INTERNET FREEDOM REPORT 2014: POLAND

Overall Internet freedom score: **30**/50
Gross domestic product per capita: €16,843 per annum[1]
Population: 38.5 million
Percent of individuals using the Internet in 2013: 62.85[2]
Facebook subscribers: 9,863,380[3]
Average broadband speed: 21.81 Mbps (45th of 192 countries)[4]

Freedom of Expression	8
Maximum potential score	15
Big Brother	10
Maximum potential score	15
Legal Maze	7
Maximum potential score	10
Open Government	5
Maximum potential score	10
Total Score	**30**
Maximum potential score	50

Free, but Mind the Gaps

Poland is a supporter of Internet freedom on the international stage, but is dragging its feet on making public information accessible at home.

by Dominika Bychawska-Siniarska and Zuzanna Warso*

Poland has the building blocks in place for an open and lively online community: decent Internet penetration, a nonpartisan Internet regulator, effective mechanisms to police content without undue interference from law enforcement authorities, a law requiring public information be posted online as a matter of course, and active Internet freedom watchdogs in both government and civil society.

Too often, however, laws are ignored or bent, and debates periodically rage over whether content should be blocked and which copyright protections apply to material online. Bureaucrats drag their feet on requirements to make information accessible online, while courts are too quick to take up cases that should be settled via notice and takedown procedures specifically devised for online content. On the other hand, prosecutions of online (and offline) hate speech are few, and tend to fizzle out before reaching a conclusion.

While there does not seem to be indiscriminate and widespread official surveillance of citizens' online activities, the thousands of court requests that police file each year to engage in such monitoring are almost always granted. There is no reliable information on how often authorities request user information from Internet service providers or hosting companies; users are notified in only a few circumstances when such requests are made; and the basis on which those requests can be made is unclear.

1 Organisation for Economic Co-operation and Development (OECD), converted from USD at European Central Bank exchange rate, December 31, 2013. See: http://stats.oecd.org/index.aspx?queryid=558
2 International Telecommunication Union statistics, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls
3 Internet World Stats, December 31, 2012, http://www.internetworldstats.com/stats4.htm
4 Ookla Net Index Explorer, accessed October 8, 2014, http://explorer.netindex.com/

** The authors are both lawyers and project co-ordinators at the Helsinki Foundation for Human Rights, Poland*

ISBN 978-80-87804-11-7

This study was written as part of the project, Internet Freedom Report 2014: Visegrad Four, a project of Transitions (TOL) and PASOS (Policy Association for an Open Society).
The preparation of the reports was supported by Google. The reports were prepared with full research independence and the views expressed herein are views of the authors only (and not of Google).

Internationally, Poland could and should become a leader in Internet freedom. In the debate over Internet governance, the Polish minister of administration and digitization, Michal Boni, stepped up and played an important role in blocking authoritarian efforts to impose government controls on the Internet at the International Telecommunications Union (ITU) summit in Dubai in December 2012. The strong Polish intervention helped solidify European opposition to an ITU takeover of the Net. At the same time, the Polish Foreign Ministry still has not made Internet freedom a priority. Unlike the Czech Republic, for example, Poland still has not joined the Freedom Online Coalition.

CONCLUSIONS AND RECOMMENDATIONS

FREEDOM OF EXPRESSION

- Defamation should be decriminalized (so it is subject only to civil actions, not as at present to criminal prosecution).
- The country's press law should be amended so that it can be applied in the online world. Outdated provisions should not be artificially "stretched" to apply to the Internet.
- Judges should make more use of the notice and takedown procedure as a first step when attempting to remove online content.
- Prosecutors should prioritize online hate speech cases. Content and service providers should also play a more active role in combating online hate speech.

BIG BROTHER

- Lawmakers should resist initiatives that would give authorities legal powers to block websites. Illegal content should be removed instead.
- Freedom of expression should always be taken into account by the prosecution when investigating Internet cases.
- Reliable statistical data should be gathered on the number of requests for user information made by state authorities to telecommunications providers.
- Users should be informed when information about them is requested.
- Surveillance should be used only in exceptional situations. Under no circumstances should it violate interests or principles that should enjoy protection, such as journalistic sources or attorney-client privilege.

LEGAL MAZE

- Content and service providers should establish better self-regulatory mechanisms to combat online hate speech.
- Copyright law should be reformed to clarify the limits of fair use so as to balance the interests of users on the one hand, and the rights of content-creators and publishers on the other hand.

OPEN GOVERNMENT

- Poland needs a broader definition of public information to cover internal documents concerning the management of public funds.
- The introduction of new exceptions to the freedom of information law (such as diplomatic secrets) should be resisted, and existing exceptions should be interpreted narrowly.
- Clear guidelines for establishing and running Public Information Bulletins should be implemented. More data in open formats should be made available online as a matter of course, without the need to recourse to freedom of information requests. Trainings and awareness-raising campaigns on access to public information should be provided for officials.

Dominika Bychawska-Siniarska and Zuzanna Warso

FREEDOM OF EXPRESSION

***3**/5: The legal framework and instances of prosecutions entailing denial of freedom of expression.*
***3**/5: Legal rights and protections for online expression and their status compared with print and broadcast rights.*
***2**/5: Cases of bloggers or online journalists being prosecuted, fined, or jailed for defamation or libel.*

No Room for Hate

In July 2011, Poland's then foreign minister, Radosław Sikorski, sued Ringier Axel Springer Polska, publisher of the *Fakt* daily and the fakt.pl discussion platform where anti-Semitic comments had allegedly been posted about him and his wife. The company closed down the Internet forum in May 2011. The case is pending before the Warsaw Appellate court.[1]

1 The case is pending before a Warsaw Appellate court , case file No. XXIV C 265/1.

Defamatory Haste, but Little Action on Hate Speech

In recent years, the space for freedom of expression online seems to have been shrinking. The biggest threat is the use of criminal defamation proceedings. In addition, courts try to apply to Internet cases (criminal or civil) the Polish press law, which dates from 1984 and has not been adapted to new technologies. Plaintiffs try to eliminate unlawful content by instituting civil and criminal proceedings without first attempting to have the content removed, and judges make insufficient use of the notice and takedown procedure. (The notice and takedown procedure enables Internet users to ask for illegal content to be taken down by the Internet service providers (ISP). If the ISP decides to leave the content on the web, the ISP becomes responsible for the content and may face civil or criminal proceedings).
At the same time, prosecution of online (and offline) hate speech is ineffective: of 473 complaints lodged with law enforcement agencies in 2012 – 119 of which concerned online content – only 74 resulted in indictments, and most of those are being discontinued by prosecutors.[5]

5 Annual Report of the Prosecutor General, available at http://www.pg.gov.pl/sprawozdania-i-statystyki/

Rules and Digressions

Andrzej Jezior used to write a popular blog about local politics that sometimes attracted comments allegedly defaming a local politician. Although Jezior said he took down such comments upon learning of them, the politician sued successfully, and a court ordered Jezior to pay him compensation.[1] The court ignored the "notice and takedown" provision of the electronic services law, which allows complainants first to request that content or Internet service providers take down such content before taking the matter further. The case, ruled upon in Poland in November 2010, is pending before the European Court of Human Rights.[2]

1 Tarnów Appellate Court ruling from November 17, 2010, case file No. Acz 1457/10.
2 European Court of Human Rights, Application No. 31955/11.

No specific legal framework exists for the Internet. When adjudicating Internet cases, courts tend to apply provisions concerning the traditional press.

The responsibility for content of intermediaries – content providers, ISPs, or forum administrators, for instance – is governed by the law on electronic services, which includes a provision enabling anyone to give notice of allegedly illegal content.[6] Intermediaries can, if necessary, take down the content.

In practice, courts typically use civil law to adjudicate the responsibility of ISPs and content providers.

Legal protections for online media are not uniform. Only publications listed on a court registry enjoy the guarantees of the Polish Press Law, such as the freedom to publish anonymously and the right to protect sources.[7]

According to the Supreme Court, only web pages that are an extension of printed titles and are updated periodically can – and must – be registered.[8] The penalty for failing to register such a website is a fine of up to 5,000 zloty ($1,500 or € 1,200).

Complaints to prosecutors about the non-registration of websites have become a weapon among competitors. The legal rights and responsibilities of online editors and publishers are not clear and depend on the approach of prosecutors and courts.

Defamation is a criminal offense in Poland, punishable by up to one year in prison. The number of defamation convictions ballooned from five in 2000 to 52 in 2011, some of which concerned bloggers or people commenting on Internet forums, although the Justice Ministry does not break down the statistics by type of media.[9] Punishment is usually a fine or community service, as in the case of Łukasz Kasprowicz, a blogger in the western town of Mosina, who was sued for defamation by a local politician he had criticized.

Host to Unwelcome Guests

In January 2014, the Supreme Court ruled that comments posted on online media should be treated as letters to the editor, holding editors and publishers responsible for them. The ruling came about after Roman Giertych, a Polish politician, lodged civil complaints against Ringier Axel Springer Polska over allegedly defamatory comments posted under an article about him. Judges in the case disregarded the notice and takedown procedure.[1]

Bans, Blogs, and Politicians

A local politician filed a suit for defamation against a blogger in the western town of Mosina. A court fined the blogger, Łukasz Kasprowicz, sentenced him to community service, and banned him from any journalistic activity. A higher court quashed this judgment and dismissed the case on the grounds that there was a lack of "social harm." The Supreme Court overturned the judgment. On January 20, 2014, the court found the blogger guilty on one count and ordered him to pay a fine of 500 zloty. The proceedings took five years in total.

6 *Law of July 18, 2002, Official Journal 2002, No. 144, Item 1204.*
7 *Press Law of January 26, 1984, Official Journal 1984, No. 5, Item 24.*
1 *The ruling is not final. The case has been remitted by the Supreme Court to the Regional Court for further clarification.*
8 *For example, the judgment in the case of gazetabytowska.pl from December 15, 2010.*
9 *The exact number of convictions for defamation on the Internet is unknown, as such statistics are not provided by the Justice Ministry.*

BIG BROTHER

***3**/5: Censorship – laws and implementation, and pressure-group activity, including requests to remove material.*
***4**/5: Filtering and blocking of Internet content by state and other actors.*
***3**/5: Published information on government surveillance/tapping – by government and by private companies.*

Civil and Criminal Routes to Remove Content

No specific legal basis exists for blocking access to websites, though the introduction of measures are being debated as a way of fighting child pornography. There are fears that, once legislation is introduced, such provisions would be abused.

The gathering of large amounts of telecoms data had been "outsourced" to commercial entities under an EU law – struck down in April 2014 – requiring them to hold on to certain information for up to two years. While the EU provision was struck down in April 2014, the obligation remains in Polish telecommunication law. On July 30, 2014, the Polish Constitutional Tribunal called for greater control over the investigating authorities asking for data retained by ISPs, but no legal changes have yet to be introduced.

ISPs have no legal obligation to monitor the data they transmit, and there are no grounds to assume that Polish authorities conduct widespread or permanent monitoring of people online.

At the same time, law enforcement and state agencies often use surveillance, subject in most cases to court approval. Evidence acquired during duly authorized surveillance is allowed in court.

Apart from the notice and takedown procedure, the removal of online content can be demanded via civil or criminal court cases.

Civil law allows individuals and companies who feel their rights have been violated (usually in damage to their reputation) to lodge complaints with the courts demanding that the content be taken down. The complainant must provide, however, the name and address of the alleged violator. This is impossible without the assistance of the Internet service provider – which usually gives out only the IP address of the alleged violator – or prosecutors, which would require a criminal case to have been launched.

Under the Telecommunications Law, a complainant cannot discover the identity of a content creator from the IP address.[10]

However, a complainant can request that the Inspector General for the Protection of Personal Data (GIODO) require the intermediary to deliver the required data or, through the launch of criminal proceedings, courts and prosecutors can compel the disclosure of such information for public interest reasons.[11]

Once the information has been provided, criminal proceedings are usually dropped, as complainants can use the information to pursue civil remedies.

Transparency about Disclosure

According to the Google Transparency Report in 2012, courts requested the removal of online content four times, while police or other agencies made such requests seven times.[12] The first half of 2013 (the most recent data available) saw four court requests and two requests from other institutions.

Since July 2010, 66 percent of items requested to be removed have related to privacy and

10 Law of July 16, 2004, Official Journal 2004, No. 171, Item 1800.
11 Law of August 29, 1997, Official Journal 1997, No. 133, Item 883.
Law of June 6, 1997, Official Journal 1997, No. 89, Item 555.
12 Available at: http://www.google.com/transparencyreport/removals/government/PL/?metric=items&p=2012-06

personal security protection, by far the largest category. Defamation complaints have accounted for 11 percent of the items targeted for removal, and copyright protection for 10 percent.

According to the Apple Report on Government Information Requests, in the first half of 2013, law enforcement authorities made only one request to disclose data – a request concerning two accounts.[13] However, Apple objected to these requests, and no data was revealed.

The responsibilities and liability of Internet content and service providers are spelled out in the law on rendering electronic services, USUDE, which implements EU law. Service providers are not liable if they merely transmit data or temporarily store it.

USUDE establishes the procedure of notice and takedown, which limits the liability of companies that offer permanent online content storage. This provision applies, above all, to hosting services.

There are no specific restrictions on the acceptance of online media advertising beyond that online media, like their traditional counterparts, are prohibited from advertising alcohol and tobacco.[14] Even so, there has been some additional regulation of online advertising. In September 2008, the Polish Office of Competition and Consumer Protection forbade some forms of pop-up advertisements, especially those that do not allow users to close them instantly. Two hundred websites were found to contain this kind of advertisement, and proceedings were opened against the businesses.[15]

In addition, the online organization or advertising of gambling is prohibited under the broader gambling law.[16] As a result, gamblers in Poland turn to foreign gaming websites. The legislation that forbids gaming was adopted without the required technical notification to the European Commission, and therefore there are doubts about its legality. Constitutional challenges to the corresponding measures are pending.

To Block or Not to Block?

In Poland, no specific law or ruling allows websites to be blocked. There have been attempts to establish a regulatory "blacklist" of websites to combat online gambling, extremist propaganda, and child pornography (the so-called "Register of Prohibited Websites and Forbidden Services"). However, after a public debate and protests by civil society organizations, the attempts were abandoned.

The issue of blocking websites has resurfaced in efforts to implement an EU directive on combating sexual abuse and child pornography. The justice minister recently vowed to re-consider blocking websites with pornographic content, but the prime minister later rejected such plans.

In July 2013, several lawmakers drafted a resolution urging the Administration and Digitalization Ministry to prepare the technical and legal groundwork to block sites with child pornography. Parents would also be able to demand Internet service providers block web pages with pornographic content, and ISPs would be required to establish filters blocking such content.[17] Nongovernmental organizations working on Internet freedom criticized the filtering requirement as a threat to the rights of Internet users.18 The resolution is still pending consideration at the parliamentary committee stage.

13 The report is available at: https://www.apple.com/pr/pdf/131105reportongovinforequests3.pdf
14 Art. 131 of the Law on prevention of alcoholism (Pol. Ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi) of October 26, 1982, Official Journal 1982, No. 36, Item 230.
15 http://uokik.gov.pl/aktualnosci.php?news_id=478
16 Law of November 19, 2009, Official Journal 2009, No 201, Item 1540.

17 The draft resolution is available at: http://orka.sejm.gov.pl/Druki7ka.nsf/0/107F92BAF489D5EAC1257BD500319B54/$File/1664.pdf

18 Post by Michał Woźniak available at: http://rys.io/pl/113, Fundacja Panoptykon: http://panoptykon.org/wiadomosc/polski-model-blokowania

The Means and Methods for Removing Content

The existing methods to remove online content include civil and criminal cases, as well as the notice and takedown procedure.

Law enforcement agencies also send requests to their counterparts abroad to remove online content. According to the most recent statistics, in 2008 police made 147 such requests regarding websites with child pornography. In 2009 they made 30 requests, and in 2010 they made 57 requests. In the first half of 2011, there were 22 requests. Data is not available on how many requests were honored.[19]

Some companies specialize in the deletion of content – particularly that which is defamatory, insulting, or vulgar – from the Internet.[20] The companies sometimes launch court proceedings or use personal contacts within the Internet business community to bring about the content removal.

Policies on, and procedures for, blocking content are opaque. The issue attracts attention only when politicians discuss new proposals. However, watchdog groups specializing in Internet freedom, such as the Panoptykon Foundation, inject the topic into the public debate, often with the help of freedom of information requests.

19 http://prawo.vagla.pl/node/9632
20: http://wyborcza.biz/Firma/1,101966,14823478,Pomysl_na_biznes__czyszczenie_sieci_z_obrazliwych.html

Online Hate Speech

The Criminal Code prohibits propaganda for the Nazi and other totalitarian regimes, as well as incitements to hatred based on nationality, ethnicity, race, religion, or lack of religious denomination. Violations carry a sentence of up to two years in prison.

The Criminal Code also prohibits public insult of a group due to nationality, ethnicity, race, religion, or lack of religious denomination, punishable by three years' imprisonment. In practice, the prosecution of online hate speech is very limited.

Internet Freedoms and Net Neutrality

The Polish government supports "the ultimate goal of the free, innovative, open, and

President in Satirical Crossfire

In May 2011, police from the National Security Agency entered the house of Robert Frycz, creator of a satirical website (www.antykomor.pl), aimed at the president of Poland, Bronisław Komorowski, and seized a computer and CD-ROMs. Frycz says the police advised him to take the site offline, and he briefly did so, before relaunching it three weeks later on a server located in the United States.[1] Frycz was accused of defaming the president via games on his website that involved shooting or throwing excrement at him. He was also accused of forging documents. The case was widely perceived as the prosecution's way of pressuring critical websites. On September 14, 2012, a regional court sentenced Frycz to one year and three months of community service for forgery and defamation. An appeals court on January 17, 2013, reduced the sentence to one year of community service for forgery, and acquitted Frycz of defamation.

1 http://freepl.info/409-order-submit-equipment-used-run-blo

unfragmented Internet"[21] and respect for and protection of "the core values and features of Internet, such as:

- privacy of Internet users;
- open and free technical standards and protocols;
- human rights and freedoms of Internet users, in particular freedom of speech;
- access to information and prohibition of preventive censorship;
- net neutrality and technological neutrality of the Internet infrastructure;
- the Internet's potential to promote democracy and cultural diversity."[22]

The "net neutrality" rule was recently introduced into Polish law to implement an EU directive that seeks to ensure that users can access and distribute information, or run applications and services of their choice.[23]

In 2011, the Office of Electronic Communication, a regulatory body, surveyed telecoms and business representatives about their methods for broad-based traffic management and whether there were cases of unequal treatment of communication signals.

The respondents said there are situations that necessitate the management of traffic, although some acknowledged that this may impede competition.[24] They all agreed there is a need for transparency about how the traffic is managed. There were a variety of opinions regarding the need to regulate the issue of net neutrality.[25]

21 "Poland's food for thought on Internet governance aspects in the pre-Sao Paulo discussions," Polish Ministry of Administration and Digitalization, 2014, available at: https://mac.gov.pl/files/polands_food_for_thought_on_internet_governance_aspects_in_the_pre-sao_paulo_discussions.pdf

22 Ibid.
23 http://prawo.vagla.pl/node/9589
24 Opinions were submitted by, among others, the Polish Chamber of Electronic Communication (Polska Izba Komunikacji Elektronicznej), the Polish Electronics and Telecommunications Chamber of Commerce (Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji),the Polish Chamber of Information Technology and Telecommunications (Polska Izba Informatyki i Telekomunikacji), Telekomunikacja Polska SA, and the Polish Confederation of Private Employers Lewiatan (Polska Konfederacja Pracodawców Prywatnych Lewiatan).
25 http://www.uke.gov.pl/podsumowanie-konsultacji-dotyczacych-neutralnosci-sieci-6695

In 2006, an investigation by the Office of Electronic Communication found that Telekomunikacja Polska SA (TP SA), a national telecommunications provider with a dominant position on the market, divided Internet traffic into three categories, two of which were subject to significantly reduced speed. In 2007, the Office of Competition and Consumer Protection fined TP SA for violating the competition law.

Content Control

Based on official sources, there seem to be no grounds to assume that authorities in Poland conduct widespread or permanent monitoring of people online.

So-called "operational surveillance" of online activity by law enforcement or intelligence agencies requires court permission and can be ordered for only the most serious crimes and only when other means of intelligence gathering appear ineffective. However, in urgent cases operational surveillance may occur before a court authorization. The constitutionality of laws on operational surveillance has been challenged by the ombudsman.[26]

26 See the opinion of the Helsinki Foundation for Human Rights submitted in the case: http://www.hfhrpol.waw.pl/precedens/images/stories/opinia_srodki_techn_13_06_12.pdf

A License to Snoop

According to the prosecutor general, in 2012 courts granted 94 percent of requests from police or other security agencies to surveil 4,206 people. In 2011, authorities sought to surveil 5,188 people, with courts again agreeing in about 94 percent of cases. In 2010, the courts permitted surveillance of 6,453 people, about 96 percent of the 6,723 requested.[1]

1 http://www.pg.gov.pl/aktualnosci-prokuratury-generalnej/informacja-prokuratora-generalnego-o-pods-uchach-2-690.html

In addition to operational surveillance, during pretrial and trial proceedings, on the motion of a prosecutor a court may order surveillance of mobile phones, electronic communications, and by other means. In urgent situations, the prosecution may institute surveillance, but a post facto court review is required. This "procedural" surveillance is allowed in serious cases such as murder, extortion, robbery, corruption, human trafficking, or spying.[27]

In October 2013, after Edward Snowden revealed information about the global surveillance by the U.S. National Security Agency (NSA), the Polish Helsinki Foundation for Human Rights (HFHR), together with the Panoptykon Foundation and Amnesty International, sent several freedom of information requests to state agencies in Poland, asking whether authorities make use of technology that would enable them to monitor online communications. The HFHR asked, among other things, if Polish intelligence agencies use the XKeyscore system or ever were invited to use it, or if they transmit data to the NSA. On the grounds of protecting state secrets, some agencies refused to answer some of the questions.[28]
According to USUDE, ISPs are not obliged to monitor the data they transmit, store, or make available.

Currently, the gathering of large amounts of telecoms data appears to be "outsourced" to commercial entities. To access this data, authorities must make a formal request to those companies. It remains unclear whether authorities need only invoke the law on rendering electronic services, which obliges ISPs to disclose data needed in legal proceedings carried out by state authorities, or whether the request should contain a more specific legal basis.[29]

In general, individuals learn that their data has been disclosed only if the request is made by a court or prosecutor.

It is difficult to estimate the scale of requests made by state authorities. Although telecoms are obliged to report annually the number of requests to the Office of Electronic Communication, the reliability of the data released by the office was put into question by a recent report of the Supreme Chamber of Control.[30] ISPs are under no obligation to record the number of requests. These difficulties were pointed out in a recent study by the Panoptykon Foundation, a leading Polish organization active in the field of digital rights.[31]

Hacking is a criminal offense. Commercial entities in Poland have been subject to several cyberattacks, especially in the early 2000s, at least partly due to their poor security systems, according to a security expert. One of the most frequent targets was Telekomunikacja Polska SA. Hackers also targeted government websites. More recently, several attacks took place at the beginning of 2012 during protests against the Anti-Counterfeiting Trade Agreement (ACTA). Groups disabled the websites of the prime minister, the lower house of parliament, and the ministry of culture, which was thought to support ACTA.

27 http://prawo.money.pl/kodeks/postepowania-karnego/dzial-v-dowody/rozdzial-26-kontrola-i-utrwalanie-rozmow/art-237
28 Answers available at: http://www.panoptykon.org/wiadomosc/ukladanka-odpowiedzi-w-sprawie-prism
29 in Polish - http://panoptykon.org/sites/panoptykon.org/files/panoptykon_dostep_panstwa_do_danych_internet_16.12.2013_0.pdf
in English – http://panoptykon.org/sites/panoptykon.org/files/transparency_report_pl.pdf

30 http://www.nik.gov.pl/plik/id,5421,vp,7038.pdf
31 in Polish - http://panoptykon.org/sites/panoptykon.org/files/panoptykon_dostep_panstwa_do_danych_internet_16.12.2013_0.pdf
in English – http://panoptykon.org/sites/panoptykon.org/files/transparency_report_pl.pdf

LEGAL MAZE

***4**/5: Transparency of legal procedures and appeals mechanisms*
***3**/5: Copyright laws, fair use – laws and practice*

Who Regulates the Internet?

The Office of Electronic Communication is an independent body regulating the Internet services market. In 2006, the European Commission opened infringement proceedings against Poland due to the lack of guarantees of independence for the office. In April 2009, the Telecommunication Law was amended to include a five-year term for the head of the office and to specify when he or she could be dismissed (by the prime minister). Grounds for firing include violation of the law, a court ruling disabling him or her from exercising the function of the job, a criminal conviction, or health problems preventing him or her from managing the office. In June 2009, the European Commission closed the proceedings against Poland.[32]

These changes, combined with judicial review of its decisions, make the Office of Electronic Communication an apolitical body. There have been no complaints about the influence of politics in its decision-making process.

Both the ombudsman and the Inspector General for the Protection of Personal Data (GIODO) are active in the field of digital rights. For example, the ombudsman has weighed in on the possible impact of ACTA on individual rights and freedoms, and facilitated a debate with civil society representatives on blocking access to websites containing child pornography.[33] For its part, in January 2012 GIODO published a negative opinion on ACTA and in September 2013 issued a warning about a proposal to allow parents to demand that ISPs block pornography.[34]

The market for Internet services is regulated by the Office of Electronic Communication, which is apolitical and independent. As far as self-regulation, no formal network of service or content providers exists. Self-policing focuses primarily on comment sections. One of the biggest Polish news sites allowing comments from users, gazeta.pl, pre-moderated its content only once, after the Smoleńsk crash of the presidential airplane in 2010.[35] Post-moderation is much more common but remains too costly for small content providers. Most providers have terms of service, accessible to users, covering commentaries and blocking of content.

Copyright Versus Fair Use

Polish copyright law has not been adapted to the online reality – existing copyright law was simply extended to the Internet.[36] The law's broad definition of fair use has triggered debate, as civil society groups advocate more open access to cultural and educational materials on the Internet, while publishers attempt to protect their economic rights.

In general, websites are considered protected works, but this is complicated by the notion of fair use. Polish law allows reuse, without consent of the author, of some works already made public. Information such as articles and statements on current events, as well as news photographs, can be disseminated in newspapers, on the radio, and on television (in practice also on the Internet). Fair use also covers public speeches

32 Decision IP/09/1006.
33 The opinion is available at: http://www.rpo.gov.pl/sites/default/files/13298261560.pdf

34 The opinion is available at http://www.giodo.gov.pl/1520128/id_art/4495/j/pl/
Press information available at http://wiadomosci.wp.pl/kat,1342,title,Boni-za-racjonalnym-i-skutecznym-ograniczeniem-pornografii-w-sieci,wid,15980676,wiadomosc.html?ticaid=111ea7
35 Anna-Maria Siwińska, Moderacja forów jako instrument walki z mową nienawiści w sieci ("Forum moderation as a tool of fighting online hate speech", in Dominika Bychawska-Siniarska, Dorota Głowacka, Mowa nienawiści w sieci: jak z nią walczyć, Helsinki Foundation for Human Rights, Warsaw 2013.
36 Law of February 4, 1994, Official Journal 1994, No. 24, Item 83.

and short summaries of public compositions (documents that the authorities have prepared for public needs, from public funds), and allows the reuse of existing works for educational purposes or critical analyses.

However, editors and authors are protected by another provision of the law that states that fair use may not impede the normal use of the work and may not interfere with creators' interests. Polish copyright law and fair use are constantly debated. Internet activists call for a wider definition of fair use (especially where access to cultural goods and education is concerned).[37] On the other hand, content creators argue that such a wide interpretation of fair use violates their economic interests.

In July 2013, the Warsaw Regional Court ruled that the simple inserting of links on websites or embedding movies from YouTube, which themselves violate copyright, constitutes a violation of copyright law, as the practice represents the dissemination of illegal content.[38]

Legislative acts and governmental proposals are exempted from copyright law, as they fall under the law on public information. In practice, however, the line between public information and copyrighted works is sometimes blurred. Public transportation schedules and photographs on the president's website, for instance, are protected by copyright law, even if produced with public resources.[39] In November 2013, the Constitutional Tribunal ruled that expertise prepared for the purpose of legislative changes should be treated as public information and made available to the public.[40]

37 The NGO Centrum Cyfrowe prepared a draft amendment to the copyright law: http://centrumcyfrowe.pl/dozwolony-uzytek-czy-piractwo-debata-wokol-kserowania-podrecznikow-szkolnych/
38 Case file No. IC 504/12.
39 Article of Paweł Płaza, Gazeta Wyborcza, April 24, 2012, available at: http://technologie.gazeta.pl/Internet/1,104665,11437618,Prawa_rzadowe_zastrzezone.html
40 Case file No. K 25/12.

OPEN GOVERNMENT

***3**/5: Quality of access to information legislation and Internet provisions.*
***2**/5: Access on Internet to government and parliament decisions, court cases and decisions; right and speed of access to data through requests, and capacity of authorities to answer complex information requests.*

The Bad News

Not enough public information is readily available in Poland. Authorities publish little data as a matter of course, and citizens and civic groups must often rely on freedom of information requests.

Provisions on access are scattered across different statutes, and exceptions abound. Public agencies use this lack of clarity to reject freedom of information requests in controversial cases, which often end up in court. Even in simple cases, replies are often delayed beyond the 14-day deadline.

Key problems with access to information in Poland include a tendency among public bodies to define public information too narrowly and to abuse exemptions, insufficient regular disclosure of public information outside the framework of freedom of information requests, frequently tardy or nonexistent responses to requests, and unwarranted restrictions on the reuse of public information.

The Polish constitution guarantees citizens the right to obtain information about the activities of public bodies as well as persons discharging public functions. That right extends to receiving information on organizations outside government that perform the duties of public authorities and manage public assets or state property. Restrictions on access may be imposed by statute solely to protect freedoms and rights of other persons and economic subjects, public order, security, or important economic interests of the state.

The 2001 Act on Access to Public Information calls for the regular publication of Public Information Bulletins (BIPs) at both the national and local levels.[41]

> *"According to studies by civil society groups, about half of public offices provide incomplete or late responses to freedom-of-information requests."*

Other statutes provide for access to information in specific cases, such as for archives, geodesic or cartographic information, or information about the environment. Civil society organizations say the scattering of provisions on access to public information throughout different statutes and a lack of coordination among departments complicate matters for citizens who wish to exercise their constitutional right.[42]

The Good News

In official statements, authorities acknowledge the need to make public information more accessible, and it was cited as one of the substantial challenges in realizing the idea of an open state addressed in the "Good Government 2020" ***(Spravne Państwo 2020)*** government strategy. At the same time, civil society groups fear that potential amendments to existing provisions could limit the right to access, for example by introducing a new exemption for "diplomatic secrets."[43]

The government and parliament have their own online Public Information Bulletins, which include working agendas and voting records, allowing citizens to track the legislative process.

In addition, court decisions and case law have become more readily available in recent years. The Constitutional Tribunal, the Supreme Administrative Court, and the Supreme Court publish their judgments on a regular basis. In 2012, the Justice Ministry began posting online the judgments of general courts (civil and criminal courts, but excluding administrative courts). Although more are gradually being made available, most older judgments of general courts have not been put online.[44]

Areas for Improvement

The main obstacles to the functioning of the law on access to public information in practice are:

1. Overly narrow definition of "public information."

According to recent reports of civil society organizations, officials sometimes deem "internal documents" those produced in the course of their work, exempting them from disclosure requirements.

Some statutes substantially limit access to documents concerning the management of public funds. For instance, the law on public finances excludes results of internal audits from the definition of public information. The ombudsman is challenging this provision before the Constitutional Tribunal. Many local laws also further limit the definition of "public information."[45]

41 Law of September 6, 2001, Official Journal 2001, No. 112, Item 1198
42 http://watchdog.org.pl/81,1367,czekajac_na_otwarte_rzady_raport_otwarcia.html, p.13

43 http://informacjapubliczna.org.pl/wwwdane/files/watchdog_panoptykon___msz_tajemnica_dypl_87x6.___opinia.pdf
44 http://prawo.vagla.pl/node/9883
45 http://watchdog.org.pl/81,1367,czekajac_na_otwarte_rzady_raport_otwarcia.html

Finally, the notion of "processed information" – public data that must be compiled, analyzed, or edited before being provided to the requestor – is overused. According to rules established by the courts, access to "processed information" is allowed only if there is a particularly important public interest at stake. According to the Non-Governmental Centre on Access to Public Information, officials interpret "processed" in an overly broad way, applying it when they are requested to disclose larger amounts of data or when the information must be made anonymous, despite the fact that neither of these circumstances constitutes "processing."[46]

2. Insufficient regular disclosure of public information in Public Information Bulletins.

Public Information Bulletins (BIP) were devised as a system of websites to enable universal access to public information. However, the system lacks coordination. Although the government should have established an application that would allow all public bodies to create a BIP on the same model, there are no clear guidelines on how a BIP should be run. In addition, there are no penalties for not disclosing public information in this way. Even when disclosed, information is often presented in closed formats such as jpg or pdf (limiting searchability and the possibility to reuse the information), and lacks correct annotations (such as the person responsible and date). This makes its reliability questionable. Finally, according to the case law of the Supreme Administrative Court, citizens cannot file complaints against public bodies for not disclosing public information on a BIP.[47]

3. Failure to act and the lack of timely responses to freedom of information requests.

According to studies by civil society groups, about half of public bodies do not reply to freedom of information requests satisfactorily or fail to do so within the 14-day deadline.

For instance, a 2012 study by the Stańczyk Institute of Civic Thought Foundation found that in the Małopolskie province 54.4 percent of municipalities failed to reply to freedom of information requests for at least two months.[48]

A similar study by the Bona Fides Civil Activity Association in the Śląskie province found that 44 percent of written requests received no or incomplete replies.[49]

The Civic Network - Watchdog Poland sent one freedom of information request to each of the country's 2,479 municipalities, but received only 1,185 replies – 48 percent – within the 14-day time limit.

4. Problems with the reuse of public information.

The law was amended in 2011 to allow the "reuse of public information," such as maps, timetables, and the like, but critics say the procedure for obtaining permission for reuse is overly complicated. In addition, some institutions arbitrarily exclude some types of data.

This report is based on desk research (articles, Internet, and publication analysis), analysis of data, case studies, information gathered via public information requests, and interviews (Marcin Serafin - Google; Piotr Toczyski - Information Processing Institute; Marek Troszyński - Collegium Civitas, New Media Department; Michał Woźniak - Free and Open Source Software Foundation (hacker society); and two representatives from the Warsaw Police Headquarters - IT Department – Marcin Siwiecki, Michał Zalewski).

46 http://informacjapubliczna.org.pl/wwwdane/files/stanowisko_ws_nowelizacji_ustawy_dip_d1fp.pdf
47 Case no. I, OSK 169/09, October 7, 2009

48 http://www.stanczyk.org.pl/wp-content/uploads/2012/11/raport-przyjazny-urzad-malopolska.pdf, p. 26
49 http://bonafides.pl/images/przyjazny_urzad/raport_slask.pdf, p. 19

NOTE ON METHODOLOGY:

The four country reports were drawn up based on a common methodology, with a set of questions for each section. The research teams' scores were drawn up by the analysts in the respective countries, peer-reviewed in-country, reviewed by Transitions Online and PASOS, then subject to a final comparative peer-review across the four countries.

The scale for each question is from 0 to 5, where 0 indicates no openness/freedom at all, and 5 indicates maximum degree of openness.

For each score, researchers were asked the following questions:

- *Is the body of laws/regulations/practice optimal/not needing any reforms to protect freedoms on the internet?*
- *Is the body of laws/regulations/practice generally adequate to protect freedoms on the internet?*
- *Are there significant gaps in the given area, where it is necessary to introduce and implement changes/statutory reforms to sustain open government/protection of freedoms/protection of privacy/clarity and transparency of legal framework?*
- *Is there a serious lapse in open government/protection of freedoms/protection of privacy/clarity and transparency of legal framework?*

The score (0-5) was assessed for each of the following questions within the four main chapters:

Section 1: Freedom of Expression

Freedom of expression on the Internet – laws, definitions, and de facto regulation

- *The legal framework and instances of prosecutions entailing denial of freedom of expression.*
- *Legal rights and protections for online expression and their status compared with print and broadcast rights.*
- *Cases of bloggers or online journalists being prosecuted, fined, or jailed for defamation or libel.*

Section 2: Big Brother

- *Censorship – laws and implementation, and pressure-group activity, including requests to remove material.*
- *Filtering and blocking of Internet content by state and other actors.*
- *Published information on government surveillance/tapping – by government and by private companies.*

Section 3: Legal Maze

- *Transparency of legal procedures and appeals mechanisms*
- *Copyright laws, fair use – laws and practice*

Section 4: Open Government

- *Quality of access to information legislation and Internet provisions.*
- *Access on Internet to government and parliament decisions, court cases, and decisions; right and speed of access to data through requests, and capacity of authorities to answer complex information requests.*

This study was written as part of the project, Internet Freedom Report 2014: Visegrad Four, a project of Transitions (TOL) and PASOS (Policy Association for an Open Society). The preparation of the reports was supported by Google. The reports were prepared with full research independence and the views expressed herein are views of the authors only (and not of Google).

The research is based on detailed analysis of the current situation - in law and in practice - using a methodology that examines Internet Freedom by looking into four main areas, namely *Freedom of Expression*, *Big Brother* (surveillance, regulation, and interference by the state), the *Legal Maze* (the clarity of the legal framework in terms of its letter and practice), and *Open Government* (transparency and online disclosure by government of its functioning and decisions, such as budget information and tender contracts).

The study, Internet Freedom 2014: Visegrad Four, was conceived with a view to raising the public profile of Internet freedom and censorship issues in the Visegrad countries within the region and internationally. Further objectives included the aim of addressing governments in the four countries to persuade them to take a consistent, open approach to Internet freedoms and transparency of government on the Internet, and the generation of empirical-based input to consultations in the European Union on digital rights and Internet freedom. The project also provides a template for evaluating and monitoring Internet freedom over time.

Internet Freedom 2014: Visegrad Four, compiled by independent think-tanks in the four countries, is the result of a project led by Transitions (TOL) to a methodology designed by PASOS (Policy Association for an Open Society). The participating think-tanks were the Association for International Affairs (AMO), Czech Republic, the Center for Media & Communication Studies, School of Public Policy, Central European University, Hungary, the Institute of Public Affairs (IPA), Poland, and the Institute for Public Affairs (IVO), Slovakia.

This publication has been peer-reviewed, but the final text is the responsibility of the authors. The publisher confirms that this policy analysis has been prepared in accordance with the PASOS principles for effective quality controls in the work of independent think-tanks.

INSTITUTE OF PUBLIC AFFAIRS

pasos
Policy Association for an Open Society

TOL

The Institute of Public Affairs, Warsaw, is a leading independent think-tank in Poland.

Institute of Public Affairs
ul. Szpitalna 5 lok.22, 00-031 Warszawa, Poland
Tel. +48 22 5564261
Email: isp@isp.org.pl
www.isp.org.pl

PASOS (Policy Association for an Open Society) is a network of independent think-tanks working to strengthen participatory policymaking at the local, national, and international level.

PASOS
Těšnov 3, 110 00 Praha 1, Czech Republic
Tel: +420 2223 13644
Email: info@pasos.org
www.pasos.org

Transitions (TOL) is a publishing and training organization with a mission of strengthening the professionalism, independence, and impact of the news media in the post-communist countries of Europe and the former Soviet Union.

Transitions
Baranova 33, 130 00 Praha 3, Czech Republic
Tel: +420 222 780 805
Email: info@tol.org