KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE
www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY
1634 Eye Street, NW
Suite 1100
Washington, DC 20006

Intervention

Szabó and Vissy v. Hungary
Application No. 37138/14

Introduction and summary

1. The Center for Democracy & Technology ('CDT') is honoured to submit this intervention in the case of *Szabó and Vissy v. Hungary* (Application No. 37138/14). CDT is a non-governmental organisation that works to advance human rights online, and is committed to finding forward-looking and technically sound solutions to the most pressing challenges facing users of electronic communications technologies. Since its founding 20 years ago, CDT has played a leading role in shaping policies, practices and norms that empower individuals to use these technologies effectively as speakers, entrepreneurs and active citizens.

2. CDT's intervention addresses states' obligations under Articles 8 and 13 of the European Convention on Human Rights ('the Convention') in the context of secret-surveillance programmes conducted for purposes of national security. Although the Hungarian legislation at issue permits different types of surveillance, this intervention focuses on the surveillance of electronic data, including data transmitted by or stored on personal computing devices and mobile telephones.

3. **Summary of the intervention:** This intervention provides an overview of the advances in states' electronic surveillance abilities due to the development of highly sophisticated and intrusive techniques, as well as individuals' increasing use of computers and mobile telephones for a range of tasks. CDT details, for example, how states can now obtain an array of private data by physically seizing and searching an individual's mobile phone or computer, intercepting data as it flows through the cables that constitute the Internet 'backbone', capturing text messages or location information sent from mobile phones, and even remotely activating individuals' electronic devices in order to take photographs and videos of them without their knowledge. CDT concludes that in the light of these technological advances, the procedural obligations of Article 8 now require judicial oversight of Contracting

Parties' secret-surveillance programmes. The intervention sets out the specific criteria that CDT believes Article 8 imposes where an exceptional situation genuinely renders judicial oversight of a secret-surveillance programme impossible; in doing so, however, the organisation emphasises that ultimate control of such a process must still be judicial in order to ensure full compliance with the Convention. CDT further urges the Court to give strong consideration to the possibility that, in the light of states' modern surveillance capabilities, Article 8 requires that the initial authorisation of secret surveillance measures (in addition to overall supervision of their implementation) be judicial.

The intervention also sets out CDT's view of the requirements of Article 13, read together with Article 8, in this context. In particular, an effective remedy for Article 8 violations arising from secret-surveillance programmes requires that the remedial body must conduct an impartial and effective investigation of any credible complaints, and must also furnish effective redress for any confirmed violation. Such redress includes (where appropriate) ordering the discontinuance of any ongoing abusive surveillance as well as the destruction or sequestration of private data.

I. Article 8 and the oversight of secret surveillance conducted for national-security purposes

4. Section (a) below describes the scale and intrusiveness of the surveillance capabilities that are now available to states. Section (b) then sets out the response we believe these advanced capabilities demand from Article 8 of the Convention.

a. Surveillance capabilities of modern states

5. Following the June 2013 disclosures concerning state secret-surveillance practices by former US National Security Agency contractor Edward Snowden, reports in the global media have revealed the ubiquitous and extremely sophisticated nature of surveillance capabilities that are now available to states. As the Office of the High Commissioner for Human Rights has noted in a recent report, "[t]he State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before."[1]

[1] Office of the UN High Commissioner for Human Rights, *The right to privacy in the digital age*, UN Doc. A/HRC/27/37 (30 June 2014), ¶ 2 (hereinafter 'OHCHR Report').

6. Individuals' increasing integration of communications and computing devices into their daily lives has facilitated these state surveillance practices.[2] Even in the absence of highly developed remote surveillance programmes of the kind described below, a state can obtain a great deal of private data simply by physically seizing and searching a personal electronic device. As the US Supreme Court has recently remarked, today's mobile phones—and, we would add, personal computers—'*could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.*'[3] In other words, the amount of private data a state can obtain by directly examining the contents of a computer or mobile phone is vast.

7. Today, states also have the ability to intercept communications data remotely: for example, they can capture such data as it flows through the cables that constitute the Internet 'backbone' or as it moves between servers of Internet or telephone companies.[4] A state can also intercept large quantities of text messages and mine them for data (e.g. contacts and location information) that allow the state to build a very detailed picture of an individual's activities and relationships.[5] Moreover, states can collect the routing information that mobile phones routinely send to nearby communications towers, and use this information to determine where an individual is, where he or she has travelled and with which other mobile-phone-carrying persons he or she may have interacted (such as family, friends and professional associates).[6] States also have the ability to intercept and record, in a wholesale fashion, the content of very large quantities of mobile phone conversations.[7]

8. In addition to these indiscriminate forms of surveillance, states are also able to conduct very intrusive forms of surveillance that are targeted at specific individuals. For example, they have the ability to install equipment on the Internet backbone that

---

[2] *Ibid.* at ¶¶ 1-2.
[3] *Riley v. California*, US Supreme Court (2014), p. 17 of slip opinion.
[4] James Ball, 'NSA's Prism surveillance program: how it works and what it can do', *The Guardian*, 8 June 2013; Philip Dorling, 'Edward Snowden reveals tapping of major Australia-New Zealand undersea telecommunications cable', *The Sydney Morning Herald*, 15 September 2014.
[5] James Ball, 'NSA collects millions of text messages daily in "untargeted" global sweep', *The Guardian*, 16 January 2014.
[6] Barton Gellman and Ashkan Soltani, 'NSA tracking cellphone locations worldwide, Snowden documents show', *The Washington Post*, 4 December 2013.
[7] Ryan Devereaux et al., 'Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas', *The Intercept*, 19 May 2014.

screens passing data for certain 'triggers', then automatically hacks into the personal device that sent the data and plants malicious software there (such as key-logger tools, which record every key typed on the device).[8] States are also able to activate the cameras of personal communications devices remotely in order to take videos or photographs of individuals in secret.[9]

9. Both individually and in the aggregate, these surveillance capabilities allow the state to build detailed pictures of the most intimate aspects of individuals' lives.[10]

10. Reportedly, at least 10 Council of Europe Member States are actively engaging in these surveillance practices, and/or are participating in intelligence-sharing arrangements with other states that conduct these activities.[11] It is possible that other Council of Europe Member States, such as Hungary, may be involved in these or similar programmes or data-sharing arrangements even though their participation has not yet been reported; further, it is possible that even those Member States that do not yet engage in such activities may do so in future. Additionally, we observe that states' surveillance and data-sharing capabilities are likely to continue to increase as the relevant technology evolves.

b. Implications for the oversight of secret surveillance programmes

11. It is our view that, in the light of the technological advances described above and the serious interferences with the right to respect for private life and correspondence of which states are capable, Article 8 now requires judicial oversight over all secret-surveillance programmes conducted for national-security purposes. This is the only appropriate response under the Convention to the comprehensive and extremely intrusive surveillance methods that are available to states—including, potentially, Hungary—in the modern era.

---

[8] See, e.g., James Ball et al., 'NSA and GCHQ target Tor network that protects anonymity of web users', *The Guardian*, 4 October 2013.
[9] Ian Burrell, 'Nosey Smurf, Gumfish and Foggy Bottom: The snooping tools that may have got GCHQ in hot water', *The Independent*, 13 May 2014.
[10] Cf. *Digital Rights Ireland* (Judgment) [2014] EUECJ C-293/12, ¶¶ 26-27.
[11] Julian Borger, 'GCHQ and European spy agencies worked together on mass surveillance', *The Guardian*, 1 November 2013; Ewen MacAskill and James Ball, 'Portrait of the NSA: No detail too small in quest for total surveillance', *The Guardian*, 2 November 2013. Contracting States that these sources report as taking part in intelligence-sharing arrangements include Belgium, Denmark, France, Germany, Italy, the Netherlands, Norway, Spain, Sweden and the United Kingdom.

12. As a foundational matter, we recall that public authorities' clandestine interception, use, sharing, or storage of personal data all constitute an interference with the right to respect for private life and correspondence, meaning that these forms of surveillance must pursue a legitimate aim, be necessary in a democratic society and be performed in accordance with the law in order to avoid a breach of Article 8 of the Convention.[12] We further recall that where the data itself is concerned, e-mail and telephone correspondence, as well as personal information pertaining to Internet usage, all fall within the ambit of Article 8.[13]

13. Additionally, we recall the Grand Chamber's finding in *Rotaru v. Romania* that any secret-surveillance programme operated by a Contracting Party must include '*adequate and effective safeguards against abuse, since a system of secret surveillance designed to protect national security entails a risk of undermining or even destroying democracy on the ground of defending it*'.[14] The Grand Chamber further confirmed 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*'.[15]

14. We further recall the Grand Chamber's repeated expression of the view that the Court must interpret the Convention dynamically: '*the Convention is a living instrument which must be interpreted in the light of present-day conditions*'.[16] As Judge Garlicki has observed, in this sense '*the role of [the] Court is not very different from the role of national Constitutional Courts, whose mandate is not only to defend constitutional provisions on human rights, but also to develop them*.'[17] In this context, we note that the Court has set out the procedural requirements of Article 8 in response to various emerging issues in Europe, such as child abductions and forced evictions.[18]

---

[12] *E.g.*, *Weber and Saravia v. Germany* (Decision, 2006), ¶ 79; *Amann v. Switzerland* (Grand Chamber, 2000), ¶ 69.
[13] *Copland v. United Kingdom* (2007), ¶¶ 43-44; *Liberty and others v. United Kingdom* (2008), ¶ 56.
[14] *Rotaru v. Romania* (Grand Chamber, 2000), ¶ 59 (citing *Klass and others v. Germany* (Plenary, 1978), ¶¶ 49-50).
[15] *Ibid.* (citing *Klass and others*, *supra* n. 14, ¶ 55).
[16] *E.g.*, *Hirsi Jamaa v. Italy* (Grand Chamber, 2012), ¶ 175; *Soering v. United Kingdom* (Plenary, 1989), ¶ 102.
[17] *Öcalan v. Turkey* (Grand Chamber, 2005), partly concurring opinion of Judge Garlicki, ¶ 4.
[18] *X v. Latvia* (Grand Chamber, 2009), ¶¶ 106-108; *Winterstein et autres c. France* (2013), ¶ 148.

15. We are aware that in two cases concerning the oversight programmes adopted by Germany in respect of its secret-surveillance programmes (*Klass and others v. Germany* and *Weber and Saravia v. Germany*), the Court found that a non-judicial supervisory regime characterised by certain exceptionally strong indicia of independence, authority, competence and democratic validity was sufficient to ensure compliance with Article 8.[19] Even in the most significant of these two cases, however, the Court stated 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*'.[20]

16. Furthermore, we observe that the Court issued its judgment in *Klass and others* in 1978, and its decision in *Weber and Saravia* in 2006. The former of these two opinions predates the widespread adoption of mobile telephones and other Internet-capable personal computing devices by many years. Meanwhile, the latter—while significantly more recent—predates June 2013's groundbreaking disclosures of today's secret-surveillance practices by seven years.[21]

17. It is thus our conclusion, in view of the increasing potential of secret surveillance programmes for abuse as well as the fact that '*judicial control [over surveillance programmes] affords the best guarantees of independence, impartiality and a proper procedure*', that the Court should determine that Article 8 now requires judicial oversight over all secret-surveillance programs in the national-security context.

18. In the rare circumstance where a Contracting Party faces an exceptional situation genuinely requiring surveillance measures without immediate judicial supervision, we believe Article 8 imposes a set of universally-applicable criteria for determining whether a non-judicial oversight process is sufficiently independent, authoritative, competent and democratically valid to be able to provide '*adequate and effective safeguards against abuse*' of individuals' Article 8 rights.[22]

---

[19] *Klass and others*, *supra* n. 14, ¶ 56; *Weber and Saravia*, *supra* n. 12, ¶¶ 116-117.
[20] *Klass and others*, *supra* n. 14, ¶ 56.
[21] *See* Glenn Greenwald, 'NSA collecting phone records of millions of Verizon customers daily', *The Guardian*, 5 June 2013.
[22] *Rotaru*, *supra* n. 14, ¶ 59.

19. In line with the Court's case-law and other relevant authorities, we believe the following specific criteria are required in order for a non-judicial surveillance oversight process to ensure strict respect for Article 8 rights:

- The members of the supervisory mechanism have access to classified materials, witness testimony and any other evidence necessary to allow the mechanism to assess whether '*the reasons adduced by the national authorities to justify [the surveillance measures] are relevant and sufficient*' to ensure that the measures comply with Article 8 as well as domestic law[23];

- The supervisory mechanism as an institution, and its individual members, are fully '*independent of the authorities carrying out the surveillance*'[24];

- The mechanism as whole, and its individual members, possess the necessary legal and substantive expertise to ensure that the surveillance programmes are not causing, or creating an undue risk of, abuse;

- The mechanism is '*vested with sufficient powers and competence to exercise an effective and continuous control*' over the surveillance programmes[25];

- The mechanism's composition and procedures bear strong indicia of democratic legitimacy[26];

- The mechanism authorises the exercise of secret surveillance powers on an individualised basis[27];

- The mechanism may only authorise (or renew) the exercise of secret surveillance powers for a reasonable, finite period, and may only do so upon a showing that the surveillance (or the continuation thereof) meets Article 8's necessity and legality requirements[28]; and

- The mechanism has the ability to refer instances of abuse for investigation and/or prosecution.[29]

20. We reiterate our view, based on the analysis in this Section, that even where the immediate oversight of a surveillance measures is non-judicial due to exceptional circumstances, judicial control must still be available '*in the last resort*'.[30]

---

[23] *S. and Marper v. United Kingdom* (Grand Chamber, 2008, ¶ 101). *See also* UN Human Rights Council, 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 (17 May 2010), ¶ 14 (hereinafter "Compilation of good practices"); OHCHR Report, *supra* n. 1, ¶ 41.
[24] *Klass and others*, *supra* n. 14, ¶ 56.
[25] *Ibid.*
[26] *Ibid.*
[27] *Cf.* OHCHR report, *supra* n. 1, ¶ 25 ('Mass or "bulk" surveillance programmes may … be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime').
[28] *Klass and others*, *supra* n. 14, ¶ 52; *Weber and Saravia*, *supra* n. 12, ¶ 98.
[29] *See Leander v. Sweden* (1987), ¶¶ 38, 65.

21. Where the initial authorisation of surveillance measures is concerned, we invite the Court to conclude that the same Article 8 considerations that necessitate overall judicial control over secret-surveillance programmes also require that surveillance measures be approved by a judicial authority at the outset, except where an exceptional situation genuinely precludes the application of this safeguard.

II. Article 13 and the right to an effective remedy for human-rights violations arising from secret-surveillance programmes

22. In analysing the necessary elements of an effective remedy for violations of Article 8 rights that occur in the course of secret-surveillance programmes conducted for purposes of national security, we recall that an applicant must have access to an effective remedial procedure for such violations, even if his or her chances of success in obtaining the remedy are not certain.[31]

23. We acknowledge the Grand Chamber's assertion in *Rotaru* that '*where secret surveillance is concerned, objective supervisory machinery may be sufficient*' to meet the requirement for a remedy whilst the surveillance measures themselves remain secret.[32] However, we observe that in a more recent case, the Court has stated that even where a secret-surveillance measure remains in effect, a Contracting Party may nevertheless be able to provide a '*limited remedy*' for privacy violations: '*for instance, one where the proceedings are secret and where no reasons are given, and the persons concerned are not apprised whether they have in fact been monitored*'.[33] We note that the Court found in the latter case that Bulgaria had violated Article 13 by making access to a remedy for surveillance-related violations impossible in practice, except where the violation had led to a prosecution or where the complainant had received leaked information confirming that he or she had been monitored.[34]

---

[30] *Rotaru*, *supra* n. 14, ¶ 59; *see also* UN Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression and Special Rapporteur for freedom of expression of the Inter-American Commission on Human Rights, *Joint Declaration on surveillance programs and their impact on freedom of expression* (2013), ¶ 9 ('The collection of [correspondence and personal] information [through surveillance] shall be monitored by an independent oversight body and governed by sufficient due process guarantees *and judicial oversight*, within the limitations permissible in a democratic society' (emphasis added)).
[31] *E.g.*, *Segerstedt-Wiberg and others v. Sweden* (2006), ¶ 117; *see also* OHCHR Report, *supra* n. 1, ¶ 40.
[32] *Rotaru*, *supra* n. 14, ¶ 69; *see also Segerstedt-Wiberg and others*, *supra* n. 31, ¶ 117.
[33] *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (2007), ¶ 100.
[34] *Ibid.* at ¶¶ 100-103.

24. Additionally, we observe that there is a substantial body of international law and practice that strongly discourages impunity for human-rights violations, particularly those that are severe and/or widespread.[35] The Grand Chamber has expressed concern about both impunity and the appearance thereof, and (in the context of an alleged violation of the procedural arm of Article 3 of the Convention) has concurred with the Committee of Ministers of the Council of Europe that states must fight impunity '*as a matter of justice for the victims, as a deterrent to prevent new violations, and to uphold the rule of law and public trust*' in systems of accountability and redress.[36]

25. Taken together, these developments lead us to conclude that a Contracting Party cannot comply with Article 13 in the context of secret surveillance in the absence of (at minimum) fully-functioning and effective '*objective supervisory machinery*', and furthermore that even where such machinery exists, the Contracting Party must provide an individual who suspects that she or he has suffered an Article 8 violation with a meaningfully available avenue of obtaining effective redress.

26. It is our view that in order to ensure the availability of an effective remedy, the Contracting Party must mandate that the remedial body is *obligated* to conduct an impartial and effective investigation of any credible complaints.[37] Further, the remedial body must be *obligated* to furnish effective redress if it concludes that a secret-surveillance practice (either in law or as applied) is not compatible with Article 8 of the Convention.[38] We observe in particular that a remedial body will only be able to conduct an impartial and effective investigation if it has the ability to order the production of evidence and witness testimony, including evidence and testimony whose content is classified.[39] Any decision by the remedial body to decline to award redress should be susceptible to challenge before a judicial body.[40]

---

[35] *See, e.g.*, Guidelines of the Committee of Ministers of the Council of Europe on eradicating impunity for serious human rights violations (hereinafter "Guidelines on eradicating impunity"); Updated Principles for the protection and promotion of human rights through action to combat impunity, U.N. Doc. E/CN.4/2005/102/Add.1 (2005).
[36] *El-Masri v. "The Former Yugoslav Republic of Macedonia"* (Grand Chamber, 2012), ¶ 192 (quoting Guidelines on eradicating impunity, *supra* n. 35, Section I, ¶ 3).
[37] *See Leander*, *supra* n. 29, ¶ 81; *Segerstedt-Wiberg and others*, *supra* n. 31, ¶ 118; Guidelines on eradicating impunity, *supra* n. 35, Section V; Human Rights Committee, General Comment 31: Nature of the General Legal Obligation on States Parties to the Covenant, ¶ 15, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004) ; OHCHR Report, *supra* n. 1, ¶ 41.
[38] *See* General Comment 31, *supra* n. 37, ¶ 16; OHCHR Report, *supra* n. 1, ¶ 39.
[39] *See* Compilation of good practices, *supra* n. 23, ¶ 17; OHCHR Report, *supra* n. 1, ¶ 41.
[40] *See* Guidelines on eradicating impunity, *supra* n. 35, Section V.5.

27. We accept that in the context of secret surveillance conducted for national-security purposes, the remedial body may require a certain degree of flexibility in determining the specific type of redress that is most appropriate. Nevertheless, we observe that in order to provide an effective remedy at the individual level and ensure future compliance with Article 8, the remedial body must—at minimum—have the ability to order the discontinuance of any ongoing abusive surveillance as well as the destruction or (where the Article 8 violation arises primary from data-sharing) sequestration of private data.[41] The remedial body must have the legal and practical ability to enforce these or any other orders for redress.[42]

Conclusion

28. For the reasons explained above, we submit that the Court should find, in light of today's state surveillance capabilities, that Article 8 now requires judicial oversight over all secret-surveillance programs conducted for purposes of national security. Regarding those exceptional cases where judicial oversight is impossible, we urge the Court to provide clear guidance to Contracting Parties and applicants by adopting a set of specific criteria for determining whether a non-judicial oversight process is sufficient to prevent the abuse of Article 8 rights (although we maintain that Article 8 still requires judicial control in the last resort). Finally, we conclude that anyone within the jurisdiction of a Contracting Party who has a credible claim to have been the victim of an Article 8 violation arising from a secret national-security surveillance programme must have access to a remedy that is effective, in the sense that the remedial body is (i) obligated to conduct an investigation of the complaint, and (ii) both empowered and obligated to furnish effective redress for the violation. Where a violation has occurred, this redress must include, at minimum, the ability to order the discontinuance of any ongoing abusive surveillance as well as the destruction or sequestration of private data.

Sarah St.Vincent
Center for Democracy & Technology
23 September 2014

[41] *Segerstedt-Wiberg and others*, *supra* n. 31, ¶¶ 120-122; *see also* OHCHR Report, *supra* n. 1, ¶ 41.
[42] *Segerstedt-Wiberg and others*, *supra* n. 31, ¶ 120; *Silver and others v. United Kingdom* (1983), ¶ 115; *see also* OHCHR Report, *supra* n. 1, ¶ 39.