PRIVACY INTERNATIONAL

Briefing to National Intelligence Oversight Bodies

Human Rights Implications of Intelligence Sharing

September 2017

Introduction

The effective oversight of secret surveillance is among the fundamental guarantees against a government's unlawful interference with the right to privacy. But there is an alarming lack of effective oversight of secret surveillance in a range of countries around the world. As noted by the United Nations High Commissioner for Human Rights:

"[A] lack of effective oversight has contributed to a lack of accountability for arbitrary or unlawful intrusions on the right to privacy in the digital environment. Internal safeguards without independent, external monitoring in particular have proven ineffective against unlawful or arbitrary surveillance methods. While these safeguards may take a variety of forms, the involvement of all branches of government in the oversight of surveillance programmes, as well as of an independent civilian oversight agency, is essential to ensure the effective protection of the law."[1]

Greater transparency is needed to ensure effective oversight. In particular, there has been a lack of transparency regarding bilateral and multilateral intelligence sharing arrangements. Below, Privacy International describes:

- Intelligence sharing arrangements
- The international and domestic legal frameworks governing intelligence sharing
- The international human rights implications of intelligence sharing

Privacy International concludes with a series of recommendations for national intelligence oversight bodies. The recommendations urge these bodies to increase transparency regarding the intelligence sharing arrangements to which their respective governments are party and to subject such arrangements to greater scrutiny, including assessing their compliance with international and domestic law.

1 Report of the Office of the U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37, para. 37 (30 June 2014).

Intelligence Sharing

Intelligence sharing arrangements cover an array of potential activity between governments including, inter alia, information sharing, operational cooperation, facilities and equipment hosting, training and capacity building, and technical and financial support.[2] Within each of these categories, the spectrum of potential engagement is broad. Information sharing, for example, might range from arrangements for ad hoc sharing of intelligence briefs subject to specific request and approval to the automated exchange of raw signals intelligence or the joint management of databases.[3]

One of the most commonly cited sharing arrangements is the Five Eyes alliance – a secretive, global surveillance arrangement comprised of the United States National Security Agency ("NSA"), the United Kingdom's Government Communications Headquarters ("GCHQ"), the Communications Security Establishment Canada ("CSEC"), the Australian Signals Directorate ("ASD"), and New Zealand's Government Communications Security Bureau ("GCSB"). Despite being over 70 years old, very little is known about the alliance and the agreement(s) that govern it.[4] Even less is known about the other surveillance partnerships that have grown from the Five Eyes, such as the 9-Eyes (the Five Eyes plus Denmark, France, the Netherlands and Norway), the 14-Eyes (the 9-Eyes plus Belgium, Germany, Italy, Spain and Sweden), and the 43-Eyes (the 14-Eyes plus the addition of the 2010 members of the International Security Assistance Forces to Afghanistan).[5]

2 For further reading, see Hans Born et al., Making International Intelligence Cooperation Accountable, pp. 18-25 (2015).

3 For a review of intelligence sharing practices, particularly in the context of the highly-integrated relationship between the U.S. and U.K. intelligence agencies, see Witness Statement of Eric King, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and the Government Communication Headquarters, Investigatory Powers Tribunal, IPT/13/92/CH, paras. 70-90 (8 June 2014), available at www.privacyinternational.org/sites/default/files/Eric%20King%20witness%20statement_0.pdf.

4 For an overview of what we do know about the Five Eyes alliance, see Privacy International, Eyes Wide Open, 26 Nov. 2013, available at https://www.privacyinternational.org/node/301.

5 For further reading on the 43-Eyes see Five Eyes, 9-Eyes, and Many More, Electrospaces.net, 15 Nov. 2013, http://electrospaces.blogspot.co.uk/2013/11/five-eyes-9-eyes-and-many-more.html. The full list of 43 Eyes states are as follows: U.S., U.K., Canada, Australia, New Zealand, Denmark, France, Netherlands, Norway, Belgium, Germany, Italy, Spain, Sweden, Albania, Armenia, Austria, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Finland, Georgia, Greece, Hungary, Iceland, Ireland, Latvia, Lithuania, Luxembourg, Macedonia, Montenegro, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Switzerland, Turkey, and Ukraine. Privacy International acknowledges that the make-up of these alliances, particularly the 43-Eyes, may have shifted over time. The general lack of clarity around intelligence sharing arrangements makes it difficult to confirm their exact scope.

There are additional bilateral and multilateral intelligence sharing arrangements spanning other geographical regions. For example:

- The Club de Berne is an intelligence sharing arrangement between the intelligence services of the members of the European Union ("EU"). The European Union Agency for Law Enforcement Cooperation ("EUROPOL") is the EU's law enforcement agency and also promotes intelligence sharing between the EU members.[6]
- The Africa-Frontex Intelligence Community ("AFIC") is an intelligence sharing arrangement between European and African countries in the field of border security.[7]
- The Great Lakes Regions Intelligence Fusion Centre facilitates intelligence sharing between 11 countries in that region.[8]
- The Shanghai Cooperation Organization ("SCO") is an intelligence sharing arrangement between China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.[9]
- Russia, Iraq, Iran and Syria have formed an intelligence sharing arrangement to facilitate cooperation in combating the Islamic State.[10]

6 James Igoe Walsh, The International Politics of Intelligence Sharing, 88-110 (2010).
7 See generally, Frontex Publishes Africa-Frontex Intelligence Community (AFIC) Report (6 Apr. 2017), available at http://frontex.europa.eu/news/frontex-publishes-africa-frontex-intelligence-community-afic-report-acjRuQ.
8 Steven Addamah, Central Africa: Great Lakes Countries Upgrade Intelligence Sharing Cooperation, Medafrica Times, 26 June 2012, available at http://medafricatimes.com/329-central-africa-great-lakes-countries-upgrade-intelligence-sharing-cooperation.html. The 11 countries are: Angola, Burundi, the Central African Republic, Congo, the Democratic Republic of Congo, Kenya, Rwanda, Sudan, Tanzania, Uganda, and Zambia.
9 Eleanor Albert, Council on Foreign Relations, The Shanghai Cooperation Organization Backgrounder (14 Oct. 2015), available at https://www.cfr.org/backgrounder/shanghai-cooperation-organization.
10 J. Dana Stuster, Russia, Iran, Iraq, and Syria to Share Intelligence on Islamic State, Foreign Policy, 28 Sept. 2015, available at http://foreignpolicy.com/2015/09/28/russia-iran-iraq-and-syria-to-share-intelligence-on-islamic-state/.

Intelligence Sharing and International and Domestic Legal Frameworks

Intelligence sharing arrangements 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.[11] By doing so, the agreements can circumvent the requirement of ratification under the constitutional procedures and/or domestic laws of each member State as well as that of registration with the U.N. Secretariat in accordance with Article 102 of the U.N. Charter.

In addition, most countries around the world lack domestic legislation governing intelligence sharing. Indeed, many countries have only introduced, in recent decades, a legislative basis for the activities of their intelligence agencies. This legislative basis should cover intelligence sharing arrangements so as to similarly imbue them with democratic legitimacy. Where it fails to do so, agencies may potentially use such arrangements to side-step international and domestic legal constraints on their intelligence-gathering activities. The U.N. Special Rapporteur on Counter-Terrorism has stated in this regard that:

"The absence of laws to regulate information-sharing agreements between States has left the way open for intelligence agencies to enter into classified bilateral and multilateral arrangements that are beyond the supervision of any independent authority. Information concerning an individual's communications may be shared with foreign intelligence agencies without the protection of any publicly accessible legal framework and without adequate (or any) safeguards . . . . Such practices make the operation of the surveillance regime unforeseeable for those affected by it and are therefore incompatible with article 17 of the [International] Covenant [on Civil and Political Rights]."[12]

11 See, e.g., Memorandum of Understanding Between the National Security Agency/Central Security Service (NSA/CSS) and the Israeli SIGINT National Unit (ISNU) Pertaining to the Protection of U.S. Persons, available at www.statewatch.org/news/2013/sep/nsa-israel-spy-share.pdf (noting that "this agreement is not intended to create any legally enforceable rights and shall not be construed to be either an international agreement or a legally binding instrument according to international law"). This agreement was first published by The Guardian on 11 September 2013. See Glenn Greenwald et al., NSA Shares Raw Intelligence Including Americans' Data with Israel, The Guardian, 11 Sept. 2013, available at https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

12 Report of the U.N. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397, para. 44 (23 Sept. 2014).

The International Human Rights Implications of Intelligence Sharing

Article 17 of the International Covenant on Civil and Political Rights protects the right to privacy.[13] The U.N. Human Rights Committee has repeatedly stated, in reviewing the intelligence sharing practices of certain member States, that laws and polices regulating such sharing must be in full conformity with obligations under the Covenant. The Committee has specifically noted the need to adhere to Article 17, "including the principles of legality, proportionality and necessity," as well as the need to put in "effective and independent oversight mechanisms over intelligence-sharing of personal data."[14]

The European Court of Human Rights has also expressed concerns regarding the practice of intelligence sharing and the need for greater oversight:

"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."[15]

13 See also Article 12 of the Universal Declaration of Human Rights.

14 See Concluding Observations on the Seventh Periodic Report of Sweden, U.N. Human Rights Committee, U.N. Doc. CCPR/C/SWE/CO/7, paras. 36-37 (28 Apr. 2016); Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, U.N. Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7, para. 24 (17 Aug. 2015); Concluding Observations on the Sixth Periodic Report of Canada, U.N. Human Rights Committee, U.N. Doc CCPR/C/CAN/CO/6, para. 10 (13 Aug. 2015).

15 See Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment, para. 78 (12 Jan. 2016).

16 For a more detailed list of the potential international human rights risks posed by intelligence sharing, see Born, supra note 2, at pp. 40-59.

The interference with privacy posed by intelligence sharing is equivalent to that posed by direct state surveillance. Just as government surveillance must be transparent and subject to adequate safeguards and oversight, so too must intelligence sharing arrangements. Non-transparent, unfettered and unaccountable intelligence sharing threatens the foundations of the human rights legal framework and the rule of law. In particular, Privacy International emphasizes three areas of concern:[16]

1. Intelligence sharing may permit States to circumvent international and domestic constraints on direct surveillance by allowing them to rely on their partners to obtain and then share information. An example of a common constraint is domestic restrictions on a State's ability to conduct surveillance on its own citizens.[17] It is not clear, for instance, how this constraint might meaningfully apply where a State accesses or receives data obtained in bulk by another State. States may also explicitly use intelligence sharing arrangements to obtain information they could not otherwise obtain through direct surveillance, such as that relating to their own citizens.

2. States may share intelligence with States known for violating international law, including international human rights and international humanitarian law. Such sharing can place individuals in those States at particular risk. These States could, for example, use the intelligence received to persecute minority groups, immigrant populations, human rights defenders, dissidents and journalists.[18]

3. Intelligence sharing can weaken accountability generally. Agencies are incentivized not to inquire into the source and the means by which information is obtained in order to ensure "plausible deniability." And even if they were to make robust inquiries, the claims of the acquiring agency are difficult to substantiate in practice.[19] Intelligence oversight mechanisms often have remit only over the activities of their national agencies. Moreover, many intelligence sharing arrangements prohibit disclosure of shared information with third parties, which may include oversight mechanisms.[20]

16 For a more detailed list of the potential international human rights risks posed by intelligence sharing, see Born, supra note 2, at pp. 40-59.

17 See Craig Forcese, The Collateral Casualties of Collaboration: The Consequences for Civil and Human Rights of Transnational Intelligence Sharing, in International Intelligence Cooperation and Accountability, Pre-Conference Draft Paper, Conference on Intelligence Sharing, sponsored by the Norwegian Parliamentary Intelligence Oversight Committee, pp. 90-92 (5 Mar. 2009), available at https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=1354022; Commissioner for Human Rights, Council of Europe, 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).

18 See, generally, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32, para. 59 (22 May 2015); Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet, para. 150 (31 Dec. 2013).

19 For further reading, 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, paras. 115-121 (11 June 2007).

20 For further reading, see Parliamentary Assembly of the Council of Europe (PACE), Resolution on Mass Surveillance 2045, para. 19.2 (21 Apr. 2015).

To address these concerns, governments must establish, through primary legislation, publicly accessible legal frameworks governing intelligence sharing, which require:

- Intelligence sharing arrangements to constitute legally binding agreements subject to the international and domestic procedures governing such agreements;

- Clarity as to the circumstances in which their intelligence agencies will exchange information and the procedures governing such exchange, including limiting any such sharing to where it is necessary and proportionate;

- That international and domestic legal constraints – including effective safeguards and oversight – that regularly apply to direct surveillance by the State equally apply to information acquired through intelligence sharing arrangements;

- Due diligence obligations on States obtaining and then sharing information as well as States accessing or receiving information. Both countries share responsibility for the collection, storage, analysis, use, and dissemination of information. States' due diligence obligations may encompass the following:

    - States obtaining and then sharing information must analyse the human rights records of agencies with whom information is shared, with a particular focus on whether those agencies have appropriate safeguards to protect privacy, and whether information may later be used to facilitate human rights abuses;

    - Countries accessing or receiving information must analyse the accuracy and verifiability of the information received prior to relying on that information.

- Oversight mechanisms to exercise their powers with respect to the intelligence sharing activities of their governments and have the remit, resources and access necessary to review all aspects of intelligence sharing arrangements.

Recommendations to Oversight Bodies

Privacy International specifically urges national intelligence oversight bodies, to the extent permitted under their mandates, to:

- Make publicly available as much information as possible as to the nature and scope of intelligence sharing arrangements to which their governments are party, as well as the rules governing such arrangements;

- Review existing legislation and rules governing intelligence sharing with a view to assessing their compliance with international and domestic law, including their respect for the right to privacy and other human rights; and

- Initiate independent investigations into the intelligence sharing practices of their governments and make the results of such investigations publicly available.

Privacy International is happy to provide additional expertise and support as is necessary to achieve these recommendations.