PRIVACY INTERNATIONAL

Privacy International's Submission to the Investigatory Powers Commissioner's Consultation on the Consolidated Guidance

October 2018

About Privacy International

Established in 1990, Privacy International is a non-profit, non-governmental organisation, which defends the right to privacy around the world. Privacy International conducts research and investigations into government and corporate surveillance activities with a focus on the policies and technologies that enable these practices. It has litigated or intervened in cases implicating the right to privacy in the courts of the United States, the United Kingdom, and Europe, including the Court of Justice of the European Union and the European Court of Human Rights. It is frequently called upon to give expert evidence on privacy issues and has advised and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional, and international laws that protect this fundamental right. As part of this mission, Privacy International works with various partner organisations across the world to identify and address threats to privacy.

Contact

Scarlet Kim
Legal Officer
020 3422 4321
scarlet@privacyinternational.org

A. Introduction

Privacy International welcomes the invitation by the Investigatory Powers Commissioner's Office ("IPCO") to submit to the public consultation on the "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" ("Consolidated Guidance").[1]

Privacy International's submission is confined to addressing the portions of the Consolidated Guidance on "the Passing and Receipt of Intelligence Relating to Detainees." Our submission is informed by our work on intelligence sharing and its human rights implications. This work encompasses litigation challenging the UK's intelligence sharing practices, including its access to information collected through an array of US mass surveillance programs, as well as its provision of information collected through its own mass surveillance programs to foreign partners.[2] We have also published several reports on intelligence sharing, which touch upon the UK's intelligence sharing practices.[3]

Our work on intelligence sharing has revealed that in most countries around the world, the public remains in the dark regarding arrangements to share intelligence. Moreover, in most countries, those arrangements lack the necessary safeguards to ensure that intelligence sharing does not violate or facilitate the violation of human rights, including the right to be free from torture and cruel, inhuman or degrading treatment or punishment ("CIDT"). The UK is no exception. In a report published this year, the Intelligence and Security Committee ("ISC") of Parliament documented hundreds of cases where UK officials shared or received information with foreign partners despite knowledge that those partners were committing or likely to commit torture or CIDT.[4]

---

[1] 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 ("Consolidated Guidance"), July 2010, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62632/Consolidated_Guidance_November_2011.pdf.

[2] *10 Human Rights Organisations v. the United Kingdom*, European Court of Human Rights; Application No. 24960/15; *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs et al.*, Investigatory Powers Tribunal, No. IPT/15/110/CH.

[3] *See, e.g.*, Privacy International, Secret Global Surveillance Networks: Intelligence Sharing between Governments and the Need for Safeguards, April 2018, available at https://privacyinternational.org/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20%28200%29_0.pdf; Privacy International, Eyes Wide Open, November 2013, available at https://privacyinternational.org/sites/default/files/2018-02/Eyes%20Wide%20Open%20v1.pdf.

[4] Intelligence and Security Committee of Parliament, Detainee Mistreatment and Rendition: 2001-2010, 28 June 2018, pp. 51-60, available at https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20180628_HC1113_Report_Detainee_Mistreatment_and_Rendition_2001_10.pdf?attachauth=ANoY7cpWNu3temwz-ZvhWsS04T2ZoknEP12mCU8BLf_JRiGQZJf6bP5Z4PssA9lPvYqcrL8DQ6j7Z6ATTSGudYRCq1J88EoR1fHlXA_b6uvC0Dlx3_ALLn_-nb_j_A2W4fkyyK9p5am5uquGFmv_HgaJ00EQ4Y3Xw7mFGObBTaHxrd901_4qTLnq0javmKzFycgfiSf_Oedy5czPowrR6lueyGYtNv7_6WTi3yjgPvp6FEhgOhJ1kQIdQUPGup9ScwevWaZlvoNifxAoKQ_5WuhxlJwgBmywLF52hGVgJC8b01pwrlAphwU%3D&attredirects=1.

Our submission proceeds as follows. First, it provides background on the relationship between intelligence sharing and serious human rights abuses as well as the documented relationship between UK intelligence sharing and such abuses. Second, it discusses why the scope of the Consolidated Guidance is inappropriately narrow with respect to intelligence sharing. Third, it explains why the Consolidated Guidance provides insufficient assistance to UK agencies when considering the human rights implications of intelligence sharing, including its relationship to torture or CIDT. Fourth, it reviews why the "assurance process" as it pertains to intelligence sharing is inadequate. Fifth, and finally, it discusses the need for an establishment of a notification requirement. An attached annex consolidates the recommendations made throughout the submission.

B. Background

1. Intelligence Sharing and Serious Human Rights Abuses

As the United Nations Special Rapporteur for Counter-Terrorism has stated:

> "Both the sending and receipt of intelligence can have important implications for human rights and fundamental freedoms. Information sent to a foreign Government or intelligence service may not only contribute to legal limitations on the rights of an individual, but could also serve as the basis for human rights violations. Similarly, intelligence received from a foreign entity may have been obtained in violation of international human rights law."[5]

As outlined above, intelligence sharing consists of both the "sending and receipt of intelligence." The "sending", or provision, of intelligence can contribute to or facilitate a variety of serious human rights abuses. This risk is particularly acute where intelligence is provided to states with authoritarian governments, weak rule of law and/or a history of violating human rights. In these contexts, such intelligence may form the basis for extrajudicial killings or contribute to unlawful arrest, detention, or torture or CIDT.[6] A state that shares intelligence that a foreign partner then uses to facilitate such abuses may also bear responsibility for those abuses.[7]

---

[5] Martin Scheinin, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, UN Doc. A/ HRC/14/46, 5 May 2010, para. 47.

[6] *See* Born et al., Making International Intelligence Cooperation Accountable, 2015, pp. 43-45, available at https://www.dcaf.ch/sites/default/files/publications/documents/MIICA_book-FINAL.pdf; Eminent Jurists Panel, International Commission of Jurists, Assessing Damage, Urging Action, 2009, pp. 81-85, available at https://www.icj.org/wp-content/uploads/2012/04/Report-on-Terrorism-Counter-terrorism-and-Human-Rights-Eminent-Jurists-Panel-on-Terrorism-series-2009.pdf.

[7] Report of the Special Rapporteur on counter-terrorism, Compilation of good practices, *supra*, at para. 47 ("State responsibility may be triggered through the sharing of intelligence that contributes to the commission of grave human rights violations."); *see also* Born et al., Making International Intelligence Cooperation Accountable, *supra*, at p. 42; Eminent Jurists Panel, International Commission of Jurists, Assessing Damage, *supra*, at p. 90.

Conversely, intelligence provided by a foreign partner may have been obtained in violation of international law, including through torture or CIDT. This intelligence may be the product of answers to questions a state has specifically requested be fed to detainees held by its foreign partner. Where such detainees have been or are subject to detention and interrogation under torture or CIDT, the provision of questions can amount to complicity in these unlawful activities. Even where intelligence is received in an unsolicited manner, states may bear responsibility where they know or ought to have known that its foreign partner violated or is violating international law, including by committing torture or CIDT, to produce such intelligence.[8]

2. UK Intelligence Sharing and Serious Human Rights Abuses

The ISC report, "Detainee Mistreatment and Rendition: 2001-2010" ("ISC Report"), documents the repeated willingness of UK officials to share or receive intelligence despite knowledge that a foreign partner was engaging in or likely to engage in torture or CIDT.

With respect to the "awareness of mistreatment", the ISC Report found that:[9]

- The UK government had "a clear warning" that the US government intended to mistreat detainees, which "should have been sufficient to alert them to any subsequent indication that words were being matched by actions."

- UK personnel "witnessed at first hand a detainee being mistreated by others – such that it must have caused alarm and should have led to action" 13 recorded times.

- UK personnel were "told by detainees that they had been mistreated by others" 25 recorded times.

- UK officials were "told by foreign liaison services…about instances of what appears to be detainee mistreatment" 128 recorded times.

With respect specifically to the "sharing of intelligence", the ISC Report found that:

- In the post-9/11 period, UK agencies "shared an unprecedented amount of intelligence with foreign liaison services to facilitate the capture of detainees" but

[8] *See* International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, 2001, Articles 6, 16-18, 41; *see also* Joint Committee on Human Rights, Allegations of UK Complicity in Torture, 23rd Report, 2008-09, paras. 29-35 ("[I]n our view, the following situations would all amount to complicity in torture, for which the State would be responsible…The provision of questions to…a foreign intelligence service to be put to a detainee who has been, is being, or is likely to be tortured…The systematic receipt of information known or thought likely to have been obtained from detainees subjected to torture."); Born et al., Making International Intelligence Cooperation Accountable, *supra*, at pp. 66-69.

[9] Intelligence and Security Committee of Parliament, Detainee Mistreatment and Rendition: 2001-2010, *supra*, at p. 2.

"failed to consider whether it was appropriate to pass intelligence where mistreatment of detainees was known or reasonably suspected."[10]

- UK personnel "continued to supply questions or intelligence to liaison services after they knew or suspected (or, in our view, should have suspected) that a detainee had been or was being mistreated" 232 recorded times.[11]

- UK personnel "received intelligence from liaison services obtained from detainees whom they knew had been mistreated, or…where, in our view, they should have suspected mistreatment" 198 recorded times.[12]

- GCHQ has "held that its part was peripheral…despite the fact that it is by far the largest sharer of material with the US" and "was in fact aware of the risks of large-scale sharing of information with the US but regarded it as neither practical, desirable nor necessary to second guess how that material might be used."[13]

- Defence Intelligence "appears to have failed to understand its potential involvement in mistreatment of detainees through the supply of evidence."[14]

In addition, the ISC Report found with respect to rendition that:

- UK agencies "provided intelligence to enable a rendition operation to take place" in 22 instances.[15]

- "GCHQ's lack of consideration of rendition and attempts to distance itself from such knowledge" is "concerning, given the potential link between its intelligence and US rendition operations."[16]

C. The Scope of the Consolidated Guidance Is Inappropriately Narrow[17]

The scope of the Consolidated Guidance as it pertains to intelligence sharing is inappropriately narrow in two key respects.

First, as IPCO has noted, the Consolidated Guidance only "applies where UK agencies seek intelligence from a person detained by a foreign liaison service, or receives unsolicited intelligence, but not expressly where the UK merely provides intelligence, albeit our understanding is that it is engaged in this situation."[18] The

[10] *Id.* at p. 3.
[11] *Id.* at p. 3.
[12] *Id.* at p. 3.
[13] *Id.* at p. 56.
[14] *Id.* at p. 57.
[15] *Id.* at p. 3.
[16] *Id.* at p. 105.
[17] This section responds to Consultation Question 7: "Is the scope of the Consolidated Guidance appropriate?"
[18] Investigatory Powers Commissioner's Office, Consultation on the Consolidated Guidance, August 2018, p. 10, question 7(c).

Consolidated Guidance should be explicit that it applies also in the circumstances where the UK provides intelligence to foreign partners.

The failure of the Consolidated Guidance to cover these circumstances is notable given that some of the most egregious failures noted by the ISC Report involved instances where the UK provided, rather than received, intelligence. The ISC reported that there were "232 cases recorded where it appears that UK personnel continued to supply questions or intelligence to liaison services after they knew or suspected (or, in our view, should have suspected) that a detainee had been or was being mistreated."[19] The ISC Report also noted that "GCHQ and Defence Intelligence were also potentially complicit in mistreatment, given their extensive sharing of intelligence with partners (in particular the US)."[20] In one example, "during the lead-up to operations in Iraq in 2003, Defence Intelligence provided a list of some 5,000 personnel allegedly associated with the Iraqi Weapons of Mass Destruction programme to forces", which "was available to the US on a shared IT system." Defence Intelligence informed the ISC that it "cannot rule out that some of this information may have been used by the US for detention/rendition".[21]

Alarmingly, both GCHQ and Defence Intelligence failed to understand that their provision of intelligence to foreign partners could implicate them in human rights abuses later committed by those partners. The ISC Report determined that "[e]ven as recently as the beginning of this Inquiry, GCHQ still held its part was peripheral" and despite its awareness "of the risks of large-scale sharing of information with the US…regarded it as neither practical, desirable nor necessary to second guess how that material might be used."[22] It similarly concluded that "Defence Intelligence also appears to have failed to understand its potential involvement in mistreatment of detainees through the supply of intelligence."[23]

Second, the Consolidated Guidance should be explicit that it applies in all circumstances where UK agencies share intelligence, regardless of the nature of that sharing. Modern intelligence sharing can take many forms, ranging from exchanging intelligence analysis to sharing access to "raw" (i.e. unanalysed) information obtained in bulk. Indeed, the ISC Report alludes to this type of sharing, noting that GCHQ "was in fact aware of the risks of large-scale sharing of information with the US" and "is by far the largest sharer of material with the US."[24]

The Consolidated Guidance's approach to the scope of intelligence sharing is unduly narrow. In addition to the fact that it does not address the UK's provision of intelligence at all, it implies that UK agencies may only "receive" intelligence in two relatively narrow forms – solicited or unsolicited. It ignores the reality that UK agencies through various intelligence sharing arrangements have direct and wide-

[19] Intelligence and Security Committee of Parliament, Detainee Mistreatment and Rendition: 2001-2010, *supra*, at p. 3.
[20] *Id.* at para. 116.
[21] *Id.* at para. 119.
[22] *Id.* at p. 56, para. M.
[23] *Id.* at p. 57, para. N.
[24] *Id.* at . 56, para. M.

ranging access to intelligence collected by foreign partners. Just as GCHQ conducts "large-scale sharing of information with the US", the US and other foreign partners conduct equally "large-scale sharing of information" with the UK. When UK agencies access intelligence, just as much as when they explicitly "receive" it, they must consider whether it was obtained through the commission of serious human rights abuses, including torture or CIDT. The Consolidated Guidance should therefore be explicit that it applies whenever UK agencies share intelligence, regardless of the nature of that sharing.

D. The Consolidated Guidance Fails to Provide Sufficient Assistance When Making Relevant Decisions including When Considering the Risk of Torture or CIDT[25]

The Consolidated Guidance provides insufficient assistance to UK agencies when considering the human rights implications of intelligence sharing, including its relationship to torture or CIDT. As noted above, it does not address at all the provision of intelligence to foreign partners, which may contribute to or facilitate serious human rights abuses, including torture or CIDT.

With respect to circumstances where foreign partners provide intelligence to the UK agencies, the Consolidated Guidance's assistance is vague and bare bones. For example, the Consolidated Guidance provides that "[b]efore feeding in questions to or otherwise seeking intelligence from a detainee in the custody of a liaison service, personnel must consider the standards to which the detainee may have been or may be subject."[26] However, it provides nothing further as to how personnel should conduct this assessment, including, for example, the types of information they should draw from, the factors they should consider or the process they should follow, including any reporting requirements. Similar lacunae exist in circumstances where "personnel believe there is a serious risk that a detainee has been or will be subject to unacceptable standards" and "where personnel receive unsolicited intelligence from a liaison service that they know or believe has originated from a detainee."[27]

Privacy International understands that, as acknowledged by the ISC, there exists internal agency guidance, which serves to reinforce the Consolidated Guidance and provide more detailed assistance to UK personnel.[28] We support and reiterate

---

[25] This section responds to Consultation Question 5: "Does the Consolidated Guidance provide sufficient assistance when making relevant decisions including when considering an unmitigated risk or torture or CIDT?"

[26] Consolidated Guidance, *supra*, at para. 23.

[27] *Id.* at paras. 24, 27.

[28] Intelligence and Security Committee, Detainee Mistreatment and Rendition: Current Issues, 28 June 2018, p. 14, available at https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20180628_HC1114_Report_Detainee_Mistreatment_and_Rendition-Current_Issues.pdf?attachauth=ANoY7crOJYAUSh6qQj0Ndbn2W7MIxqwJK6GEum2gOoWAMVFeby1HMZZIMA0GCi87KoEgWXs7ZWyddX2atLrND-BEuZpzfBVY3Jb2uBhKIi_tilfb1X4HoGszIc58e6Mhe_0PIIjm3hf5kOnIFP6mnknMAfNshzEgjBPScI1iKE3eXqxQFjxo7u6p22RhDV6niqPuVigZwNOQvDpUUHqaxuIId0pPtroo9UrrD_8uFaRo8h1vKMNJPlwUXx_LjbWtKS5PM6PCgCiwYJ57GU5O5EVBOcAAF-x0thE0FifpkdSqkfO30nzGYsw%3D&attredirects=0.

Reprieve and Freedom from Torture's recommendation that the agencies must make publicly available all internal agency guidance, which is intended to be used in parallel with the Consolidated Guidance.[29] The publication of such guidance would assist in establishing whether the Government and the agencies provide sufficient assistance to personnel making decisions regarding involvement in torture or CIDT, including in the intelligence sharing context. This recommendation is also consistent with the ISC's recommendation that "the public should be given as much information as possible about the underlying decision-making process in this area" and that "there is more information which could be published about the way officers apply the Guidance."[30]

To the extent that the issues below are not covered by existing internal policy guidance that is made publicly available, Privacy International further recommends the development of written and publicly available policies that:

Outbound Sharing

- Prohibit the sharing of intelligence with foreign partners where there exists a serious risk that such sharing will contribute to or facilitate torture or CIDT.

- Establish due diligence and risk assessment procedures for determining whether there exists a serious risk that sharing intelligence will contribute to or facilitate torture or CIDT.[31]

- Require the attachment of conditions and assurances when sharing intelligence to ensure intelligence is not used in a manner that contributes to or facilitates torture or CIDT.

- Establish a continuing obligation to correct or update intelligence shared with foreign partners as soon as practicable upon discovering errors or concerns regarding its reliability.

- Require reporting to IPCO instances where an agency suspects or becomes aware that intelligence shared with a foreign partner contributed to or facilitated torture or CIDT, including a report on any remedial actions the agency has taken or proposes to take.

---

[29] Reprieve & Freedom from Torture, Reprieve and Freedom from Torture Joint Submission to the Investigatory Powers Commissioner's Consultation on the Consolidated Guidance, October 2018, Recommendation 4.

[30] Intelligence and Security Committee, Detainee Mistreatment and Rendition: Current Issues, *supra*, at p. 100.

[31] Privacy International supports and reiterates Reprieve's recommendation that the Government consider how the Consolidated Guidance and policy on Overseas Security and Justice Assistance Guidance might be combined in order to, *inter alia*, create a single human rights risk assessment framework by which all public bodies must abide. This recommendation contains the caveat that both documents are deeply flawed and any harmonised policy must not replicate those failings. Reprieve & Freedom from Torture, Reprieve and Freedom from Torture Joint Submission to the Investigatory Powers Commissioner's Consultation on the Consolidated Guidance, *supra*, at Recommendation 3.

Inbound Sharing

- Prohibit the use of intelligence where there exists a serious risk that a foreign partner obtained it through torture or CIDT.

- Establish due diligence and risk assessment procedures for determining whether there exists a serious risk that a foreign partner obtained intelligence through torture or CIDT.

- Require an analysis of the provenance, accuracy and verifiability of intelligence shared by a foreign partner.

- Require reporting to IPCO instances where an agency suspects or becomes aware that intelligence shared by a foreign partner was obtained through torture or CIDT, including a report on any remedial actions the agency has taken or proposes to take.

Training

- Require all UK personnel whose responsibilities relate to intelligence sharing, to receive training on, *inter alia*:

    - Relevant domestic and international law, including international human rights law and international humanitarian law;

    - Identifying, reporting and mitigating the risks that sharing intelligence with foreign partners will contribute to or facilitate torture or CIDT;

    - Identifying, reporting and mitigating the risks that agencies will use intelligence obtained by foreign partners through torture or CIDT.

In addition, Privacy International recommends that IPCO:

- Undertake regular investigations into agencies' policies and practices related to intelligence sharing.

- Regularly review and evaluate:

    - Intelligence agencies' compliance with relevant international and domestic law and their own internal policies when sharing intelligence;

    - Intelligence agencies' training programs for staff whose responsibilities relate to intelligence sharing;

    - Instances where an agency suspects or becomes aware that intelligence shared with a foreign partner contributed to or facilitated torture or CIDT, any remedial actions taken by the agencies and whether further remedial action is necessary;

- Instances where an agency suspects or becomes aware that intelligence shared by a foreign partner was obtained through torture or CIDT, any remedial actions taken by the agencies and whether further remedial action is necessary.

- Cooperate with foreign oversight bodies in states with whom intelligence is shared, including establishing procedures for:

  - Informing each other of risks that intelligence sharing may contribute to or facilitate torture or CIDT;

  - Requesting that a foreign oversight body investigate and share unclassified reports relating to intelligence sharing and its contribution to or facilitation of torture or CIDT.

E. The "Assurance Process" in the Consolidated Guidance Is Inadequate[32]

The "assurance process" as it pertains to intelligence sharing in the Consolidated Guidance is similarly inadequate. In general, the Guidance instructs that personnel merely "consider attaching conditions to any information to be passed…and/or obtaining assurances…as to the standards that have been or will be applied" but provides no further assistance.[33] It is unclear, for example, how personnel should determine whether a condition or assurance is appropriate at all and, if so, what types of conditions or assurances might be appropriate for what types of circumstances. It is also unclear what type of reporting or auditing occurs of this process, including to ensure foreign partner compliance with conditions and assurances.

Privacy International therefore recommends the development of written and publicly available policies that:

- Establish due diligence and risk assessment procedures for determining whether a condition or assurance would be an appropriate means of mitigating the risk that intelligence shared with a foreign agency will contribute to or facilitate torture or CIDT.

- Establish audit trails documenting, *inter alia*, intelligence shared, the manner in which it was shared, and any conditions or assurances placed on the intelligence.

- Establish procedures for monitoring adherence to conditions or assurances.

- Establish procedures for addressing breaches of conditions or assurances, which mandate remedial action where a breach has occurred.

[32] This section responds to Consultation Question 6: "Is the "assurance process" in the Consolidated Guidance adequate?"
[33] Consolidated Guidance, *supra*, at para. 23.

- Require reporting to IPCO on:
    - Intelligence shared, the manner in which it was shared, and any conditions or assurances placed on the intelligence;
    - Instances where a foreign partner has breached a condition or assurance, including a report on any remedial actions the agency has taken or proposes to take.
- Require all staff whose responsibilities relate to intelligence sharing to receive training on establishing and maintaining relevant audit trails and reporting obligations to IPCO regarding conditions and assurances.

In addition, Privacy International recommends that IPCO conduct a regular review and evaluation of:

- Agencies' due diligence and risk assessment procedures and practices related to conditions and assurances.
- Conditions and assurances attached to intelligence shared with foreign partners as well as agencies' procedures for monitoring adherence to and addressing breaches of conditions and assurances.
- Breaches of conditions and assurances by foreign partners, any remedial actions taken by the agencies and whether further remedial action is necessary.
- Agencies' training programs for staff relating to conditions and assurances.

F. Establish a Notification Requirement

Privacy International recommends the establishment of a notification requirement, which applies, at minimum, to instances where:

- An agency has provided intelligence about an individual to a foreign partner and the partner has used that information, including to contribute to or facilitate serious human rights violations such as torture or CIDT;
- An agency has examined intelligence about an individual provided by a foreign partner.

As discussed above, intelligence sharing may contribute to or facilitate serious human rights abuses. Fundamentally speaking, however, intelligence sharing – in and of itself – constitutes an interference with human rights, including the rights to privacy and freedom of expression. It must therefore be subject to relevant protections under international human rights law.

International human rights authorities have recognised notification as an important procedural safeguard in protecting against abusive interference with the right to

privacy. This recognition is founded on the linkage between notification and access to "[e]ffective remedies for violations of privacy." Because "remedies must be known and accessible to anyone with an arguable claim that their rights have been violated…[n]otice (that either a general surveillance regime or specific surveillance measures are in place)…thus become[s a] critical issue[ ] in determining access to effective remedy."[34] The European Court of Human Rights has also tied notification "to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers." It has observed: "There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively".[35] For that reason, the ECtHR has counselled that "as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned."[36]

Notification is arguably even more critical in circumstances where intelligence sharing may have contributed to or facilitated torture or CIDT, particularly because of its relationship to the right to access an effective remedy. The UN Committee Against Torture has indicated that the right to redress under article 14 of the UN Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment requires a State party to "promptly initiate a process to ensure that victims obtain redress, even in the absence of a complaint, when there are reasonable grounds to believe that torture or ill-treatment has taken place".[37] It has further stated that "under no circumstances may arguments of national security be used to deny redress for victims".[38] Currently, victims of torture or CIDT have few avenues to determine whether those abuses were facilitated by other countries, including through the sharing of intelligence. Without notification, they may never know and therefore may subsequently never be able to exercise their right to remedy for such complicity.

---

[34] Office of the U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37, 30 June 2014, para. 40.
[35] Zakharov v. Russia, European Court of Human Rights, App. No. 47143/06, 4 Dec. 2015, para. 234.
[36] Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, European Court of Human Rights, 28 June 2007, para. 90; see also Weber and Saravia, supra, at para. 135 ("The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively."). Privacy International notes its criticism of the "error reporting" requirement in the Investigatory Powers Act and associated Codes of Practice, which are insufficient to fulfil the notification requirement. *See* Privacy International, Privacy International's Submission to the Home Office Investigator Powers Act 2016 Consultation on the Draft Codes of Practice, 6 April 2017, para. 15, available at https://privacyinternational.org/sites/default/files/2017-12/Privacy%20International%20-%20Response%20to%20Consultation%20on%20IPA%20Codes%20of%20Practice%20-%20April%202017.pdf.
[37] Committee Against Torture, General Comment No. 3: Implementation of Article 14 by States parties," U.N. Doc. No. CAT/C/GC/3, para. 27.
[38] *Id.* at para. 42.

ANNEX: RECOMMENDATIONS

Scope of the Consolidated Guidance

- Expand the scope of the Consolidated Guidance to address circumstances where the UK provides intelligence to foreign partners and all circumstances where UK agencies share intelligence, regardless of the nature of sharing.

Considering the Risk of Torture or CIDT

- Make publicly available all internal agency guidance intended to be used in parallel with the Consolidated Guidance.

- Develop written and publicly available policies that:

  Outbound Sharing

  - Prohibit the sharing of intelligence with foreign partners where there exists a serious risk that such sharing will contribute to or facilitate torture or CIDT;

  - Establish due diligence and risk assessment procedures for determining whether there exists a serious risk that sharing intelligence will contribute to or facilitate torture or CIDT;

  - Require the attachment of conditions and assurances when sharing intelligence to ensure intelligence is not used in a manner that contributes to or facilitates torture or CIDT;

  - Establish a continuing obligation to correct or update intelligence shared with foreign partners as soon as practicable upon discovering errors or concerns regarding its reliability;

  - Require reporting to IPCO instances where an agency suspects or becomes aware that intelligence shared with a foreign partner contributed to or facilitated torture or CIDT, including a report on any remedial actions the agency has taken or proposes to take;

  Inbound Sharing

  - Prohibit the use of intelligence where there exists a serious risk that a foreign partner obtained it through torture or CIDT;

  - Establish due diligence and risk assessment procedures for determining whether there exists a serious risk that a foreign partner obtained intelligence through torture or CIDT;

- Require an analysis of the provenance, accuracy and verifiability of intelligence shared by a foreign partner;

- Require reporting to IPCO instances where an agency suspects or becomes aware that intelligence shared by a foreign partner was obtained through torture or CIDT, including a report on any remedial actions the agency has taken or proposes to take;

Training

- Require all UK personnel whose responsibilities relate to intelligence sharing, to receive training on, *inter alia*:

  - Relevant domestic and international law, including international human rights law and international humanitarian law;

  - Identifying, reporting and mitigating the risks that sharing intelligence with foreign partners will contribute to or facilitate torture or CIDT;

  - Identifying, reporting and mitigating the risks that agencies will use intelligence obtained by foreign partners through torture or CIDT.

- Require IPCO to:

  - Undertake regular investigations into agencies' policies and practices related to intelligence sharing;

  - Regularly review and evaluate:

    - Intelligence agencies' compliance with relevant international and domestic law and their own internal policies when sharing intelligence;

    - Intelligence agencies' training programs for staff whose responsibilities relate to intelligence sharing;

    - Instances where an agency suspects or becomes aware that intelligence shared with a foreign partner contributed to or facilitated torture or CIDT, any remedial actions taken by the agencies and whether further remedial action is necessary;

    - Instances where an agency suspects or becomes aware that intelligence shared by a foreign partner was obtained through torture or CIDT, any remedial actions taken by the agencies and whether further remedial action is necessary;

- Cooperate with foreign oversight bodies in states with whom intelligence is shared, including establishing procedures for:
    - Informing each other of risks that intelligence sharing may contribute to or facilitate torture or CIDT;
    - Requesting that a foreign oversight body investigate and share unclassified reports relating to intelligence sharing and its contribution to or facilitation of torture or CIDT.

The "Assurance Process"

- Develop written and publicly available policies that:
    - Establish due diligence and risk assessment procedures for determining whether a condition or assurance would be an appropriate means of mitigating the risk that intelligence shared with a foreign agency will contribute to or facilitate torture or CIDT;
    - Establish audit trails documenting, *inter alia*, intelligence shared, the manner in which it was shared, and any conditions or assurances placed on the intelligence;
    - Establish procedures for monitoring adherence to conditions or assurances;
    - Establish procedures for addressing breaches of conditions or assurances, which mandate remedial action where a breach has occurred;
    - Require reporting to IPCO on:
        - Intelligence shared, the manner in which it was shared, and any conditions or assurances placed on the intelligence;
        - Instances where a foreign partner has breached a condition or assurance, including a report on any remedial actions the agency has taken or proposes to take;
    - Require all staff whose responsibilities relate to intelligence sharing to receive training on establishing and maintaining relevant audit trails and reporting obligations to IPCO regarding conditions and assurances.
- Require IPCO to conduct a regular review and evaluation of:
    - Agencies' due diligence and risk assessment procedures and practices related to conditions and assurances;

- Conditions and assurances attached to intelligence shared with foreign partners as well as agencies' procedures for monitoring adherence to and addressing breaches of conditions and assurances;

- Breaches of conditions and assurances by foreign partners, any remedial actions taken by the agencies and whether further remedial action is necessary;

- Agencies' training programs for staff relating to conditions and assurances.

Notification

- Establish a notification requirement, which applies, at minimum, to instances where:

    - An agency has provided intelligence about an individual to a foreign partner and the partner has used that information, including to contribute to or facilitate serious human rights violations such as torture or CIDT;

    - An agency has examined intelligence about an individual provided by a foreign partner.