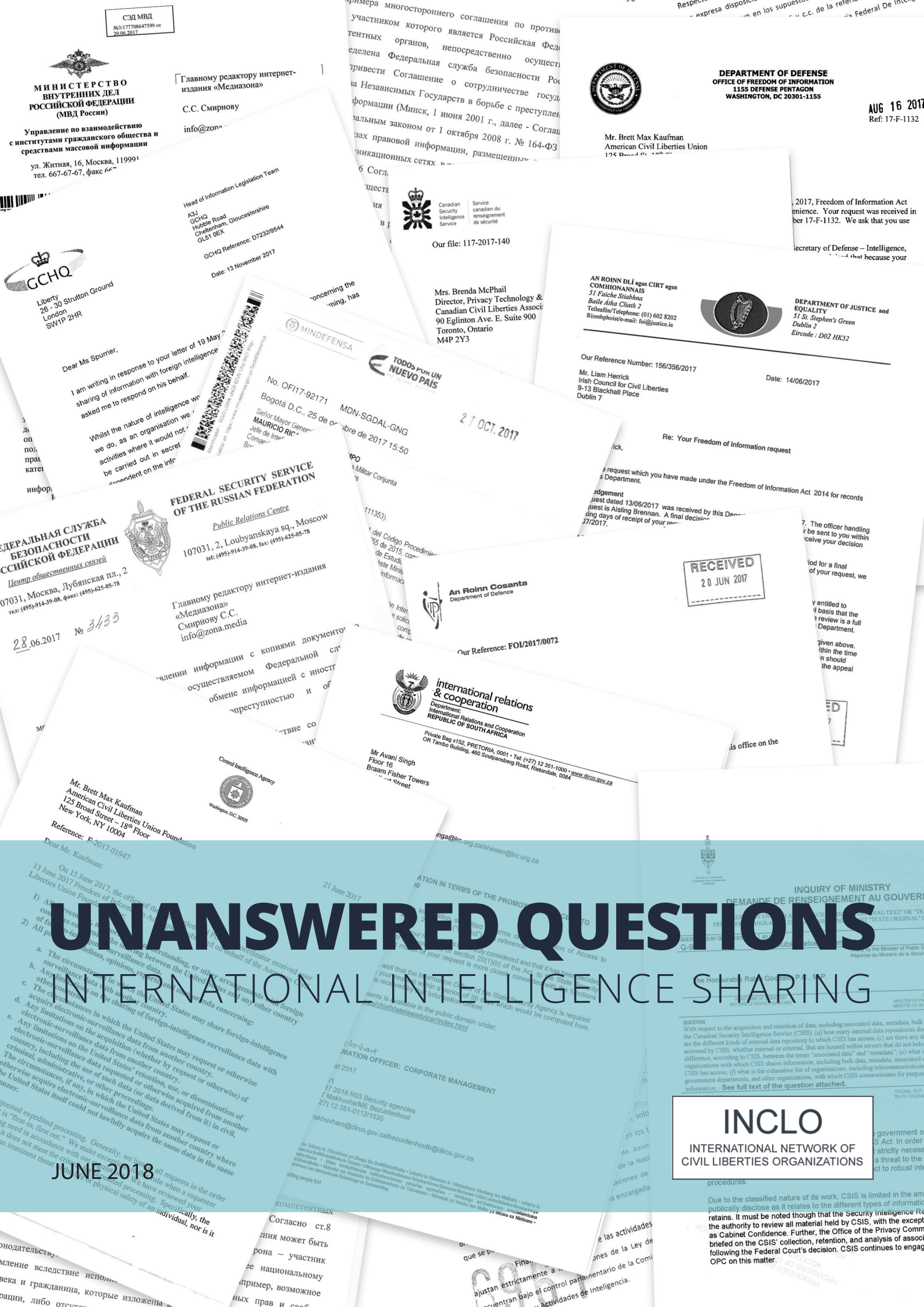

UNANSWERED QUESTIONS

INTERNATIONAL INTELLIGENCE SHARING

JUNE 2018

INCLO

INTERNATIONAL NETWORK OF CIVIL LIBERTIES ORGANIZATIONS

About INCLO

June 2018

This report was produced by the International Network of Civil Liberties Organizations (INCLO), a group of 13 independent national human rights organizations from different countries in the South and North. INCLO members work together to promote fundamental rights and freedoms. We support and mutually reinforce the work of our member organizations in their respective countries and collaborate on a bilateral and multilateral basis. Each organization is multi-issue, multi-constituency, domestic in focus, and independent of government. INCLO members advocate on behalf of all persons in their respective countries through a mix of litigation, legislative campaigning, public education, and grassroots advocacy.

We are: the Agora International Human Rights Group (Agora) in Russia, the American Civil Liberties Union (ACLU), the Association for Civil Rights (ACRI) in Israel, the Canadian Civil Liberties Association (CCLA), the Centro de Estudios Legales y Sociales (CELS) in Argentina, Dejusticia in Colombia, the Egyptian Initiative for Personal Rights (EIPR), the Human Rights Law Network (HRLN) in India, the Hungarian Civil Liberties Union (HCLU), the Irish Council for Civil Liberties (ICCL), the Kenya Human Rights Commission (KHRC), the Legal Resources Centre (LRC) in South Africa, and Liberty in the United Kingdom.

Table of Contents

Acknowledgements

The report was written by Elizabeth Farries and Eric King.

INCLO is also grateful to Lucila Santos (INCLO), Brett Max Kaufman and Asma Peracha (ACLU), Avner Pinchuk (ACRI), Damir Gainutdinov (Agora), Brenda McPhail (CCLA), Margarita Trovato and Paula Litvachky (CELS), Vivian Newman (Dejusticia), Amr Gharbeia (EIPR), Kranti Chinappa and Devika Nair (HRLN), Márton Asbóth (HCLU), Aoife Masterson (ICCL), Andrew Songa (KHRC), Tsanga Mukumba (LRC), and Hannah Couchman (Liberty) for their contributions to this report.

Introduction

This report builds on a coordinated records access project by INCLO members to their national governments. Ten members of INCLO filed Freedom of Information (FOI) requests[1] in an attempt to shine a light on how intelligence sharing practices operate following Edward Snowden's revelations in 2013. This is the first multinational coalition of human rights organizations demanding that governments release information regarding agreements between intelligence agencies and provide answers about a practice largely shielded from accountability.[2]

Our report is informed by FOI requests, desk research, confidential interviews with former and current intelligence and oversight officials, and experiences in thirteen INCLO countries. The FOI records requests are ongoing, but the trends emerging include statutory exemptions, delays, or lack of response in INCLO countries. There are also:

- **Insufficient laws** governing how intelligence sharing partnerships are formed or operate;
- **Insufficient government oversight** and review of agency agreements; and
- **Insufficient transparency** and access to information about these agreements.

Democracy requires that international intelligence sharing agreements are guided by adequate laws, oversight, and transparency. This provides necessary protection for our enshrined human rights including privacy, freedom of expression, freedom of association, and access to information.[3] By continuing to shroud these arrangements in secrecy, governments have removed the public's ability to challenge their actions.

Part I of this report describes international intelligence cooperation and shares INCLO concerns about these practices. **Part II** itemizes domestic legislation in INCLO member countries, identifies the deficits in these laws, and recommends clear laws and procedures. **Part III** describes oversight practices and recommends stronger oversight protocols. **Part IV** shares the results from our FOI attempts and recommends heightened public transparency and accommodation for access to information.

[1] See the Appendix for INCLO FOI requests, responses and related materials.

[2] In a parallel 2017 action Privacy International partnered with civil society organizations including INCLO members and wrote to oversight bodies in 42 countries as part of a project to increase transparency around intelligence sharing and to encourage oversight bodies to scrutinise the law and practice of intelligence sharing in their respective countries. INCLO shares Privacy International's concern that non-transparent, unfettered and unaccountable intelligence sharing poses substantive risks to human rights and the democratic rule of law. See Privacy International, 'Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards' (April 2018) available at: https://privacyinternational.org/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20%28200%29.pdf

[3] See Articles 17, 19 and 22 of UN General Assembly, 'International Covenant on Civil and Political Rights' (16 December 1966); Articles 12, 19 and 20 of UN General Assembly, 'Universal Declaration of Human Rights' (10 December 1948); Articles 9, 10 and 11 of Council of Europe, 'European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14' (1 June 2010); Article 9 of the African Charter on Human and Peoples' Rights.

I. INCLO concerns about intelligence sharing

> In India, opacity is the norm as far as surveillance and intelligence sharing is concerned. This is reflected in our statutes such as the Right to Information Act 2005 and Information Technology Act 2008. Oversight is minimal and concerning. Aadhaar, India's massive biometric metadata project is currently under judicial scrutiny at our Supreme Court. This is the same constitutional court which held that privacy is a fundamental right as enshrined in our constitution. The decisions in this case will decide the course in India for citizen surveillance and intelligence sharing between countries.
>
> - Kranti L Chinnapa, Executive Director, Human Rights Law Network

A. International intelligence cooperation in practice

While there remains an alarming lack of publicly available information about exchange of intelligence between different countries, this section details how intelligence sharing is integral to work within intelligence services, the types of exchange involved, and how agreements can be built around the exchange of unequal resources.

Sharing is integral to intelligence services work

Even before the advent of the internet and digital communications technologies, intelligence agencies shared a large amount of their intelligence analysis. Subsequently, international cooperation has become an even more integral part of the work of intelligence services. Most, if not all, functions of intelligence services now include an international dimension. Some intelligence agencies will have hundreds of relationships with foreign counterparts.[4] Indeed, specific national intelligence requirements may result in countries who are potential adversaries entering into a cooperation arrangement on a particular narrow issue of shared concern.[5]

The level of information that these relationships can provide is significant. Former British intelligence officers have suggested most Western intelligence output is exchanged with at least one foreign partner.[6] Witness statements provided by UK intelligence officials in response to litigation have also

[4] For example, the Director General of the French General Directorate for External Security (DGSE) stated that his service works with more than 200 foreign partners. Testimony of DGSE Director General Érard Corbinde Mangoux before the National Assembly's Defence Committee (20 February 2013).
[5] See for example the UK's well-documented intelligence cooperation and information with Gaddafi's Libya on the narrow issue of countering terrorism. See also the Iran Contra Affair (while not related to information exchange, it demonstrates how intelligence cooperation can still occur between adversaries).
[6] Michael Herman, *Intelligence Power in Peace and War* (University of Cambridge Press 1996).

revealed that intelligence shared by foreign governments with the UK intelligence services 'represents a significant proportion of the intelligence services' total store of intelligence.[7]

Refined and bulk exchange

International intelligence exchange has traditionally involved refined intelligence product and assessment. It is often provided in response to a specific request from a foreign partner. This might include providing information already in the possession of the intelligence agency, or asking a partner to leverage their own surveillance systems to collect the desired information. Intelligence gathered might include:

- **strategic information** such as assessments of a situation in a certain country, or broad potential security threats;
- **operational information** such as the capabilities of a specific armed non-state actor; and
- **tactical information** relevant to a current operational intelligence investigation.

In addition to intelligence gathering upon request, an increasingly common form of cooperation is also the exchange of raw signals intelligence, i.e. intelligence derived from electronic signals and systems used by foreign targets ('SIGINT'). Countries will enter exchange agreements which allow each partner to have direct access to the other's electronic networks in bulk.[8] Many intelligence services can have direct access to joint databases.

Not all sharing is equal

Leaked documents[9] show us that a number of international intelligence cooperation agreements also cover different types of exchange beyond just refined and bulk intelligence products. Exchange agreements allow access to different technological and analytical capabilities. They provide technical support, training and financial resources. Cooperating with foreign partners allows governments to share resource burdens and avoid duplicating efforts by dividing their labour around shared priorities.

Exchange is therefore not always equal between partners and can hold different values. These agreements in particular give better-resourced agencies access to networks and 'local' knowledge that even the largest intelligence services would not be able to acquire without partnering. Or larger

[7] Witness statement of Charles Farr in Privacy International, Liberty and others v Secretary State for Foreign and Commonwealth Affairs and others before the Investigatory Powers Tribunal, IPT/13/92/CH, 16 May 2014. INCLO member Liberty has undertaken this litigation in representation of CCLA, EIPR, HCLU, ICCL and LRC challenging the UK intelligence agency Government Communications Headquarters (GCHQ')s use of intelligence sharing.

[8] The Five Eyes alliance is the most well-known example of this practice, but its model is applied in other jurisdictions. See for example, a National Security Agency (NSA) database entitled ICREACH. This is a Google-like search engine and includes the bulk sharing of raw SIGINT with second and third parties. See Ryan Gallagher, 'The Surveillance Engine' (*The Intercept*, 25 August 2014) available at: https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/

[9] RAMPART-A is an NSA program in which 13 foreign partners 'provide access to cables and host US equipment'. The raw SIGINT generated is directly accessible to each party. See Ryan Gallagher, 'How Secret Partners Expand NSA's Surveillance Dragnet' (*The Intercept*, 18 June 2014) available at: https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/

intelligence agencies often exchange equipment and training in return for access to particular undersea cable landing points in another country.[10]

B. Problems with these practices

INCLO acknowledges there may be national benefits to international intelligence cooperation agreements and that there is nothing improper with such agreements on their face. However, we have ongoing concerns that agencies have histories of evading existing legal frameworks using a shopping list of loopholes and techniques that we describe here.

Absent or ineffective legal frameworks

In some countries international intelligence agreements are not guided or restrained by statute at all. Even in countries with statutes that regulate intelligence sharing with foreign governments, these countries often lack:

- Binding policies, regulations or procedures governing or implementing them;
- Independent and legislative oversight and review; and
- Clear, accessible information available to the public.[11]

This creates significant scope for intelligence agencies wishing to push the limits of what the law permits to interpret open technical and jurisdictional issues in ways that challenge established human rights. There is also little or no ability for the public to ever challenge these secretive interpretations.

Given the lack of rigorous laws, oversight and review intelligence cooperation agreements have often take the form of secret Memoranda of Understanding directly between the relevant intelligence agencies.[12] These shield intelligence sharing relationships from the public and the agencies' own governments alike.[13] Indeed, the international cooperation arrangements that have been leaked expressly state that they are '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'.[14] Such restrictions create an interlocking set of obligations that limit the ability of the government to intervene or the public to secure the release of any information.

---

[10] Ryan Gallagher, 'How Secret Partners Expand NSA's Surveillance Dragnet' (*The Intercept*, 18 June 2014) available at: https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/

[11] International Commission of Jurists' Eminent Jurists Panel, 'Assessing Damage, Urging Action' (2009), p. 90.

[12] Leaked intelligence sharing agreements also suggest that it is common practice for the agreement to mandate secrecy, with text stipulating 'it will be contrary to this agreement to reveal its existence to any third party unless otherwise agreed.' See 'UKUSA Agreement Release 1940-1956' available on the NSA's website at: https://www.nsa.gov/news-features/declassified-documents/ukusa/

[13] Leaked documents explain the US NSA's view that 'for a variety of reasons, our intelligence relationships are rarely disrupted by foreign political perturbations, international or domestic...In many of our foreign partners' capitals, few senior officials outside of their defence-intelligence apparatuses are witting to any SIGINT connection to the US.' See 'What Are We After With Our Third Party Relationships?' (2009) available at: https://search.edwardsnowden.com/docs/WhatAreWeAfterWithOurThirdPartyRelationships%3F2014-03-13_nsadocs_snowden_doc

[14] Memorandum of Understanding (MOU) between the National Security Agency/Central Security Service (NSA/ CSS) and the Israeli SIGINT National Unit (ISNU), available at: www.statewatch.org/news/2013/sep/nsa-israel-spy-share.pdf

Lawful in one country but not in another

Intelligence agencies can also exploit their international intelligence partnerships to reap the benefits of other jurisdictional collection capabilities even when they are legally prohibited from doing so in their own country. For a country to undertake surveillance and collect information about a target at the behest of a foreign partner, it is reasonable that the legal frameworks and restrictions of both countries would apply. However, based on information obtained during our interviews with former and current intelligence personnel,[15] we suspect that such practices are rare. Therefore, agencies can receive surveillance from a country where the law permits collection even if the receiving agency is prevented from doing as such according to their own country's rules.

This question has arisen in the Netherlands,[16] where intelligence agencies are prohibited from intercepting communications from undersea fibre optic cables but not from receiving information from other foreign intelligence agencies who have. The Dutch Review Committee on the Intelligence and Security Services (CTIVD) reviewed this potentially unlawful infringement of privacy and felt compelled to permit the ongoing practice.[17] CTIVD reasoned that a) in many cases it is impossible to know how the foreign partners acquired the material, b) the Dutch cannot reasonably insist that all shared material be accompanied by explanations describing the technique used and the legal authorities permitting collection, c) there is no agreed international norm condemning fibre cable interception, and d) Dutch domestic law is silent on the permissibility of the international exchange practice.

Side stepping warrants

We have also seen the circumvention of warrants in INCLO member countries.[18] Countries may withhold information when applying for warrants or side step the warrant requirement entirely based on narrow and arguably flawed legal arguments. In Canada, when the intelligence agencies the Canadian Security Intelligence Service (CSIS) and Canadian Security Establishment (CSE) wished to monitor two Canadians who were travelling abroad, they were required to apply for a warrant.

---

[15] Eric King's interviews with former and current intelligence personnel were provided on the condition of anonymity.

[16] Dutch Review Committee on the Intelligence and Security Services (CTIVD), 'Review Report on the processing of telecommunications data by GISS and DISS' (5 February 2014) available at: https://english.ctivd.nl/binaries/ctivd-eng/documents/review-reports/2014/03/11/review-report-38-on-the-processing-of-telecommunications-data-by-giss-and-diss/report-38-processing-telecommunications-data.pdf

[17] Dutch Review Committee on the Intelligence and Security Services (CTIVD), 'Review Report on the processing of telecommunications data by GISS and DISS' (5 February 2014) available at: https://english.ctivd.nl/binaries/ctivd-eng/documents/review-reports/2014/03/11/review-report-38-on-the-processing-of-telecommunications-data-by-giss-and-diss/report-38-processing-telecommunications-data.pdf

[18] Circumvention is of course not limited to INCLO member countries. A clear example comes from New Zealand. There, the Government Communications Security Bureau (GCSB) is not permitted to surveil New Zealanders. However, news reports reveal that the GCSB asked the US NSA to collect intelligence and intercept the phone calls of a New Zealand journalist. The journalist was reporting on the New Zealand military's handling of detainees in Afghanistan, and the GCSB asked the NSA to uncover the journalist's confidential sources. The matter is currently under investigation by the New Zealand Inspector General. See Nicky Hager, 'US spy agencies eavesdrop on Kiwi' (*Stuff*, 28 July 2013) available at: http://www.stuff.co.nz/national/8972743/US-spy-agencies-eavesdrop-on-Kiwi

When applying, they deliberately left out key information referencing their intention to rely on their Five Eyes[19] partners for assistance.[20]

Similarly, while the UK Government Communications Headquarters (GCHQ) requires a warrant to collect bulk raw SIGINT data, secret documents suggest the GCHQ do not need a warrant to receive unlimited raw bulk data from the US National Security Agency (NSA).[21] They relied on secret arrangements claiming that if it was not technically feasible for the GCHQ to acquire the material themselves, then collection from others would not trigger the statutory warrant application[22] or be unlawful. In the United States, a senior US intelligence official has similarly claimed that although US authorities may be legally precluded from either obtaining a warrant to surveil US persons from foreign states or requesting such intelligence from other states, nothing prevents US authorities from *receiving* that type of intelligence.[23]

Infrastructure in foreign countries

Agencies can also evade domestic laws by hosting facilities or infrastructure in other countries. When SIGINT is collected by an intelligence agency operating out of a foreign country, a number of jurisdictional and accountability issues arise. There is no clarity within these arrangements as to whether the legal frameworks of both countries have to be satisfied, or just one, or any. The extreme example of such a concern would be a country permitting a foreign intelligence agency to operate SIGINT collection from a base in their own country, potentially collecting information which they themselves would not be permitted to collect, and instead obtaining that data via intelligence cooperation.[24]

Point of transfer or possession

Point of transfer or possession has become a contentious issue around which intelligence sharing is permitted. Intelligence agencies may claim they do not technically have possession of intelligence material until they look at the information. Historically, when information was physically passed to a foreign intelligence agency by hand in a manila envelope, it was clear when the new agency had possession. However, now that intelligence services have secure electronic networks and shared platforms with close partners permitting the immediate sharing of strategic information and raw,

[19] The Five Eyes is an intelligence alliance comprising the UK, US, Australia, Canada and New Zealand.
[20] See Re (X), 2013 FC 1275, Canadian Federal Court 2013. To read more about this case, see INCLO, 'Surveillance and Democracy: Chilling Tales from Around the World', pp. 42–48, available at: https://www.inclo.net/pdf/surveillance-and-democracy.pdf
[21] Liberty, 'Secret policy reveals GCHQ can get warrantless access to bulk NSA data' (29 October 2014) available at: https://www.libertyhumanrights.org.uk/news/press-releases/secret-policy-reveals-gchq-can-get-warrantless-access-bulk-nsa-data. Litigation initiated by INCLO member Liberty has challenged this.
[22] Privacy International, 'Snowden Vindicated: The Truth About Raw Intelligence Sharing' (29 November 2014) available at: https://privacyinternational.org/feature/1675/snowden-vindicated-truth-about-raw-intelligence-sharing
[23] Human Rights Watch, 'Joint letter to European Commission on EU-US Privacy Shield' (26 July 2017) available at: https://www.hrw.org/news/2017/07/26/joint-letter-european-commission-eu-us-privacy-shield
[24] The NSA is one long-standing example of an intelligence agency that has foreign intelligence bases in other countries. In the UK, Menwith Hill is allegedly an NSA-run base. Governments refuse to answer questions about the practices running out of this base. See for example Ryan Gallagher, 'UK Government pressured over secret base's role in Trump's drone strikes' (*The Intercept*, 30 November 2017) available at: https://theintercept.com/2017/11/30/drone-strikes-gchq-trump-menwith-hill-uk/

bulk SIGINT, the point of possession can buried in somewhat arbitrary linguistic distinctions that can evade privacy rights.[25] For example, under the Canadian CSE's existing mandate, 'information acquired through automated means and maintained in a data buffer is not considered intercepted until an analyst has queried it using a search tool'.[26] See also the UK, where GCHQ officials have stated that collecting communication from fibre optic cables alone is not an invasion of privacy until it is examined by non-automated means, i.e. a human being.[27]

Monopolistic effects

There are also risks of monopolistic effects in intelligence cooperation agreements that can enhance the ability of specific agencies to side step domestic rules. Due to the often bilateral nature of the agreements, we have concerns that more powerful intelligence agencies are able to enlist a large number of partners, and use the accesses provided to build a large network of intelligence collection points.[28] For example, if an agency seeks access to a particular undersea cable, it could enter into two separate cooperation arrangements with two different countries that each have access to the cable. While both countries might stipulate that access cannot be used to acquire communications from their citizens, the foreign intelligence agency could use the first country access to acquire communications about the second country's citizens, and vice versa, without breaching the terms of either arrangement.[29]

A lack of self policing

The rules regulating intelligence collection partners are often not rigorous. Between very close partners, agreement requirements will sometimes only permit SIGINT material collection by a foreign partner for use consistent with the legal obligations of the collecting countries. However, these protections tend not to be strongly enforced. See for example the system controls monitoring access to New Zealand SIGINT databases by other Five Eyes members.[30] To gain access, Five Eyes analysts need to enter a system called 'iLearn' and undertake a 'NZSID7' legal briefing.[31] This appears to be a tick box exercise, which can be done remotely at an agent's own desk via 'multiple choice,

[25] Testimony of DGSE Director General Érard Corbinde Mangoux before the National Assembly's Defence Commitee (20 February 2013).
[26] For a general summarised discussion on these distinctions, see Library of Parliament, 'Legislative Summary of Bill C-59: An Act respecting national security measures' (pre-release) (Library of Parliament, 2017) pp.14–15.
[27] See further, Library of Parliament, 'Legislative Summary of Bill C-59: An Act respecting national security measures' (pre-release) (Library of Parliament, 2017) pp.14–15.
[28] These concerns were also expressed by Edward Snowden in testimony before the European Parliament. Available at: http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf
[29] Such a scenario was described by Edward Snowden in testimony before the European Parliament. Available at: http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf
[30] Analysts can access both 'strong selected data and full-take feed.' See Ryan Gallagher and Nicky Hager, 'New Zealand Spies on Neighbors in Secret 'Five Eyes' Global Surveillance' (*The Intercept*, 4 March 2015) available at: https://theintercept.com/2015/03/04/new-zealand-gcsb-surveillance-waihopai-xkeyscore/
[31] According to the leaked GCSB legalities, similar legal briefings exist for the UK and US in the form of 'HRA' and 'USSID-SP0018' training. See 'GCSB access' (2011) available at: https://search.edwardsnowden.com/docs/GCSBaccess2015-03-06_nsadocs_snowden_doc

open-book' assessment. There are no external reviews, additional requirements, or technical enforcement[32] preventing analysts from skipping the step entirely.[33]

Further, there is no evidence that agencies have control of the use of their intelligence by other partners. While policy controls may exist in the cooperation agreements, those controls are lost as soon as the intelligence is transferred to the foreign body. No intelligence agencies or oversight bodies have jurisdiction to enter another territory and scrutinize the subsequent use. Oversight bodies have warned that intelligence cooperation agreements do not adequately take this into account, and that intelligence agencies need to be more aware that the interests they are protecting do not always run parallel with the interests of those foreign services, and vice versa.[34]

[32] Agents are requested to 'copy and paste the results into a word document' to access whatever shared database they wish, suggesting there is no technical enforcement in place. See 'GCSB access' (2011) available at: https://search.edwardsnowden.com/docs/GCSBaccess2015-03-06_nsadocs_snowden_doc

[33] 'GCSB access' (2011) available at: https://search.edwardsnowden.com/docs/GCSBaccess2015-03-06_nsadocs_snowden_doc

[34] Dutch Review Committee on the Intelligence and Security Services (CTIVD), 'Review Report on the processing of telecommunications data by GISS and DISS' (5 February 2014) available at: https://english.ctivd.nl/binaries/ctivd-eng/documents/review-reports/2014/03/11/review-report-38-on-the-processing-of-telecommunications-data-by-giss-and-diss/report-38-processing-telecommunications-data.pdf

Side stepping warrants in Canada - Re (X)

> The Court must be concerned that the authority granted it by parliament to authorise intrusive investigative activities by the Service may be perceived in the public arena as approving the surveillance and interception of the communications of Canadian persons by foreign agencies
>
> - Justice Mosley

In this case, the Canadian Federal Court found that CSIS had committed 'a breach of the duty of candour owed by the service and their legal advisors to the court.'[35] In 2009, Justice Mosley granted permission for the CSE to assist CSIS in undertaking surveillance of two Canadian citizens while they were overseas. Such permission is rare, as normally the CSE is not legally allowed to intercept the communications of Canadians. Justice Mosley granted the warrant because he was persuaded that, by ensuring the surveillance was collected and controlled from within Canada, CSIS and CSE would be able to ensure that the private communications of Canadians they intercepted would be used only if they were essential for national security purposes. It was an important precedent for the CSIS: over the next four years the Federal Court issued 35 similar warrants based on Judge Mosley's decision.

Four years later, Judge Mosley spotted in an oversight report a recommendation that CSE tell its CSIS partner to 'provide the Federal Court of Canada with certain additional evidence about the nature and extent of the assistance CSE may provide to CSIS.' He took the rare step of calling lawyers for CSIS and CSE to reappear before him and to explain what exactly was going on. It transpired that CSE had asked its counterparts in other agencies, its Five Eyes allies, to help carry out the digital electronic surveillance. This clearly violated the letter and spirit of the CSE's original assurances. The warrant was granted under the specific understanding that CSIS and CSE would control the information about these Canadian targets, and that the information they gathered about these Canadians would stay in Canada. It was revealed that the failure of CSIS and CSE to mention their intention to ask for help from allies was not inadvertent. Rather, the CSE employee who appeared before the judge explicitly admitted that his initial submission was carefully 'crafted' with legal counsel to leave out mention of second parties who might be asked to help with the surveillance.

[35] See Re (X), 2013 FC 1275, Canadian Federal Court 2013. To read more about this case, see INCLO, 'Surveillance and Democracy: Chilling Tales from Around the World', pp. 42–48, available at: https://www.inclo.net/pdf/surveillance-and-democracy.pdf

II. In Accordance with the Law

The majority of intelligence agencies today are now creatures of statute. There are legal authorities to conduct intelligence collection, with associated safeguards and privacy protections to act as a bulwark against overly intrusive acts and abuse. This has happened as part of a slow legal transformation of intelligence agencies to ensure surveillance powers are grounded in domestic law and are compliant with human rights law. However, there are still deficits or complete absences in domestic legislation guiding the application of legal frameworks to international intelligence cooperation or agreements. We list below domestic legislation in INCLO member countries, describe the spectrum of emergent deficits, and recommend clear statutes and procedures as an international standard

A. Domestic legislation in INCLO member countries

Argentina

In Argentina, the National Intelligence Law nº 25.520 is very general and ambiguous in its mandate and regulations.[36] It maintains an old and inefficient regulatory system of authorities attribution, oversight mechanisms and access to information. This law does not expressly authorize the Federal Agency of Intelligence (AFI) to enter into international intelligence sharing arrangements, nor does it provide any safeguards for the exchange of raw intelligence. However, it is very likely that there is further regulation of the AFI, which is all kept secret. The law only makes one unspecific reference to other countries' intelligence bodies: Article 13.4 states that AFI can 'direct and articulate the activities and functioning of the National Intelligence System, including its relationships with States' intelligence bodies.'

Canada

In Canada, CSIS is the body which has the central function of collecting, analyzing and retaining information and human intelligence on threats to the security of Canada. It has statutory authority to work internationally with foreign agencies. It relies on the Canadian Security Intelligence Service Act (CSIS Act) when exchanging intelligence with foreign partners. Section 17(1)(b) states that CSIS can, with the approval of the Minister, enter into an arrangement or cooperate with the government of a foreign state or an institution for the purpose of performing its duties and function.[37]

As part of its cooperation with foreign partners, the Minister has stated that CSIS does not share raw associated data with foreign or domestic partners; rather, assessment products are shared 'which are only determined to be related to a threat'.[38] It is not clear what is meant by 'assessment products' in this formulation.

The CSE, Canada's signals intelligence agency, is currently administered under the Department of

[36] National Intelligence Law No. 25.520, Art. 8
[37] Canadian Security Intelligence Service Act, RSC 1985, cC-23, s.17(1)(b).
[38] Canadian Security Intelligence Service Act, RSC 1985, cC-23, S.17(1)(b).

National Defence and its mandate is enshrined in the National Defence Act.[39] The current Act does not contain any explicit authority, nor any limitations, regarding information sharing with foreign entities. There is however a Ministerial Directive for addressing risks in sharing information with foreign entities (recently updated in 2017) that among other issues, addresses the use of information gained through torture.[40] The deficit in authority, if not limitations, for intelligence sharing is addressed in Bill C-59, An Act respecting national security matters, tabled in June 2017. The Bill provides for a new statute, The Communications Security Establishment Act, which states that CSE may 'enter into arrangements with entities' that have powers and duties similar to the Establishment's. These include entities that are institutions of foreign states or that are international organizations of states or institutions of those organizations. The arrangements are for the purposes of the furtherance of CSE's mandate, including for the purposes of sharing information with them or otherwise cooperating with them, subject to approval from the Minister of National Defence, who first must consult with the Minister of Foreign Affairs.[41]

Colombia

In Colombia, international cooperation between intelligence agencies[42] is explicitly permitted. Article 11 of Law 1621 of 2013 states: 'The intelligence and counterintelligence agencies may cooperate with counterpart intelligence agencies in other countries, for which the necessary security protocols will be established in order to guarantee the protection and classification of information, in accordance with the provisions contemplated in this Law.'

Article 6 of Decree 4179 of 2011[43] also encourages cooperation by the National Intelligence Directorate on issues relating to intelligence and counterintelligence, but within the framework of binding international treaties for Colombia and with respect for the faculty of the President of the Republic to direct the international relations.

[39] National Defence Act, R.S.C. 1985, c. N-5.

[40] Some legislation provides limited positive practice such as in Canada, the CSIS Act 1984, s17(2) requires that the Review Committee (currently the CSIS-specific Security Intelligence Review Committee or SIRC) will be given copies of all CSIS agreements with foreign governments and international organizations. This requirement will carry over in the proposed national security legislation currently before the Canadian parliament, although the review would be conducted by a new, integrated National Security and Intelligence Review Agency.

[41] Bill C-59, An Act respecting national security matters, 1st Sess, 42nd Parl, 2018, s76.

[42] In Colombia, the intelligence community is composed of more than 24 different intelligence agencies. These include the National Intelligence Directorate, the Financial Analysis Unit and the Police Intelligence Directorate. For all the identified agencies, see Dejusticia, 'Access to intelligence and counterintelligence archives in the post-agreement framework' pp. 120–121, available at: https://www.dejusticia.org/en/publication/access-to-intelligence-and-counterintelligence-archives-in-the-framework-of-the-post-agreement/

[43] As stated in Article 6 of Decree 4179 of 2011, one of the functions of the National Intelligence Directorate (*Dirección Nacional de Inteligencia* – DNI) is to 'advance international cooperation agreements on issues related to intelligence and counterintelligence, taking into account government policies and current regulations, within the framework of binding international treaties for Colombia and with respect for the faculty of the President of the Republic to direct the international relations.'

Hungary

In Hungary, Act 125 of 1995 permits Information Office and National Security Services to share information internationally for national security purposes and government decisions.[44] It encourages cooperation with foreign intelligence agencies and forwarding personal data, but only within the limits prescribed by legal regulations protecting personal data.

Specifically, Act 125 of 1995 permits the Information Office and National Security Services to obtain, analyse, evaluate and forward information of foreign relevance or foreign origin that can be used to promote the security of the nation, necessary for government-level decision-making [Art. 4(a)]; cooperate with foreign intelligence agencies on the basis of international agreements and commitments [Art. 28(4)]; and forward personal data to foreign data managers within the limits of the legal regulations applying to the protection of personal data (Art. 45).

Ireland

Section 28 of the Garda Síochána Acts 2005-2015 allows for the Garda Commissioner, with the consent of the Government, to enter into agreements with police forces or law enforcement agencies outside the State for a range of purposes. Similarly, the 2008 Irish Criminal Justice (Mutual Assistance) Act's explicit purpose is to give effect to certain international agreements between the state and other states relating to mutual assistance in criminal matters. Section 75 of this latter Act provides an avenue of access to retained data for the purpose of complying with a request by a foreign police or security agency.

It has also been confirmed on a number of occasions that intelligence sharing takes place between this country and overseas intelligence agencies.[45] In 2013, then Minister for Department of Justice, Equality and Defence, Alan Shatter, said that there are intelligence liaisons between the Defence forces Directorate of Military Intelligence (G2) and other countries regarding matters of state security.[46] The G2 do not have a statutory basis and are practically regarded as a branch of the Defence Forces, which are legislated for by the amended Defence Act 1954.[47]

---

[44] Act 125 of 1995 permits the Information Office and National Security Services to obtain, analyse, evaluate and forward information of foreign relevance or foreign origin that can be used to promote the security of the nation, necessary for government-level decision-making [Art. 4(a)]; cooperate with foreign intelligence agencies on the basis of international agreements and commitments [Art. 28(4)]; and forward personal data to foreign data managers within the limits of the legal regulations applying to the protection of personal data (Art. 45).

[45] See for example Alan Shatter, Minister for Justice and Equality: 'The Defence Forces Intelligence Branch provide regular assessments, reports and briefings to the Chief of Staff, the Minister for Defence and the Secretary General of the Department of Defence, relating to internal or external threats to the security of the State and to national interests. Intelligence led liaison is conducted between Intelligence Branch and national authorities in other countries to counter any threat to the security of the State.' Dáil Debates, written answers, 18 June 2013.

[46] Available at: https://www.kildarestreet.com/wrans/?id=2013-06-18a.42

[47] In Ireland, the Defence Forces trace their origins to the Irish Republican Army (IRA), a guerrilla organization that fought British government forces during the Irish War of Independence. On 16 January 1922, the British administration handed over Dublin castle and the Provisional Government assumed power. On 31 January 1922, a former IRA unit (the Dublin Guard) assumed its new role as the first unit of the new National Army. On 3 August 1923, the new State passed the Defence Forces (Temporary Provisions) Act, which provided a legal basis for the existing armed forces. This Act allowed for 'an armed force to be called Óglaigh na hÉireann (hereafter referred to as the Forces) consisting of such number of officers, non-commissioned officers, and

India

In India, intelligence agencies[48] appear to be subject to statutory regulation; however, opacity is the norm as far as surveillance and intelligence sharing are concerned. This is reflected in statutes such as the Information Technology Act 2008. This Act allows for the interception, monitoring and decryption of digital information in the interest of 'friendly relations with foreign nations' together with the defence of India, security of the State, public order, preventing the incitement to the commission of any cognizable offence, investigation of an offence and the sovereignty and integrity of India.

Israel

In Israel, there is no specific legislation which explicitly authorises the state's intelligence agencies to exchange information or raw intelligence with similar organizations abroad. However, the General Security Service Law 5762-2002 permits Israel's national intelligence agency, the General Security Service (GSS) to share information with other bodies at s8(a): 'For the purpose of fulfilling its functions the Service shall be competent, through its employees…to pass on information to other bodies in accordance with rules to be prescribed and subject to the provisions of any law.'

Additionally, there is no legislation that regulates the conduct of the national military intelligence agency, the Military Intelligence Unit 8200.

Kenya

In Kenya, there is a lack of explicit statutory provisions guiding intelligence sharing agreements with other states. While intelligence sharing is not explicitly referenced in statute, section 36 (5) of the Prevention of Terrorism Act 2012 addresses the admissibility of intercepted communication as evidence. Section 36(5) (b) specifically provides admissibility for communication 'intercepted and retained in a foreign state in accordance with the law of that foreign state and certified by a Court of that foreign state to have been so intercepted and retained'. In order to expand the scope of security agencies that could undertake surveillance under this law, s36A was introduced via amendment to grant national security agencies the power to intercept communications for the 'purposes of detecting, deterring and disrupting terrorism in accordance with procedures to be prescribed by the Cabinet Secretary'.

men as may from time to time be provided by the Oireachtas.' The Defence Forces were established on 1 October 1924, and the term National Army fell into disuse.

[48] In India, the intelligence community is composed of numerous agencies including (but not limited to) the Research and Analysis Wing, the Intelligence Bureau, the National Technical Research Organisation, the Defence Intelligence Agency, the Joint Cipher Bureaus and the intelligence directorates of the Army, Air Force and Navy.

Intelligence Sharing in Kenya

There are prominent Kenya examples of intelligence sharing with foreign states.

- During a 2016 official state visit, Israeli Prime Minister Benjamin Netanyahu said that Israel would cooperate with Kenya on intelligence matters related to terrorism.[49]
- US Ambassador Bob Godec in May 2017 acknowledged that the US provides technical assistance to Kenya's security services in relation to a variety of policing skills which include terrorism investigations and intelligence gathering.[50]
- Kenya's Ministry of Information Communication Technology in June 2017 stated that Kenya and the US had agreed to collaborate on matters of cybersecurity and digital economy.[51]

Russia

In Russia, Article 13 of the Federal Law 'On the Federal Security Service'[52] gives the Federal Security Service (FSB) the right to carry out foreign relations with intelligence services and law enforcement agencies of foreign states. It specifically permits them to exchange with foreign agencies on a reciprocal basis operational, technical and other information. All the specific provisions and information about such cooperation are classified.

South Africa

In South Africa, the national executive has the constitutional power to undertake binding agreements with other states, including intelligence sharing agreements.[53] Where these are of a 'technical, administrative or executive nature' not requiring 'either ratification or accession', as is the case with intelligence sharing agreements, all that is required for South Africa to be bound is for the agreement to be tabled in Parliament.[54] The relevant Committee is the Joint Standing Committee on Intelligence, which operates as a default in secret. Therefore, where intelligence sharing agreements are concluded there is some oversight, but no public scrutiny.

The actual sharing of intelligence is done by the State Security Agency (SSA) which is empowered under the National Strategic Intelligence Act 39 of 1994 s2(2)(c) to liaise with intelligence or security services or other authorities, of other countries or intergovernmental forums of intelligence or security services'. Under s2(2)(f) the SSA may 'cooperate with any organization in the Republic or

[49] See a brief video available at: https://youtu.be/CW_B4jGSvbM; Nancy Agutu, 'Israel will share intelligence in anti-terror war, Netanyahu tells Kenya' (The Star, 5 July 2016) available at: https://www.the-star.co.ke/news/2016/07/05/video-israel-will-share-intelligence-in-anti-terror-war-netanyahu_c1380975)
[50] Statement contained in remarks available at: https://ke.usembassy.gov/ambassador-godecs-remarks-outstanding-police-service-awards/
[51] Statement from Ministry of Information, Communications and Technology available at: http://www.ict.go.ke/kenya-to-collaborate-with-us-in-cyber-security/
[52] See Agreement No. 40-FZ of April 3, 1995.
[53] Constitution of the Republic of South Africa s. 231.
[54] Constitution of the Republic of South Africa s. 231(2).

elsewhere to achieve its objectives'.[55] The Minister of State Security has the power to regulate the manner of intelligence sharing and any ancillary matters under s6 of the National Strategic Intelligence Act. All these provisions read together provide the means for individual instances of sharing intelligence products.

United States

In the United States, the intelligence community primarily relies on Article II of the US Constitution and Executive Order 12333[56] ('EO 12333') — which itself is grounded in Article II — to coordinate the sharing of information and to enter into intelligence-sharing agreements with foreign governments. In addition, section 104A(f) of the National Security Act of 1947 authorises the Central Intelligence Agency (CIA) Director to 'coordinate the relationships between elements of the intelligence community and the intelligence or security services of foreign governments . . . on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means.' EO 12333 gives the Director of National Intelligence the responsibility to 'enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations.'.

Section 1.7 of EO 12333 provides that: 'the heads of departments and agencies with organizations in the Intelligence Community or the heads of such organizations, as appropriate, shall: (f) Disseminate intelligence to cooperating foreign governments under arrangements established or agreed to by the Director of Central Intelligence.'

United Kingdom

The Investigatory Powers Act 2016 now includes express, albeit limited, reference to the exchange and disclosure of material overseas.[57] The safeguards[58] apply to the disclosure of material, collected using bulk interception or 'equipment interference' warrants overseas. Safeguards include requirements that only the minimum necessary number of people at a foreign agency are provided access to the material, and that the minimum necessary copies of any intelligence product are made. Additionally, 'the Secretary of State must be satisfied that the overseas authority has safeguards in place corresponding to those in the Bill in relation to the selection of data for examination.' Such safeguards include that the selection of material for examination must be carried out for specified purposes and be necessary and proportionate.

[55] It is worth noting that a liberal reading of s2(2)(f) could open the gates to the SSA sharing or receiving intelligence from non-state actors.
[56] Executive Order No. 12333, 3 C.F.R. (1981), available at: https://www.archives.gov/federal-register/codification/executive-order/12333.html
[57] Investigatory Powers Act 2016, available at: http://www.legislation.gov.uk/ukpga/2016/25/section/151/enacted
[58] Ibid, at Part 6, chapters 1 and 3.

Colombian Constitutional Court Review of C-540 of 2012.

In Colombia, international cooperation between intelligence agencies is explicitly permitted. Article 11 of Law 1621 of 2013[59] permits intelligence agencies to cooperate with their counterparts in other countries for security purposes. Protocols are required under this statute to protect the confidentiality of the private citizens' information exchanged by security agencies.

The constitutionality of this law was subject to a mandatory review by the Colombian Constitutional Court (C-540 of 2012).[60] The Court declared that Article 11 was valid. However, it made a number of important statements.

First, the statutory provision allowing the international cooperation of intelligence agencies must be preceded by the intervention of the President of the Republic. When involving international relations, it must be accompanied by international cooperation instruments, especially for matters of utmost constitutional relevance such as the defence and security of the Nation and the resultant fundamental rights of people living in Colombia.[61]

Second, the data transfer is only legitimate if the recipient country offers comparable data protection guarantees of the exporting country. This reflects the guidelines set out in recent but unrelated court decision regarding the Data Protection Law (Law 1581 of 2012).

Third, data protection guarantees must include a rights framework for data holders, personal data processor obligations, and a data protection regulator or similar mechanism to enforce data protection laws based on European data protection principles.[62]

Fourth, any established security protocols must take into account UN human rights mechanisms. The court specifically referenced the Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.[63]

[59] Article 11 of Law 1621 of 2013 states: '[t]he intelligence and counterintelligence agencies may cooperate with counterpart intelligence agencies in other countries, for which the necessary security protocols will be established in order to guarantee the protection and classification of information, in accordance with the provisions contemplated in this Law.'
[60] Available (in Spanish) at: http://www.corteconstitucional.gov.co/relatoria/2012/C-540-12.htm
[61] Available (in Spanish) at: http://www.corteconstitucional.gov.co/relatoria/2012/C-540-12.htm
[62] Such principles articulated by the court include 'The limitation of the purpose; Data quality and proportionality; Transparency; Security; Access, rectification and opposition; Restrictions on successive transfers to other countries and; Sectorial or additional provisions for the treatment of special type data, including sensitive data, direct marketing and automated individual decision'.
[63] Available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf. See Practices 31 to 35 which require that international intelligence sharing agreements (i) Comply with national legislation and international human rights regulations, in unambiguous terms, including the conditions that must be met, with whom they can be exchanged, and the safeguards applicable to information security; (ii) Provide a statement from the parties in which they commit to respect human rights and ensure the security of personal data, and that the intelligence service that sends the information may request explanations about its use; (iii) Establish responsibility guidelines for the sharing of information; (iv) Ensure that all the information sent is relevant according to the recipient's mandate, which will be used in accordance with the prescribed conditions and that will not be used for purposes contrary to human rights; and (v) Leave a written record of all information exchange activities'.

B. A spectrum of deficits

INCLO member research on domestic laws regulating international intelligence sharing in INCLO countries reveal a spectrum of deficits in statutory oversight ranging from a complete lack of statutory engagement to the absence of rigorous controls and oversight.

In countries like Argentina, there is no legislative limit on what can be shared, to whom or with what purpose. In other countries, intelligence agencies are acknowledged in statute, but little is known about how these provisions have been interpreted and implemented. In Israel, the relevant law requires that intelligence sharing activity should be conducted 'in accordance with rules to be prescribed' but does not disclose these rules to the public.[64] In Hungary, due to a challenging political environment leading to the recent election of Viktor Orban, there are few mechanisms available to shed light on how the statutory provisions actually work. The same issues arise in Russia where all the specific statutory provisions about cooperation are classified. In Ireland, the relevant legislation does not demonstrably comply with the European Union Charter and the European Convention on Human Rights (ECHR). The lack of explicit legislative regulation of cooperation with other intelligence services or publicly available information regarding any internal documents, regulations or guidelines governing such cooperation in these locations is deeply troubling.

Countries that have more explicit rules legislating international intelligence sharing agreements can still have significant problems. In the UK for example, the safeguards applying to interception and disclosure need be applied only 'to the extent [if any] as the Secretary of State considers appropriate.' There are also no transparency requirements regarding which overseas authorities will apply which safeguards or how they will apply them. There is nothing in the UK scheme to cover the receipt of raw SIGINT material, an issue that Intelligence and Security Committee had criticised on the basis that 'the proportion of intercept material obtained from international partners is such that it is not appropriate to exclude it from legislation which purports to cover interception.'[65]

Similarly, in the US while the executive branch has placed certain limitations on its exchanges of raw intelligence the limitations are largely unenforceable. Limitations include the 'minimization' of records relating to US persons.[66] They require security assurances and protections for the protection of classified information and sensitive information. However, those limits are developed by the executive branch itself and are unenforceable in American courts. Further, Presidential Policy Directive 28 on Signals Intelligence Activities permits sharing of 'unevaluated SIGINT' on the only

[64] See General Security Service Law, 5762-2002, s22(a): 'Rules, Service directives and Service procedures under this Law need not be published in *Reshumot* or any other public publication.' *Reshumot* is the Official Government Gazette - publications of Principal Legislation, Government Bills, Subsidiary Legislation and Official Government Gazette. Available at: http://www.justice.gov.il/En/Units/OfficialPublications/Pages/default.aspx

[65] Intelligence and Security Committee of Parliament, 'Report on the draft Investigatory Powers Bill' (9 February 2016), available at: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20160209_ISC_Rpt_IPBill%28web%29.pdf?attachauth=ANoY7crUSED1hym_S-nCb3jS0n4Z84G3IUl2XrHmskxULqPOu5Ri0cybEIjtVmFQwqol0Sh-HYVp4i4I0pyHB3BU0D4IkvGUo7hAfG-NsBf8tgC89I69FZw8lmm9Tw_qigw_MNgkYsgMRaB7yznL7gTTuGFGrYLpJe0wCuzMoGxdB-x6RWzIiTo9EiZhg9rbtjOVvidOSHCqgxTfgKFX69xRYpJobeeCjaNfOOZDKE2BMOygvPbmrdpPnbW0tFk5mwKnh0cG0MeD&attredirects=0

[66] U.S. Signals Intelligence Directive SP0018, Legal Compliance and U.S. Persons Minimization Procedure s. 7 (25 January 2011)

apparent and very permissive condition that the government 'inform the recipient that the dissemination may contain personal information so that the recipient can take appropriate steps to protect that information.'[67]

Likewise, in Colombia, the safeguards applying to exchanged information are set by administrative authorities and not by the parliament. By ordering intelligence agencies to establish security protocols attached to information exchange, Article 11 of Law 1621 of 2013 gives intelligence agencies the power to regulate basic aspects of one's fundamental right to data protection. This clearly raises constitutional questions about the ability of agencies to set rules about fundamental rights without parliamentary oversight.

Further, in Canada, the Canadian government's new national security legislation will not require independent judicial or quasi-judicial oversight for intelligence sharing arrangements, although there will be, potentially, after-the-fact review by the new National Security and Intelligence Review Agency. The newly-created National Security and Intelligence Committee of Parliamentarians may also have some role, although there is a provision within their enabling legislation by which government ministers may refuse the Committee access to information 'injurious to national security'[68] which leaves their effectiveness in the area of information sharing currently unclear. The quasi-judicial agency created to provide oversight for some ministerial authorizations, the Intelligence Commissioner, is not specifically given oversight of signals intelligence sharing by the CSE. Such arrangements will require only the approval of the Minister of National Defence, after the Minister has consulted with the Minister of Foreign Affairs'.[69]

INCLO Recommendation I: Clear statutes and procedures

Despite the growing body of statutes overseeing intelligence agencies, there are serious deficits in these laws for INCLO countries. A lack of strong domestic statutes and policies guiding intelligence sharing agreements undermines democratic processes to their core.

To adequately protect our enshrined human rights, INCLO supports the recommendation of the International Commission of Jurists Eminent Jurists Panel that states should establish clear policies, regulations and procedures covering the exchange of information with foreign intelligence agencies. [70] Policies should also necessarily reflect relevant human rights standards and mechanisms, and in particular the right to privacy, freedom of expression, and freedom of association.[71] They should

[67] PPD-28 Section 4 Procedures s. 7.2 (12 January 2015), available at: https://www.nsa.gov/news-features/declassified-documents/nsa-css-policies/assets/files/PPD-28.pdf
[68] An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts, S.C. 2017, c. 15, s. 16(1)(b).
[69] Bill C-59, An Act respecting national security matters, 1st Sess, 42nd parl, 2018, s. 76.
[70] International Commission of Jurists' Eminent Jurists Panel, 'Assessing Damage, Urging Action' (2009), p. 90.
[71] See Articles 17, 19 and 22 of UN General Assembly, 'International Covenant on Civil and Political Rights' (16 December 1966); Articles 12, 19 and 20 of UN General Assembly, 'Universal Declaration of Human Rights' (10 December 1948); Articles 9, 10 and 11 of Council of Europe, 'European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14' (1 June 2010); Article 9 of the African Charter on Human and Peoples' Rights.

include principles of proportionality and necessity[72] and eliminate the practices of bulk collection in keeping with leading case law at the European Court of Justice.[73] They should require effective notice provisions and remedial processes with the capacity to cross borders to affected persons.[74]

III. Escaping oversight and accountability

Human rights protections require strong oversight and review of intelligence sharing practices between states to ensure intelligence agencies adhere to domestic laws and human rights norms via their international intelligence sharing partnerships. Strong laws must be drafted to ensure that exemptions including the Third Party Rule[75] do not evade oversight. This rule sets out that information shared with foreign intelligence agencies cannot be further shared with additional third parties without permission of the intelligence agency that originally supplied the information. Frequently, oversight bodies are found to be considered 'third parties' and as such are not able to appropriately probe information relating to international cooperation.

A. Oversight and review practices in INCLO member countries

Argentina

In Argentina, the Congress' Bicameral Intelligence Commission, created by the National Intelligence Law, has the responsibility to supervise the AFI's procedures for obtaining and gathering intelligence, including intelligence cooperation. However, the commission has not been very active and has never stated anything about intelligence cooperation in any of its reports.

Canada

Canada has after-the-fact review of intelligence sharing, on a selective basis. The Canadian Security Intelligence Review Committee (SIRC), CSIS's review body, has made references to and recommendations on CSIS's information sharing practices in its three most recent reports. In fact, one of SIRC's objectives is to better 'understand CSIS's relationship with its domestic and foreign

[72] See for example the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (31 December 2013) para. 165, available at: http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_internet_eng%20_web.pdf

[73] See the case of *Tele2 Sverige*, European Court of Justice, C-203/15, ECLI:EU:C:2016:970, mn. 103: 'Further, while the effectiveness of the fight against serious crime, in particular organized crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight.' Available at: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd4fc86499d441497a8c79b137b006e4ef.e34KaxiLc3qMb40Rch0SaxyNbNv0?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1255745

[74] See the First Report of the UN Special Rapporteur on the right to privacy to the Human Rights Council, A/HRC/31/64 (8 March 2016), p. 4, available at: http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc

[75] Within the context of US intelligence relationships, the US is known as the 'first party', with the UK, Canada, Australia and New Zealand being considered 'second parties', and all other countries with a relationship being considered 'third parties'.

partners by examining liaison activities, as well as operational cooperation and information exchanges carried out 'by foreign stations.'[76] In its last three reports, SIRC has paid attention to CSIS's intelligence sharing practices, including its cooperation with foreign entities.

The CSE Commissioner's office has been clear in the past that it cannot accurately assess whether or not the Five Eyes partners keep their promises to protect information about Canadians. The Canadian Press reported on a redacted copy of a 2013 report by then Commissioner Robert Decary, who wrote that he was concerned about this issue because 'these activities may directly affect the security of a Canadian person.' What he found was that beyond 'certain general statements and assurances' between CSE and its partners, he was 'unable to assess the extent' to which the Five Eyes partners 'follow the agreements with CSE and protect private communications and information about Canadians in what CSE shares with the partners.'

In the 2016-17 CSE Commissioner's annual report, the Commissioner conducted a review of CSE information sharing with foreign entities from February 2010 to March 2015.[77] He found that the two different sections dealing with risk assessments within CSE were not equally good at following consistent protocols, maintaining records, or applying caveats, and similarly noted an absence of general policy guidance on information sharing with foreign entities and issued recommendations to improve privacy measures in some formal agreements with a number of unidentified foreign entities.

Colombia

In Colombia Article 19 of Law 1621[78] came into force in 2013 and mandated the creation of a Parliamentary Legal Commission. This Commission is intended to be in charge of monitoring intelligence and counterintelligence activities. Its role is directed towards ensuring efficiency in resources used, respect for constitutional guarantees, and compliance with the statutory principles, limits, and purposes regulating intelligence and counterintelligence activities.

Although this Law came into force almost 5 years ago, the Commission has not yet been able to carry out all its mandated activities due to claimed procedural challenges. Therefore, as far as Dejusticia is aware, this oversight body has made no call for intelligence sharing to be better regulated.

Hungary

In Hungary, there is no effective oversight of intelligence sharing agreements currently. The National Security Committee at the parliament that oversees National Security Services has become caught in

[76] Security Intelligence Review Committee, 'Accelerating Accountability: Annual Report 2016-2017' (Public Works and Government Services Canada, 2017), p. 28.
[77] Office of the Communications Security Establishment Commissioner. *Annual Report 2016 - 2017* (June 2017), available at http://www.ocsec-bccst.gc.ca/a246/ann-rpt-2016-20127-eng.pdf. The Commissioner's review included the process for sharing foreign signals intelligence with foreign entities; the legislative and policy framework relating to sharing information with foreign entities; whether CSE acquired from foreign entities and/or disclosed to foreign entities private communications or information about Canadians; a sample of exchanges of information, including 161 mistreatment risk assessments that were conducted for information sharing; and existing formal agreements with foreign entities.
[78] Available (in Spanish) at: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf

intense political battles that have disabled its mandate. The head of the opposition party is on the Committee - their presence has led governing parties to refuse to participate in the Committee's work. According to the narrative of governing parties, the opposition parties themselves pose a threat to national security, although all members at the committee have been scanned by secret services.

Ireland

In Ireland, there is no Irish parliamentary or independent body oversight of intelligence sharing functions, so in practice these functions are only controlled by executive oversight.[79] The Data Protection Commissioner has a limited power to review surveillance and intelligence sharing. However, there is a general exclusion which provides that data protection law 'does not apply to... personal data that in the opinion of the Minister [for Justice] or the Minister for Defence are, or at any time were, kept for the purpose of safeguarding the security of the State.'[80]

India

Matters pertaining to intelligence agencies in India are apparently subject to oversight by parliament through its oversight committees. However, for each agency this process differs and citizens do not have access to the data of the committees on each. For example, the Joint Intelligence Committee (JIC) of the government of India analyses intelligence data from the Intelligence Bureau and the Research and Analysis Wing, the Directorate of Military Intelligence, the Directorate of Naval Intelligence and the Directorate of Air Intelligence. JIC has its own secretariat that is under the command of the Prime Minister through the Cabinet Secretariat. It is an independent committee. However, the level of oversight it provides, if any, is unclear. The process is very opaque and parliamentary committees vary periodically. Intelligence agencies enjoy a level of secrecy which keeps them beyond the scope of access to information legislation, media reports, or public inquiries.

South Africa

The Inspector General of Intelligence (IGI) is an independent, constitutionally mandated body tasked with oversight over South African intelligence services. The IGI is required to oversee all aspects of every intelligence service in South Africa through its mandate found in s7(7) of the Intelligence Services Oversight Act 40 of 1994 to monitor compliance with the law, review specific actions of the intelligence services, and handle complaints from the public or whistleblowers within the intelligence services. The IGI has the power to access all intelligence documentation, information or premises under s.7(8) of the same Act.

The incumbent Chairperson of the IGI, Dr Sethlomamaru Dintwe, has further stated that he considers oversight over intelligence sharing as an important part of his office's mandate.[81]However, he recognised that due to significant budget and human resource constraints his office is forced to focus on its complaints function and undertake monitoring and reviewing of critical areas of

[79] For a discussion on Irish national intelligence authorities see Dr TJ McIntyre, 'National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies - Legal update' 29 June 2016.
[80] Section 1(4) of the Data Protection Acts 1988 and 2003.
[81] Interview conducted by LRC with Setlhomamaru Dintwe, Inspector General of Intelligence, and others.

intelligence gathering and therefore intelligence sharing has not been a focus of recent oversight reports.

The Joint Standing Committee on Intelligence is also tasked with oversight of the intelligence services. This is a multi-party, proportionally representative committee consisting of members from both houses of parliament.[82] As noted previously, when an international intelligence sharing agreement is concluded it is this Committee which receives the text of the agreement under the Rules of the National Assembly. This Committee also receives reports produced by the IGI which may include matters relating to intelligence sharing. As an organ of the legislature, the Committee can hold the Minister of State Security accountable for the actions of the SSA in sharing or receiving intelligence products. While on its face this this process may seem relatively transparent, the Rules of the National Assembly provide that tabling of such agreements is effected by referral to the relevant Portfolio Committee.[83]

Naidoo's unanswered questions[84]

Kumi Naidoo, a South African national, has deep roots as an activist. He was previously the International Executive Director for Greenpeace and has recently been appointed as the Secretary General of Amnesty International. In 2015, an Al Jazeera reporter contacted Naidoo and told him that leaked intelligence cables revealing that South Korea had identified him as a possible security threat during the 2010 G20 summit in Seoul. South Korea asked South Africa for 'specific security assessments' of Naidoo, linking him with two other South Africans who had been swept up in an anti- terrorist raid in Pakistan and then released. South Africa never informed Naidoo of South Korea's request and Naidoo believes its intelligence service made the request because of his outspoken opposition to nuclear power.

In July 2015, the LRC issued an access to information request on behalf of Naidoo to the SSA for records relating to the requested surveillance operation. The SSA has not issued any response to that request. That inaction is considered a refusal of the request under South African law and so the LRC launched an internal appeal, again with no response. The LRC lodged a complaint with the Inspector General of Intelligence on 15 September 2017[85] and may institute court proceedings depending on the outcome of the complaint to secure access to any intelligence products shared or agreements under which the sharing was conducted.

Meanwhile, the South African government's public response to the leaked information suggesting it may have been surveilling a citizen, who is a world- renowned, peaceful activist, has been especially troubling. Rather than opening a dialogue about the possible surveillance activities, the South African Security Service (SSA) condemned the leaks and indicated that a full investigation – into the leaks, not the possible surveillance of Naidoo – had been launched.

[82] National Strategic Intelligence Act s. 2
[83] Rules of the National Assembly of South Africa, 9th ed., rule 343
[84] For further reading, see INCLO, 'Surveillance and Democracy: Chilling Tales from Around the World' available at: https://www.inclo.net/pdf/surveillance-and-democracy.pdf; see also Appendix VII for relevant documentation.
[85] See appendix VII for copy of this letter request.

United Kingdom

In the UK, there was no reference to raw bulk intelligence sharing before the Snowden revelations. However after campaigning and litigation focused on the issue, the Interception of Communication Commissioners Office stated that they commissioned an investigation into the international sharing of intercept material.[86] The report explained that they 'commissioned an investigation in 2015 into the arrangements in place within GCHQ for the sharing of intercepted material and related communications data with foreign partners in order to review compliance with the section 15 safeguards. We are still in the process of carrying out this investigation. Once our in-depth investigation has been completed we will require an annual update on any changes or new arrangements. This is an area we have been discussing with our international counterparts.' The investigation remains ongoing.

10 Human Rights Organizations v the United Kingdom[87]

This case is the consolidated result of challenges lead by a number of human rights groups including seven INCLO members[88] at the Investigatory Powers Tribunal (IPT). The case began at the IPT, a special court established to hear complaints of unlawful surveillance. The revelations by Edward Snowden raised the possibility that civil liberties and non-governmental organizations worldwide were being watched not just by their own governments but by spy agencies located in other states. The group of organizations joined together to try to establish whether they had been under the surveillance of GCHQ.[89]

For the first time in its 11-year history the IPT made a finding against the government in the complaint filed by the ten human rights organizations. It held that the process that the UK government used for receiving information that the US government had gathered[90] had been unlawful for years because the safeguards for looking at any shared material were not known to the public.

But the court also held that that, thanks to the disclosures made during the litigation, the safeguards were now sufficiently public and the regime was compliant with human rights law.

Disappointingly, the IPT decided that the UK government’s mass surveillance programmes did not constitute a human rights violation. Rather, it stated that mass surveillance was in fact an

[86] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/548075/IOCCO_Report_March_2015__Web_.pdf

[87] App No. 24960/15

[88] The INCLO members included Liberty, ACLU, CCLA, EIPR, HCLU, ICCL and LRC. Shortly after Edward Snowden's revelations in June 2013, Liberty filed a complaint with the UK's Investigatory Powers Tribunal (IPT). Privacy International filed a similar complaint with the IPT in July 2013. The IPT ultimately consolidated these claims with those of several other domestic and international groups.

[89] For further reading, see INCLO, 'Surveillance and Democracy: Chilling Tales from Around the World', pp. 105–108, available at: https://www.inclo.net/pdf/surveillance-and-democracy.pdf

[90] Specifically, the NSA had been using PRISM and Upstream, programs for collecting communications from internet companies.

'inevitable' consequence of modern technology, and the powers granted in the Regulation of Investigatory Powers Act, 2000 allowed the British government to spy on foreign nationals without a warrant identifying the subject of surveillance.

However, in June 2015, the IPT delivered a further ruling in which it revealed that two of the claimant organizations had been subjected to unlawful surveillance by GCHQ. The LRC was one of the two organizations. In relation to the LRC, the IPT found that:

> communications from an email address associated with the [LRC] were intercepted and selected for examination pursuant to s 8(4) of [the Regulation of Investigatory Powers Act]. The [IPT] is satisfied that the interception was lawful and proportionate and that the selection for examination was proportionate, but that the procedure laid down by GCHQ's internal policies for selection of the communications for examination was in error not followed in this case.

The IPT concluded that this was a violation of Article 8 of the ECHR, but that it was satisfied that 'no use whatever was made by the intercepting agency of any of the intercepted material, nor any record retained.' Consequently, it ruled that the LRC had not suffered any material detriment, damage or prejudice, and no award of compensation was made.

The ten organizations have now taken this matter to the European Court of Human Rights (ECtHR). The case was heard in late 2017 and we are awaiting judgment. The decision of the ECtHR will constitute one of the first times that a regional human rights tribunal will rule on the lawfulness of speculative mass surveillance regimes in the post-Snowden era. In the face of government intransigence and stymied domestic legal systems, this is a key opportunity for the ECtHR to affirm and give content to the right to privacy and to insist on accountability from states.

United States

In the United States there have been no recent formal statements or hearings regarding intelligence sharing with foreign governments in the two Congressional committees that oversee the U.S. intelligence community—the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. Nor has the Privacy and Civil Liberties Oversight Board issued any reports that look at the issue of international intelligence cooperation.

INCLO Recommendation II: Strong oversight practices

Even where strong protections exist in statute and policy, until accompanying oversight practices are put explicitly in place, there will be ongoing potential for intelligence agencies to circumvent domestic laws and human rights norms via their international intelligence sharing partnerships. INCLO recommends the Council of Europe's Venice Commission observations that oversight bodies should be 'deciding the general rules regarding who, and under what circumstances, signals intelligence can be exchanged with other signals intelligence organizations'.[91] We further echo the concerns articulated by the ECtHR that 'The governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance ... is yet another factor in requiring particular attention when it comes to external supervision'.[92]

IV. Shielded from public scrutiny

> When civil society talks about national security, we face charges of being unrealistic, naive, or insufficiently aware of the threats and operational realities. However, if more information was public we would know more. It should never be unrealistic to ask for better protection for fundamental rights and freedoms in a democracy. It may be difficult, rights compete and balance is tricky—but asking for accountability for agencies with extraordinary powers and responsibilities is not naive, it is profoundly practical. It is also necessary for trust, legitimacy and social license for our intelligence agencies.
>
> *- Brenda McPhail, Director, Privacy, Technology & Surveillance Project, Canadian Civil Liberties Association*

[91] 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' (March 2015) available at: http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e

[92] See Szabó and Vissy v Hungary, ECtHR, App. No. 37138/14 (12 January 2016), para. 78

A. Status of INCLO FOI requests

In our attempt to secure the release of information pertaining to intelligence cooperation, 10 INCLO members filed coordinated FOI requests to the relevant domestic bodies within participating member countries. We asked for:[93]

- All agreements, memoranda of understanding and/or other arrangements with foreign countries concerning the sharing between the INCLO member country and any other country, or international institution, of foreign-intelligence surveillance data;

- All policies, guidelines, opinions, reports and memoranda concerning:
    - The circumstances in which the INCLO member company may share foreign-intelligence surveillance data with another country.
    - Any limitations on the sharing of foreign-intelligence surveillance data with other countries.
    - The circumstances in which the member country may request or otherwise acquire from another country electronic-surveillance data.
    - Any limitations on the acquisition (whether by request or otherwise) of electronic-surveillance data from another country.
    - Any limitations on the INCLO member country's retention, use, or dissemination of electronic-surveillance data requested or otherwise acquired from another country, including the use of such data or data derived from it in civil, criminal, administrative, or other proceedings.
    - The circumstances, if any, in which the INCLO member country may request or otherwise acquire electronic-surveillance data from another country.

Despite INCLO initiating these requests a full year ago,[94] many of the requests have been rejected outright, often due to exemptions, with others requesting lengthy time extensions. Following this FOI exercise, INCLO can conclude that we still know very little about international intelligence cooperation generally in our member countries. We itemize below the experiences of participating INCLO member countries.

Argentina

CELS and other local members of a Citizen Initiative for the Oversight of the Intelligence Systems (ICCSI) submitted two FOI request[95] to the AFI. The Agency's response[96] simply stated that the requested information was classified. As it usually happens in these cases, the response itself was also classified. CELS challenged that decision in court. The court first responded that ICCSI should submit the request again, this time under the new access to information law which had just become

[93] See the Appendix for a full list of FOI requests sent out by participating INCLO member organizations. See also our published requests and responses at https://www.inclo.net/international-intelligence-sharing-project.html. We were not able to publish all FOI efforts due to risks to member organizations.
[94] The first requests went out in June 2017, see the Appendix.
[95] First sent on 13 June 2017 to the Director-General of Argentina's Federal Intelligence Agency, and again 4 December 2017 due to changes in the law which required refiling. See Appendix I.
[96] Sent by the Director-General of Argentina's Federal Intelligence Agency on 23 August 2017, see Appendix I.

applicable. CELS together with its ICCSI partners presented the FOI request again. The Agency's response was exactly the same as in the first time - the information was classified. ICCSI again challenged their response in court. More than seven months later, due to poorly functioning, complex and ineffective judicial processes, the AFI has not yet even been notified of the existence of this challenge. Cases such as this demonstrate the problematic processes within both the executive (AFI) and the judicial branch of Government, which become significantly more complicated when state security issues are addressed

Canada

In Canada, there are mandatory exceptions for information received in confidence from a foreign government.[97] In response to the FOI filed by the CCLA[98], CSIS provided some documents[99] with only one brief extension, while the CSE indicated a 210-day extension would be required to consider the request. Some limited disclosure has been provided in response to the request, including some information regarding caveats and assurances to be included with information shared with foreign partners. However, due to the mandatory exemptions, all material relating to specific agreements with other countries has been refused.

Colombia

Dejusticia put a FOI request to the JIC.[100] The JIC transferred this to the Joint Military Intelligence and Counterintelligence Chief.[101] The Joint Military Intelligence and Counterintelligence Chief responded [102] stating that in accordance with protocols, security, and legislation, information can only be disseminated to authorised recipients. Dejusticia appealed this decision on the grounds that the refusal violates their right to petition access to public information.[103] They argued that a proportionality test should be conducted and that at least the existence (as opposed to the content) of any agreement should be made public. Dejusticia is now waiting for the review of an administrative judge.

[97] *Access to Information Act*, RSC 1985, c. A-1, s.13. There are other discretionary exemptions regarding 'information obtained or prepared for the purpose of intelligence' in s 15 of the Act, and Canada's Information Commissioner has the power to review classified documents in the case of an access appeal.
[98] Sent on 13 June 2017 to CSE and CSIS, see Appendix II.
[99] Sent by CSIS on 13 June 2017, see Appendix II.
[100] Sent on 18 October 2017, see Appendix III.
[101] Sent from the Office of Legal Affairs of the National Defence Ministry of Colombia on 27 October 2017, see Appendix III.
[102] Sent from the Office of Joint Military Intelligence and Counterintelligence on 16 November 2017, see Appendix III.
[103] Sent on 21 November 2017, see Appendix III.

FOI Challenges in Egypt

Egypt did not file FOIs on this project. Any FOI activities we exercise to assist our work in Egypt are more likely to be made outside of Egypt and therefore requires closely working in tandem with other parties. An FOI act in Egypt may change all this and a Bill is currently under development. This presents an opportunity for sober reflection on how FOI should be designed legally in order to access government information. The Egyptian government is currently a black box with respect to intelligence sharing practices, and so we have no idea how the developing FOI act will run in practice. What are the costs? What will the transition phase look like and what are the caveats? I am the leading FOI expert in my country and I would not know where to begin filing a request if I had to. Someone must have been in the same place in the US in the late 1960s or in Sweden before 1776.

- Amr Gharbeia, technology and human rights researcher, Egyptian Initiative for Personal Rights

Hungary

In Hungary, the FOI filed by the HCLU was rejected by the responsible ministers and also by the National Security Committee at the parliament. Despite there being language on the face of the statue referencing intelligence sharing, requests for further information and specific documents describing agreement policies were rejected on the grounds that no-one held the requested information.

Ireland

> For security reasons, it is not the practice to publicly comment on the detail of counter-terrorism arrangements. It should be noted that our history on this island means that regrettably we have been engaged in counter-terrorism work for decades and the arrangements currently in place have served the Irish people well in countering threats to the security of the State. The Gardaí and Defence Forces have a long and proud record in protecting and defending the State from a sustained terrorist threat over many years.
>
> - Private Secretary to Minister for Justice and Equality, Mr Charlie Flanagan[104]

In Ireland, the ICCL put FOI requeststo An Garda Síochána, Ireland's police force, the Department of Defence, and the Department of Justice and Equality.[105] An Garda Síochána refused the request arguing that they are subject to the FOI Act only in relation to 'administrative records relating to human resources, finances, or procurement matters.'[106] The Department of Defence also refused saying 'that the information requested cannot be disclosed on security grounds.'[107] The Department of Justice and Equalityresponded that they did a thorough search of their request and that the search produced '1 record that has been identified as coming within the scope of your request,' but its release was refused because it 'concerns matters that may prejudice or impair the prevention, detection or investigation of offences' and also since this record is 'a confidential and international instrument for law enforcement, its release would affect adversely the security of the State and international relations of the State'.[108]

India

In India, under the Right to Information Act 2005 there is no obligation to give any citizen information which is considered prejudicial to the sovereignty and integrity of India, the security, strategic, scientific or economic interests of the State, including its relations with foreign state, or lead to the incitement of an offence.

[104] Response from Department of Justice and Equality to Dr Hosein, Dr McIntyre, and Liam Herrick on behalf of Privacy International dated 4th April, 201, See Appendix V.
[105] Sent on 13 June 2017 to *An Garda Síochána*, Department of Defence and Department of Justice and Equality. See Appendix V.
[106] Sent from *An Garda Síochána* on 23 June 2017, see Appendix V.
[107] Sent from Department of Defence on 20 June 2017, see Appendix V.
[108] Sent from Department of Justice and Equality on 14 June 2017, see Appendix V.

Israel

> When the rules governing the exchange of information between intelligence agencies take place between walls of secrecy, that are protected by statutory exception, democrat accountability is severely restricted.'
>
> - Avner Pinchuk, Human Rights Lawyer, Association for Civil Rights in Israel

In Israel, ACRI did not file FOI applications because the GSS and the Military Intelligence Unit 8200 are exempt from responding to FOIs under Israel's Freedom of Information Act. While the Prime Minister is subject to Freedom of Information Requests, the GSS exemption means that even something as general as the number of wiretapping permits the Prime Minister approves each year remains classified. When the Prime Minister was pressed directly on the question of wiretapping, he insisted that the information is not in his 'physical' possession, because he returns all requests and approvals of wiretaps to the GSS. This argument was accepted by the Supreme Court after ACRI filed a petition to access this information.[109]

Kenya

In Kenya, the KHRC did not file FOI applications due to FOI statute limitations. The Access to Information Act, 2016 and its Restrictions in Relation to National Security were enacted to, among other things, 'provide a framework for public entities and private bodies to proactively disclose information that they hold and to provide information upon request in line with the constitutional principles'.

While its boundaries are yet to be judicially tested, s6(1)(a) of this Act limits the right of information if its disclosure is deemed to undermine the national security of Kenya. Under s6(2) information relating to national security is stated to include among other things: foreign government information with implications on national security, intelligence activities, sources, capabilities, methods or cryptology and foreign relations.

Russia

In Russia, Agora submitted a FOI request to the Ministry of Foreign Affairs, the FSB, and the Ministry of Internal Affairs.[110] The Ministry of Foreign Affairs refused the request on the basis of multi- and bilateral agreements on the exchange of information and the 'fight against crime in the sphere of

[109] In 2014, ACRI filed a FOI to the district court seeking an order that would compel the Prime Minister's Office (PMO) to provide ACRI with the number of warrants issued by the prime minister to execute security wiretaps over the past five years, including the number of people – and the number of Israeli citizens and residents – covered by such warrants. The district court dismissed ACRI's petition. ACRI appealed to the Supreme Court but lost. See *ACRI v The Prime Minister Office*, ruling APA 4349/14 (3 November 2015) available (in Hebrew) at: https://supremedecisions.court.gov.il/Home/Download?path=HebrewVerdicts\14\490\043\g08&fileName=14043490_g08.txt&type=2; see also ACRI, 'Court Denies ACRI's FoI Petition on Secret Security Wiretaps' (20 May 2014) available at: https://www.acri.org.il/en/2014/05/20/foi-wiretaps-2/

[110] See Appendix VI.

computer information'.[111] The Minister recommended referral to competent state bodies including the FSB, which Agora had already applied to.

The FSB replied with a very similar response, including directing the FOI request away to other state bodies, confusingly including the FSB!

The Ministry of Internal Affairs justified the secret collaboration between the Russian Federation and the state in question in order to reveal the illegal activities of the suspected individuals and to allow law enforcement agencies 'to make procedural decisions'. It stated that sharing cross-border information on service providers or users is justified when the perpetrators use the internet to commit crimes. The response stated that IP addresses do not fall under the category of 'personal data' protected in Russia.

South Africa

In South Africa, the LRC put a FOI request to the Department of Justice and Constitutional Development and the SSA.[112] The Department of Justice and Constitutional Development responded [113] that the application was transferred to the Department of International Relations and Cooperation as 'the record's subject matter is more closely connected with the functions of the Department of International Relations and Cooperation.' Following this, the Department of International Relations and Cooperation notified LRC[114] that the request had been duly considered and it had been decided to transfer it to the SSA since the subject matter of the request is more closely connected with the functions of that Department. The SSA had only acknowledged the receipt of the initial FOI request and did not respond to the transfer from the Department of International Relations and Cooperation or further correspondence from the LRC. South African FOI legislation imposes a deemed refusal where no response is received within 30 days of lodging the request. The 30 day period expired in terms of both the initial request and the transferred request, leading the LRC to launch an internal appeal against the deemed refusal.[115] This appeal was also ignored by the SSA.

Given that there is a clear national security exemption to FOI requests in the South African Promotion of Access to Information Act the prospects of success in litigation were minimal. The LRC therefore decided to pursue advocacy with oversight bodies which have some form of mandate over intelligence services or access to information. Therefore, meetings were set up with the Joint Standing Committee on Intelligence,[116] IGI[117] and the Information Regulator of South Africa.[118]

---

[111] The response cited as a source the ministry's website: www.mid.ru. There are multilateral agreements between Russia and countries belonging to the Shanghai Cooperation Organization, and the Commonwealth of Independent States. The highlighted bilateral agreements mention Brazil, Belarus, Cuba, China and India. For the second point in the FOI request the ministry recommends referring to 'the competent state bodies,' primarily the 'Ministry of the Interior, the Prosecutor General's Office and Russia's Federal Security Service'.
[112] Sent on 13 June 2017, see Appendix VII.
[113] Sent by the Department of Justice and Constitutional Development on 15 June 2017, see Appendix VII.
[114] Sent by the Department of International Relations and Cooperation on 3 August 2017, see Appendix VII.
[115] Sent on 4 December 2017, see Appendix VII.
[116] Letter sent on 13 December 2017, see Appendix VII.
[117] Letter sent on 13 December 2017, see Appendix VII.
[118] Letter sent on 13 December 2017, see Appendix VII.

The Inspector General of Intelligence v the State Security Agency

In South Africa, when the LRC was not initially successful with FOI requests, they sent a series of correspondence to the IGI, Information Regulator of South Africa, and the Joint Standing Committee on Intelligence requesting meetings to discuss their role in oversight of intelligence sharing.

The LRC has subsequently met with the Chairperson of the IGI, Dr. Setlhomamaru Dintwe,[119] to raise concerns about international intelligence sharing and to discuss the inadequacies in state oversight and to raise concerns about the lack of effective oversight of secret surveillance.[120]

During the meeting on the 28th of February 2018, Dr Dintwe confirmed that the IGI was the oversight body entrusted with investigating complaints about alleged abuses or malfeasance within the SSA. Following the meeting, Dr Dintwe expressed his frustration at the compromised institutional independence of his office and requested that the LRC consider challenging the Intelligence Oversight Act. Dr Dintwe cited concerns such as the fact that the IGI's budget was a cost item within the broader SSA budget meaning he had to request funds from the Director General of the SSA and account to them for the spending.

On 11 April 2018 the IGI filed an urgent application to interdict the SSA Director General from revoking his security clearance or otherwise frustrating an investigation into alleged abuse of office by the SSA Director General Arthur Fraser.[121] Part B of this application sought to challenge several provisions of the Intelligence Oversight Act which compromised the IGI's institutional independence as noted above. However, on 17 April Arthur Fraser was moved to the Department of Correctional Services, as its Director General and the Minister of State Security reversed Fraser's decision to withdraw Dr Dintwe's security clearance.[122] This undermined the urgency of the application, although it remains on the court roll. The LRC has indicated its intention to intervene as amicus curiae to support the IGI in its argument for greater institutional independence, emphasising budgetary independence, freedom to appoint its own staff (IGI staff are currently in the SSA organigram) and the need to account to parliament rather than the executive.

[119] The LRC also secured a meeting with the Chairperson of the Joint Standing Committee on Intelligence, but it was postponed on the day of the meeting due to it being on the that President Zuma resigned. Efforts to secure a rescheduling continue.
[120] Letter from the LRC to the IGI dated 13 December 2017, see Appendix VII.
[121] Issued application for interim relief at the High Court of South Africa, Gauteng Division, Pretoria from the Inspector General of Intelligence against the Minister of State Security, the Director General of State Security, Minister of Finance, Joint Standing Committee on Intelligence and the President of the Republic of South Africa, Case No. 25/21/18.
[122] Available at:
https://www.enca.com/south-africa/inspector-general-of-intelligences-security-clearance-reinstated

United Kingdom

In the UK, Liberty's FOI to the GCHQ[123] was refused as GCHQ has an absolute exception from Freedom of Information legislation. In a letter explaining the refusal,[124] the GCHQ claimed that 'foreign states may choose to have intelligence sharing relationships with the UK on the strict understanding that those relationships will be kept confidential' and on that basis it is 'obviously not possible, and never could be possible' to provide the requested information. However, the response also stated that 'GCHQ is currently working with various of our international partners to establish whether further information can be placed in the public domain about intelligence cooperation, including the sharing of raw data and other information, in a way which does not damage the public interest.'[125]

United States of America

In the US, the ACLU put FOI requests to the NSA, CIA, the Office of the Director of National Intelligence (ODNI), the Federal Bureau Investigation (FBI) and the Department of Defence.[126] The Department of Defence responded that they conducted a search in the Office of the Under Secretary of Defence '[locating] no records responsive' to the request. The office advised that because the request appears to be specific to national intelligence information and does not relate to military intelligence the request should be directed to the ODNI.

The ODNI[127] and the CIA[128] refused the request for expedited processing, advising they handle all requests in the order they receive them on a 'first-in, first-out' basis.[129] The NSA also denied the request for expedited processing stating 'while there may be some public interest regarding the topic ('arrangements with foreign countries concerning the sharing between the United States and any other country of foreign-intelligence surveillance data'), the value of the information will not be lost if not disseminated quickly.'[130] They also stated that 'due to significant increases in the number of requests being received by this Agency, we are experiencing delays in processing. We will provide a more substantive response to you as soon as we are able.' The FBI denied a request for expedited processing stating 'you have not provided enough information concerning the statutory requirements for expeditation.'[131]

[123] Sent on 19 May 2017, see Appendix VIII.
[124] Sent by GCHQ on 13 November 2017, see Appendix VIII.
[125] Privacy International have challenged this absolute disclosure exception at the ECtHR. See 'Privacy International v United Kingdom (UK Five Eyes FOIA)' available at https://www.privacyinternational.org/node/1764
[126] Sent on 13 June 2017 to NSA, CIA, ODNI, FBI and Department of Defense, see Appendix IX.
[127] Sent by ODNI on 23 June 2017, see Appendix IX.
[128] Sent by CIA on 21 June 2017, see Appendix IX.
[129] Exceptions to this rule are only made when a requester establishes a compelling need under the standards in regulations. A 'compelling need' exists 1) when the matter involves an imminent threat to the life or physical safety of an individual, or 2) when a person primarily engaged in disseminating information makes the request and the information is relevant to a subject of public urgency concerning an actual or alleged federal government activity.
[130] Sent by NSA on 27 June 2017, see Appendix IX.
[131] Sent by FBI on 29 June 2017 see Appendix IX.

INCLO Recommendation III: Transparency

Five years following the release of documents by Edward Snowden, we should not have to continue to rely on leaked information to ascertain the status of agreements. INCLO remains deeply concerned that these agreements continue to step beyond the reach of government statute and oversight and public scrutiny. By shrouding these arrangements in secrecy, governments have removed the public's ability to challenge their actions threatening our human rights, our democracies, and the rule of law.

INCLO therefore argues that strong, transparent public agreements are required to promote accountability and to prevent intelligence agencies from exploiting their international intelligence partnerships to circumvent the rule of law. We support the conclusions of The Global Principles on National Security and the Right to Information that bilateral and multilateral agreements and other major international commitments by the state on intelligence matters are a category of information with a high presumption or overriding interest in favour of disclosure.[132] Publically available and periodic reports on the activities of agencies involved in intelligence sharing agreements in relation to the overarching statues and policies that bind their behaviour; disclosure of the existence and terms of bilateral and multilateral agreements, and other major international commitments by the state on intelligence matters; and record keeping of all information disclosed to and received by a foreign intelligence agency are minimum requirements.

Conclusion

Despite the uproar over Snowden's revelations of vast and secretive surveillance networks that span the globe, there are still no public agreements governing intelligence sharing anywhere in the world. Today, the only agreements that are public are historical artefacts[133] or those leaked by whistleblowers. INCLO has thus embarked on an ambitious access to information task in an attempt to learn more and to ask for better protections of our fundamental rights and freedoms.

This is becoming an ever important task. The scope and scale of intelligence exchange and cooperation is steadily increasing, but with inadequate corresponding increases in statutory regulation, oversight, or transparency. Yet these checks and balances must be applied to such a secretive area. Governments must better legislate for international intelligence sharing to ensure adequate oversight, review, and public access to information in order to hold intelligence agencies accountable.

To this end, INCLO is urging all states to act and bring intelligence sharing under the rule of law, so that the citizens of all nations enjoy protection from unwarranted surveillance. Until INCLO's broad recommendations are strictly followed, the ability for intelligence agencies to exploit international intelligence partnerships is an ongoing threat to democracy and the rule of law.

---

[132] See principle 10 of 'The Global Principles on National Security and the Right to Information' (12 June 2013), available at: https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf

[133] Available at: https://www.nationalarchives.gov.uk/ukusa/

Acronyms and Terms

ACLU - American Civil Liberties Union
ACRI - Association for Civil Rights in Israel
AFI - Argentina's Federal Agency of intelligence
AGORA - Agora International Human Rights Group
CCLA - Canadian Civil liberties Association
CELS - Centro de Estudios Legales y Sociales
CIA - US Central Intelligence Agency
CSE - Canadian Communications Security Establishment
CSIS - Canadian Security Intelligence Service
CSS - US Central Security Service
CTIVD - Dutch Review Committee on the Intelligence and Security Services
DGSE - French General Directorate for External Security
DISS - Dutch Defence Intelligence and Security Service
ECHR - European Convention on Human Rights
ECtHR - European Court of Human Rights
EIPR - Egyptian Initiative for Personal Rights
EO 12333 - US Constitution and Executive Order 12333
FBI - US Federal Bureau Investigation
Five Eyes - an intelligence partnership between the US, UK, Australia, Canada and New Zealand
FOI - Freedom of Information
FSB - Russian Federal Security Service
G2 - Irish Defence Forces
GCHQ - UK Government Communications Headquarters
GCSB - New Zealand Government Communications Security Bureau
GISS - Dutch General Intelligence and Security Service
GSS - Israeli General Security Service
HCLU - Hungarian Civil Liberties Union
HRLN - Human Rights Law Network
ICCL - Irish Council for Civil liberties
ICCSI- Citizen Initiative for the Oversight of the Intelligence Systems from Argentina
IGI - South African Inspector General of Intelligence
INCLO - International Network of Civil Liberties Organizations
IPT - Investigatory Powers Tribunal
ISNU - Israeli SIGINT National Unit
JIC - Spanish acronym for Colombian Joint Intelligence Board
JIC - Indian Joint Intelligence Committee
KHRC - Kenya Human Rights Commission
LRC - Legal Resource Centre
MOU - Memorandum of Understanding
NSA - US National Security Agency
ODNI - US Office of the Director of National Intelligence
PRISM - A program used by the NSA for intercepting communications traffic from the Internet.
SIGINT - Signals intelligence derived from electronic signals and systems used by foreign targets
SIRC - Canadian Security Intelligence Review Committee
SSA - South African State Security Service
Third Party Rule - A common requirement in intelligence sharing agreements that material shared under the agreement can't be shared with any third party
Upstream - A program used by the NSA for intercepting communications traffic from the Internet

APPENDIX: FOI requests, responses, and related materials

I. Argentina

- Request from CELS to AFI dated 13th June, 2017.
- Response from AFI to CELS dated 28th August, 2017.
- Request from CELS to AFI received 4th December, 2017.
- Response from AFI to CELS dated 27th December, 2017.

II. Canada

- Request from CCLA to Canadian Security Establishment dated 13th June, 2017.
- Request from CCLA to CSIS dated 13th June, 2017.
- Response from CSIS to CCLA dated 25th October, 2017 together with accompanying disclosure materials.

III. Colombia

- Request from Dejusticia to President, Joint Intelligence Board (Presidente, Junta de Inteligencia Conjunta) dated 18th October, 2017.
- Response from Joint Intelligence Board President Office to Joint Military Intelligence and Counterintelligence Chief dated 25th October, 2017.
- Response from Joint Military Intelligence and Counterintelligence Chief to Dejusticia dated 16th November, 2017.
- Appeal from Dejusticia to President, Joint Intelligence Board (Presidente, Junta de Inteligencia Conjunta) dated 21 November, 2017.

IV. Hungary

- Request from HCLU to Chairman, Committee of National Security dated 8th June, 2017.
- Request from HCLU to Minister of the Prime Ministers Office dated 8th June, 2017.
- Request from HCLU to Ministry of Interior dated 8th June, 2017.
- Response from Ministry of Interior to HCLU dated 11th June, 2017.
- Response from Chairman, Committee of National Security to HCLU dated 20th June, 2017.
- Response from Minister of the Prime Ministers Office to HCLU dated 27 June, 2017.

V. Ireland

- Request from ICCL to An Garda Siochána, Department of Defence and Department of Justice and Equality dated 13th June, 2017.
- Response from Department of Justice and Equality to ICCL dated 14th June, 2017.
- Response from Department of Defence to ICCL dated 19th June, 2017.
- Response from An Garda Síochána to ICCL dated 20th June, 2017.
- Response from Department of Justice and Equality to Dr Hosein, Dr McIntyre, and Liam Herrick on behalf of Privacy International dated 4th April, 2018.

VI. Russia

- Translated request from AGORA to Ministry of Foreign Affairs of the Russian Federation, Federal Security Service of the Russian Federation, Ministry of Internal Affairs of the Russian Federation.
- Response from Ministry of International Affairs of the Russian Federation to AGORA dated 20th June, 2017.
- Response from Federal Security Service of the Russian Federation to AGORA dated 28th June, 2017.
- Response from Ministry of Foreign Affairs of the Russian Federation to AGORA dated 11th August, 2017.

VII. South Africa

- Request from LRC to Department of Justice and Constitutional Development dated 13th June, 2017.
- Response from Department of International Relations and Cooperation to LRC dated 3rd August, 2017.
- Response acknowledging receipt of the LRC FOI from Department of Justice and Constitutional Development to LRC dated 15th June, 2017.
- Request from LRC to Chairperson, IGI for an investigation into the surveillance of Naidoo dated 15 September 2017.
- Request from LRC to Chairperson, Joint Standing Committee on Intelligence dated 13th December, 2017.
- Request from LRC to Chairperson, Information Regulator of South Africa dated 13th December, 2017.
- Request from LRC to IGI dated 13th December, 2017.
- Response acknowledging request from SSA to LRC dated 13th June, 2017.
- Follow up email from from LRC to SSA dated 13th October, 2017.
- Response from LRC to SSA regarding deemed refusal of FOI request dated 4th December, 2017.

VIII. United Kingdom

- Request from Liberty to Director, GCHQ, dated 19th May, 2017.
- Response from Head of Information Legislation Team, GCHQ, to Liberty dated 13th November, 2017.

IX. United States of America

- Request from ACLU to NSA, CIA, ODNI, FBI, Department of Defence dated 13th June, 2017.
- Response from Department of Defence to ACLU dated 19th June, 2017.
- Response from CIA to ACLU dated 21st June, 2017
- Response from ODNI to ACLU dated 23rd June, 2017.
- Response from NSA to ACLU dated 27th June, 2017.
- Response from FBI to ACLU dated 28th June, 2017.
- Response from FBI to ACLU dated 29th June, 2017.
- Response from Department of Defence to ACLU dated 16th August, 2017.