Intervention

Big Brother Watch and Others v. the United Kingdom
Application No. 58170/13

Introduction and Summary

Access Now is honoured to submit this intervention in *Big Brother Watch and Others v. the United Kingdom* (Application no. 58170/13). Access Now is a global civil society organization dedicated to defending and extending the digital rights of users at risk.[1] Through representation in 10 countries around the world – including in the European Union - Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and universality and wields an action-focused global community of nearly half a million users from more than 185 countries. Access Now also operates a 24/7 digital security helpline that provides real-time direct technical assistance to users around the world. Access Now is non-partisan, not-for-profit, and not affiliated with any country, corporation, or religion.

The issues the Court is being asked to rule upon in *Big Brother Watch and Others v. the United Kingdom* implicate human rights to privacy and free expression for internet users around the world. The internet empowers individuals and enables citizens to take part in struggles for justice, participate in society, and realize human rights around the globe. But government surveillance has turned the internet into a tool of repression, granting unprecedented abilities to invade privacy and quell political dissent and the spread of non-conforming ideas. Human rights must be preserved equally on the internet as they have traditionally been implemented in the physical world.

This intervention provides an overview of issues that will further color the Court's consideration of the vital questions for consideration in this case. Specifically, Access Now provides context on international human rights standards implicated by the UK's mass surveillance programs, the full scope of government surveillance, and cross-jurisdictional data transfers. The mass surveillance at issue here fails to comport with the International Covenant on Civil and Political Rights (ICCPR) and the International Principles on the Application for Human Rights to Communications Surveillance; the UK has made no showing that such surveillance is strictly necessary or proportionate, particularly in light of the large range of personal information that is collected through other surveillance programs and transferred from other governments. This transfer, in particular, is troubling because it conducts an "end run" around even the limited legal protections for human rights provided for by law.

[1] Access Now, "Our Mission," www.accessnow.org/about-us.

Intervention

I. Internationally accepted standards for human rights prohibit the mass surveillance at issue in this case

1. The threat to human rights by surveillance activities is tangible. "Privacy is a fundamental human right, and is central to the maintenance of democratic societies. It is essential to human dignity and it reinforces other rights, such as freedom of expression and information, and freedom of association, and is recognized under international human rights law. Communications surveillance interferes with the right to privacy among a number of other human rights."[2] The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, has further noted "[e]ven a narrow, non-transparent, undocumented, executive use of surveillance may have a chilling effect [on freedom of expression] without careful and public documentation of its use, and known checks and balances to prevent its misuse."[3]
2. In respect to those rights, the United Kingdom has signed and ratified the International Covenant on Civil and Political Rights.[4] The ICCPR is a multilateral treaty adopted by the United Nations General Assembly on 16 December 1966. One hundred and sixty-eight nations have signed on to the ICCPR.[5] The ICCPR provides, inter alia, for the right to privacy: "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[6] The ICCPR also protects the freedom of expression, including "freedom to seek, receive[,] and impart information and ideas of all kinds, regardless of frontiers."[7]
3. Based on well-established human rights law and policy including, partially, on the ICCPR,[8] the International Principles on the Application of Human Rights to Communications Surveillance (hereinafter, "the Principles") provide a legally-grounded explanation of human rights standards and a detailed description of the human rights obligations that are a

[2] International Principles on the Application of Human Rights to Communications Surveillance (hereinafter, "N&P") (May 2014), https://necessaryandproportionate.org. *See also, inter alia,* Universal Declaration of Human Rights, art. 12; UN Convention on Migrant Workers, art. 14, UN Convention of the Protection of the Child, art. 16.
[3] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/23/40 (17 Apr. 2013) (by Frank La Rue), *available at* www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.
[4] International Covenant on Civil and Political Rights (ICCPR), 23 Mar. 1976, 999 U.N.T.S. 171, *available at* www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
[5] Only 29 states are not party to the ICCPR.
[6] ICCPR art. 17.
[7] ICCPR art. 19(2).
[8] International Principles on the Application of Human Rights to Communications Surveillance, "Principle by Principle Explanation" (May 2014) (citing Art. 8-11 ECHR, Art. 12, 17, 18, 19, 21, and 22 ICCPR, and Art. 11, 12, 13, 15, and 16 IACHR), https://en.necessaryandproportionate.org/LegalAnalysis/principle-principle-explanation.

requisite precedent for communications surveillance.[9] The Principles have been endorsed by more than 400 different organizations around the world. The Principles were cited extensively in the United Nations Office of the High Commissioner for Human Rights report on "The Right to Privacy in the Digital Age,"[10] as well as in the report of U.S. President Obama's Review Group on Intelligence and Communications Technologies.[11] Some of the most prominent technology companies in the world, including Microsoft, Google, and Yahoo, have publicly supported a separate framework that largely echoes the Principles,[12] and both Sweden and the United States have used the Principles as a basis for human rights frameworks adopted internally.[13]

4. Any restrictions on rights to privacy and expression are subject to a "permissible limitations" test.[14] Pursuant to UN Human Rights Committee General Comment Number 34, such "permissible" restrictions must be provided by law; strictly serve a legitimate aim (respect of the rights and reputation of others, protection of national security or of public order, or of public morals or health); and meet a high standard of legality, proportionality, and necessity.[15] The Principles provide a further framework for the protection of human rights, requiring that "Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights."[16]
5. The United Nations General Assembly has resolved, "surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory and that any interference with the right to privacy must not be arbitrary or unlawful..."[17] In fact, "[i]nadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the rights to privacy in communications and, consequently, also threaten the protection of the right to

[9] N&P, *supra* fn 2.
[10] Report of the Office of the United Nations High Commissioner for Human Rights, "The right to privacy in the digital age," U.N. Doc. A/HRC/27/37 (30 June 2014), www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.
[11] Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World" (12 Dec. 2013), www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
[12] Reform Government Surveillance, "The Principles," www.reformgovernmentsurveillance.com (last visited 4 Feb. 2016).
[13] *See*, Carly Nyst, "Sweden's Foreign Minister declares his support for principles to protect privacy in the face of surveillance," Privacy International (21 Oct. 2013), www.privacyinternational.org/node/135; Drew Mitnick, "US endorses principles it's not living up to," Access Now (1 Apr. 2014), www.accessnow.org/us-endorses-principles-it-is-not-living-up-to.
[14] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/23/40 ¶¶ 28-29 (17 Apr. 2013) (by Frank La Rue).
[15] *Id*.
[16] N&P, *supra* fn 2.
[17] The right to privacy in the digital age, G.A. Res. 69/166, U.N. Doc. A/RES/69/166 (10 Feb. 2015).

freedom of opinion and expression."[18] Activities that infringe upon the right to privacy must be "the least intrusive instrument among those which might achieve the desired result."[19] Secret surveillance is to be even more closely scrutinised to determine if it meets this objective.[20] By extension, a legal explainer to the Principles explains, "proportionality is particularly important in the context of mass surveillance, which is based on the indiscriminate collection and retention of communications and metadata without any form of targeting or reasonable suspicion."[21]

6. Mass surveillance is inherently at odds with human rights standards and with international law as provided for in the ICCPR and the Principles.[22] As explained by the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, "the adoption of mass surveillance technology undoubtedly impinges on the very essence of [the right to privacy]" and "the very existence of mass surveillance programmes constitutes a potentially disproportionate interference with the right to privacy."[23] The report goes on to explain, "An assessment of the proportionality of [mass surveillance programmes] must...take into account of the collateral damage to collective privacy rights," concluding, "such programmes can be compatible with article 17 of the [ICCPR] *only if* relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people in any part of the world."[24]
7. The programs at issue in this case, specifically Tempora, do not comport with human rights standards, specifically the rights recognized in the ICCPR. The UK has failed to describe how its laws provide notice that such a program could exist, let alone a clear or precise legal framework for its commission.
8. The introductory text to the UK's draft investigatory powers bill, released in 2015, provides sparse rationale for mass surveillance, namely that "[a]ccess to large volumes of data

[18] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/23/40 (17 Apr. 2013) (by Frank La Rue).
[19] General Comment No. 27, 1999, CCPR/C/21/Rev.1/Add.9, reproduced in Human Rights Instruments, Volume I, Compilation of General Comments and General Recommendations adopted by Human Rights Treaty Bodies, HRI/GEN/1/Rev.9 (Vol. I) 2008, pp. 223 – 227, ¶¶ 11 – 16. ("Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instruments amongst those, which might achieve the desired result; and they must be proportionate to the interest to be protected.").
[20] Klass v. Germany, Eur. Ct. H.R. ¶ 42 (1978).
[21] Necessary and Proportionate, Background and Supporting International Legal Analysis for the International Principles on the Application of Human Rights to Communications Surveillance, https://en.necessaryandproportionate.org/LegalAnalysis (last visited February 8, 2016).
[22] *See* Privacy International, Electronic Frontier Foundation, Access Now, APC, ARTICLE 19, Human Rights Watch et al., "OHCHR consultation in connection with General Assembly Resolution 68/167 'The right to privacy in the digital age'" (1 Apr. 2014), *available at* www.eff.org/files/2014/04/17/ngo_submission_final_31.03.14.pdf.
[23] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, U.N. Doc. A/69/397 ¶ 18 (23 Sept. 2014) (by Ben Emmerson) (citing A/HRC/27/37).
[24] *Id.*, citing A/HRC/27/37 (emphasis added).

enables the security and intelligence agencies to piece together communications and other data and identify patterns of behaviour." The UK's explainer does not provide adequate justification for the infringement of the human rights of billions of internet users.[25] Neither in the years that this case has remained pending nor independently has any explanation been provided as to why less intrusive programmes could not address legitimate aims of the UK. Accordingly, the UK's surveillance programs fail to meet the high burden that international law and policy has established for the commission of mass surveillance and are strictly at odds with human rights standards.

II. The invasiveness and interference with human rights of surveillance programs are compounded when analyzed holistically with other authorities and capabilities

9. The collection and compilation of multiple types of protected information from different sources creates new risks to human rights. Specific data collection programs which may appear to meet human rights standards for necessity and proportionality when considered independently will fail when viewed in relation to the entirety of a nation's surveillance activities. A single data stream that may seem innocuous can contribute to a highly invasive portrait of an individual, akin to the tessera of a mosaic, when combined with other data streams.
10. In the commercial space we see this with data mining companies - members of industry which exist to create massive profiles on individuals using both public and private data that they derive from multiple sources.[26] Even sparse data mining profiles without reference to an individual can often be re-identified easily.[27] In one high-profile case, reporters were able to identify several anonymous users based solely on their AOL search history.[28] Facebook is able to use digital data to predict romantic relationships.[29] So-called "big data" is often used in data mining, data sets that are so large that it is "inconceivable."[30] Large data sets have been easier to collect with the movement of communications to the internet. "As our offline activities and records move online—our shopping, our consumption of news and entertainment, our financial and legal and medical records and transactions, and

[25] Internet Live Stats, "United Kingdom Internet Users," www.internetlivestats.com/internet-users/united-kingdom (last visited 4 Feb. 2016).
[26] Joel Stein, "Data Mining: How Companies Now Know Everything About You," Time (10 Mar. 2011), http://content.time.com/time/magazine/article/0,9171,2058205,00.html.
[27] Adam Tanner, "Harvard Professor Re-Identifies Anonymous Volunteers in DNA Study," Forbes (25 Apr. 2013), www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study.
[28] Michael Barbaro & Tom Zeller Jr., "A Farce Is Exposed for AOL Searcher No. 4417749," The New York Times (9 Aug. 2006), www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all.
[29] Ellis Hamburger, "Facebook knows when you fall in love… and when you'll break up," The Verge (13 Feb. 2014), www.theverge.com/2014/2/13/5408968/facebook-relationships-singles-data.
[30] SAS Institute, "Big Data: What it is and why it matters," www.sas.com/en_us/insights/big-data/what-is-big-data.html (last visited 5 Feb 2016).

an ever-increasing number of personal and business communications of every kind, even the most sensitive—the depth and breadth of this massive data set continues to expand."[31]

11. The development of machine learning has increased the invasiveness of big data sets and data mining. Machine learning is "the branch of computer science that studies systems that can draw inferences from collections of data, generally by means of mathematical algorithms."[32] The use of machine learning has an impact on human rights. "Machine learning algorithms are able to deduce information— including information that has no obvious linkage to the input data—that may otherwise have remained private due to the natural limitations of manual and human-driven investigation."[33]
12. The United Kingdom has developed specific programs in order to track through the large databases of information that are collected through GCHQ's disparate surveillance programs. For example, GCHQ uses a system called 'Mutant Broth' to take a single piece of information about a user such as an IP address, username, or email address to build out a profile of that user. Any selector can be used as the starting point to create an invasive profile of an individual that can include details such as passwords, types of browsers, physical location, and even "pattern of life analysis."[34] XKEYSCORE, developed by the U.S. National Security Agency, is another such search tool that allows GCHQ and other Five Eyes nations to query databases shared by intelligence agencies.[35]
13. This case involves specific surveillance programs. However, we have learned since the revelation of these programs about several others. On the surface, and individual surveillance program may seem proportionate; however, when combined with other data streams these programs create a highly invasive portrait of an individual. In order to consider whether an individual program satisfies human rights obligations, it must be considered in the totality of surveillance programs and powers. Below, Access Now lays out some of the other UK surveillance programs that have been revealed:

[31] Kevin S. Bankston, "Big Data RFI - OTI comments on the White House's Big Data Initiative," New America Open Technology Institute (4 Apr. 2014), https://static.newamerica.org/attachments/7727-oti-to-white-house-internet-surveillance-is-the-biggest-big-data-issue-of-all-2/OTI_Big_Data_Comments.075a75494a084081824f903223d78c24.pdf.

[32] Steven M. Bellovin et al., "When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning," New York University Journal of Law and Liberty (2014), http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2379&context=fac_pubs.

[33] *Id*.

[34] Ryan Gallagher, "Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities," The Intercept (25 Sept. 2015), https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities.

[35] Other known search tools that combine databases include Samuel Pepys, Social Anthropoid, and Blazing Saddles. GCWiki, "Blazing Saddles Overview," hosted by The Intercept at: https://theintercept.com/document/2015/09/25/blazing-saddles-tools.

a. Black Hole - Collects all internet metadata traversing fiber optic networks and stores them in a database. According to leaked documents dated 2009, Black Hole can store more than 1.1 trillion metadata records.[36]
b. Karma Police - Connects individuals to the websites they visit, creating either "(a) a web browsing profile for every visible user on the internet, or (b) a user profile for every visible website on the internet."[37] This program was used to identify, track, and build a profile of the browsing habits over 200,000 internet radio listeners in 185 countries, focusing on individuals that listened to stations broadcasting sermons from the Quran.[38]
c. Optic Nerve - Collects still images of Yahoo! webcam chats in bulk.[39]
d. Memory Hole - Collects search engine queries and connects searches with specific users.[40]
e. Infinite Monkeys - Collects information and posts from online message boards.[41]
f. Marbled Gecko - Collects information from searches on Google Maps and Google Earth to determine what individuals have been looking at.[42]
g. Badass - GCHQ has the ability to monitor mobile phone users through "supercookie" or "zombie" tracking headers installed by telecommunications providers into unencrypted HTTP traffic for advertising purposes.[43]

14. UK-based multinational telecommunications company Vodafone notes that the Intelligence Services Act 1994 ("ISA") allows the Secretary of State to "issue a warrant in respect of any property so specified or in respect of wireless telegraphy." The company remarks, "There is the possibility that this power is broad enough to permit government direct access to Vodafone's network by the Security Services in some instances."[44]
15. Governments that enjoy direct access to telecom networks can bypass due process safeguards and interfere with private communications without the knowledge of third parties, whether companies or their targeted customers. For these reasons, Vodafone and

[36] GCHQ, "QFDs and BLACHOLE Technology behind GCHQ/INOC" (Mar. 2009), hosted by The Intercept at: https://theintercept.com/document/2015/09/25/qfd-blackhole-technology-behind-inoc.
[37] GCHQ, "PullThrough Steering Group Meeting #16" (29 Feb. 2008), hosted by The Intercept at: https://theintercept.com/document/2015/09/25/pull-steering-group-minutes.
[38] Gallagher, "Profiled," *supra* note 33.
[39] Spencer Ackerman & James Ball, "optic Nerve: millions of Yahoo webcam images intercepted by GCHQ," The Guardian (28 Feb. 2014), www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.
[40] GCHQ, *supra* note 35.
[41] *Id*.
[42] *Id.*
[43] *See*, GCHQ, "Mobile apps doubleheader: BADASS Angry Birds" hosted by Der Spiegel at: www.spiegel.de/media/media-35670.pdf (last visited 4 Feb. 2016); Ryan Gallagher, "Operation Auroragold: How the NSA Hacks Cellphone Networks Worldwide," The Intercept, (4 Dec. 2014), https://theintercept.com/2014/12/04/nsa-auroragold-hack-cellphones.
[44] Vodafone, Law Enforcement Disclosure Report, Legal Annexe (Feb. 2015) www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/law_enforcement_disclosure_report_2015_update.pdf.

other telecom companies recommend amending any legislation granting such unlimited, covert powers.[45]

16. These surveillance programs and powers, and others that are yet unknown, contribute to the question of the necessity of the surveillance programs at issue. As noted above, activities that infringe upon the right to privacy must be "the least intrusive instrument among those which *might achieve the desired result*."[46] The relevant relationship, therefore, is not between any program and the specific information it seeks to collect, but rather to its contribution to the UK's legitimate aim that gives the surveillance purpose. Whereas individual programs may seem necessary to that legitimate aim in a vacuum, when considered in relation to the totality of data that is being collected for the same purpose, the same arguments collapse.

III. The agreements between the U.S. and the UK bypass human rights protections, including those in publicly-available Mutual Legal Assistance Treaties (MLATs)

17. In addition to surveillance programs run by GCHQ, evidence also points to a longstanding and significant transfer of surveillance information between UK and American intelligence services. Formal communications intelligence sharing between the United Kingdom and United States grew out of the 1946 British-U.S. Communication Intelligence Agreement under which intelligence authorities in each nation agreed to the "unrestricted exchange" of the products of various intelligence operations including "collection of traffic" relating to foreign intelligence.[47] In subsequent years, Canada, Australia, and New Zealand were included in this treaty, thus forming the Five Eyes intelligence sharing network.[48]
18. As a result of the cooperation between the Five Eyes nations, information collected by GCHQ may be transferred to foreign governments, and the UK receives similar information in return, bypassing British and EU privacy safeguards. The relationship is said to be so strong intelligence officials often cannot determine which government acquired or accessed intelligence.[49] The U.S. has operated intelligence programs from bases within the UK that may have been used to to conduct surveillance of British individuals.[50] Thus, while

[45] Vodafone, Law Enforcement Disclosure Report (June 2014), www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf.
[46] General Comment No. 27, *supra* note 19 (emphasis added).
[47] British - U.S. Communication Intelligence Agreement (5 Mar. 1946), *available at* www.nsa.gov/public_info/_files/ukusa/agreement_outline_5mar46.pdf.
[48] Amendment No. 4 To The Appendices To The UKUSA Agreement (Third Edition) (10 May 1955), *available at* www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf.
[49] Carly Nyst & Anna Crowe, "Unmasking the Five Eyes' global surveillance practices," Global Information Society Watch (2014), www.giswatch.org/sites/default/files/unmasking_the_five_eyes.pdf.
[50] Chris Blackhurst, "US spy base 'taps UK phones for MI5,'" The Independent (21 Sept. 1996), www.independent.co.uk/news/uk/home-news/us-spy-base-taps-uk-phones-for-mi5-1364399.html.

governments remain fiercely protective of their jurisdiction and competency over national security questions, they often collaborate with allies when expedient, and the internet has only strengthened traditional ties.

19. In February 2015 the Investigatory Powers Tribunal found that "the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities pursuant to Prism and/or… Upstream" had operated in violation of Articles 8 or 10 ECHR due to the secret principles governing rules governing the American Surveillance programmes.[51]
20. Mutual legal assistance treaties (MLATs) enable the exchange of information for criminal matters, including for investigation and prosecution of offenses, between State Parties. MLATs create formal process within which the central authority of one State Party may issue requests to the central authority of another State Party, which can access and transfer information. The MLAT system has been designed to respect the human rights of individuals and the procedural protections for those human rights afforded in different jurisdictions. The United Kingdom is Party to least fourteen MLATs.[52]
21. The MLAT between the UK and US ("Treaty") governs all criminal matters.[53] It requires requests be presented to the proper judicial or administrative authorities of the country receiving the request and permits the Party receiving the request to refuse compliance if a search or seizure could not otherwise be conducted under domestic law.[54] Further, the Treaty generally limits the use and further dissemination of information transferred under a request.[55] Such requirements provide some legal protections to individuals, including non-UK persons, whose data is subject to transfer despite the lack of normal, domestic investigatory procedure.
22. Notably, the Treaty permits the Party receiving the request to refuse compliance if a search or seizure could not otherwise be conducted under domestic law.[56] As described above, information transferred between the US and UK pursuant to intelligence agreements allows both countries to conduct an "end run" around their own legal requirements by receiving surveillance information that the government would have been legally unable to collect in the first instance.
23. MLATs provide greater transparency than signals intelligence programs. The Treaty, along with other MLATs to which the UK is a Party, is public. The UK Home Office also makes

[51] Liberty v. Secretary of State for Foreign and Commonwealth Affairs, [2014], UKIPT rib 13-77-H, *available at* www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf.
[52] Access Now, "Mutual Legal Assistance Treaties Country Profile: United Kingdom," https://mlat.info/country-profile/united-kingdom (last visited 4 Feb. 2016).
[53] Treaty Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Mutual Legal Assistance in Criminal Matters, 6 Jan. 1994, Treaty Doc. 104-2, *available at* www.state.gov/documents/organization/176269.pdf.
[54] *Id*. art. 5(2), 14(1).
[55] *Id*. art. 7(2).
[56] *Id*. art. 5(2), 14(1).

publicly available Guidelines with instructions on making MLAT requests and companies release aggregate data on received requests.[57] The transparency provides individuals necessary insight into how their data may be transferred between jurisdictions, as required under human rights law. Such insight is not available when data is transferred between the U.S. and U.K through secretive intelligence programs.

24. As noted above, participation of UK intelligence agencies in intelligence sharing agreements, such as the Five Eyes, is prohibited by international human rights standards. Some information obtained through mass surveillance programs could instead be obtained through the MLAT process or a similar process that is public and designed to respect human rights.

25. Because the UK government has used intelligence cooperation to bypass safeguards of the MLAT system, it has failed to meet the necessity requirement of communications surveillance. Necessity requires that when there are multiple means of achieving a legitimate aim, the means used are "the least likely to infringe upon human rights."[58] The MLAT system is less likely than intelligence sharing to infringe upon the human rights to privacy and freedom of expression.

Conclusion

26. In light of the above, we submit to the Court that, both in international law and broadly-accepted standards, that the UK's mass surveillance programs do not respect human rights protections. The programs are not necessary and most definitely not proportionate. The UK has failed to provide any notice of the types of surveillance that it is conducting, what the legal framework is for the commission of that surveillance, or how it justifies the invasion of the rights of internet users around the world. We urge the Court to hold as such and to strike down the UK's interpretation of its human rights obligations in favor of one that will respect its international obligations.

Amie Stepanovich, U.S. Policy Manager
Peter Micek, Global Policy and Legal Counsel
Drew Mitnick, Policy Counsel
Keir Lamont, Privacy Fellow
Access Now
9 February 2016

[57] International Criminality Unit, Home Office, "Requests for Mutal Legal Assistance in Criminal Matters: Guidelines for Authorities Outside of the United Kingdom" (2015), www.gov.uk/government/uploads/system/uploads/attachment_data/file/415038/MLA_Guidelines_2015.pdf; *see, e.g.*, Mutual Legal Assistance Treaties, Frequently Asked Questions, https://mlat.info/faq (last visited Feb. 8, 2016).
[58] N&P, *supra* fn 2.