PRIVACY INTERNATIONAL

Privacy International's submission in advance of the consideration of the seventh periodic report of Poland, Human Rights Committee, 118th, 17 October – 04 November 2016

September 2016

1. Introduction

This report underlines the on-going concerns of Privacy International with the unfettered surveillance and interception powers of the Polish intelligence and law enforcement agencies, in particular as they are reflected in the 15 January 2016 Amendments to the Police Act and Certain Other Acts (2016 Amendments.)

In its List of Issues Prior to Reporting (LoIPR), which was adopted by the Human Rights Committee at its 111th session, the Committee requested the Republic of Poland to "provide information on legislation governing electronic surveillance, including phone, email and fax communications, and on legal safeguards against unwarranted government access to private communications as well as their respect in practice".[1]

In its State Party Report the Polish Government responded to the Committee's request by detailing the far more curtailed powers of the Prosecutor, under the Code of Penal Procedure (CPP), to obtain certain evidence for the purposes of a pending proceeding or in the prevention of a future crime ("Trial Wiretapping").[2]

However, "Secret Surveillance"[3] under Article 19 of the amended Police Act and Trial Wiretapping under Article 237 of the CPP form part of two different legal regimes.[4] As the European Commission for Democracy through Law (the Venice Commission) elaborated, "secret surveillance often *precedes* the opening of a criminal case, providing justification to initiate it."[5] The powers of the prosecutor under the CPP would thus only be triggered upon the launching of such criminal investigation, but Polish investigative bodies may launch secret surveillance operations even before the opening of a criminal case.

The Polish Government's replies provide no information concerning the secret surveillance powers of Polish authorities under different legislation besides the CPP. This report will focus on the 2016 amendments, and whether they are in compliance with Poland's international obligations under the Covenant, particularly as they relate to Article 17.

2. The Amendments to the Police Act and Certain Other Acts of 15 January 2016

On 30 July 2014 the Polish Trybunał Konstytucyjny (Constitutional Tribunal) pronounced as unconstitutional a number of provisions which granted Polish law enforcement, security, and intelligence agencies with powers of secret

---

[1] Human Rights Committee, List of issues prior to submission of the seventh periodic report of Poland, U.N. Doc. CCPR/C/Pol/PQR/7, adopted by the committee at its 111th Session, para. 23 (7-25 July 2014).

[2] Human Rights Committee, State Party Report of the Republic of Poland for its Seventh Periodic Review, U.N. Doc. CCPR/C/POL/7, paras. 167-172 (received on 26 October 2015, distributed on 8 February 2016); *See Also*, Code of Criminal Procedure, Article 237 (6 June 1997).

[3] While the Venice Commission uses the term "Secret Surveillance", the Act itself refers only to "Zarządzenie kontroli operacyjnej" (managing Operational Control). For the sake of consistency and clarity we will use the Venice Commission's terminology throughout this report.

[4] European Commission for Democracy Through Law (Venice Commission), Opinion on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts, Opinion No. 839/2016, CDL-AD(2016)012, adopted by the Venice Commission at its 107th Plenary Session, para. 13 (10-11 June 2016) [hereinafter: Venice Commission Report].

[5] *Id*.

surveillance.[6] By doing so the Constitutional Tribunal reaffirmed the fundamental nature of the human right to privacy as enshrined under Article 47 of the Polish Constitution.[7]

The Tribunal granted the Polish legislature 18 months from the publication of the judgment (i.e. until 7 February 2016) before the unconstitutional provisions become ineffective. On 15 January 2016, the Sejm (Poland's Lower House) adopted the Amendments Act and on 29 January 2015 the Senate approved the act. On 3 February 2016, the Polish President signed the Act which became law on 7 February 2016.[8] The amendments did not change substantively the secret surveillance powers of Polish security agencies, but rather introduced certain safeguards and oversight measures. On 18 February 2016 Adam Bodnar, the Polish Commissioner for Human Rights, submitted an application to the Constitutional Tribunal challenging the constitutionality of the 2016 Amendments Act.[9] The application is pending review.

Articles 19 and 20c of the 2016 Amendments Act

The Police Act establishes two legal regimes of intelligence collection during the "preliminary investigation" stage. The first, under Article 19, concerns the collection and analysis of the contents of telephone conversations, emails, texts, and postal correspondence, as well as images, videos, and audio files (the "Secret Surveillance" program),[10] whereas the latter, under Article 20c, concerns the collection and analysis of telecommunications information data (the Metadata program). As explained by the Venice Commission, the latter program may include such information as: "information about phone calls placed or received, numbers dialled, duration of calls, geographical location of mobile devices at a given moment, web-sites visited, log-ins, personal settings, addresses of e-mail correspondence, etc."[11] Each of the two programs follows different legal procedures.

Secret Surveillance, under Article 19, may be ordered for the purposes of preventing or investigating a closed list of crimes. Such surveillance may be performed with the prior authorisation of a district court. However, in cases of "the utmost urgency," the authorization of a prosecutor may suffice to start surveillance. If a court's authorisation is then not granted within five days, surveillance will be suspended and all data collected must be destroyed. Any operation of secret surveillance must be logged and registered.

---

[6] These agencies include the Central Anti-Corruption Bureau (Centralne Biuro Antykorupcyjne), the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrzego), the Border Guard (Straż Graniczna), the Military Counter-Intelligence Service (Służba Kontrwywiadu Wojskowego), the Military Police (Żandarmeria Wojskowa), the Treasury Control (Kontrola Skarbowa) and the Customs Service (Służba Celna), and the Police (Policja).

[7] Trybunał Konstytucyjny (Constitutional Tribunal), Judgment, Ref. No. K 23/11, Doc. No. 80/7/A/2014, Official English Translation, para. 1.12 (30 July 2014) [hereinafter: 2014 CT Judgment] ("Although not absolute, the constitutional right to the protection of privacy is of a special character in the system of constitutional rights and freedoms... this stems from the fact that the said value is deeply rooted in the dignity of the person... Taking the above into account, obtaining information on the private life of individuals by [public authorities], especially when this is done in secret, must be limited to necessary situations, [permitted] in a democratic state ruled by law, only for the protection of constitutionally recognised values and in accordance with the principle of proportionality. Conditions for [collection] and processing [of] data by public authorities must be regulated by statute in a way that is most transparent and which excludes any arbitrariness...").

[8] For further reading on the legislative history surrounding the amendments see Helsinki Foundation for Human Rights, Comments on the Amendment to the Act on Police and Other Legal Acts Regulating Surveillance by the Law Enforcement Agencies and Security Services (28 April 2016) *available at* www.hfhr.pl/wp-content/uploads/2016/05/HFHR_hand_out_Venice_Commission_Act_on_Police_FNL.pdf [hereinafteR: Helsinki Report].

[9] Application to the Constitutional Tribunal by Dr. Adam Bondar, Commission for Human Rights, Doc. No. II.519.109.2015.KLS/VV/AG (18 February 2016) *available at* www.rpo.gov.pl/sites/default/files/Application%20to%20the%20Constitutional%20Tribunal%20on%20the%20amendment%20to%20the%20Act%20on%20the%20Police.pdf.

[10] As enumerated under Article 19(6) of the Act, secret surveillance covers a broad range of possible activities by Polish public authorities including: (1) extracting and recording the content of conversations carried out using technical resources, including telecommunications networks; (2) extracting and recording images and sounds of people in inside spaces, transport or any non-public places; (3) extracting the content of correspondence, including correspondence exchanged through electronic means of communication; (4) extracting and recording data from data storage media, telecommunications terminal equipment, information and communication systems; (5) gaining access to and checking the contents of mail.

[11] Venice Commission Report, *supra* note 4, at para. 15.

The legal grounds for collecting metadata are far broader and encompass in essence "any useful purpose related to the broad mandate of the police to maintain peace and order."[12] Furthermore, there is no *ex-ante* judicial authorisation for metadata collection, only a general *ex-post* requirement of submission every six months of a generalized metadata report to a competent district court. Certain metadata information does not even require the *ex-post* review.[13]

3. Legal Obligations of Poland under Article 17 of the ICCPR

Under Article 17 of the ICCPR interference with an individual's right to privacy is permissible only if it is neither arbitrary nor unlawful. The Committee had established in General Comment 16 that the gathering of information by public authorities "must be regulated by law" and "effective measures have to be taken by States" to prevent misuse.[14] The Committee had further clarified in *Toonan v. Australia* that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case".[15] This three prong test of legality, necessity, and proportionality has been reconfirmed by the High Commissioner for Human Rights in her 2014 on the Right to Privacy in the Digital Age.[16] In clarifying the nature of the legality test, the Commissioner stated the following:

"*The State must ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse.*"[17]

On the issue of differentiation in safeguards and procedural rules between the collection and analysis of content and metadata, the High Commissioner had noted that: "the aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication".[18] This conclusion, confirmed by other human rights experts and reflected in the jurisprudence of the Court of Justice of the European Union, echoes the fact that with the advancement of telecommunications and telecommunications' interception technologies, there is no justification for making distinctions in legal protections based on the nature of the data collected.[19]

---

[12] Venice Commission Report, *supra* note 4, at para. 15. In particular the Act allows for the collection of metadata "in order to prevent or detect crimes, or in order to save human life and health, or in order to support rescue and find missions".

[13] This includes the types of information listed under Article 20cb and covers, *inter alia*, a service provider's "directory of subscribers, users, or network termination points" including those users first and last names, parent's names, place and date of birth, addresses, ID numbers (PESEL), passport numbers, etc.

[14] Human Rights Committee, General Comment 16 on the Right to Privacy, U.N. Doc. HRI/GEN/1/Rev.1 at 21, para. 10 (1994).

[15] Human Rights Committee, *Toonan v. Australia*, Comm. No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 para. 8.3 (31 March 1994).

[16] Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/27/37, para. 23 (June 30, 2014). *See also Roman Zakharov v. Russia*, App. No. 47143/06, Eur. Ct. H. R. (4 Dec., 2015); *Szabó and Vissy v. Hungary*, App. No. 37138/14, Eur. Ct. H. R. (12 Jan., 2016).

[17] *Id.*, at para. 28. These principles correlate with the six minimal safeguards enumerated by the European Court of Human Rights in the *Weber v. Germany* case (the minimal safeguards that must be set out in the surveillance legislation include: (1) the nature of the offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their communications intercepted; (3) a limit on the duration of interception; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which the data collected may or must be erased). *See Weber & Saravia v. Germany*, app no. 54934/00, Euro. Ct. Hum. Rts., para. 95 (2006).

[18] *Id.*, at para. 19.

[19] This position has been reaffirmed by the European Court of Justice in the *Digital Rights Ireland* case, where they noted that: "[Metadata] taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them." *See* Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment, paras. 26-27, and 37 (8 April 2014).

4. Compatibility of Articles 19 and 20c of the 2016 Amendments Act with Poland's ICCPR Obligations

Privacy International is concerned with a number of substantive elements pertaining to both the Secret Surveillance program, under the amended Article 19, and the Metadata program under the amended Article 20c.

4.1 Legality (Accessibility and Foreseeability)

Both Article 19 and under Article 20c of the 2016 Amendments Act contain ambiguous terms that fail to meet the legality requirement. Under Article 19 (6) the Police is allowed to "gain access to... mail". The provision does not state how such access is to be achieved, and leaves open the possibility of various forms of potentially unlawful hacking and tapping for the purposes of intelligence collection.

Similarly, Article 20c relies on the term "internet data" without defining it (only referencing other pieces of legislation for the definition, including the Telecommunications Act, the Postal Act, and the Electronic Services Act). This lack of a precise definition potentially means that any parcel of information that flows through internet cables may under this term.

The closed list of crimes enumerated under Article 19(1) and on the basis of which Polish authorities may resort to "secret surveillance" measures is significantly broad, including for investigation of crimes such as anyone who "takes part in betting that concerns sports" (Article 19(1)(2a)), or as it relates to anyone who possesses small amount of psychotropic substance (Article 19(1)(5)).

Even broader are the grounds for Metadata collection under Section 20c, which as stated above allows for the police to collect any telecommunication information it deems necessary in order to prevent or detect crimes, or in order to save human life and health, or in order to support rescue and find missions.[20]

Both the Article 19(1) and Article 20c programs do not require a standard of reasonable suspicion against a person or a group of persons to conduct either the secret surveillance or metadata collection.[21] The provisions further do not seek to define or limit the "extent of connection to people/groups in question to the criminal activity under investigation".[22] For example, the Facebook friends of a person under surveillance might themselves be surveiled for both their content of their communications as their metadata.

4.2 Necessity and Proportionality

Bulk collection is the untargeted acquisition of information, including on people who are not and will never be subject of interest for the public authorities, and which results in providing the authorities with access to large depositories and streams of data, a significant portions of which are not associated with potential targets for surveillance.

Under Article 19(6) there is not sufficient information about the way information is to be extracted for the purposes of the secret surveillance. For example, section 19(6)(4) involves "extracting and recording data from data storage media, telecommunications terminal equipment, information and communication systems". If this provision allows for the interception of a whole fibre-optic cable or a communications switch, it could involve the bulk collection of disproportionate amount of information.

Similarly, Article 20c does not require the targeting of a particular individual or group of individuals. Rather it aims at the collection of significant portions of subscribers' data, billing information, IP address, mobile phones' location, browsing history, and operating systems, all for the purposes of the future-looking "prevention" of crimes.

As the High Commissioner for Human Rights stated: "Mass or 'bulk' surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime".[23]

---

[20] *See supra* fn 13.

[21] As the Venice Commission noted "the law should be clear that in order to conduct surveillance the police and the prosecutor must have at least some prima facie evidence of a criminal activity, and that the court must examine such evidence before authorising the surveillance.", Venice Commission Report, *supra* note 4, at para. 44.

[22] *Id*., at paras. 72-74. Moreover the Venice Commission notes the fact that under certain circumstances non-targeted third party information obtained "by accident" in the course of the surveillance may be introduced in the criminal proceeding against those bystanders as evidence.

[23] U.N. High Commissioner for Human Rights, Report on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37, para. 25 (30 June 2014).

Similarly, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism stated "it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately" and that "[t]he very essence of the right to the privacy of communication is that infringements must be exceptional, and justified on a case-by-case basis."[24] In 2016, a report of the UN Office of the High Commissioner on Human Rights reiterated that "[m]ass secret surveillance is not permissible under international human rights law, as an individualised necessity and proportionality analysis would not be possible in the context of such measures."[25]

4.3 Insufficient Safeguards

Duration of surveillance and deletion of data

Article 19(8)-(9) does set time limits for the duration of the secret surveillance, though that period can be as long as 18 months.[26] As the Venice Commission noted that is a significantly long period. No maximum limits are set on metadata collection, and there is no indication in the law as to how much historical data may the police retrieve from ICT companies, or how long may it monitor live metadata flows.[27]

Professional privilege

While Article 19 does establish certain restrictions on the interception and collection of communication which is subject to certain professional privilege, there remains significant shortcomings. These include the fact that the provision does not explicitly prohibit the surveillance of lawyers to clients' communications; the fact that Article 19f merely demands that information obtained in breach of the privilege may not be submitted as evidence to the Court and must be destroyed, without setting a prohibition on the public authorities listening to the conversation; the fact that the law allows for the submission into evidence of information obtained in breach of the privilege of other professionals "if necessary in the view point of the justice system".

Of significant concern is the fact that Article 20c does not establish a similar system, thus allowing for the collection of lawyers', doctors', mediators', and psychiatrists' metadata and the submission of said metadata as evidence before the Courts without any additional safeguards.

4.4 Ineffective oversight, notification and access to remedy

Judicial authorisation

While the Article 19 process does involve *ex ante judicial* authorization process, the Court makes its decision only on the basis of the request by the investigating authorities, without benefiting, for example, from a "privacy advocate".[28] Moreover introducing an *ex post* review process either by the authorizing judge or by an independent body would also significantly improve the efficacy of the oversight.[29]

There is no *ex ante* authorization procedure under Article 20c, and the *ex post* review is extremely limited. This is particularly worrisome and prone to abuse given that the police is entitled to direct access metadata "without participation of the employees of the ICT". The Venice Commission has recommended both the introduction of judicial pre-authorization and stronger *ex-post* controls over the metadata collection program.[30]

---

[24] U.N. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Annual Report to the General Assembly, U.N. Doc. A/69/397, para. 18 (23 September 2014)
[25] U.N. High Commissioner for Human Rights, Report on Best Practices and Lessons Learned on how Protecting and Promoting Human Rights Contribute to Preventing and Countering Violent Extremism, A/HRC/33/29, para. 58 (21 July 2016).
[26] Secret surveillance shall be ordered for a period not exceeding three months. A competent entity with legitimate reason, may motion the District Court to extend the surveillance for an additional three months. Another prolongation may be allowed by a higher Court, for a total of up to 12 additional months. Therefore, the overall duration of surveillance measures may not exceed 18 months.
[27] Venice Commission Report, *supra* note 4, at paras. 87-88.
[28] *Id.*, at para. 97.
[29] *Id.*, at paras. 104-108.
[30] *Id.*, at paras. 110-119.

Notification and access to remedy

The Constitutional Tribunal has twice now called on the Polish authorities to establish a "duty to inform individuals covered by operational surveillance that such has been conducted". First in the 25 January 2006 (Ref. No. S 2/06) and more recently in the 2014 judgment.[31] Nonetheless, the 2016 Amendments Act did not introduce any form of notification, complaint procedure or remedy mechanisms. Therefore, an individual may only learn of her/his surveillance if such evidence is later presented in court. It remains unclear whether that individual may challenge said surveillance before the authorizing District Court or before a higher court.

While it is generally understood that notification of secret surveillance may sometimes jeopardize certain investigations, that cannot be used as a justification for denying access to effective remedies. Hence, the Polish authorities should legislate that the person under surveillance is notified as soon as such notification does not put in serious jeopardy the purpose for which the surveillance measure was originally authorised.[32]

5. Intelligence Sharing

According to revelations made by former NSA contractor Edward Snowden, Poland is considered a "third party Signals Intelligence Designator" as part of its membership within the "41-Eyes" alliance. Poland is additionally a party to a number of other intelligence sharing arrangements including the NATO Advisory Committee on Special Intelligence (NACSI) and the European "Club de Berne".[33] In the past, Poland's cooperation with other intelligence agencies had resulted in serious human rights violations.[34] Given this track record, and in light of the involvement of some of Poland's intelligence partners in mass surveillance, it is of concern that the government has provided no information on the laws and practices regulating intelligence sharing and extraterritorial surveillance operations.

6. Recommendations

Based on the above observations, Privacy International suggests the following recommendations for the Polish government:

1. Publicly avow the surveillance capacities of law enforcement, security, and intelligence agencies, and ensure that the use of such measures (domestically and internationally) is properly regulated and overseen by independent authorities to prevent abuse;

2. Take all necessary measures to ensure that surveillance activities, both within and outside the scope of the 2016 Amendments Act, conform to Poland's obligations under ICCPR (Art. 17). In particular, measures should be taken to ensure that any potential interference with the right to privacy complies with the principles of legality, necessity, and proportionality, and that minimization procedures and institutional safeguards are in place to effectively limit risks of abuse. Relevant authorities should comply with such principles regardless of the nationality or location of the individuals whose communications are under surveillance, including by refraining from engaging in all forms of mass surveillance.

[31] For more information *see* Helsinki Report, *supra* note 8, at p. 16.
[32] Venice Commission Report, *supra* note 4, at paras 98-109.
[33] *See generally* Five Eyes, 9-Eyes, and many more, electrospaces.net (22 January 2014), *available at* http://electrospaces.blogspot.co.uk/2013/11/five-eyes-9-eyes-and-many-more.html.
[34] *See e.g.*, *Al Nashiri v. Poland*, App. No. 28761/11, Eur. Ct. H.R., Judgment (22 July 2014); *Husayn (Abu Zubaydah) v. Poland*, App. No. 7511/13, Eur. Ct. H.R., Judgment (24 July 2014).