight mechanisms must not only be able to access and scrutinize intelligence sharing arrangements, but also the intelligence sharing activities undertaken by the State.

The Council of Europe Commissioner for Human Rights has made specific recommendations on the scope of such scrutiny, indicating that it should include but not be limited to "examining: (a) ministerial directives and internal regulations relating to international intelligence co-operation; (b) human rights risk assessment and risk-management processes relating to relationships with specific foreign

26 UN Special Rapporteur on counter-terrorism and human rights, submission to the Office of the High Commissioner for Human Rights, https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/SRCT.pdf

c) outgoing personal data and any caveats (conditions) attached thereto; (d) security service requests made to foreign partners: (i) for information on specific persons; and (ii) to place specific persons under surveillance; (e) intelligence co-operation agreements; (f) joint surveillance operations and programmes undertaken with foreign partners."[27]

4. Joint responsibility and due diligence

• Due diligence obligations apply to States acquiring and then sharing the information as well as to States accessing or receiving the data. Both states share responsibility for the collection, storage, analysis, dissemination, and use of the data. Both states may be liable for human rights violations that occur as a result of the transfer of the data or its later utilization.

Intelligence sharing poses significant challenges to accountability. Some of these challenges are inherent to the trans-border, cross-jurisdictional nature of intelligence sharing. Generally, intelligence agencies lack control over the actions of their foreign partners. They cede control over information once shared, despite whatever limitations ("caveats") may be attached to the sharing of that information. Their ability to influence or verify how that information will be used or to subsequently substantiate how it was used will be subject to significant limitations. Their ability to verify or substantiate the provenance and other details regarding information shared by another state will be similarly constrained.

These inherent limitations can however facilitate the shirking of accountability over intelligence sharing. Because it can be so difficult to influence, verify or substantiate the use of information – or the means by which information was obtained – it can be easy for states sharing intelligence to assert "plausible deniability". Indeed, intelligence agencies have strong incentives not to make robust inquiries, for fear of damaging partnerships with foreign agencies[28].

States' due diligence obligations encompass the following:

• States acquiring information must conduct an analysis regarding the human rights record of the state authority with whom information is shared, with a particular focus on whether that authority has appropriate safeguards to protect privacy, and whether information may later be used to facilitate human rights violations;
• States accessing or receiving data must conduct an analysis as to the accuracy and verifiability of the data received prior to relying on that data.

27 Commissioner for Human Rights, Council of Europe, Issue Paper on Democratic and Effective Oversight of National and Security Services, Commissioner's Recommendations (May 2015), *supra*.

28 See European Commission for Democracy through Law (Venice Commission), Report on the Democratic Oversight of the Security Services, Study No. 388/2006 CDL-AD(2007)016, 11 June 2007, paras. 120-21.

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

UK Registered Charity No. 1147471