KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENT TO THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD REGARDING REFORMS TO SURVEILLANCE CONDUCTED PURSUANT TO EXECUTIVE ORDER 12333

June 16

The Center for Democracy & Technology[1] submits the following comments detailing the organization's views and recommendations regarding the conduct and oversight of Intelligence Community activities undertaken pursuant to Executive Order 12333 ("EO 12333") in response to the request of the Privacy and Civil Liberties Oversight Board ("PCLOB") for public comment as the Board continues to review the extent and exercise of Executive power pursuant to EO 12333. These comments are intended to aid the PCLOB in its research on the topic by examining human rights and examples of best practices in the oversight of secret-surveillance programs, and concise academic discussions of the restrictions that apply to surveillance, including transborder surveillance, under international law.

I. Best practices and compliance with international human rights law in the oversight of secret surveillance programs.

The discussion below concerns best practices and the general requirements of human rights law where the oversight of secret surveillance programs is concerned.

The oversight of secret surveillance has been the subject of extensive commentary by United Nations institutions and experts, as well as detailed findings by the European Court of Human Rights ("ECtHR").[2] While some of these assessments have been intended to provide a general framework for determining whether oversight schemes are consistent with the major human rights treaties, others—particularly the ECtHR's judgments—have described or cited certain elements of the oversight systems of specific countries as examples of good practices. Some of the UN bodies' findings or recommendations explicitly concern the US' oversight system, various aspects of which have been singled out for praise or criticism.

These sources suggest that the following elements are critical to oversight schemes in order to guarantee full respect for individual rights:

i. A mixed, multilayered review system that includes judicial, parliamentary/congressional, executive, internal, and independent bodies

[1] The Center for Democracy & Technology is a non-profit public interest organization dedicated to keeping the Internet open, innovative, and free. Among our priorities is preserving the balance between security and freedom.

[2] At the time of writing, the ECtHR appears to remain the only international human-rights court to have considered issues related to the oversight of secret-surveillance activities.

ii. A requirement for *ex ante* approval as well as *ex post facto* review of surveillance measures by entities other than the ones conducting the surveillance (preferably judicial bodies);
iii. Comprehensive supervision of all aspects and stages of surveillance activities;
iv. Adequate resources, expertise, and powers, including the ability to view (and compel the production of) classified materials and witness testimony;
v. The flexibility and power to investigate matters *sua sponte*;
vi. A requirement that the authorities conducting the surveillance, including intelligence agencies, cooperate with the oversight mechanism(s);
vii. As much transparency as possible where oversight activities and findings are concerned; and
viii. The ability of individuals to hold authorities directly accountable for surveillance-related abuses before courts, tribunals, or other bodies bearing strong indicia of democratic legitimacy and legal expertise.[3]

While the discussion below includes accountability mechanisms before which individuals may bring complaints about abusive surveillance practices, it does not address the individual right to a remedy for violations of fundamental rights. CDT may address the right to a remedy—an essential component of the international legal framework—in a future submission.

A. The UN General Assembly and the Human Rights Council.

The UN General Assembly has recently adopted two resolutions specifically addressing the issue of the oversight of secret-surveillance regimes. In November 2013, following the Snowden disclosures, it called upon all States to "establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and collection of personal data."[4] In December 2014, it reiterated this call in terms that were identical save for the insertion of language demanding that these domestic oversight mechanisms be "adequately resourced and impartial" as well as "judicial, administrative, and/or parliamentary" in nature.[5]

In April 2014, the Committee on Civil and Political Rights, which is tasked under the International Covenant on Civil and Political Rights with monitoring signatories' compliance with the Covenant, issued a set of concluding observations following an examination of the US' human-rights practices. The Committee expressed a variety of concerns about NSA surveillance "both within and outside the United States" before noting its trepidation that "the current oversight system of the activities of the NSA fails to effectively protect the rights of the persons affected."[6] The body went on to issue a formal recommendation urging the US to:

[3] For a similar set of elements, see Council of Europe, *Democratic and effective oversight of national security services* (May 2015), available at https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2758654&SecMode=1&DocId=2275638&Usage=2.

[4] U.N. Doc. A/RES/68/167 (Dec. 18, 2013), ¶ 4(d).

[5] U.N. Doc. A/RES/69/166 (Dec. 18, 2014), ¶ 4(d).

[6] U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014), ¶ 22 *et seq.*

> [r]eform the current oversight system of surveillance activities to ensure its effectiveness, including by providing for judicial involvement in the authorization or monitoring of surveillance measures, and considering the establishment of strong and independent oversight mandates with a view to preventing abuses[.][7]

B. Reports of UN Special Rapporteurs and the Office of the High Commissioner for Human Rights.

Since 2009, several UN Special Rapporteurs have made significant recommendations concerning the oversight of secret surveillance. Most pertinently, in 2010 the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, published a set of "good practices" based upon international law as well as the "existing and emerging" conduct of States across the globe. Citing specific State legislation and policies, Scheinin identified the following "good practices" in respect of oversight:

> **Practice 6.** Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialized oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution that is independent of both the intelligence services and the executive. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices.
>
> …
>
> **Practice 7.** Oversight institutions have the power, resources and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses, as well as obtaining documentation and other evidence.
>
> …
>
> **Practice 8.** Oversight institutions take all necessary measures to protect classified information and personal data to which they have access during the course of their work. Penalties are provided for the breach of these requirements by members of oversight institutions.[8]

Elaborating on Practice 7, Scheinin noted that "[a] number of States have taken steps to reinforce the investigation competences of oversight institutions by criminalizing any failure to cooperate with them" and emphasized the importance of adequate resources and

---

[7] *Ibid.* at ¶ 22(c).

[8] U.N. Doc. A/HRC/14/46 (May 17, 2010), ¶¶ 13-15; *cf.* Hans Born and Ian Leigh, *Democratic Accountability of Intelligence Services*, 37 STOCKHOLM INT'L PEACE RESEARCH INST. Y.B. 193 (2006), *available at* http://www.sipri.org/yearbook/2007/files/SIPRIYB0705.pdf.

staffing.[9] In 2009, Scheinin had praised the United States for some of its then-recent oversight reforms (particularly the expansion of judicial review).[10]

Other Special Rapporteurs have issued recommendations that largely echo Scheinin's. For example, Scheinin's successor Ben Emmerson has emphasized the need for "strong independent oversight bodies that are adequately resourced and mandated" to conduct both *ex ante* and *ex post facto* review of secret surveillance.[11]

In an influential June 2014 report on the right to privacy in the digital age, the Office of the UN High Commissioner for Human Rights ("OHCHR") asserted that "[i]nternal safeguards without independent, external monitoring … have proven ineffective against unlawful or arbitrary surveillance methods," and that "the involvement of all branches of government in the oversight of surveillance programmes, as well as of an independent civilian oversight agency, is essential to ensure the effective protection of the law."[12] According to the OHCHR, judicial review is generally desirable but "should not be viewed as a panacea"; the body warns that in several unnamed countries, "judicial warranting or review of the digital surveillance activities of intelligence and/or law enforcement agencies have amounted effectively to an exercise in rubber-stamping."[13] This risk is one reason that "mixed models of administrative, judicial and parliamentary oversight" may be preferable.[14]

The OHCHR also suggests that states should consider allowing relevant third parties, such as Internet service providers, to "participate in the authorization of surveillance measures affecting their interests or … challenge existing measures."[15]

C. The European Court of Human Rights.

The ECtHR has examined the oversight schemes of a number of Council of Europe Member States, and its Grand Chamber has stated that '*interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure*'.[16] The Court has also emphasized in the past that '*in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge*'.[17]

Notwithstanding this general preference for judicial oversight *per se*, the Court has previously found that some oversight systems complied with the Convention where they included a possibility of judicial review and/or bore other exceptionally strong indicia of independence, competence, impartiality, and democratic legitimacy. These decisions predate the Snowden revelations by years or even decades, and CDT has suggested in a

---

[9] *Ibid.* at ¶ 14.

[10] U.N. Doc. A/HRC/13/37 (Dec. 28, 2009),¶ 52.

[11] U.N. Doc. A/69/397 (Sept. 23, 2014), ¶¶ 47-48. For additional recommendations by the then-Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, see U.N. Doc. A/HRC/23/40 (Apr. 17, 2013), ¶¶ 86, 93.

[12] U.N. Doc. A/HRC/27/37 (June 30, 2014), ¶ 37.

[13] *Ibid.* at ¶ 38.

[14] *Ibid.*

[15] *Ibid.*

[16] *Rotaru v. Romania* (Grand Chamber, 2000), ¶ 59 (citing *Klass and Others v. Germany* (Plenary, 1978), ¶ 55).

[17] *Klass and Others*, *supra* n. 14, ¶ 56.

recent submission to the Court that the increasing omnipresence and intrusiveness of secret surveillance methods means that judicial oversight is now strictly required in order to ensure full respect for the individual rights found in the Convention.[18] Previously, however, the Court has approved the oversight regime in **Germany** on at least two occasions, observing that:

- Authorities conducting surveillance were required to comply with "strict conditions and procedures" set out in statutory laws adopted by Parliament;
- Those laws "define[d] precisely, and thereby limit[ed], the purposes for which" the surveillance could be conducted;
- The laws provided that surveillance could only be authorized pursuant to "an administrative procedure designed to ensure that measures [were] not ordered haphazardly, irregularly or without due and proper consideration";
- The authorization was only valid for three months, at which point it terminated unless a renewal application was made;
- The implementation of the surveillance measures was subject to "initial control … carried out by an official qualified for judicial office" who "examine[d] the information obtained" before transmitting it to the entities that had sought it (while destroying any intelligence that could not be used in accordance with the relevant legislation);
- Although judicial recourse for complaints about the ordering or execution of surveillance measures was not directly available, "subsequent control or review" was provided by "two bodies appointed by the people's elected representatives" in Parliament;
- These bodies were "independent of the authorities carrying out the surveillance, and [were] vested with sufficient powers and competence to exercise an effective and continuous control";
- The bodies were politically "balanced" and included members of the opposition party;
- The authorities responsible for conducting the surveillance were required to report at least once every six months to one of the two oversight bodies—a Parliamentary Board consisting of five current parliamentarians;
- In practice, the authorities conducting the surveillance sought *ex ante* approval from the other oversight body (the G 10 Commission), which would determine whether the measures would be lawful and necessary; and
- At least in certain exceptional circumstances, an individual or other entity who had brought a complaint before one of the two oversight bodies could ultimately have recourse to the Constitutional Court.[19]

The Court approved the German system again in a 2006 decision.[20] It has also expressed approval of systems in which persons who believe they may have been victims of unlawful surveillance may seek recourse from an independent body comprised of current or former judges and/or experienced lawyers (e.g., the Investigatory Powers Tribunal of the **United Kingdom**), and emphasized that independent review must occur *ex ante* as well as *ex post*.[21]

In addition to these aspects of the German and UK systems, the Court has also upheld a number of components of the oversight system in **Sweden** as complying with the

[18] Center for Democracy & Technology, Third-Party Intervention, *Szabó and Vissy v. Hungary*, App. No. 37138/14 (on file with CDT).

[19] *Klass and Others*, *supra* n. 14, ¶¶ 43-60.

[20] *Weber and Saravia v. Germany* (2006) (dec.).

[21] *Kennedy v. United Kingdom* (2010), ¶¶ 166-170; *Telegraaf Media Nederland Landelijke Media B.V. and Others v. Netherlands* (2012), ¶¶ 98-102.

Convention. These included the ability of the Parliamentary Ombudsman, a four-person body appointed by Parliament, to conduct investigations, receive individual complaints, recommend amendments to legislation, monitor judicial and administrative proceedings to ensure adherence to fundamental rights, and refer instances of abuse for prosecution or disciplinary proceedings. The Swedish oversight system also included (at least at the time of the relevant judgment) a National Police Board that included six current or former Members of Parliament, including members of the opposition, and a multi-party Parliamentary Standing Committee on Justice, which "scrutinised the expenses of the security police, its organisation activities."[22]

Notably, although the Court has approved other aspects of the UK's oversight system, it has found in a 2008 judgment that *ex ante* authorization in the form of broad interception warrants issued by the Home Office was not consistent with the Convention, as these warrants conferred "virtually unfettered" discretion on the executive in respect of the capture of communications.[23]

D. Conclusion.

In order to adhere to best practices and human-rights obligations, oversight mechanisms for secret surveillance must operate comprehensively at both the approval and *ex post* review stages of the surveillance, and must also bear strong indicia of independence and authority. Additionally, these mechanisms should demonstrate transparency and expertise, and should form part of a multi-body system in which supervision is undertaken by a variety of credible entities. Finally, the subjects of the surveillance should have a meaningful ability to challenge abusive surveillance practices directly before courts or bodies with similar levels of authority, professionalism, and efficacy. Elements of the oversight systems of several countries demonstrate that this type of oversight can be undertaken in a manner that safeguards national security while ensuring full respect for fundamental rights.

II. Recommended readings on restrictions that apply to surveillance, including transborder surveillance, under international law.

- G. Alex Sinha, NSA Surveillance Since 9/11 and the Human Right to Privacy, 59 LOY. L. REV. 861 (2013), *available at* http://ssrn.com/abstract=2327806.
- Elizabeth Sepper, Democracy, Human Rights, and Intelligence Sharing, 46 TEX. INT'L L. J. 151 (2010), *available at* http://ssrn.com/abstract=1742091.
- Simon Chesterman, The Spy Who Came In from the Cold War: Intelligence and International Law, 27 MICH. J. INT'L L. 1071 (2006), *available at* http://ssrn.com/abstract=969551.
- Raphael Bitton, The Legitimacy of Spying Among Nations, 29 AM. U. INT'L L. REV. 1009 (2014), *available at* http://ssrn.com/abstract=2323021.

III. Conclusion.

We appreciate the opportunity to present our views to PCLOB and hope these resources and analysis will aid the Board in its examination of Executive Order 12333, and development of recommendations to support privacy, separation of powers, and international

[22] *Leander v. Sweden* (1987).

[23] *Liberty and Others v. United Kingdom* (2008), ¶ 64.

human rights. If you have any questions regarding our comments, please contact Greg Nojeim, Director of the Freedom, Security and Technology Project, gnojeim@cdt.org, Sarah St. Vincent, Human Rights and Surveillance Legal Fellow sstvincent@cdt.org, or Jake Laperruque, Privacy, Surveillance, and Security Fellow, jlaperruque@cdt.org.

Sincerely,

Greg Nojeim
Director of the Freedom, Surveillance, and Security Project

Sarah St.Vincent
Human Rights and Surveillance Legal Fellow

Jake Laperruque
Privacy, Security and Surveillance Fellow