INTERNET FREEDOM REPORT 2014: CZECH REPUBLIC

Overall Internet freedom score: **37**/50
Gross domestic product per capita: €19,844 per annum[1]
Population: 10.5 million
Percent of individuals using the Internet in 2013: 74.11[2]
Facebook subscribers: 3,834,620[3]
Average broadband speed: 28.44 Mbps (28th out of 192 countries)[4]

Freedom of Expression	14
Maximum potential score	15
Big Brother	12
Maximum potential score	15
Legal Maze	6
Maximum potential score	10
Open Government	5
Maximum potential score	10
Total Score	**37**
Maximum potential score	50

Freedom Flagship Needs Compass

The Czech Republic is a leading proponent of Internet freedom on the international stage, as well as freedom of expression at home, but lacks a clear legal framework governing rights and responsibilities on the Internet.

by Tomáš Rezek*

The Czech Republic stands out among the Visegrad Four countries for its commitment to defending and promoting a free and open Internet, most prominently as a founding member of the Freedom Online coalition, the three-year-old organization of 21 countries dedicated to defending Internet freedom. Very few cases have come to light where a public authority, individual, or legal entity has exerted pressure on Internet sites to remove content. Moreover, strong legal protections for freedom of expression are in place to prevent attempts to take down content and to hold Internet platforms directly liable for content.

More work needs to be done, however, to modernize legislation in line with developments in the online world, and to educate judges about the legal framework governing the Internet. Public officials must become more responsive to freedom-of-information requests. Similarly, there is a need for more transparency about the scope and extent of online surveillance, and of content takedown requests.

The Czech government should build on its leadership role and promote Internet freedom as an integral part of its foreign policy goals.

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 author is a Research Fellow at the Association for International Affairs (AMO) Research Center.*

ISBN 978-80-87804-12-4

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).

Few Czechs seem aware of their country's efforts in support of Internet freedom. Despite the government's support for resolution L13 of the United Nations Human Rights Council on the protection of human rights online,[5] direct support for this issue is not a stated priority in Czech foreign policy.

> *"Few Czechs seem aware of their country's efforts in support of Internet freedom."*

Advocacy around the Czech Republic's comparative success and commitment to Internet freedom could be a common focus for government and civil society alike.

CONCLUSIONS AND RECOMMENDATIONS

FREEDOM OF EXPRESSION

- Freedom of expression is consistently protected in the Czech Republic.
- Discussion forums have been the focus of some of the most controversial challenges to freedom of expression online.

BIG BROTHER

- The Supreme Court should issue an official interpretation of the law governing online surveillance so as to avoid courts issuing inconsistent verdicts that unnecessarily breach privacy.
- More transparency in publicizing cases of online surveillance would allay fears that the excessive wiretapping of recent years extends to cyberspace.
- Similarly, the government should publicize takedown requests made to private companies instead of leaving the public in the dark in instances where private companies do not report the takedowns themselves.

LEGAL MAZE

- Current Czech legislation often remains behind the times when it comes to the Internet, and judges sometimes act without really understanding the online world.
- Setting strict principles for Internet-related cases would help eliminate discrepancies when judges rule differently upon similar cases.
- Enforcement of intellectual property rights and copyright related to online content is slowly improving.

OPEN GOVERNMENT

- Freedom-of-information legislation has served its purpose, and pushed the authorities toward greater transparency, such that a large amount of information is available online.
- Modern technology should be embraced to facilitate interaction between public authorities, citizens, and the private sector.
- Gray areas still exist in current laws, allowing various offices to refuse freedom-of-information requests, claiming commercial confidentiality or privacy concerns.
- Legislation should be tightened up to hold individually responsible those public officials who do not respect the law. This would improve responsiveness to requests.

Tomáš Rezek

5 http://geneva.usmission.gov/2012/07/05/internet-resolution/

FREEDOM OF EXPRESSION

5/5: *The legal framework and instances of prosecutions entailing denial of freedom of expression.*
5/5: *Legal rights and protections for online expression and their status compared with print and broadcast rights.*
4/5: *Cases of bloggers or online journalists being prosecuted, fined, or jailed for defamation or libel.*

Free Speech Center-Stage

Freedom of expression is consistently protected in the Czech Republic, and freedom of speech is enshrined in the constitution (with the caveat that this right might be restricted to protect the rights of other citizens, national security, public health, or morality).

Regulation relates specifically to content considered illegal, namely child pornography; expressions deemed extremist or racist; terrorism-related material; and violations of international property rights. Extremist content is defined by the Criminal Code,[6] which outlaws

6 Act No. 40/2009 Col., Criminal Code, Paragraphs 352, 353, 354, 355, 356, 403, 404, 405.

Violations and Vigilance

In April 2014, a Facebook group called "Požadujeme beztrestné vystřílení cikánů" ("We demand impunity for the shooting of gypsies") was launched, and quickly attracted 120 members. Despite dozens of complaints, Facebook originally refused to take down the page, claiming the page did not violate any Facebook rules. However, faced with additional complaints, including translation of offensive content into English, Facebook removed the page. Other Facebook pages have included calls for the murder of the head of Romea, a Roma media NGO, and prominent Roma figures.[1] According to the magazine Reflex, Facebook often takes a very long time, or takes no action at all, when requests are made to remove pages that violate legal norms against the spread of racial hatred and propagation of violence.[2]

However, websites with such content are usually located in the United States or other jurisdictions where it is possible under local legislation to freely publish content regarded as illegal in the Czech Republic.[3]

Bloggers or other individuals publishing on the Internet have been prosecuted only rarely for defamation or libel, in part because legal proceedings are usually generally very slow and the legal costs prohibitive.

One high-profile case arose after a Czech citizen, Karel Šiktanc, founded an unofficial Facebook profile for the Česká Lípa municipal police in February 2013, and began publishing photographs and information about police activities.[4] Most posts were critical, claiming, for example, that the police focused only on ticketing parked cars. His activities culminated in an action called "Day without Clamps," when volunteers warned drivers that they were parking in a place frequently patrolled by the municipal police. Česká Lípa officials complained that some comments were false and de facto libelous.[5] After Šiktanc refused to publish an apology, the municipal authority took him to court. In May 2013, a judge sentenced him to six months in prison, suspended for one year. He appealed against the decision[6] and continues to run the Facebook profile. No action has been made to remove it so far.

1 Vladimír Ševela, Facebook šíří nenávist a výzvy k vraždám. ‚Neporušuje zásady', Echo24.cz, June 5, 2014. http://echo24.cz/a/iJp5N/facebook-siri-nenavist-a-vyzvy-k-vrazdam-neporusuje-zasady
2 Reflex, "Požadujeme beztrestné vystřílení cikánů, hlásila facebooková skupina" (A Facebook Group Announced: We demand impunity for shooting of Gypsies), April 12, 2014.
3 Police of the Czech Republic: Extremism on the Internet, November 25, 2010, accessed January 23, 2014: http://www.mvcr.cz/clanek/projevy-extremismu-na-internetu.aspx
4 Facebook profile made by Šiktanc, accessed on January 21, 2014.
5 Jan Šebelka: Sentenced for criticizing the municipal police on Facebook, November 12, 2013, accessed December 29, 2013: http://liberec.idnes.cz/mestska-policie-siktanc-facebook-boticky-pomluva-soud-vypoved-p7h-/liberec-zpravy.aspx?c=A131112_084318_liberec-zpravy_ddt
6 Court hearing due in March 2015. See: http://liberec.idnes.cz/soud-s-karlem-siktancem-v-ceske-lipe-dbi-/liberec-zpravy.aspx?c=A141031_163836_liberec-zpravy_tm

the founding of, support for, or propagation of, movements aspiring to suppress human rights and freedoms; incitement of violence against individuals or social groups; or defamation of a nation, individual, or race. Any such published content must be removed. The state, and not private companies – such as Internet Service Providers (ISPs) – is the final arbiter of the legality of content posted online.

Generally speaking, the legislation applicable for print or broadcast media is valid also for online media. There are some specific laws regarding advertising, but the main legislation influencing freedom of expression on the Internet comprises laws on the right to privacy[7] and, as discussed above, the constitution.[8]

Most court cases involving free expression stem from individuals suing media outlets for breaching their privacy or for libel. To date, the major cases have concerned print publications. Since major media also operate online news portals, it is only a matter of time before such lawsuits extend to the online world.

The Right to Shock

In 2006, the financial news site Měšec.cz (www.mesec.cz) published an article on selling property without a broker. An online chat accompanied the article.[1] One user posted critical comments about a particular company, Prolux Consulting, using abusive language. The company deemed this discussion string libelous, and demanded its removal. The operator of the website refused. A municipal court in 2010, and later an appeals court in 2011, ruled that only one libelous statement (an insult) had to be removed.[2] The verdict cited a Constitutional Court resolution declaring that the right to freedom of speech applies to opinions that might be shocking, offending, or disturbing to a part of the population – provided that such opinions are made in good faith, can be explained in reasonable fashion, are in line with democratic principles, and do not violate the rights of others.[3]

1 Jan Zahradníček: Responsibility of ISPs comment to the Prolux case, accessed November 10, 2013: http://www.epravo.cz/top/clanky/odpovednost-poskytovatelu-sluzeb-informacni-spolecnosti-nekolik-postrehu-k-zaverum-vrchniho-soudu-v-praze-v-kauze-prolux-88471.html; Martin Janák: Responsibility of administrators for the content of online discussions, June 11, 2010, accessed October 24, 2013: http://www.lupa.cz/clanky/odpovednost-provozovatelu-portalu-za-diskuser/
2 Municipal court decision number 10 Cm 47/2009-39.
Appeals court decision number 3 Cmo 197/2010-82
3 Constitutional Court resolution II.US 76/2000

Balancing Freedom and Offensive Content

Some of the most controversial cases focused on online expression have revolved around allegedly extremist content in comments posted either in discussion forums or on news media sites. A recent court decision was interpreted to mean that private companies can be held responsible for the posting of such content if they could have done more to prevent it from being published.[9] In other words, sites won't be held accountable if they remove offensive content within a reasonable amount of time. In order to try to stem potentially illegal posts, the country's largest discussion forums now require commenters to register using at least an e-mail account.

If agreement cannot be reached between the disputing parties, the content is removed from the Internet based on a preliminary or final ruling. In the rare instances when the defendant does not comply, the relevant web hosting company might be required to remove the disputed content.

The liability of intermediaries is based on a European directive,[10] which has been incorporated into Czech legislation.[11] Accordingly, an ISP is not held liable for transmitted information as long as the ISP has not initiated the transfer of that data or selected

7 Act No 89/2012 Col., paragraphs 84 - 90, defining the rights to privacy, dignity, and honor.
8 Article 17.
9 Municipal court decision number 10 Cm 47/2009-39, Appeals court decision number 3 Cmo 197/2010-82.
10 European directive 2000/31/ES, on electronic commerce.
11 Act No. 480/2004 Col., on certain services of ICT companies.

the recipient, and – importantly – has not selected or modified the transferred information. Intermediaries providing data storage services are held responsible for the content only if they could have discovered the illegal nature of the users' behavior or of the stored data.[12] Intermediaries can be held responsible for the content if they were informed about the illegal aspect of the stored data and did not act accordingly to prevent further illegal activities.

BIG BROTHER

***5**/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.*

Online Surveillance Not Yet on Radar Screen

The Criminal Code[13] bans the promotion of any movement that tries to suppress human rights and freedoms, or proclaims racial, ethnic, national, religious, or class hatred. But no law exists in the Czech Republic that would specify particular types of websites or content to be blocked. The Code, and to some extent the constitution, defines illegal content. That content must then be removed, but only based on a court decision, which will always specify in what way the content is illegal and why it has to be taken down.

12 Martin Loučka: Analysis of the ISPs' responsibility for content, August 12, 2013, accessed November 27, 2013: http://www.lawportal.cz/rozbor-pripad-odpovednosti-provozovatele-diskuse-za-obsah-komentaru/
13 Act No. 40/2009 Col., the Criminal Code, Paragraphs 352, 353, 354, 355, 356, 403, 404, 405

Thus, the only "censorship" that exists concerns content deemed illegal according to the Criminal Code. Only the National Security Agency (NSA), citing national security concerns, may order the removal of content without a court decision, but there is no public record of this ever having happened to date.

The state-owned company providing telecommunications services (and later also Internet-related services) was privatized in 2005. Since then, there has been no direct state control over telecommunications services or the Internet. Three dominant ISPs cover the vast majority of the Czech market, either directly or indirectly through intermediaries. The Czech Telecommunications Office is the market regulator, issuing licenses for operators and overseeing competition. The state does not have a centralized telecommunications infrastructure that would allow for massive surveillance.

ISPs and telecoms operators are required to cooperate with the police, provided that there is a court order. Major ISPs are also required to provide the NSA's cybersecurity division with technical information regarding information transfer and the overall situation in Czech cyberspace. This activity is meant to prevent cyberattacks aimed at critical infrastructure systems.

No evidence has surfaced of government-initiated online surveillance in the Czech Republic or of steps taken to filter or block content by state authorities. According to the NSA, it does not monitor content.

Sex, Spies, and Wire-Taps

The surveillance of mobile text messages or emails is usually possible only with a court order, which must specify the range of the surveillance or data access. The only exception is granted to the Security Information Service (the BIS, the domestic intelligence service), which is answerable to the prime minister. Any evidence gained without a court order is inadmissible in court. Surveillance of websites or other online entities cannot be conducted in the Czech Republic outside of investigations into the origins of prohibited content, such as

child pornography. The supervision over court-authorized wiretapping and surveillance is in the hands of a parliamentary commission.

The special privileges accorded to the BIS have come into focus recently. The then head of the prime minister's office, Jana Nagyová, was accused of using Military Counterintelligence for surveillance of the then prime minister's wife; at the time, Nagyová was having an affair with the prime minister, Petr Nečas (after his divorce, he later married Nagyová, now Nečasová).[14] The case has already brought to light lapses in the BIS's supervision of Military Counterintelligence, which allegedly took actions that were not authorized and were therefore illegal.

Over the years, questions have been raised over the high level of police wiretapping in the Czech Republic,[15] which suggests that some form of online surveillance might be taking place. According to the Czech Ministry of the Interior, during 2012 the Czech police tapped the phone calls of almost 4,000 individuals; 4,258 individuals in 2013. But no evidence has yet been published to support the hypothesis that the authorities must be heavily monitoring online communications, as well.

ISPs and content providers can be required to cooperate with law enforcement bodies. If this cooperation contravenes other laws, such as the law on personal data protection, the police must present a detailed court order requiring cooperation from the ISP or content provider and stating what type of data should be provided.

Major telecommunications companies and ISPs are regarded as parts of the critical national infrastructure and are therefore required to report regularly to the authorities on the state of their systems and to share mainly technical information. This information does not include personal data or user-related data. For example, according to current legislation, the tracking of the geographical position of a user, together with his or her IP address, could be regarded as illegal because it might thereby be possible to identify the user.

To Block or Not to Block?

No Czech government statistics are available regarding content removal or the number of court decisions authorizing police to require certain information from private, Internet-related companies. The Czech Telecommunications Office keeps general statistics on content removal and localization requests, which are made public.[16] But the level of detail does not reveal, for instance, whether a request was related to specific information or to an entire email account. There have been very few reported cases of a public authority, individual, or legal entity exerting pressure on online sites to remove particular content. Where pressure has been exerted, the attempts were often followed by legal actions, as in the Česká Lípa case.

Unfortunately, there are no statistics regarding the removal of content in the private sector – apart from reports published by global companies such as Google or Facebook. The Google Transparency report report cites six court requests in 2012-2013 to take down 15 pieces of content of particular users.[17] A total of 75 percent of the requests were related to libel issues. Google complied with three requests. In 2013, Facebook received 25 official requests for data in the Czech Republic.[18] Requests were related to 32 user accounts in total. Facebook complied with almost 70 percent of the requests.

There are no laws that specifically address cyberattacks, although they could fall under laws protecting the property of companies and

14 For basic information see http://cs.wikipedia.org/wiki/Kauza_Nagyov%C3%A1
15 The analysis of wire tapping and surveillance made by Police for years 2010, 2011, 2012: http://www.mvcr.cz/soubor/analyza-odposlechu-a-zaznamu-pdf.aspx http://www.mvcr.cz/clanek/analyza-odposlechu-a-sledovani-osob-a-veci-dle-trestniho-radu-za-rok-2010.aspx http://www.mvcr.cz/clanek/analyza-odposlechu-a-sledovani-osob-a-veci-dle-trestniho-radu-za-rok-2011.aspx http://www.mvcr.cz/soubor/ppr-102-31-cj-2014-990390-analyza-odposlechu-a-sledovani-za-rok-2013-pdf.aspx

16 http://www.ctu.cz/aktuality/tiskove-zpravy.html?action=detail&ArticleId=11341
17 https://www.google.com/transparencyreport/removals/government/CZ/?metric=items&p=2011-12
18 https://www.google.cz/search?q=facebook+transparency+report+czech+republic&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:cs:official&client=firefox-a&channel=sb&gfe_rd=cr&ei=idGEU5_OKOqg8wfthoC4BQ

individuals or laws on terrorism. There have been few reported cyberattacks in the Czech Republic, but a recent case involved a Czech radio station whose website was targeted by a DDoS (distributed denial of service) attack and was inaccessible for several hours. The radio IT staffers were not able to solve the problem on their own, and asked for help from the National Security Agency.[19] The perpetrators were not found.

19 National Security Agency is responsible for the cybersecurity based on the resolution of the government number 781 from 19th October 2011.

Pride in Brno

In 2010, the municipal authority in Brno, the country's second largest city, launched a campaign to promote the city and civic pride under the slogan "Žít Brno" (Living Brno). Unfortunately, the authorities forgot to register the web domain, and in 2011 a local journalist registered the site (http://www.zitbrno.cz/) and began posting satirical texts.[1]

The website became popular, especially among younger people, reaching more than 50,000 views each month, and Žít Brno was soon transformed into a political initiative in opposition to the presiding municipal authority. A Facebook profile was added as another communication channel. In February 2014, the municipal authority asked Facebook to remove the profile, arguing it violated trademark property rights.[2] Facebook promptly removed the profile (which remains down). The initiative deemed that move an act of censorship and immediately established a new Facebook profile.[3] Žít Brno did surprisingly well in the municipal elections of October 2014 and entered into a coalition government to run the city.

1 Description and history of the ZitBrno initiative: http://cs.wikipedia.org/wiki/%C5%BD%C3%ADt_Brno#cite_note-respekt2011-44-2
2 Tomáš Trnka: Mayor confirms to initiate the removal of Zít Brno profile from Facebook, February 15, 2014, accessed February 18, 2014: http://www.lidovky.cz/primator-onderka-potvrdil-ze-profil-zit-brno-prikazal-smazat-on-sam-1gz-/zpravy-domov.aspx?c=A140215_115611_ln_domov_ttr#utm_source=clanek.lidovky&utm_medium=text&utm_campaign=a-souvisejici.clanky.clicks
3 https://www.facebook.com/ZitBrnoRIP/info

Respect for Net Neutrality

There have been no reported instances of ISPs violating the "net neutrality" principle based on content or source of content.

With regards to the transformation of Internet governance, the Czech Republic supports the multistakeholder principle to avoid any potential attempts to influence content and suppress human rights online, especially freedom of speech. This approach was reaffirmed, for example, when the Czech Republic opposed efforts to impose government controls on the Internet at the International Telecommunication Union summit in Dubai in December 2012.[20]

LEGAL MAZE

***3**/5: Transparency of legal proc-edures and appeals mechanisms*
***3**/5: Copyright laws, fair use – laws and practice*

Who Regulates the Internet?

Czech legislation addresses many Internet-related issues only indirectly, and only a few laws specifically address particular aspects of online activity. As there is usually no readily applicable law, judges must apply general legal principles, sometimes without really understanding the particularities of the Internet. This may lead to discrepancies when in similar cases judges decide differently. In addition, it will take several years before ambiguities are resolved in the new Civil Code that entered into force in January 2014. Certain changes in the Civil Code might indirectly influence the legal approach toward online content by, for example, introducing a new online form of agreement between commercial parties, stating what information has to be available in regards to online shopping and service provision.

20 http://www.mpo.cz/dokument118667.html

There is no independent body such as an ombudsman supervising the Internet in the Czech Republic. Such an office exists in the Czech parliamentary system, but the ombudsman's tasks are more general and the office's powers are limited. The ombudsman can, however, theoretically intervene in the case of unfair or illegal actions taken by a public authority in an Internet-related case.

Based on a national strategy to improve Czech cybersecurity, in 2011 the NSA was given the responsibility of overseeing the online sphere. A special office in the NSA was established to monitor developments in Czech cyberspace, and a national Computer Security Incident Response Team (CSIRT) was created. Nevertheless, the NSA states that it does not scan or monitor the content of particular web pages, and no evidence has surfaced to prove otherwise.

Apart from the NSA, the Czech Telecommunications Office is responsible for supervising the telecommunications industry. Since all major ISPs are active on the telecommunications market, they are partially affected by this office's actions. But the Czech Telecommunications Office is not focused on supervising online content.

The country's broadcasting regulator is the Council for Radio and Television Broadcasting. The appearance of online channels and broadcasting on the Czech Internet raised questions about regulation. Moreover, the regulation of online media was addressed by an EU directive,[21] and therefore had to be incorporated into Czech legislation. The original draft of the new law would have given the regulator wide authority over online content, but it was still unclear whether the regulator would have been the Council for Radio and Television Broadcasting or the Czech Telecommunications Office.

The discussion resulted in a new law[22] giving the authority over online broadcasting to the Council for Radio and Television Broadcasting, but its authority covers only services that can be defined as online television. If the service does not resemble television broadcasting or does not have any commercial aspect, then it does not fall under this regulation. But the discussion about supervision continues – both about the possible role of the Czech Telecommunications Office and about the force of the supervision.

Political influence on such oversight bodies cannot be excluded completely, although there have been no suspicious decisions or reports of activity by the NSA's specialized cybersecurity office that would suggest politicization.

ISPs founded the civic society CZ.NIC in 1998,[23] mainly to run the register of .cz domain names. The society also operates a national CSIRT (Computer Security Incident Response Team) and has other tasks regarding the integrity of the Czech Internet, but it is not a true self-regulatory body.

The Copyright Conundrum

Enforcement of intellectual property rights and copyright related to online content (including movies or even software) is slowly improving. Twenty years ago, even mid-sized companies in the Czech Republic were using illegal copies of software, and there was little regard for intellectual property rights online. That is changing, partially thanks to more sophisticated protection of assets as well as through anti-piracy educational efforts. In addition, movies and other online content are now more affordable than at the beginning of the Internet era in the Czech Republic, so the risk of prosecution increasingly outweighs potential profits from piracy. An important step in greater online copyright protection has been the judiciary's interpretation of the law that a company may be prosecuted for hosting illegal content if the host could reasonably have found out that posting the content infringed the law.[24]

A more serious hurdle than any gaps in legislation related to Internet freedom is the enforceability

21 Directive of the European Parliament and Council number 2007/65/ES
22 Act No. 132/2010 Col., the act on audiovisual media services on demand and on adjustment of certain laws

23 Basic information on CZ.NIC: http://www.nic.cz/page/351/
24 Act No. 480/2004 Col., on certain services of ICT companies.

Whose Song Is It Anyway?

Josef Štěpánek, an amateur musician, posted several cover versions of the songs of folk singer Karel Kryl on YouTube in 2013.[1] Soon after, one of these songs was taken down based on a report from a third party (according to published information it was OSA (Ochranný svaz autorský pro práva k dílům hudebním), a Czech organization that protects authors' rights for musical works. Štěpánek then had the option of protesting the decision through the submission of a complex application form. He contacted OSA and found out that cover versions in general do not violate any ownership rights, a principle also supported by an existing agreement between Google and OSA.

Armed by this reassurance by OSA, Štěpánek protested against the content removal. YouTube subsequently made the content available again. For some, the case illustrated the apparent ease in which content can be taken down without a proper investigation of the legality of the content, where the burden of proof was then placed on the "defendant" rather than the organization making the claim.

1 http://josefstepanek.cz/3693/jak-mi-z-youtube-smazali-idylu-aneb-cover-verze-a-osa.html

of the law and the length of proceedings. The average length of a trial in a civil case in 2012 was 356 days in district courts and 510 days in regional courts. The speed of justice thus lags far behind the speed of developments in the online world. Therefore, it can be less costly for companies to make concessions than to risk lengthy legal procedures.

Official sites provide information during major crises such as floods, and their content can be shared if referenced properly. While online information channels are becoming increasingly important, during times of crisis they are not regarded as the primary source of information, particularly among the older generation.

Plans are underway to improve the use of collected data. Information about public transport schedules collected by the municipal authority or responsible company is partially owned by the state or local municipality, but certain information such as maps and schedules collected by state authorities or state-related enterprises will now be made accessible to anyone. On the other hand, the Czech Statistical Office has always made all statistics freely available online. There are also open-source projects run by nongovernmental organizations collecting, analyzing, and publicizing certain data, such as maps of police activity.

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 Good News

For the most part, the government, parliament, and other public institutions fulfil their legal obligations under freedom-of-information legislation to make the required information accessible to the public, either online or directly in response to inquiries. The law granting the right of access to information stipulates that the information should be provided within 15 days, a period that can be extended by 10 days if cooperation with other offices is needed. The law states that the requestor may be required to pay search costs.[25]

25 Act No. 106/ 1999 Col., law on the free access to information.

Although only a minority of relevant laws relate explicitly to the Internet, the websites of public institutions have become de facto noticeboards with the corresponding legal responsibilities. Online access to transcripts, records, or documents from the lower house of parliament, the Senate, and the government is generally well-managed; the same is true for information on court cases. Recent e-government initiatives have also improved the situation, as the authorities have released a great deal of information online – above and beyond their legal obligations.

Political parties are obliged by law to submit to parliament their annual financial reports, which are made public and readily accessible but not necessary online. Parties also often publish such information online on their websites, even though the law does not expressly require them to do so.

Influenced by the EU harmonization process, the personal data protection law[26] grants individuals the right to know what information the public authorities (and private companies) keep about them – if the release of such information does not violate any other laws (e.g. in the case of classified information or police investigations).

The Bad News

Despite this indisputable progress, too many gray areas still exist that allow public authorities to invoke different laws as an excuse for not publishing information. Authorities, for example, have withheld details about the winning bid in a public tender under a commercial confidentiality exemption, or refused to publish the salaries of public employees, claiming that this would violate the law on privacy of personal data.

Politicians have also resisted calls for the establishment of a register of all contracts paid from public budgets. The adoption of legislation to establish such a register (neighboring Slovakia passed such a law in 2011) is one of the main priorities of the civil society watchdog group *Rekonstrukce státu* (Reconstruction of the State),[27] which argues that publication in the register would reduce corruption in public tenders.

Experts call for such loopholes to be closed, and for more supervision and enforcement of existing regulations. Much still hinges on individual officials' readiness to respond to freedom-of-information requests. Such willingness is generally quite low owing to the lack of personal accountability. There is no mechanism to prevent officials or institutions from repeatedly violating the law and, even if an institution is penalized for not following the law, no one is held individually responsible. If personal data (such as salaries of public employees) is exempt from publication, this should be explicitly stipulated in law,[28] activists contend. Even when reams of data are made available online, the format is often poorly structured or unsearchable (e.g. scanned documents) so that users face considerable hurdles to finding what they want.

Such problems also exist on the local level. There have been cases when local authorities denied access to information, refused to publish it, or simply neglected their duties.

Areas for Improvement

The case backlog in the Czech legal system is a priority for action, not least because it deters many from taking a state institution to court for refusing to provide information. That can happen only after the direct supervisory body presiding over the institution also rejects the request for information. Any challenge to such a refusal can take many years to resolve, discouraging journalists or other citizens from seeking information in the first place.
The recent European Public Sector Information Platform Report applauded the Czech Republic

26 Act No. 101/2000 Col., the personal data protection law.

27 http://www.rekonstrukcestatu.cz/en

28 Radek Kedroň, Hradní kancelář znovu tají platy Hájka a Jakla. Kolik dostali na odchodnou? (Prague Castle Hides Salaries of Hájek and Jakl again. How Much Was their Farewell Pay Packet?), April 10, 2013, accessed November 14, 2013: http://www.lidovky.cz/hradni-kancelar-znovu-taji-platy-hajka-a-jakla-kolik-dostali-na-odchodnou-143-/zpravy-domov.aspx?c=A130409_191335_ln_domov_hm

for joining the Open Government Partnership in 2011 and highlighted important progress since then. The authors of the report pointed out areas for improvement, including the publication of "high-priority" datasets, a better communications strategy, and standardization across public sector bodies.[29]

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?*

29 European Public Sector Information Platform. Topic Report No. 2014/03, Open data and PSI in the Czech Republic. www.epsiplatform.eu/sites/default/files/2014-03-Open_Data_CzechRepublic2.pdf

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.

pasos
Policy Association for an Open Society

SEAL OF POLICY EXCELLENCE

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.

Asociace pro mezinárodní otázky
Association for International Affairs

pasos
Policy Association for an Open Society

TOL

The Association for International Affairs (AMO), Prague, is a leading independent foreign policy think-tank in the Czech Republic.

Association for International Affairs
Žitná 608/27, 110 00 Praha 1, Czech Republic
Tel +420 224 813 460
Email: info@amo.cz
www.amo.cz

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
www.tol.org