# GLOBAL INFORMATION SOCIETY WATCH 2014

*Communications surveillance in the digital age*

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

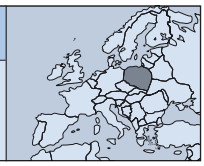
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

# POLAND

Access to telecommunication data in Poland: Specific problems and general conclusions



**Panoptykon Foundation**
Katarzyna Szymielewicz and Anna Walkowiak
panoptykon.org

## Introduction

Poland, as a member state of the European Union, was obliged to introduce mandatory telecommunication data retention as part of the implementation of the so-called Data Retention Directive.[1] As a result, all telecommunications service providers in Poland have to collect and store so-called *metadata* (i.e. data showing originator, destination, date and time) for at least 12 months. According to the directive, such data should be made available to the competent national authorities only in specific cases and in accordance with national law for the purpose of the investigation, detection and prosecution of serious crimes (as defined by relevant national law).[2] However, when implementing the directive, Poland failed to introduce these rules regarding the use of telecommunications data for law enforcement purposes. As a result, such information – collected about every person using telecommunication services in Poland – is used even in the prosecution of common crimes (like theft) and for the sake of crime prevention.

Moreover, Polish law does not provide for any safeguards that would prevent abuses, such as an external supervisory mechanism, court oversight, the obligation to inform the person concerned about the use of his or her data or the obligation to destroy data after the end of proceedings.[3]

## Policy and political background

The distinction between security and freedom and the argument that it is not possible to have both are very powerful notions in Polish public debate. It also seems to be commonly accepted that if a certain activity is related to national security, it should be kept secret by default. The argument "because it is useful for law enforcement, it must be good for public security" is raised whenever the lack of accountability of intelligence agencies is mentioned. In addition, law enforcement and intelligence agencies have a strong influence in drafting the laws that are meant to regulate their powers.

This political climate has enabled what human rights advocates perceive as possibly the worst implementation of the Data Retention Directive: Poland opted for the longest possible data retention period (24 months) and, as mentioned, failed to introduce any legal safeguards. Therefore, Polish regulation providing for retention and use of telecommunications metadata has been heavily criticised by human rights advocates, the Ombudsman and the national Data Protection Authority.

As a result of persistent pressure exerted by both human rights organisations and public authorities, in 2011 this legal landscape gradually started to change. The Ombudsman and Prosecutor General filed six official complaints to the Constitutional Court, arguing that various powers attributed to intelligence and law enforcement (including the use of telecommunication data) should be limited. This case is still pending.[4] In January 2013 the period of telecommunications data retention was shortened to 12 months, but other problems remained.[5] Further changes, however, are expected because of two legislative proposals that are under discussion: (i) a draft law introducing a special commission to supervise intelligence agencies that investigate complaints from individuals; and (ii) a draft law lim-

1 European Union. (2006). Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

2 European Union. (2006). Op. cit.

3 Panoptykon Foundation. (2012, April 3). How many times did the state authorities reach out for our private telecommunications data in 2011? We publish the latest research. *Panoptykon Foundation*. panoptykon.org/wiadomosc/how-many-times-did-state-authorities-reach-out-our-private-telecommunications-data-2011-we

4 Klicki, W. (2014, April 4). Służby przed Trybunałem. *Fundacja Panoptykon*. panoptykon.org/wiadomosc/sluzby-przed-trybunalem

5 Klicki, W., & Szymielewicz, K. (2012, October 15). Sejm jednomyślnie przyjął nowelizację Prawa telekomunikacyjnego. *Fundacja Panoptykon*. panoptykon.org/wiadomosc/sejm-jednomyslnie-przyjal-nowelizacje-prawa-telekomunikacyjnego

iting the access to citizens' telecommunication data by intelligence agencies.[6]

## Surveilling the media: The case of Bogdan Wróblewski

In 2010 one of the most influential Polish daily newspapers, *Gazeta Wyborcza*, published an article claiming that several journalists who specialised in politics were under illegal surveillance. Polish intelligence agencies – namely the Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego* or ABW) and the Central Anti-Corruption Bureau (*Centralne Biuro Antykorupcyjne* or CBA) – gained access to telecommunications data retained for public security purposes to spy on at least 10 journalists between 2005 and 2007. The intelligence agencies denied these allegations, but proof of their requests sent to telecommunications service providers proved otherwise. Bogdan Wróblewski, author of the abovementioned article, was among the alleged victims of illegal surveillance.

According to published information, the CBA spied on Wróblewski (back then a journalist specialised in court cases, now at the Supreme Audit Office, the highest public auditing body) by accessing and analysing his telephone accounts for six months – accounts which revealed a list of his contacts, including journalistic sources. This happened exactly when Wróblewski was working on critical articles dealing with special operations conducted by the CBA, which came under public scrutiny because of various irregularities. It seemed clear that the CBA tried to find out who Wróblewski's sources of information were.

Because of these suspicions, the public prosecutor conducted an investigation to verify whether intelligence agencies acted against the law. Oddly enough, although there was evidence that the CBA and ABW asked telecommunications service providers for data related to journalistic activity, the investigation was closed due to "the failure to detect a crime". Most of the records of the prosecutor's proceedings were classified, which made it very difficult for individuals concerned to challenge the outcome.[7]

Due to a lack of other legal measures available to him, in 2011 Wróblewski decided to sue the CBA in civil proceedings, indicating that their actions violated his right to privacy, secrecy of correspondence, freedom of expression and freedom of the press. Wróblewski obtained additional support from civil society organisations that submitted their opinions to the court (*amicus curiae*), emphasising human rights violations. One of those organisations was the Panoptykon Foundation.[8]

In 2012, a district court in Warsaw ruled that the use of Wróblewski's billing data by the CBA violated his right to privacy and constituted "typical surveillance for unknown purposes". According to the judge, the CBA should be able to use billing data only for the purpose of anti-corruption proceedings (in accordance with the statutory duties of this agency). The court ordered the CBA to apologise to Wróblewski and to delete all data relating to him that the agency had obtained.[9] The Court of Appeal dismissed the CBA's appeal and upheld the ruling – finally, the CBA publicly apologised.[10]

Wróblewski's case showed that imposing the obligation on telecommunications service providers to retain and give intelligence agencies access to their clients' data without adequate safeguards inevitably leads to human rights violations. What turned out to be very problematic in this case is that Polish law does not require intelligence agencies to delete data once it is no longer necessary to retain it. As a result it may be possible to collect and retain data about a given person for years, even though he or she is not formally suspected of any crime. It is sufficient for intelligence agencies to prove that such person belongs to a "group under special scrutiny" for security purposes. Security purposes vary from allegations of belonging to a terrorist organisation to being part of a religious, political or sexual minority – and in many cases these groups do not justify surveillance.

Without introducing strict control over intelligence agencies' powers to access citizens' telecommunications data, and without further legal

6 Ministry of the Interior. (2013). Projekt ustawy o Komisji Kontroli Służb Specjalnych. legislacja.rcl.gov.pl/docs//2/181401/181409/181410/dokument87492.pdf; Senate of the Republic of Poland. (2014). Projekt ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych. www.senat.gov.pl/gfx/senat/userfiles/_public/k8/komisje/2014/kpcpp/materialy/wniosek_nik_bilingio31200201402210957 24.pdf

7 Czuchowski, W. (2010, October 8). Dziennikarze na celowniku służb specjalnych. *Gazeta Wyborcza*. wyborcza.pl/1,76842,8480752,Dziennikarze_na_celowniku_sluzb_specjalnych.html .

8 Panoptykon Foundation. (2011). Opinia przyjaciela sądu (amicus curiae) Fundacji Panoptykon w postępowaniu Bogdan Wróblewski przeciwko CBA. panoptykon.org/sites/panoptykon.org/files/opinia_wroblewski.pdf

9 Klicki, W. (2012, April 26). Zwycięstwo dziennikarza w sporze z CBA – będą przeprosiny. *Panoptykon Foundation*. panoptykon.org/wiadomosc/zwyciestwo-dziennikarza-w-sporze-z-cba-beda-przeprosiny

10 Gazeta Wyborcza. (2013, April 26). CBA ma przeprosić dziennikarza „Gazety Wyborczej" Bogdana Wróblewskiego za to, że za rządów PiS kontrolowało jego billingi telefoniczne. *Gazeta Wyborcza*. wyborcza.pl/1,76842,13815430,CBA_ma_przeprosic_dziennikarza__Gazety_Wyborczej_.html#ixzz32LVDhTpP

changes that would limit the legitimate purposes of surveillance, it is likely that cases like Wróblewski's will be repeated.

## Conclusions

Telecommunications data retention, by definition, constitutes a serious violation of the right to privacy. Mobile phones are a part of our everyday life and therefore our telecommunications data reveals a lot about our life: from professional to intimate relationships to daily routines. With increasing amounts of data stored by private companies (not only telecommunications or internet service providers, but also shops, banks, insurance companies, health services or energy providers), the issue of legitimacy of data retention and access rules must be revisited. The trend towards retaining more data and broadening the catalogue of purposes that justify its further use should be reversed.

Any surveillance mechanism that targets innocent citizens and leads to the collection of data "just in case it may turn out to be useful" cannot be reconciled with a presumption of innocence. This position has been reinforced by the Court of Justice of the European Union in its recent judgement that declared the Data Retention Directive "invalid from the beginning" because of insufficient human rights safeguards.[11] This judgement should be implemented in all European countries.

Currently Polish law does not provide for any independent oversight over intelligence agencies. Only internal control mechanisms are in place, which cannot be treated as independent. As a result there is no way to verify whether Polish intelligence agencies observe at least existing legal safeguards, other than through journalistic investigation or whistleblowing. Wróblewski's case shows beyond doubt that strict control over intelligence agencies' powers to access citizens' telecommunications data is necessary. Such control mechanisms should cover not only the use of data retained for security purposes, but access to all types of data, the use of other surveillance technologies (SIGINT, CCTV, open source intelligence, predictive profiling, etc.) and international cooperation among intelligence agencies.

Institutional checks and balances with regard to surveillance carried out by the state cannot work without sufficient information. Therefore, the main obstacle that we face in demanding more accountability for illegitimate surveillance is secrecy and a lack of transparency. Polish law does not provide for any reliable mechanism for verifying how many times and for what purposes public entities (law enforcement or any of the nine intelligence agencies) asked for citizens' personal data. This problem affects all types of data and all types of requests, whether telecommunications, electronic services, banking, or social security data.

Currently Polish public authorities are under no legal obligation to register their data requests, nor publish the number of requests or other details. Only telecommunications service providers are required to collect statistics showing how many times they were asked for their clients' personal information. However, research conducted by Panoptykon Foundation in Poland showed that even data that is collected by public authorities cannot be relied on. A simple comparison of statistics published by the Office for Electronic Communications (the supervisory body for telecommunications service providers) and data obtained directly from police and intelligence agencies via freedom of information requests, shows that there is a significant discrepancy. The law should provide for one methodology that would apply to collecting information about the scale and purpose of requests for citizens' data from various sources.

## Action steps

Given the above, the following steps should be taken in Poland to secure a human rights framework for surveillance:

- Thanks to Edward Snowden's disclosures, European citizens learned that there is a link between mandatory retention of telecommunications data, introduced by the EU in 2006, and US programmes of mass surveillance. Measures which human rights advocates across Europe have been fighting for the last seven years turned out to be part of something much bigger and much more disturbing. This common context of international mass-surveillance operations should be further explored for advocacy purposes by civil society on both sides of the Atlantic.
- Following the recent ruling of the Court of Justice of the EU, Poland and other European countries should revise their laws that provide for telecommunications data retention without adequate safeguards. However, it will not be an automatic process resulting from the judgement. The judgement itself only affected the Data Retention Directive – not respective national laws. It might be necessary for citizens and the European Commission to take further legal

11 The Court of Justice declares the Data Retention Directive to be invalid. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

action. The possibility of bringing a complaint to the European Commission on the grounds that existing national laws are in violation of the European law is worth exploring.

- The need for more transparency in the area where law enforcement and intelligence agencies "meet" private companies and demand citizens' data has become evident, not only with regard to telecommunications data, but even more so with regard to all types of data that are stored by internet service providers. One way of pursuing this goal is by drafting so-called transparency reports – reports that show not only the scale of surveillance but also explore its purposes and human rights impact. While companies focus on numbers, civil society and researchers should focus on problem analysis, asking pertinent questions on the basis of available data. Panoptykon Foundation drafted such a transparency report for Poland in 2013.[12] Other organisations could build further on this methodology.

12 Panptykon Foundation. (2013). *Access of public authorities to the data of Internet service users: Seven issues and several hypotheses*. Warsaw: Panoptykon Foundation. panoptykon.org/sites/panoptykon.org/files/transparency_report_pl.pdf