



association pour la prévention de la torture
asociación para la prevención de la tortura
association for the prevention of torture

- **BEWARE THE GIFT OF POISON FRUIT**
Sharing information
with States that torture





association pour la prévention de la torture
asociación para la prevención de la tortura
association for the prevention of torture

Beware the gift of poison fruit

**Sharing information with
States that Torture**

The Association for the Prevention of Torture (APT) is an independent non-governmental organisation based in Geneva, working globally to prevent torture and other ill-treatment.

The APT was founded in 1977 by the Swiss banker and lawyer Jean-Jacques Gautier. Since then the APT has become a leading organisation in its field. Its expertise and advice is sought by international organisations, governments, human rights institutions and other actors. The APT has played a key role in establishing international and regional standards and mechanisms to prevent torture, among them the Optional Protocol to the UN Convention against Torture.

APT's vision is a world free from torture where the rights and dignity of all persons deprived of liberty are respected.

Copyright © 2012, Association for the Prevention of Torture (APT).
All rights reserved.

Materials contained in this publication may be freely quoted or reprinted, provided credit is given to the source. Requests for permission to reproduce or translate the publication should be addressed to the APT.

ISBN 978-2-940337-65-1

Design and layout: minimum graphics

Cover illustration: Yara Kassem

Printing: Villi®

Contents

Acknowledgements	v
Introduction	1
Executive Summary	3
Context: Upholding Fundamental Principles in the fight against Terrorism	5
National practices	9
What is the problem?	17
How should we respond to the moral dilemma?	19
Does it violate international law?	21
Existing national standards from the perspective of International Law	29
International principles for executive agencies	35
Conclusion	43
Annex. Former Special Rapporteur Martin Scheinin's compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies	45



Federal Foreign Office



Human Rights

*The APT would like to thank the German Federal Foreign Office
for its support*

Acknowledgements

This text was prepared by the Association for the Prevention of Torture (APT) based on consultation with following individuals and organisations present at a meeting in Geneva in November 2013. The APT would like to acknowledge the role of Matthew Sands, Legal Advisor, who compiled this report, and to Linda Beatrice Louis for assisting with this project.

- Juan Mendez, Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment
- Andrew Clapham, Professor of Public International Law at the Graduate Institute, Geneva and the Director of the Geneva Academy of International Humanitarian Law and Human Rights
- Sarah Fulton, International Legal Officer, REDRESS
- Gwilym Hughes, Director, Oxford Intelligence Group
- Ziad Kaed Bey, Head of Human Rights Department, Internal Security Forces (Ministry Of Interior), Lebanon
- Michael Kellett, former UK police officer and CPT adviser
- Alex Neve, Secretary General, Amnesty International Canada
- Monalisa Noowe Kakono, Head Human Rights Department, Chieftaincy of Military Intelligence Uganda
- Mona Rishmawi, Chief of Rule of Law, Equality and Non Discrimination Branch, OHCHR
- James Ross, Legal and Policy Director, Human Rights Watch
- Matthew Sands, Legal Advisor, APT
- Gerald Staberock, Secretary General, OMCT
- Mark Thomson, Secretary General, APT

The meeting was held under the Chatham House Rule, under which participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

No statement contained in this report may be attributed to any participants, either jointly or individually.

Introduction

In November 2013, the APT hosted a group of experts to consider the practical and legal implications for the sharing and use of torture-tainted information by executive agencies. Experts were asked to consider whether and how standards for the use of information obtained by torture could be adopted, to appropriately guide this challenging aspect of State behaviour to comply with any applicable international standards. The meeting was held under the auspices of the Chatham House Rule and this report follows the arguments presented at the meeting.

Executive Summary

Torture is an abhorrent practice and absolutely prohibited. It is prohibited in international treaties, customary international law, and in the constitutional guarantees of almost every State. Yet despite its blatant illegality, torture continues to be practiced in States around the world.

In the years since the terrorist attacks in 2001, intelligence cooperation between States has expanded significantly. Police, security and intelligence agencies (hereafter “executive agencies”) in several States have demonstrated a willingness to rely on information obtained through torture, and have shared information which is later used to abuse detainees overseas. Such cooperation, particularly among States which systematically use torture, leaves executive agencies and their agents vulnerable to allegations of complicity.

In some cases, executive agencies have appeared to actively participate in torture, in ways which extend beyond complicity into direct perpetration of the abuse.

The apparent willingness of States to violate the absolute prohibition against torture is extremely regrettable. Now, more than a decade since the war against terrorism was launched, executive agencies have an opportunity to consider what the permissible limits of cooperation should be, in order to restore the dignity of the absolute prohibition against torture, which stands as a peremptory norm (*jus cogens*) of international law.

There are several important reasons why States should reconsider how they cooperate with States that torture. The information received from such States is immediately suspicious and likely to be unreliable, wasting the time and resources of executive agencies. Furthermore, by sharing information with such States, or relying on torture-tainted information, States encourage torture and create a market for its products.

Nevertheless, we cannot easily dismiss the serious practical and legal challenges faced by executive agencies in their consideration of potentially relevant information. Information is rarely labelled 'obtained by torture', and executive agents often do not know the conditions under which information they rely on was collected. Neither is it certain that even in circumstances where information is known to come from torture, it should not still be used to protect persons from serious threats, or respond and defeat an urgent threat to life.

While it is clear that States will not cease all together what may be mutually beneficial relationships with States that torture, executive agencies should consider whether a more strategic preventive approach to cooperation would better achieve an end to systematic policies of torture and avoid allegations of complicity.

Various obligations of international law might be invoked to demonstrate that an active information-sharing relationship with States that torture could lead to a violation of the prohibition against torture. While several challenges exist to limit the liability for torture committed overseas in situations beyond a State's immediate control, principles of State responsibility and individual liability illustrate that a breach of the absolute prohibition against torture may nevertheless be found.

Among the principle obligations of the absolute prohibition against torture, the evolving duties not to expose a person to the risk of torture overseas and to exclude information obtained by torture could be engaged to explore the permissible limits of executive action.

Both Canada and the United Kingdom have published guidance for their executive actors to avoid allegations of complicity in torture committed overseas in their cooperation with foreign agencies. Whether the narrow interpretation of applicable standards is acceptable or not, the submission of such guidelines for public scrutiny is a good practice which should be welcomed and developed further.

From this analysis, various principles and areas for further consideration may be identified. In the absence of clearly agreed principles and inconsistent national practice, the development of some internationally recognised standards is urgently needed to fill this norm-vacuum which has stood silent in the face of some egregious abuses of the absolute prohibition against torture.

Context: Upholding Fundamental Principles in the fight against Terrorism

“The war on terror continues to serve as a justification for the indiscriminate exchange of large amounts of highly sensitive information. Those providing the information have no overview of who it is that receives the information and to what uses or misuses this information is put. [...] [A] legal filter is now needed more urgently than ever.”¹

Since the terrorist attacks against the United States in 2001, intelligence cooperation between States has expanded significantly.² The increased demands of tracking and managing multiple global terrorist threats has required almost every intelligence, security and police service to build relationships more widely than before, and increasingly, with States with poor human rights records.

Recent scrutiny of intelligence failures has pushed intelligence sharing policies into the public domain and has resulted in wide discussions about whether the sharing and use of information obtained from torture and other abusive practices can be considered justifiable, expedient, or lawful. Information now in the public domain has made it increasingly obvious that information tainted by torture continues to be used widely across a range of executive actions.

‘Information’ or ‘intelligence’ is used by a variety of executive actors for a number of purposes. It may be used to establish a basis for criminal investigation, justify administrative detention, influence immigration decisions or sanctions, drive government policy, or direct military or intelligence actions overseas. The variety of uses

¹ ECCHR, *Torture and the Use of Information in Countering Terrorism*, Berlin, 31 October 2011, p.30.

² See Security Council Resolution 1373 (2001), which called on all States to intensify and accelerate the exchange of operational information and cooperate to prevent and suppress terrorist attacks. See also Resolution 1624 (2005), which stressed that States must ensure that any measures taken to combat terrorism comply with all of their obligations under international human rights law.

for information or intelligence leads to some serious questions about the reliability of the underlying information, and the manner in which it is collected, shared and used.

Ultimately, this report, and the expert meeting on which it was based, seeks to find some answers to the following dilemma, which has been returned to repeatedly in recent years as more allegations of executive abuses have been made public: How should authorities deal with information which has allegedly been extracted under torture or other forms of ill-treatment, or likely be used to commit torture or other ill-treatment if shared, but which is potentially relevant to the work of executive agencies and the courts?

State actors have traditionally drawn inspiration and guidance for their work from rules adopted at the national and international level. However, anti-torture laws at the domestic level rarely direct themselves to the work of security and intelligence actors, and few international rules may be invoked which address the issues with enough precision to be used in practice. Consequently, State actors admit struggling to understand the acceptable limits of their executive action. In light of this perceived lacuna of legal standards, the time is now ripe to examine the ethics and law applying to the executive use of information obtained by torture, or the sharing of information which would likely lead to torture overseas.³

States have preferred not to subject the work of their intelligence and security agencies to scrutiny or international oversight, and unlike law enforcement actors, there are no standards which offer advice or guidance for their work.⁴ The lack of guidance may lead to the erroneous conclusion that such intelligence cooperation and sharing of information between executive agencies is not subject to international law.

³ In December 2013, a report summarising the preparatory work of the Detainee Inquiry and highlighting particular themes and issues that might merit more investigation was published, adding further emphasis to the issues at the heart of this analysis. See Report of the Detainee Inquiry, at <https://www.gov.uk/government/publications/report-of-the-detainee-inquiry>.

⁴ Consider, in contrast, a number of international soft law instruments for law enforcement officials, prison officials, prosecutors, or judges. See, for instance, the UN Code of Conduct for Law Enforcement Officials, Adopted by General Assembly resolution 34/169 of 17 December 1979; or the UN Guidelines on the Role of Prosecutors, Adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, 27 August to 7 September 1990.

An impression that international law was silent on the issue would be untrue. Apart from a number of international instruments which prohibit torture and other cruel, inhuman or degrading treatment or punishment in all its forms, including by consent, acquiescence or other forms of complicity, evolving concepts of State responsibility might also show to what extent States have an obligation not to encourage or recognise as lawful torture committed overseas.

Of course, any analysis is disadvantaged by the fact that much of the information on how intelligence and security agencies receive, rely on and share information is, by its nature, secret, making it difficult to define the full extent of the problem. It is not uncommon for such executive actors themselves to assert that they do not know the sources of information shared with them, and as a result, may use information obtained by torture unwittingly. After all, tainted information is rarely labelled as such, and as a result, rules conceived to regulate its use could be difficult to apply.

While this may be true, the challenge should not be overstated. 'Intelligence', as it is, is professionally analysed by a number of executive agencies. Background information, including the source of the information and an assessment of its reliability, is known, as it must be, to be taken into account in determining its value by the executive agency which receives it. Therefore, at some level, the source of the information will be taken into account, even if such background information is not made available more widely for security reasons.

Over the last ten years in the aggressive war against terrorism, intelligence and security agencies have been under extreme pressure to obtain answers and information. As a result, if they received the information they needed from foreign agencies, there has been a tendency not to raise concerns or delve too deeply into the source or its reliability. Inevitably, such practices led to some of the tragic abuses that have been widely reported. Now we should reflect on how never to repeat such mistakes in future.

It should also be recognised that actors from professional police, security and intelligence agencies are recruited for their strong moral bearing, and work for worthy and important reasons, including the important task of protecting our own security. As moral actors, such executive actors do not lightly step outside the conduct expected

of them. Current uncertainty over what conduct is lawful therefore merits further consideration, and further guidance would benefit this area of their work.

Though we may not all be privy to secret information, all of us nevertheless have a duty to attempt to understand the scope of the problem in order to consider whether torture-tainted information might be used in a way which is consistent with fundamental human rights principles.

At a time when questions are being asked of executive agencies related to their role in surveillance, so we might also question the important role of these same agencies in the effective prohibition and prevention of torture around the world.

National practices

Suppose information is received from another State which routinely uses torture in the interrogation of suspects. The information alleges that identified persons present in your jurisdiction pose a specific, serious and urgent threat to national security. How should law enforcement and other agencies charged with security treat the information and respond?

Perhaps detainees held by another State are interrogated using information supplied by your own intelligence agencies. The State holding the persons later passes the information collected back to your intelligence agency. Your intelligence agency does not know whether the persons were tortured for the information, and does not ask how the interrogation was conducted. Does your intelligence agency bear any responsibility for the treatment of the persons held overseas?

What if one of your agents embedded in a terrorist organisation overseas learns of a serious and dangerous plot against national security. If you ask a partner agency working in the State where the terrorist organisation is based to detain the persons who made the threat, they will certainly be tortured, but if you do not pass on the information, the terrorist organisation will likely develop and may carry out the threat.

These scenarios demonstrate some of the routine questions faced by executive agencies in the treatment of information or intelligence. But beyond hypothetical scenarios, several particularly egregious examples from real life easily demonstrate some of the risks with intelligence sharing practices. That executive agencies have used torture-tainted information at least in the recent past, as part of the war on terror, has become accepted fact. First, statements made by Foreign Ministers in several European countries, including Germany, the United Kingdom and Denmark have all condoned the executive use of information obtained by torture since 2001. And second, from media reports, it is clear that in many cases, executive agencies

from these States did much more than simply use torture-tainted information. In cooperating with those States which torture, in some cases governments have appeared complicit in the acts of torture themselves.

For instance, when Bisher Amin Al-Rawi and Jamil el-Banna travelled to Gambia from the UK in 2002, the British Security Services, MI5, sent a warning to foreign agencies, labelling the men Islamic extremists. On arrival, the men were detained, interrogated in conditions which may amount to torture, and sent to Guantanamo Bay, where they languished for several years.⁵ Both men were released without charge in 2007.

An inquiry which promised to look at whether Britain was implicated in the improper treatment of detainees held by other States was commenced in the UK in July 2010. However, doubts were raised over the inquiry's independence and impartiality by several human rights organisations. After parallel criminal investigations were announced in 2012, the inquiry was concluded. In December 2013, a report summarising the preparatory work of The Detainee Inquiry raised several important questions about how British executive agencies co-operate with States that regularly torture.⁶ The report highlights particular themes and issues that would merit more investigation. It is not clear when, if ever, such an investigation will be undertaken.⁷

In the case *A and others v Secretary of State for the Home Department (N°2)*, the UK House of Lords famously found that using information tainted by torture for executive purposes was not illegal.⁸ After the ruling, Charles Clarke, then Home Secretary declared that “[the court] had held it was perfectly lawful for such information to be relied on operationally, and also by the Home Secretary in making executive decisions... This welcome decision will not change the government's current practices, but it will provide greater legal authority.”⁹

⁵ C. Whitlock, 'Courted as Spies, Held as Combatants', Washington Post Foreign Service, 2 April 2006, at <http://www.washingtonpost.com/wp-dyn/content/article/2006/04/01/AR2006040101465.html>.

⁶ See <https://www.gov.uk/government/publications/report-of-the-detainee-inquiry>.

⁷ See 'United Kingdom: UN experts on torture and counter-terrorism express concern over proposed official inquiry', in press release dated 23 December 2013.

⁸ UK House of Lords, *A and others v Secretary of State for the Home Department* [2005] UKHL 71.

⁹ C. Clarke, 'I welcome the ban on evidence gained through torture', The Guardian, 13 December 2005.

Ahmed & Anor v R [2011] EWCA Crim 184

Rangzieb Ahmed, a British citizen, was jailed in 2008 for being a member of Al Qaeda and planning mass murder.

During the trial, Ahmed claimed he had been tortured whilst he was in custody in Pakistan. He said that after being detained by the Pakistani intelligence agency in August 2006, he was beaten with sticks, whipped with electric cables, sexually humiliated, deprived of sleep, and had his fingernails removed with pliers. He also claimed that British agents had visited him and interviewed him on the first day of his detention, and their involvement may have even been to 'suggest' the Pakistani authorities detain him in the first place.

One of the important questions directed to the Court was whether it would be an abuse of process to allow the trial of a person detained and tortured with the apparent connivance of the British. The Court considered that the prosecutor had not relied on any of the information obtained by torture while he was detained in Pakistan, and consequently should not stay proceedings against the accused simply because they were broadly associated with torture.

The Court then went on to consider the complicity of the actions of British agents in the torture at the hands of the Pakistani agencies.

Ahmed alleged the British were complicit because the relationship between them was such that they had encouraged or otherwise consented to his treatment. Yet the Court rejected the arguments, accepting the view of the Trial Chamber, that stated: "As a general principle, in order to protect the lives of its citizens, the UK may exchange information with countries whose record on human rights we may rightly or wrongly regard as inferior to ours."

Critics, such as Sarah Fulton, have condemned the ruling for its apparent inconsistency with the explicit obligations of the UN Convention against Torture, to which the United Kingdom has pledged itself to uphold, as well as reports of the Special Rapporteur on torture and the UK Joint Commission on Human Rights.¹⁰

¹⁰ See S. Fulton, 'Cooperating with the enemy of mankind: Can States simply turn a blind eye to torture?', IJHR, 16:5, 773-795.

In Germany, there was also a government commitment that executive agencies should continue to use torture-tainted information. In 2005, Interior Minister Wolfgang Schäuble said: “It would be completely irresponsible if we were to say that we don’t use information where we cannot be sure that it was obtained in conditions that were wholly in line with the rule of law. We have to use such information.”¹¹

The European Center for Constitutional and Human Rights (ECCHR) has documented several cases of torture in Europe as part of their ‘10 years after 9/11 publication series’.¹² They note that Murat Kurnaz, Mohammed Zammer, and Khaled El Masri were all tortured by or at the behest of American agents and that German agencies obtained information during interviews by the German Federal Intelligence Service, the BND, with each of the men. In each case, information was collected, received and shared between the BND and American agents. A parliamentary commission of inquiry, established to investigate Germany’s secret co-operation with the USA and other states in countering international terrorism in 2006, was unable to conclude to what extent information passed by the German BND was responsible for the treatment of the men, but it did consider that the intelligence shared was not checked for reliability prior to its transfer, and that information shared with the US led directly to the arrest of at least one of the men, Khaled El Masri.

The extraordinary rendition of Khaled El Masri

Khalid El Masri, a German citizen, was abducted at the Serbian-Macedonian border in 2003. El-Masri was first detained incommunicado and tortured by Macedonian agents for nearly a month, before being handed over to the US Central Intelligence Agency. In a well-documented process of rendition, El Masri was transferred to a facility in Afghanistan where he was regularly interrogated, subjected to physical abuse, and humiliated.

“The CIA stripped, hooded, shackled, and sodomized el-Masri with a suppository – in CIA parlance, subjected him to ‘capture shock’ – as Macedonian officials stood by. The CIA drugged him and flew him to Kabul to be locked up in a secret prison known as the ‘Salt Pit’, where he was slammed into walls, kicked,

¹¹ D. Crossland, ‘Germany Talks Torture, and Finds Hypocrisy’, Spiegel Online, 20 December 2005.

¹² ECCHR, *Torture and the Use of Information in Countering Terrorism*, Berlin, 31 October 2011.

beaten, and subjected to other forms of abuse. Held at the Salt Pit for four months, el-Masri was never charged, brought before a judge, or given access to his family or German government representatives.

“The CIA ultimately realised that it had mistaken el-Masri for an al-Qaida suspect with a similar name. But it held on to him for weeks after that. It was not until 24 May 2004, that he was flown, blindfolded, earmuffed, and chained to his seat, to Albania, where he was dumped on the side of the road without explanation.”¹³

El Masri’s case is one of the best documented extraordinary renditions by the CIA to date. In 2012, the European Court of Human Rights determined El Masri had been tortured and that Macedonia was responsible both for abusing him while in their custody and for the abuse he received in Afghanistan at the hands of the Americans.¹⁴

In Denmark, Danish Foreign Minister Villy Sovndal had to retract statements he made in 2012 promising that Danish agents would not rely on information obtained through torturing suspects in other countries. He later issued a statement saying that Danish authorities would continue to use information from countries that “use methods of interrogation that may contradict Danish principles of justice.”¹⁵

During their review before the UN Committee against Torture in 2012, Canada asserted that its intelligence agencies would share information obtained by torture in exceptional circumstances, even in contexts where there was a high probability that the information was incorrect or misleading. The Canadian delegation asserted that to be effective, their Security and Intelligence Service (CSIS) had to work with foreign agencies from all around the world, but that they do exercise caution with regard to such information.

¹³ ‘European court of human rights (sic.) finds against CIA abuse of Khaled el-Masri’, The Guardian (UK), 13 December 2012.

¹⁴ BBC, Europe Court award for rendition victim Khaled al-Masri, 13 December 2012, at <http://www.bbc.co.uk/news/world-europe-20712615>.

¹⁵ IRCT, ‘Denmark may use information obtained through torture’, <http://worldwithouttorture.org/2012/03/12/denmark-may-use-information-obtained-through-torture/>.

The case of Maher Arar

Maher Arar, a Canadian software engineer, was detained at JFK airport in 2002 on his way home to Canada, after a family holiday in Tunisia. After being held incommunicado, denied access to a lawyer, and interrogated by the FBI, he was unlawfully rendered to Syria. At the hands of his Syrian captors, he was repeatedly physically and mentally abused during lengthy periods of aggressive interrogation. Arar later falsely confessed to attending a terrorist training camp in Afghanistan, simply to stop the torture.

Almost a year after Arar's detention, the Syrians released him, saying publicly they considered him completely innocent.

In 2004, a Commission of Inquiry led by Justice Dennis O'Connor identified a long list of grave mistakes made by multiple Canadian authorities which led to Arar being rendered to Syria, and made important recommendations for Canadian authorities to prevent any future recurrence.¹⁶

The inquiry made clear that the Canadian authorities had come across Arar in the course of legitimate investigations into an acquaintance of Arar, and as there was evidence suggesting that there were close ties between the two men, Arar fell within the scope of that investigation as a result. However, both Arar and his wife were erroneously labelled as 'terrorists' in border surveillance watch lists, which proved dangerously inaccurate.

In the report of the Commission of Inquiry, it is noted that the Royal Canadian Mounted Police (RCMP) provided information to American authorities without necessary screening for personal information, relevance or reliability. Arar was portrayed in an inaccurate light and his importance in their investigation (as a witness) was overstated. The information was provided without caveats on how such information should be used. He was identified by RCMP as an "Islamic extremist [...] linked to the Al Qaeda terrorist movement", despite the fact that the RCMP had no basis for the description, which had obvious potential consequences for how Arar would be treated by American authorities. The inquiry concluded it is very likely that the American's relied on this information in the detention and deportation of Arar to Syria.

Furthermore, on receiving statements from Syrian authorities about a statement made by Arar, it was distributed and relied on by Canadian executive agencies without an assessment of its likely result of torture. The RCMP also submitted further questions to Syrian

¹⁶ Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar: Analysis and Recommendations, 2006.

authorities for the interrogation of a related individual, which served to reinforce Arar as a suspect in the eyes of Syrian authorities.

In the case of *Mahar Arar*, it is clear that the information shared by the Canadians with the US, in which Arar and his wife were labelled as extremist Islamists with links to Al-Qaeda, led directly to the unlawful detention and torture of Arar in Syria. The resulting flawed intelligence from interrogations with Arar flowed back to Canada, strengthening their conviction that he was the terrorist they sought. The questions sent from Canada led the Syrian Military Intelligence to believe a link between Arar and another suspect, Abdullah Almalki, and the self-fulfilling process of interrogation, newly intensified, began again.

At their review by the Committee against Torture, the Canadians asserted that 22 of 23 recommendations made in the Arar Commission report had been implemented, including the introduction of a number of additional safeguards. However, one of the most urgent, an oversight body to monitor the work of the security services, has not been set up, hence making it impossible to say whether safeguards are being applied in practice.

From these examples, we can identify two broad groups of cases. Some cases demonstrate examples of torture and other forms of ill-treatment carried out as a result information shared with foreign executive agencies (**outgoing** information). The victims of such treatment are detained and or interrogated on the basis of the information shared with the foreign agencies, and we must consider whether and to what extent sharing information with the foreign agency caused any resulting abuses. Other examples reveal examples of torture carried out to obtain information (which may or may not be with the complicity of domestic agencies), which is then shared with domestic agencies (**inbound** information). In these cases, we must ask whether reliance on such tainted information can serve to encourage further abuse.

It is important to remember that the issues highlighted above are not limited to intelligence sharing across borders. Similar issues may present themselves when agencies share information within just one State. Frequently, information received from a foreign

agency is compiled into an intelligence report, and shared with a number of domestic agencies. It is not uncommon for a domestic law enforcement agency to not know the source of the information, nor be given any assessment of its reliability. In such cases we must also ask who has any duty to caveat the information or remove the information from use.

Intelligence sharing networks

Intelligence sharing networks have been widely used between coalitions of States both before and since 2001. These networks are necessarily better addressed by international, rather than national laws, but at least one commentator has asserted that such networks have never been so constrained in practice:

“Intelligence sharing networks are constrained almost exclusively by a shared professional ethos, rather than the law. Such an ethos can exert some degree of accountability to professional norms, but has been strained by the inclusion of less professional and often ruthless intelligence services in the network.”¹⁷

Such networks reveal that information sharing is not just a ‘one to one’ exchange, but form part of a complex web of information which is made available, shared and used by multiple actors in network countries simultaneously. Even in well-established networks, there are no requirements that information obtained in violation of a person’s human rights be withheld, nor that only States that comply with human rights obligations be part of the intelligence-sharing agreement. Currently, intelligence sharing networks seem to have little appetite for cooperation requirements, revealing a tendency of intelligence agencies to prioritise the perceived value of shared information over human rights concerns. This current practice demonstrates a lack of human rights compliant principles for the sharing of information, but also an oversight gap which has yet to be addressed.

¹⁷ E. Sepper, ‘Democracy, Human Rights and Intelligence Sharing’, Texas International Law Journal, Vol. 46:151, 2010, 151-207, at 153.

What is the problem?

What is the problem with receiving and using torture-tainted information, and sharing information with States that torture?

Using the fruits of torture encourages it, and gives torture an ill-deserved credibility. Accepting, using, and placing value on such intelligence 'legitimises' the torture used for its collection. It is hypocritical of States to condemn torture committed by others while accepting its products.

In accepting torture-tainted information, States can become customers to torture, and may implicitly legitimise and encourage its use. By encouraging torture, agencies create a market where States that torture are rewarded for their trade.

Torture-tainted information is inherently unreliable. The pain and suffering caused to a victim destroys their will and causes them to say anything to end the pain. This pain and suffering is long-lasting, and likely causes the suffering to continue long after the torture itself ends. Using torture-tainted information which has a high risk of unreliability is contrary to the interests of police, security and intelligence agencies, who require accurate information in order to operate effectively.

Relying on tainted information wastes resources. Torture necessarily generates false positives, as interrogators only accept information they want to hear. On the basis of unreliable information obtained by torture, investigations are diverted and more information is sought, again repeating the cycle of torture. Such tactics wastes time and diverts attention from proper investigations and real threats.

It is immoral. In all stages of the intelligence cycle, ethical questions must be carefully balanced against the national requirements of intelligence, security, and police services.¹⁸

The analysis and production of intelligence, often written up in the form of an intelligence report, may have significant impact. Agencies can reasonably limit the reliance placed on to the information they share by attaching necessary caveats, such as error estimates, to the conclusions of their analyses.¹⁹

Torture is an international crime, punishable in any State. Where action by an executive agent constitutes torture, either by direct perpetration or some form of complicity, every State has a duty to prosecute the crime. Often, executive agents have escaped criminal responsibility for their actions in the torture of detainees held overseas. Nevertheless, several criminal inquiries are on-going, and agents and their agencies may yet be held accountable for violations of international law.

¹⁸ For a consideration of ethics during each stage of the intelligence cycle, see H. Born & A. Wills, 'Beyond the Oxymoron: Exploring ethics through the intelligence cycle', in J. Goldman (ed.), *Ethics of Spying (Volume 2)* (Scarecrow Press, Lanham: 2010), pp.34-56.

¹⁹ The UK Butler Inquiry was critical of the British Joint Intelligence Committee which did not offer clear limitations in its assessment to the government of whether Iraq possessed weapons of mass destruction.

How should we respond to the moral dilemma?

We may be presented with an impossible moral conundrum: What would you do, if you would save countless lives threatened by a real and immediate threat by using the fruits of torture?²⁰

This moral dilemma, which is in almost every case a fictional collaboration between impossible circumstances, is in large part a distraction from the absolute prohibition against torture, which does not allow actors to weigh the morality of their actions. As noted above, such information is likely to be untrue, and to act on such information would waste resources and legitimise the abuse. Importantly, such 'moral dilemmas' also ignore the preventive approach, which encourages the use of practices and procedures which safeguard against the wasteful situation of relying on information obtained by torture, and instead promotes the sharing and use of reliable information, obtained through effective non-coercive techniques of intelligent investigation. Through effective practices of prevention, such moral dilemmas lose much of their cache.

We can't stop executive actors acting on information which could save lives (and nor should we, as every State also has a fundamental duty to protect life and security). For this very important reason, it would be impossible to implement an absolute prohibition on the use of torture-tainted information, particularly where the stakes are so high. Instead, executive agencies might reconsider *how* such information is treated, and reflect on the active information-sharing relationships with States who have a long and shameful record of systematic torture.

²⁰ This scenario is often retold as a ticking-bomb scenario, which has now been thoroughly rejected by experts examining the issues from legal, political and moral perspectives. See for instance APT, *Defusing the Ticking Bomb Scenario: Why we must say No to torture, always* (2007), available at http://www.apr.ch/content/files_res/tickingbombsscenario.pdf.

Even outside an immediate threat scenario, it would be unrealistic to expect security and intelligence agencies to abandon all cooperation with States known to torture, particularly where there are strong historical links and other demographic associations. Indeed, it would be impossible to confront threats of international crime and terrorism without such cooperation. Advocates for an ongoing relationship with States that torture also point to the plain fact that through cooperating with such regimes, meaningful changes to abusive practices can better be achieved. In balancing the often delicate relationships with allied partners overseas, States should ask what positive preventive measures can be taken to ensure that the relationships between executive agencies do not encourage or lead to abuse.

These are certainly not easy issues to grapple with and we should not assume that a clear legal prohibition is necessarily effective in responding to the challenging legal and practical dilemmas that States face. More consideration among expert actors should be considered to weigh competing principles before guidelines for executive actors might be adopted.

Does it violate international law?

Does the use of torture-tainted information, or sharing information which leads to torture, violate international law?

As State actors, intelligence, security and police staff should uphold applicable international law, both through the application of relevant treaties and customary international law. This necessarily places clear limits on the actions of all executive actors and requires positive action should breaches of human rights be threatened or occur.

Jurisdictional questions have often been presented as a barrier to the extraterritoriality of human rights obligations, particularly in circumstances where State agents are not clearly in situations of control. Yet even with some questions remaining over the extraterritoriality of human rights obligations, this should not obscure the relevance for all State actors to comply with human rights obligations, wherever they may be. As observed by the Human Rights Committee, “it would be unconscionable to so interpret [obligations under the Covenant] as to permit a State party to perpetrate violations of the Covenant on the territory of another State, which violations it could not perpetrate on its own territory.”²¹ Similarly, the International Court of Justice considered that the rights enshrined in the Covenant extend “to acts done by a State in the exercise of its jurisdiction outside its own territory.”²²

Several relevant obligations may be derived from the absolute prohibition against torture. Nevertheless, it should be noted that the boundaries of emerging areas of law remain uncertain, and conclusions drawn in such areas should not be understood as universally recognised or settled principles of international law.

²¹ CCPR, *Sergio Euben Lopez Burgos v. Uruguay*, Communication No. R.12/52, U.N. Doc. Supp. No. 40 (A/36/40) at 176 (1981).

²² *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004, I.C.J. Reports 2004, paras. 111 and 113.

Absolute Prohibition against Torture

The **absolute prohibition against torture** “entails a continuum of obligations – not to torture, not to acquiesce in torture, and not to validate the results of torture and other cruel, inhuman or degrading treatment”.²³

In supplementing the absolute prohibition provided in the Universal Declaration on Human Rights, various treaties, and in customary international law, articles 1 and 4 of the UNCAT provide that a breach of the obligation is possible both by direct participation and complicity.

While complicit liability is defined in a variety of ways in the domestic law of each State, it is not defined in the Convention, but is understood to include wide forms of commission, including incitement, instigation, consent, or acquiescence. Such forms of complicit liability lead to confusion over whether and to what extent executive actors may be individually criminally liable, or cause the State to be responsible, for breaches of the Convention.

Without a clear definition for complicity, we should be particularly mindful of the distinction between forms of complicit liability that apply to State responsibility and individual criminal liability. Each is described in more detail below.

While most acts of complicity require an action, complicit responsibility by acquiescence perhaps causes the most confusion because it is essentially a passive action supporting, or tacit consent for torture committed by another. In circumstances where principles of State responsibility and individual liability for complicit acts of State agents are insufficient to find a violation, we might instead consider whether some fault should nevertheless be directed to States and their actors under this heading of liability.

Among the principal obligations of the prohibition against torture, is the **duty not to *refouler* a person to face a ‘real risk’ of torture overseas**. In the case of *Soering v UK*,²⁴ a landmark judgement of the European Court of Human Rights, the UK sought to return Soering

²³ ICJ, *Assessing Damage, Urging Action*; Report of the Eminent Jurists Panel on Terrorism, Counter-Terrorism and Human Rights (Geneva, 2009), p.85.

²⁴ ECtHR, *Soering v. The United Kingdom* (Application no. 14038/88), Judgement, 7 July 1989.

to the US where he would likely be subjected to cruel and degrading punishment. The European Court held that Soering should not be extradited, as the prohibition against torture would be engaged by the extradition and the extraditing State would be responsible for the breach, even where it is subsequently beyond its control.

The prohibition to send a person to a State where he would be subject to torture or cruel, inhuman or degrading punishment is already a clear violation of article 3 of the UNCAT itself, but the principle articulated by the European Court and others is potentially part of a much wider **general obligation not to expose a person to torture**. If a person cannot be returned to face torture, then logically, nor should information be sent to be used to torture a person already held overseas. Yet until a clear ruling or standard adopts such reasoning, this interpretation should be regarded with some caution.

Where a person is exposed to a risk of torture or ill-treatment, the standard of risk must be considered. The obligation not to *refouler* a person back to face torture requires a ‘real risk’ that they will face torture on their return, and it seems logical to retain this burden for the analysis of related manifestations.²⁵

The **exclusionary rule**, as described in article 15 of the UNCAT, could perhaps give an immediate answer to the issue of State use of torture-tainted information. It is, however, limited by its rather weak language, which has led some to question how far it may be applied to cover the actions of executive actors.

Article 15: Each State Party shall ensure that any statement which is established to have been made as a result of torture shall not be invoked as evidence in any proceedings, except against a person accused of torture as evidence that the statement was made.

Despite the fact that criminal proceedings are not explicitly described, the wording used in article 15 has regularly been interpreted to

²⁵ While ‘real risk’ is not explicitly articulated as the threshold for non-refoulement obligations, it is recognised as such in the jurisprudence and practice of several bodies. See Lauterpacht and Bethlehem, ‘The scope and content of the principle of non-refoulement : opinion’, in Erika Feller, Volker Turk and Frances Nicholson (eds.), *Refugee Protection in International Law: UNHCR’s Global Consultations on International Protection* (2003), in paras. 245–249.

exclude torture-tainted evidence in criminal proceedings only, and only when it was *established* that such evidence had been obtained by torture. This peculiar choice of wording has caused real difficulty in the application of the rule, as the burden of proving torture is typically left on the accused, making the rule, in many cases, illusory.

As a result of these weaknesses, authoritative commentators including the Special Rapporteurs on torture and counter-terrorism have recommended that the exclusionary rule be interpreted to apply much more widely, to include the activities of executive actors.²⁶

The approach taken by the Eminent Jurists Panel on terrorism, counter-terrorism and human rights was also to recognise that, in practice, the transition from an operation that is purely executive to one that is quasi-judicial or judicial is often seamless. Operational intelligence is often relied on in legal proceedings that follow.²⁷ The case of Hassan Diab,²⁸ currently being heard before the Canadian courts, is likely to have bearing on whether and to what extent operational intelligence should be excluded prior to its activation in a judicial context.

If we recall that the purpose for the adoption of the exclusionary rule was to disincentivize torture, States should be proactive to prohibit not just information shown to be established by torture, but should also view with serious suspicion and prohibit the use of any information obtained in violation of procedural safeguards intended to preserve the physical security and dignity of an accused.

Due to the wide interpretation of article 15 permitted by the UNCAT and the lack of guidelines, now would be a good opportunity to encourage further dialogue between experts and States parties, to review the exclusionary rule in light of a goal-oriented approach, rather than focussing excessively on the strict legalistic approach. For instance, a further general comment by the Committee against

²⁶ Report by the Special Rapporteur on torture, Juan E. Méndez, UN Doc. A/HRC/16/52, 3 February 2011, paras.53-57, and report of the Special Rapporteur on countering terrorism, Ben Emmerson, UN Doc. A/67/396, 26 September 2012, paras.48-49.

²⁷ ICJ, *Assessing Damage, Urging Action*; Report of the Eminent Jurists Panel on Terrorism, Counter-Terrorism and Human Rights (Geneva, 2009), p.85.

²⁸ See 'Justice for Hassan Diab', a website supporting the release of Mr Diab and tracking the progress of the case through the Canadian courts, at <http://www.justiceforhassandiab.org/news>.

Torture on this issue would be a welcome development, particularly if it were able to articulate applicable standards in the burden of proof and define the scope for the exclusionary rule by executive actors.

Among the principle obligations of the absolute prohibition against torture provided in the UNCAT, elaboration of the emerging duties not to expose a person to a real risk of torture overseas (dealing with outgoing information) and the exclusion of information established to have been obtained by torture (dealing with incoming information) could therefore serve to provide further guidance to States, executive agencies and their actors.

Principles of State Responsibility

State actors who commit violations of the UNCAT, or in the absence of treaty ratification, violate the comparable customary standards, commit an internationally wrongful act resulting in State responsibility.²⁹

As well as direct commission of internationally wrongful acts, the Draft Articles on the Responsibility of States for Internationally Wrongful Acts adopted by the International Law Commission (ILC) provide for forms of commission by complicity. The Draft Articles, which were intended to codify existing customary rules, additionally require that no State should provide aid or assistance to an internationally wrongful act (articles 16–18) and should not recognise as lawful a situation created by a serious breach and to cooperate to bring the breach to an end (articles 40–41).

It is clear that the forms of complicity considered by the ILC Draft Articles do not include commission by acquiescence. This should therefore be considered as a separate heading of liability under the *lex specialis* regime applicable for torture. Nevertheless, we should also be mindful that any internationally wrongful act must also be properly attributable to the State, which could narrow the scope for acquiescence as a form of liability.

In relation to aiding or assisting an internationally wrongful act, we should ask whether sharing information, putting questions or

²⁹ Draft Articles on Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission at its fifty-third Session, in 2001, and submitted to the General Assembly as a part of the Commission's report covering the work of that session (A/56/10).

providing other support short of actual participation constitutes 'aid or assistance'. The ILC Commentary suggests that an act must be intended to contribute significantly to the wrongful act, and while many active actions of executive agencies would certainly qualify, it remains unclear whether the forms of passive support (such as irregular receipt and use) would qualify.

Art.16 of the ILC Draft Articles also requires that the State must know of the circumstances of the illegality. In many cases of State cooperation, torture is so widespread, documented, and pervasive that no amount of wilful blindness on the part of the executive agency could avoid actual knowledge of the illegality required for State responsibility. Nevertheless, this additional hurdle is likely to present further difficulties for a finding of responsibility under this ILC article.

Where there are serious breaches, gross or systematic violations of peremptory norms of international law, such as the prohibition against torture, the special regime of rules described in Draft Article 41 comes into effect. Breaches of such rules immediately attach additional consequences, not only for the responsible State, but for all other States. All States must cooperate to bring an end to the breach and not recognise it as lawful, nor render aid or assistance to maintain the situation.

These Draft Articles require that if a State is known to *systematically* torture detainees, no State may recognise that information it receives from the agencies was lawfully obtained. Were such a conclusion to be widely accepted, it would have potentially significant consequences for joint police investigations and for INTERPOL, which routinely relies on information from States which may have been obtained under conditions amounting to torture. However, the exact scope of Draft Article 41 is not widely agreed. As a result, until further elaboration of the rule offers guidance to States, it remains an unsettled emerging rule of international law.

While it remains unclear exactly how Draft Article 41 should be understood in the context of the executive use of information, we might tentatively recognise that by maintaining an active and ongoing information-sharing relationship with States that systematically torture, States serve to maintain the situation of illegality, contrary

to the requirements described in Draft Article 41.³⁰ Such a conclusion would appear consistent with the views of jurist Matt Pollard, who asserts that “after the fact acceptance and use of information also could forcefully be argued to constitute implicit recognition of the situation created by torture as lawful since it treats the information no differently than legally-obtained information.”³¹

Individual criminal liability

Pursuant to UNCAT article 4, commission of torture by complicity may also lead to individual criminal responsibility. However, as noted above, complicity is a complex form of liability and one in which various standards apply. The standards for complicity in domestic and international criminal law (for one example, see article 25 Rome Statute) apply distinct standards from those applying to State responsibility. Unlike forms of State responsibility, where courts might establish liability based on the *imputed* knowledge that shared information would lead to torture, where complicit liability is sought against individuals, the standard of liability is rightly much stricter due to the penal nature of the judicial sanction.

Any standards for domestic criminal liability must be understood in light of the applicable domestic law in force. In relation to the international criminal law standards for complicit liability of individuals, standards appear to have been revised in light of the successful appeal of Perišić at the International Criminal Tribunal for the former Yugoslavia in February 2013, following his earlier conviction for providing arms and logistical assistance to the Bosnian Serb army,³² and the contrary finding in the Appeal of

³⁰ For support, see the criticism of the English case, *Rangzieb Ahmed & Anor v. R* [2011] EWCA Crim 184 (2011) by Sarah Fulton. Fulton asserts that the Court erroneously held the UK to lower expectations than those imposed by international law and that “the passive receipt of information known or suspected to have been obtained from torture may amount to an internationally wrongful act.” In S. Fulton, ‘Cooperating with the enemy of mankind: Can States simply turn a blind eye to torture?’, *IJHR*, 16:5, 773-795, at 774.

³¹ M. Pollard, ‘Rotten Fruit: State Solicitation, acceptance, and use of information obtained through torture by another state’, *NQHR*, Vol.23/3, 349-378 (2005), at 377.

³² ICTY, *Prosecutor v. Momčilo Perišić*, Appeals Chamber Judgement, 28 February 2013, IT-04-81-A.

Charles Taylor at the Special Court for Sierra Leone.³³ According to the Perišić Appeals Chamber judgement, aiding and abetting must be ‘specifically directed’ toward the commission of crimes.³⁴

Despite some criticism of the Chamber’s ruling (and hence uncertainty over how the rule would be applied in future), its reasoning was to require a culpable connection between the aider and abettor and the principal perpetrator of the crime. Whatever the wisdom of their analysis, the result is that it is questionable that executive actors would be individually criminally responsible for torture when committed by complicit acts (such as sharing questions later used in the torture of a detainee) unless a sufficient degree of culpability such as specific direction is also shown.

In summary, the absolute prohibition against torture condemns both active participation and acts of complicity in torture. Yet liability for acts of complicity is complex, and various unsettled principles of law serve to limit the predicable scope of State responsibility and individual liability. In light of apparent inconsistencies in jurisprudence and practice, further examination of the applicable law would be welcome.

³³ See SCSL, *Prosecutor v. Charles Taylor*, Appeals Judgement, SCSL-03-01-A, 26 September 2013, at paras. 479–480.

³⁴ Citing ICTY, *Prosecutor v. Dusko Tadic*, Appeals Chamber Judgement, 15 July 1999, IT-94-1-A, para.229.

Existing national standards from the perspective of International Law

After significant public pressure, Canada and the UK both published guidance issued to their executive agencies on the use of information. It is important to analyse each to understand how States appreciate their obligations under international law. Lessons may be drawn for other States who are contemplating or already have similar (unpublished) guidelines.

United Kingdom

In 2010, the UK published its Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees.³⁵

*The United Kingdom Government's policy on such conduct is clear – we do not participate in, solicit, encourage or condone the use of torture or cruel, inhuman or degrading treatment or punishment for any purpose.*³⁶

Despite providing a clear public commitment to prohibit torture, however, later detail in the guidance has led to questions over how effective the prohibition is in practice. First, the guidance provides that State actors should not proceed to work with a foreign agency where there is a 'serious' risk of torture. Such a high threshold would appear to exceed what is required in international law, where it is submitted only a 'real' risk should prevent engagement.³⁷ Even in

³⁵ The UK guidance was later revised to make clearer that the hooding of detainees by foreign States in any circumstances constitutes torture or other ill-treatment.

³⁶ See UK guidance, para.6.

³⁷ A 'real risk' of torture engages the *non-refoulement* obligation of UNCAT article 3 preventing an executive order of deportation and it is submitted to be the most appropriate standard for effectively preventing the risk of torture to a detainee held overseas.

circumstances of a serious risk of torture, the guidance does not prohibit cooperation with a foreign agency. Rather, it provides that concerns should be directed to senior personnel and to Ministers, who may consider the risk on their own terms.

Yet when the guidance was challenged by the UK Human Rights Commission on the basis that the rules fail to meet the UK's obligations in both UK and international law, and consequently opened up officers to criminal liability,³⁸ the court disagreed. It ruled the guidance "makes clear that, in all relevant instances other than where there is no serious risk of CIDT (Section 2 of the table), the officer must not proceed at all (Section 1) or the matter must be referred to senior personnel or Ministers".³⁹ The court was also not persuaded there was any material difference between a 'serious risk' or 'real risk' in this context.

Recognising that the guidance might lead to confusion, and hence inconsistency in practice of executive agencies, in 2013 the UN Committee against Torture recommended the guidance be reworded to avoid ambiguity and the possibility that assurances from foreign services would suffice to permit cooperation where serious threats are identified.⁴⁰

Inevitably, there are significant shortcomings with any guidelines which leave uncertainty over whether any officer may use tainted information. Without sufficient legal precision, national actors may find themselves interpreting the text in a way that was not intended. The ambiguous language identified by the Committee against Torture could fail to give intelligence and security actors the detailed guidance necessary to ensure that they act in a way which is compatible with international and domestic law.

While the guidance does not purport to be a statement of law, inconsistencies in the text and lack of specificity in legal descriptions used could serve to undermine the purpose to prevent UK complicity in torture.

³⁸ UK High Court, *The Equality and Human Rights Commission, v. The Prime Minister*, Judgement, 3 October 2011, [2011] EWHC 2401 (Admin).

³⁹ *Ibid.*, at para.61.

⁴⁰ CAT, Concluding observations on the fifth periodic report of the United Kingdom, adopted by the Committee at its fiftieth session (6-31 May 2013), CAT/C/GBR/CO/5, para.11.

In one example of the shortcomings of such broad guidelines, a short illustrative list of prohibited practices is provided in its annex. Inevitably, such a list will be the primary tool used by officers to determine whether a practice is prohibited or not. Significantly, this list fails to examine the use of practices in combination, or other practices which have comparable effect on the victim. The annex itself over-simplifies a number of critical legal terms, being rather too brief to provide the detailed guidance necessary to avoid allegations of complicity in acts of torture, and provides an inaccurate description of the prohibition at international law.

Nevertheless, there are some welcome provisions in the UK guidance, indicating for instance, that the agencies should review their practices to avoid the impression that their receipt of information “is an encouragement of the methods used to obtain it.”⁴¹ Furthermore, the guidance does provide for a number of actions to mitigate the risk of torture in the event that a risk of ill-treatment or torture is identified, including attaching conditions to requests and shared information.

Canada

Justice O’Connor’s inquiry in to the *Mahar Arar* case in Canada led to the 2011 publication of the ‘Ministerial Direction to Canadian Security Intelligence Service (CSIS): Information sharing with foreign entities’.⁴² While the new Ministerial Directions deal with both sending and receiving of information that could in either case lead to torture, they are still very loosely worded and capable of vague interpretation.

As with the UK Guidance, the Canadian Guidance offers rather inconsistent advice to its executive agents. The Direction states in the strongest terms that Canada opposes the mistreatment of any individual by any foreign entity for any purpose, but at the same time excuses itself from full adherence by expressing its own duty to its own citizens and allies of preventing harm that could be caused by individual engaging in threat related activities.

⁴¹ See UK guidance, para.28.

⁴² Since the 2011 Direction, further ministerial Directions to the Royal Canadian Mounted Police and the Canada Border Services Agency emerged. Taken together, they are meant to establish a coherent and consistent policy on decision-making processes regarding information sharing where there may be a risk of mistreatment.

Also comparable with the UK Guidance, the Canadian Direction states where there is a ‘substantial risk’ of mistreatment as a result of sharing information, the matter should be referred to the Service Director, who will balance the obligations. As with the UK guidance, this is a high threshold for action and above the international standard of appreciating a ‘real’ risk in determining the safety of action.

Regarding inbound intelligence, the CSIS is directed not to *knowingly* rely upon information derived through mistreatment.

One of the major problems with the 2011 Ministerial Direction is that it provides a defence in the event of ‘exceptional circumstances’:

“[I]n exceptional circumstances, the CSIS may need to share the most complete information to mitigate a serious threat of loss of life, injury, or substantial damage or destruction of property before it materialises.”

Such a defence could permit executive action which leads to torture or deportation, a possibility that was first introduced into Canadian law by the case of *Suresh*.⁴³ The language of the directive clearly indicates that the Government intends to leave open the possibility that torture-tainted information or information which leads to torture may continue to be used without legal sanction.

For basic reasons, the broad defence of ‘exceptional circumstances’ is hugely problematic. The idea that certain undefined ‘exceptional circumstances’ could justify sharing information with States that torture could open the floodgates to abuse and potentially encourage State actors to cooperate widely on the basis of subjective and ill-defined concepts of necessity.

Both the Canadian and UK guidelines place reliance on the assurances received from foreign agencies and States. The practice of relying on such unenforceable assurances from States which routinely torture raises a number of serious human rights concerns. Several experts, such as the High Commissioner for Human Rights and the Committee against Torture have shown that such arrangements do not work in practice to protect persons from clear risks of torture

⁴³ *Suresh v. Canada* (Minister of Citizenship and Immigration), 2002 SCC 1.

and ill-treatment. The Committee against Torture has made critical statements on the use of diplomatic assurances, and has recalled that they are not sufficient to protect detainees in the context of cross border intelligence sharing.

Most recently, in their follow-up report to the Committee against Torture, the Canadian Government reinforced that Canada neither promotes nor condones the use of torture or other unlawful methods of investigation, yet rejected the recommendation of the Committee to modify the Ministerial Directions to ensure consistency with the Convention against Torture.⁴⁴ The Statement recalled that the Ministerial Direction had required that procedural safeguards must be in place in order for its agencies to use and share information:

*First, agencies must take all reasonable measures to reduce the risk that any action on their part might promote or condone the use of mistreatment. Second, they must have in place reasonable and appropriate measures to identify foreign entity information that is likely to have been derived from mistreatment, and must properly characterize this information in any further dissemination of it.*⁴⁵

Such advice does not exclude the possibility that Canadian agencies may use information tainted by torture, nor does the Direction exclude the possibility that information would be shared with another State which tortures a person in their custody.

While both sets of guidelines share a fair number of weaknesses, the mere fact that guidelines have been agreed and published is proof that Canada and the UK recognise a duty of care for persons held overseas, and the challenges their executive agents face in using and sharing information with partner agencies overseas. This recognition, and the commitment to provide practical and transparent advice, is good practice that other States might share.

⁴⁴ CAT, *Interim Report in follow-up to the review of Canada's Sixth Report on the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, August 2013, CAT/C/CAN/CO/6/Add.1.

⁴⁵ *Ibid.*, at para.30.

International principles for executive agencies

“Information sharing is vital, but it must take place in a reliable and responsible fashion. The need for information sharing does not mean that information should be shared without controls, particularly without the use of caveats. [...] [C]ontrols are meant to facilitate and promote the orderly flow of information, not impede or stop it.”⁴⁶

From discussions with experts and from the examples described in this report, it is possible to distil a number of principles and questions for executive agencies to consider, which might be further developed.

Clear prohibition on active collection of torture-tainted information

It is well understood that the active participation or complicity in the torture of persons overseas is unlawful. This principle applies to prevent executive agents asking questions or in any way encouraging the abuse of a person held overseas.

Practice 35: Intelligence services are explicitly prohibited from employing the assistance of foreign intelligence services in any way that results in the circumvention of national legal standards and institutional controls on their own activities. If States request foreign intelligence services to undertake activities on their behalf, they require these services to comply with the same legal standards that would apply if the activities were undertaken by their own intelligence services.⁴⁷

⁴⁶ Per Justice O'Connor, in *Arar* recommendations, *supra.*, p.331.

⁴⁷ Report of Martin Scheinin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/14/46, 17 May 2010.

The various good practices of law enforcement agencies in the collection of evidence might be applied to the use of torture-tainted information. The strict rule of exclusion for any evidence obtained in violation of the prohibition against torture and ill-treatment should be the starting point for any active process of receiving information from another State.

As noted in a recent OSCE publication providing guidance for investigations by law enforcement officials, “[t]he information or intelligence obtained by such illegal means, even when not intended to be used in court proceedings, should always be treated in the same way that a court would treat evidence obtained by illegal means and, thus, be disregarded.”⁴⁸ This, it provides, is because the reliability of such information will always be doubtful.

If it is now well understood that confessions are suspicious when they provide the only evidence of guilt, that torture-tainted evidence is inherently unreliable, and the use of such evidence damages the integrity of the judicial process, then it must also be recognised that any use of torture-tainted information in an executive process is just as problematic.

Is receipt of torture-tainted information ever really ‘passive’?

There is considerable confusion among executive actors as to where activities of agencies changes from mere *passive* receipt into *tacit* consent and acquiescence, at which point the receiving agency becomes part of the commission.

States have attempted to avoid liability for their role in abuse of persons by describing their role as merely passive, when, in reality, there is a much more active relationship. Often, States exchange information on a continuous and systematic basis, perhaps even subject to a formal agreement. As information is rarely offered without an agreement of intelligence sharing or some similar reciprocal understanding, whether information could ever be received passively is open to some doubt. As a result, even though information appears to be shared passively, international duties and obligations could still apply.

⁴⁸ OSCE, Human Rights In Counter-Terrorism Investigations: A Practical Manual For Law Enforcement Officers (2013), p.28.

Assessment of State compliance with human rights principles (due diligence)

The *Arar* Commission assessed the appropriate response for cooperation and information sharing with States known to torture. It recommended that the Relevant Ministry of Foreign Affairs officer should produce an assessment of the State, and this should be used as a basis for engagement and cooperation.

Good practice for sending information to executive agencies overseas

For outgoing information, States should provide a clear rule that no information should be shared with a foreign State where there is a credible risk that it will cause or contribute to the use of torture. Assessments should not rely on actual knowledge only, as this inevitably leads to the conclusion that officials can deliberately avoid such knowledge. Whenever there is a reasonable basis for questioning a country's human rights record, such as reports from credible NGOs, officials should err on the side of caution.

Ultimately, information should never be provided where there is a 'real' risk that sharing information with another State will cause or contribute to the use of torture.

Sir John Sawers (MI6) said clearly the role agencies should play where torture is likely:

"Torture is illegal and abhorrent under any circumstances, and we have nothing whatsoever to do with it. If we know or believe action by us will lead to torture taking place, we're required by UK and international law to avoid that action. And we do, even though it allows the terrorist activity to go ahead."⁴⁹

Information should only be shared in a way which does not identify persons of interest as suspects. Such precision in reports is essential in order to avoid harm to individuals during an investigation. Caution should also be used before using emotive or inflammatory phrases such as 'Islamic extremist' or 'jihadist'.

⁴⁹ Per Sir John Sawers, Head of UK Secret Intelligence Service, in a speech delivered 28 October 2010.

Even a visit which does not reveal any information which could impact negatively on the treatment of any suspect could have unintended consequences. Decisions to interact with States that torture must be made in a way which is controlled carefully to avoid complicity in human rights abuses, or a perception of endorsement.

Requests for information

Questions posed have the potential to lead to a violation of human rights law. Agencies should carefully evaluate the risks posed by requesting information from questionable agencies, and attempt to ensure the person is treated in line with international human rights standards.

Good practice for the receipt of information likely obtained by torture

For inbound information, a proper assessment of the information must determine whether it has likely been produced as a result of torture. Information should additionally be checked for accuracy and analysed in the light of the context from which the information originates. As noted above, acceptance of information can condone torture and lead to State responsibility for the wrongful acts. All agencies should adopt policies for the receipt of information from such States, with special focus on the reliability and accuracy of the information.

Where a State has a questionable human rights record, even the 'passive' receipt of information should be viewed with suspicion, and rejected where appropriate.

The provenance of intelligence must always be caveated in one way or another

Authorities have an interest and responsibility to ensure the information it shares is accurate and appropriate for the purpose. It is also important that the authorities control, to the extent they are able, the use of such shared information. This is known as the control principle, and is "rule number one of intelligence sharing."⁵⁰

⁵⁰ *Ibid.*

Information shared without caveats could lead to a partner agency placing reliance on information which is ill-deserved. In the *Arar* Commission, Justice O'Connor considered that as one never knows the importance information may hold in the overall intelligence picture as information from various sources are pieced together, even seemingly minor details, when taken together, can create a picture of someone who is heavily involved in illegal activities.

State officials should conduct an assessment of information's reliability, and this assessment should accompany the information when, or if, it is distributed to additional agencies.

Caveats are already used widely by both law enforcement and intelligence and security agencies, to manage information where there are questions over its source, its reliability and how it should be used. One example of the use of caveats in practice is the 5x5x5 form, which is the national information and intelligence reporting process which allows the UK Police Service and other agencies to record, evaluate and disseminate information. The form assigns a value to the source, the information and how it should be handled, thus allowing the police to handle and use information where there are questions over its truth.⁵¹

Caveats do not mean that information will not be misused, but do provide a moral obligation to use the information only in the way intended: "They are the best means available to reduce the risk of misuse."⁵² Misuse of shared information can also lead to a review of cooperation in future.

The *Arar* case demonstrates the importance of using caveats to ensure both accuracy and minimise the risk of intelligence being given too much reliance where there are concerns over its source or its reliability.

⁵¹ See, *Practice Advice: Introduction to Intelligence Led Policing, Association of Chief Police Officers (2007)*, at <http://www.acpo.police.uk/documents/crime/2007/200708-cba-intelligence-led-policing.pdf>.

⁵² *Arar* recommendations, *supra.*, p.342.

Intelligence sharing networks should require minimum guarantees

Intelligence sharing networks have greatly increased in the years since 2001. At the UN, the Counter-terrorism Committee declared one of the aims to be to further develop intelligence-sharing and cooperative action between agencies, indicating that the growth of such networks is likely to continue.⁵³

Recognising that intelligence networks should share information, robust professional standards, grounded in international law, should govern their operation. Such networks should work to improve the standards of less professional agencies in the network, in a process labelled as 'acculturation', by commentators Ryan Goodman and Derek Jinks.⁵⁴ Elizabeth Sepper supports the approach, explaining by example: "if Jordanian intelligence understands that complying with standards like caveating for reliability or not sharing information obtained through torture is a precondition for inclusion and good reputation in the network, it will obey the standards out of a desire to join or become a respected member of the group."⁵⁵

Requiring such standards from partners will inevitably cause some agencies to hesitate before sharing information. Nevertheless, the misuse of information and any human rights abuses such as torture that are solicited through requests for information will have the same effect, and reduce the effective capability of the intelligence agency.

Intelligence oversight

Oversight of cooperation agreements is a crucial element of civilian control in a democratic State. Oversight has been criticised for being unable to consider the 'originator control' or 'third party rule' of intelligence cooperation. These rules require that the originator limits the use and sharing of intelligence, including to third parties such as oversight bodies. However, even if these rules are carefully

⁵³ Sir Jeremy Greenstock, press conference, 19 October 2001, as quoted in M. Herman, 'Ethics and Intelligence after September 2001, in J. Goldman (ed.), *Ethics of Spying (Volume 2)* (Scarecrow Press, Lanham: 2010), pp.103-120, at 111.

⁵⁴ E. Sepper, 'Democracy, Human Rights and Intelligence Sharing', *Texas International Law Journal*, Vol. 46:151, 2010, 151-207, at 163.

⁵⁵ E. Sepper, 'Democracy, Human Rights and Intelligence Sharing', *Texas International Law Journal*, Vol. 46:151, 2010, 151-207, at 164.

observed, there are no reasons to prevent an intelligence oversight organ from reviewing agreements upon which intelligence sharing is based as well as intelligence sent to foreign entities.

The real practical challenges in proving complicity with regards to torture committed overseas again underlines the overriding need for democratic oversight of intelligence agencies, which can request the information which could establish 'knowledge' for the purpose of a finding of complicity in acts of torture committed overseas.

In a 2010 Joint Study on Global Practices in Relation to Secret Detention in the Context of Countering Terrorism, Special Procedures of the Human Rights Council recommended "any action by intelligence services should be governed by law, which in turn should be in conformity with international norms. To ensure accountability in intelligence cooperation, truly independent intelligence review and oversight mechanisms should be established and enhanced."⁵⁶

Pursuant to the *Arar* case, one of the principal findings of Justice O'Connor's report on recommendations for oversight of intelligence services to prevent illegal intelligence methods and better review was that an integrated approach was essential to ensure there were no gaps between domestic oversight mechanisms.

Practical training should be made available to give operational actors full instruction on these standards

It is now common to require police and law enforcement officials to undergo ongoing training to abstain from torture and other forms of ill-treatment. Such training and syllabus development is often facilitated by interested NGOs and activists, but other relevant actors (such as professional legal associations) also play an important role.

The effective prohibition and prevention of torture must also form a key part of the ongoing training delivered to security and intelligence officials, which should be dispersed into regular training, particularly in areas of key risk such as interviewing persons, and reducing the risks of torture when working with other agencies.

We have seen that periods of tension and conflict can lead to a huge amount of pressure being left on all executive agencies to deliver results. In the period of aggressive counter-terrorism operations,

⁵⁶ A/HRC/13/42, 19 February 2010.

such pressure caused agency staff to take increasingly dangerous risks to show the results that are required, both by their own agencies and foreign agencies. Published materials have confirmed that under such pressure, staff from executive agencies in various countries have been increasingly susceptible to break the rules and act unlawfully. There must be clear and unambiguous safeguards in place to prevent such actions. Training must reassure agencies that no person will be asked to break the law to fulfil their duties, even in periods of extreme tension, and that any such request must be rejected and reported.

Publish guidance for executive agencies

Even though the UK and Canada's guidelines are flawed, they do acknowledge the existence of certain duties and are useful in the sense of recognizing that some obligations are owed to persons in detention. States, by even enunciating these guidelines, recognize that they do not have *carte blanche* to treat detainees however they want.

Such detailed guidelines are encouraging, and may serve as an example for other States. As noted above, such guidance should be open to regular parliamentary scrutiny and oversight.

Conclusion

Though the moral challenge might be understood to place limits on what may practically be achieved to regulate the practices of executive agencies, a proactive preventive approach can serve to reduce the threat and enhance professional standards of executive actors in line with international human rights obligations.

With regard to affirmative steps that can be taken to further protection, while human rights concerns cannot prohibit all intelligence sharing, a realistic option can be something akin to an 'acculturation process', whereby countries which have more stringent norms on these issues can have a more positive and ongoing engagement with the intelligence agencies that are known to torture and therefore influence them to abstain from the use of torture.

Equally, States might consider whether the important relationships they maintain with States which routinely torture should include the continuous exchange of information, with the inevitable result of torture. States should further consider how to more actively acculturate executive agencies in such States. Such a process must start to show how ineffective torture is as a method of interrogation.

The lack of clear practical rules for executive actors and uncertainty over the application of legal principles indicates the adoption of internationally agreed standards on this issue would have an impact on executive agencies across the world. As actors see themselves as extremely moral actors, there is a presumption that such standards would be followed. The good practices of Martin Scheinin, former Special Rapporteur should be used as a good starting point. More comprehensive guidelines would be welcome to further implement the absolute prohibition against torture and other ill-treatment.

It should not be accepted that executive agencies, or particularly those agencies that conduct analysis of information, do not know the circumstances of its collection. It is unlikely in practice that intelligence agencies would not ask any questions of the provenance

of information, because such agencies need to know the source in order to assess the value of the information.

A 'checklist of compliance' with international law might also be adopted to assist parliamentary oversight mechanisms establish practices for police, security and intelligence services which significantly reduce the risk that torture will be used to extract information or that torture will result at the end of such cooperation.

The development of normative guidance would be welcome, but additional safeguards to ensure compliance, such as independent oversight, would also be essential additional components to ensure its success. It is only through effective oversight that the implementation of standards can be assessed.

Due to uncertainties over the specific application of general legal principles to the executive use of torture-tainted information, and the real practical challenges faced executive actors, further expert analysis is warranted. From such expert analysis, a clear set of principles and guidelines on the executive use of such information is recommended for development, which could serve to guide national policy, closing the international market for torture products and enabling States to avoid complicit liability for acts of torture committed overseas.

Annex

Former Special Rapporteur Martin Scheinin's compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies

Further to Martin Scheinin's 2009 recommendation for the adoption of specific guidelines for human rights compliance and best practice by intelligence agencies,⁵⁷ the Special Rapporteur submitted a **compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies** while countering terrorism.⁵⁸ The compilation was the outcome of consultation with governments, experts and practitioners. The report states that the good practices listed therein "not only refers to what is required by international law, including human rights law, but goes beyond these legally binding obligations."⁵⁹

Intelligence sharing good practices are listed in practices 31 to 35:

Practice 31: Intelligence-sharing between intelligence agencies of the same State or with the authorities of a foreign State is based on national law that outlines clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence.

⁵⁷ Report of Martin Scheinin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/10/3, 4 February 2009, at para.78.

⁵⁸ Report of Martin Scheinin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/14/46, 17 May 2010.

⁵⁹ *Ibid.*, in summary paragraphs.

Practice 32: National law outlines the process for authorizing both the agreements upon which intelligence-sharing is based and the ad hoc sharing of intelligence. Executive approval is needed for any intelligence-sharing agreements with foreign entities, as well as for the sharing of intelligence that may have significant implications for human rights.

Practice 33: Before entering into an intelligence-sharing agreement or sharing intelligence on an ad hoc basis, intelligence services undertake an assessment of the counterpart's record on human rights and data protection, as well as the legal safeguards and institutional controls that govern the counterpart. Before handing over information, intelligence services make sure that any shared intelligence is relevant to the recipient's mandate, will be used in accordance with the conditions attached and will not be used for purposes that violate human rights.

Practice 34: Independent oversight institutions are able to examine intelligence sharing arrangements and any information sent by intelligence services to foreign entities.

Practice 35: Intelligence services are explicitly prohibited from employing the assistance of foreign intelligence services in any way that results in the circumvention of national legal standards and institutional controls on their own activities. If States request foreign intelligence services to undertake activities on their behalf, they require these services to comply with the same legal standards that would apply if the activities were undertaken by their own intelligence services.

Torture is an abhorrent practice and absolutely prohibited in international treaties, custom and in the constitutions of almost every State. More than a decade since the launch of the war against terrorism, police, security and intelligence agencies should now consider what the limits of intelligence cooperation between States should be, in order to restore the dignity of the absolute prohibition against torture.

In November 2013, the APT hosted a group of experts to consider the practical and legal implications for the sharing and use of torture-tainted information by executive agencies. The experts were asked to consider whether and how standards for the use of information obtained by torture could be adopted, to guide State behaviour in complying with international standards.

Among the questions asked, were:

- What is the problem with police, security and intelligence agencies receiving and using torture-tainted information, or sharing information with States that torture?
- How should we respond to the 'moral dilemma', whereby rejecting information could undermine attempts to prevent terrorism?
- Does the executive use of torture-tainted information, or sharing information which leads to torture, violate international law?