PRIVACY INTERNATIONAL

Briefing

Privacy International's preliminary views on cross-border access to data for intelligence/law enforcement purposes

16 June 2017

Privacy International's preliminary views on cross-border access to data for intelligence/law enforcement purposes

16 June 2017

Introduction

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.

Privacy International welcomes this opportunity to engage in a dialogue over the implementation of the UN Security Council Resolution 2322 (2016), specifically as they related to intelligence sharing and mutual legal assistance mechanisms to access cross-border data.

Data stored extraterritorially can be accessed in a range of ways. For the purpose of the current debates on cross-border access to data, the following ways are particularly relevant:

- Channels of law enforcement information sharing, such as Mutual Legal Assistance Treaties (MLAT), mutual recognition regimes, police-to-police cooperation;
- Intelligence sharing agreements for sharing of information among intelligence agencies;
- Direct request by the national authorities to service providers in another country (this can take many forms, from voluntary cooperation to mandatory requests).

Data includes subscriber information, traffic or metadata and content. It may also include real-time surveillance.[1] They are all personal data, as far as they allow the identification of an individual.

There is growing recognition of the privacy invasive nature of the collection, retention and analysis of metadata, as expressed, for example, by the Human Rights Committee, and in reports by UN expert bodies (including the report of the High Commissioner for Human Rights, 2014 and the report of the Special Rapporteur on counter-terrorism and human rights).[2] In his 2017 report to the Council, the Special Rapporteur on the right to privacy

[1] See for example the U.S. Department of Justice proposed legislation http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf.

[2] In particular, see relevant concluding observations by the Human Rights Committee: Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7 (17 August 2015) "24. The State Party Should: …(d) Revise the Data Retention and Investigatory Powers Act 2014 with a view to ensuring that access to communications data is limited to the extent strictly necessary for prosecution of the most serious crimes and is dependent upon prior judicial authorization." Concluding Observations on the Initial Report of South Africa, Human Rights Committee, U.N. Doc.

noted that metadata is "at least as revealing of a person's individual activity as the actual content of a conversation."[3] For these reasons, the same level of protection should be afforded to metadata and content data in cross border data transfer.

The slow pace and opacity of certain cross-border data requests, namely digital data requests through the MLAT process, has frustrated criminal investigators in many countries. As a result, some states have sought to circumvent established legal mechanisms for accessing data across borders, by turning to data localization regimes and the adoption of extraterritorial enforcement powers, such as remote hacking. These policies and regulations have the potential of abusing privacy rights in profound ways.

Privacy International holds that regardless of the legal framework and practices, the procedures for obtaining data located/stored extraterritorially must always be in line with international law, and international human rights law in particular.[4]

In particular, the following principles shall apply:

1. Legality

- State requests for and dissemination of personal data 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. It should be subject to periodic review by means of a participatory legislative process.
- Whenever cross border data transfers are 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.

Privacy International is particularly concerned about the lack of transparency with regards to the legal framework governing data sharing between intelligence agencies.

Such agreements may expressly state that they are not to be construed as legally binding instruments according to international law.[5] By doing so, the agreements can circumvent the

---

CCPR/C/ZAF/CO/1 (27 April 2016) "42. [The Committee] is also concerned about the wide scope of the data retention regime under the [2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act]... 43. The State Party should... consider revoking or limiting the requirement for mandatory retention of data by third parties...".

[3] Report of the UN Special Rapporteur on the right to privacy, U.N. Doc. A/HRC/34/60. Also to note that in December 2016, the Court of Justice of the European Union confirmed its concerns about the invasive nature of metadata: "That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them […]. In particular, that data provides the means […] of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications." Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016).

[4] For a detailed list of the potential international human rights risks posed by cross border intelligence sharing, *see* Hans Born et al., *Making International Intelligence Cooperation Accountable*, pp. 40-59 (2015).

[5] *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

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.

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. In addition, most countries around the world lack domestic legislation governing intelligence sharing.

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]."[6]

Lack of transparency characterises other cross-border data sharing arrangements. For example, a bilateral agreement between the U.K. and the U.S. ("U.K.-U.S. agreement") aiming at allowing U.K authorities to make direct demands for communications content held by U.S. companies, and vice versa, replacing the current MLAT process, has already been negotiated, but the text has not been publicly released or scrutinized.

- Cross-border access to personal data must not be used to circumvent international or domestic legal constraints – including effective safeguards and oversight – that regularly apply to access to data within 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.[7] 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

---

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.

[6] 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).

[7] *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).

sharing arrangements to obtain information they could not otherwise acquire through direct surveillance, such as that relating to their own citizens.

Such concern has been noted by independent human rights mechanisms. For example, the UN High Commissioner for Human Rights noted how: "there is credible information to suggest that some Governments systematically have routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. Reportedly, some Governments have operated a transnational network of intelligence agencies through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections provided by domestic legal regimes. Such practice arguably fails the test of lawfulness because, as some contributions for the present report pointed out, it makes the operation of the surveillance regime unforeseeable for those affected by it. It may undermine the essence of the right protected by article 17 of the International Covenant on Civil and Political Rights".[8]

Similarly, the Council of Europe Commissioner for Human Rights noted that: "the principle of making data available to other authorities should not be used to circumvent European and national constitutional data-protection standards."[9]

2. Necessity and proportionality

Applying the overarching principles of necessity and proportionality to the access of cross-border data would require that any requests for authorization to access such data need, inter alia, to:

- Demonstrate a strong factual basis to believe that a serious crime or act amounting to a specific, serious threat to national security has been, is being, or will be committed and that the data is relevant and material to the investigation of the crime or act;
- Specify a person, account, or device, and be particularized as to the type, time frame, and scope of data sought;
- Satisfy the least intrusive means test, namely by examining whether the legitimate aim for which access to the data is sought cannot be achieved by other less intrusive means;
- Ensure minimization so that the data obtained is subject to a process designed to protect against the acquisition, processing and dissemination of non-relevant data.

3. Judicial authorisation

- Access to data must be authorised by an independent judicial authority.

There is growing recognition by regional human rights courts and international human rights experts that surveillance measures that interfere with the right to privacy, such as access to personal data, should only be carried out on the basis of prior judicial authorisation.[10]

Further there is growing consensus that judicial authorization is required not only for accessing content but also communications data. For example, the UN Human Rights Committee has recommended that states must ensure "that access to communication data is limited to the extent strictly necessary for the prosecution of the most serious crimes and

[8] 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/27/37 (30 June 2014), paragraph 30.
[9] Commissioner for Human Rights, Council of Europe, Positions on Counter-Terrorism and Human Rights Protection, p. 11 (5 June 2015).
[10] See, e.g., UN High Commissioner for Human Rights' report on the right to privacy in the digital age, U.N. Doc. A/HRC/27/37 (30 June 2014).

dependent upon prior judicial authorization".[11] The Court of Justice of the European Union has also held that "it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body".[12]

4. Effective oversight

- Oversight mechanisms should be able to exercise their powers with respect to cross-border data sharing activities, with broad remit, sufficient resources and appropriate access to review all aspects of sharing policies and practices.

Oversight mechanisms in States acquiring as well as accessing or receiving the data is fundamental to ensure accountability and prevent abuses.

The Human Rights Committee has repeatedly stated that laws and polices regulating intelligence sharing must be in full conformity with obligations under the Covenant. The Committee noted in particular 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".[13]

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 and recommended that such oversight include but is not 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 specifc foreign security services and to specific instances of operational co-operation; (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."[14]

In the context of cross-border access requests by law enforcement agencies, some arrangements and MLAT reform proposals are moving towards allowing companies to directly respond to requests from overseas authorities must include appropriate oversight, particularly to ensure that only data strictly necessary to the investigation is transferred to requesting countries. States must publish annual reports on the number, type, and temporal

[11] Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7 (17 August 2015).
[12] Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016).
[13] Concluding Observations on the Seventh Periodic Report of Sweden, Human Rights Committee, U.N. Doc. CCPR/C/SWE/CO/7 (28 April 2016).
[14] Commissioner for Human Rights, Council of Europe, Issue Paper on Democratic and Effective Oversight of National and Security Services, Commissioner's Recommendations (May 2015). See also *See* Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment, para. 78 (12 Jan. 2016), where the Court 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."

scope of the data requests they request and issue under this framework. Companies should also disclose information on the request they receive.

5. Notification and access to effective remedy

- The person to whom the data pertains, regardless of where they reside, must be notified of the request for access to their data. Delay in notification is only justified where notification would seriously jeopardize the purpose for which access was requested, or endanger the life or physical safety of an individual, and authorisation to delay notification is granted by an impartial and independent judicial authority.

6. 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, irrespective of "originator rule" provisions governing the sharing arrangements. Both states are liable for any human rights violation that occurs as a result of the transfer of the data or its later utilization.

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.