GLOBAL INFORMATION SOCIETY WATCH 2011

INTERNET RIGHTS AND DEMOCRATISATION

Focus on freedom of expression and association online

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

This edition of Global Information Society Watch is dedicated to the people of the Arab revolutions whose courage in the face of violence and repression reminded the world that people working together for change have the power to claim the rights they are entitled to.

Printed in Goa, India
by Dog Ears Books & Printing

Global Information Society Watch
Published by APC and Hivos
South Africa
2011

ISSN: 2225-4625
APC-201111-CIPP-R-EN-PDF-0105
ISBN: 978-92-95096-14-1

APC and Hivos would like to thank the Swedish International Cooperation Agency (Sida) for its support for Global Information Society Watch 2011.

Sida

SWITZERLAND

SURVEILLANCE AND SECURITY MANIA VIOLATING BASIC RIGHTS

Comunica-ch
Wolf Ludwig
www.comunica-ch.net

Introduction

Switzerland is generally not perceived as a country conflicting with international human rights standards. According to United Nations (UN) reports and other specialised human rights sources, basic rights like freedom of speech and association and the right of access to information are normally granted. Problem areas, with obvious deficits and demands for improvement, are the rights of asylum seekers, migrants or religious minorities such as Muslims living in the country.[1] In the 2010 World Press Freedom Index published by Reporters Without Borders, Switzerland again shares first place with a number of Nordic countries: "These six countries set an example in the way they respect journalists and news media and protect them from judicial abuse."[2]

But in the context of digital access rights, Switzerland is still not at the forefront compared to Nordic countries like Finland. And issues of privacy, amongst other concerns, have been raised regarding new surveillance regulations that are part of national security and telecommunication laws. As in other countries, widespread security considerations – mostly referring to terrorist threats or child pornography – are increasingly threatening and undermining the principles of access and openness, as well as civil rights.

Policy and political background

Most attempts to revise legal instruments and laws in Switzerland have been strongly disputed and criticised in the last years. Even if "most internet users are concerned about security," according to a 2010 survey on internet use conducted by the Federal Statistical Office (FSO), the proposed law revisions seem to be inappropriate and do not find approval from civil society organisations and the business sector.[3]

The proposed revision of the Federal Act on Measures for Safeguarding National Security (BWIS)[4] wants to introduce new preventive security measures, but was rejected by Parliament in spring 2009. One of the main concerns is the suggested surveillance of non-public spaces. From a human rights viewpoint, a thorough assessment of legally protected interests as well as of the concept of freedom versus security is needed.[5] The process of revision is still ongoing and will not be completed until the end of 2012.

Another law that is strongly contested is the Revision of the Federal Act on the Surveillance of Post and Telecommunications (BÜPF). The Federal Department of Justice and Police argues that the act "needs to be adapted to new technological developments, including the Internet" and related communication tools.[6] In the BÜPF consultation, from May to September 2010, the official language sounds merely technical, and avoids stating any political implications. Government officials just promise: "Not more but better surveillance."[7]

1 UN Committee on Economic, Social and Cultural Rights, Concluding observations of the Committee on Economic, Social and Cultural Rights, Switzerland, 26 November 2010; UN Human Rights Committee, Concluding observations of the Human Rights Committee, Switzerland, 3 November 2009. www.unhcr.org/refworld/country,,HRC,,CHE,4562d8b62,4afbda552,0.html; Internet should remain as open as possible – UN expert on freedom of expression, Press Releases, Special Rapporteur on freedom of expression, June 2011. www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=11108&LangID=E

2 Reporters without Borders (2010) 2010 World Press Freedom Index. www.reporter-ohne-grenzen.de/fileadmin/rte/docs/2010/101019_Europa_GB.pdf

3 Omnibus 2010 Survey on Internet Use conducted by the Federal Statistical Office (FSO), February 2011. www.admin.ch/aktuell/00089/index.html?lang=en&msg-id=37540

4 Please note that English is not an official language of the Swiss Confederation. The legal and other translations provided here are not necessarily "official" translations and therefore have no legal force.

5 Zusatzbotschaft und Entwurf für die Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit, press release, October 2010. www.vbs.admin.ch/internet/vbs/de/home/documentation/news/news_detail.35915.nsb.html; Staatsschutz in Lightversion – Wichtige Punkte werden später geregelt, humanrights, Focus Switzerland (Update: 08.11.2010). www.humanrights.ch/de/Schweiz/Inneres/Person/Sicherheit/idart_8257-content.html?zur=827

6 „Ablehnende Stellungnahme zum Entwurf BWIS II", press release, 29 September 2006. www.humanrights.ch/de/Schweiz/Inneres/Person/Sicherheit/idart_4576-content.html

7 Überwachung des Fernmeldeverkehrs an die technische Entwicklung anpassen, Vernehmlassung zur Änderung des BÜPF eröffnet, press release EJPD, 19 May 2010. www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2010/2010-05-19.html

Broad-scale surveillance widely contested

Over the last years the legal instruments and options to increase state surveillance were systematically extended in Switzerland – by the two legislative revisions mentioned, and through other laws still pending. The official tapping of phone lines and computers, wiretapping of private spaces or the use of other surveillance methods are, according to various civil and human rights organisations and networks, "violating several basic rights granted by the constitution and are not appropriate under rule of law considerations."[8] A spokesperson for the Swiss Pirate Party recently said: "[There] are many little steps that we accept in the name of security. But suddenly we have a surveillance state."[9]

State security forces are permitted to stake out people in public and generally accessible spaces, including using cameras and bugging devices. But the private sphere has been legally protected since the Secret Files Scandal which shocked the public in 1989.[10] Following this, the Federal Court affirmed that measures by security forces interfering in the private sphere needed a judicial writ.[11]

According to the proposed BÜPF law, internet service providers (ISPs) are forced to upgrade their surveillance and storage capacities to completely control broadband internet communication – in real time. This enables a systematic surveillance of any surfing behaviour of internet users in the country. The technology and devices for surveillance upgrades on behalf of state security must be paid for by the service providers themselves. According to some, the cost could amount to anything from half a million to more than one million Swiss francs, depending on the size of the access provider. The usual compensation for these sorts of collaborative efforts and services will not be given under the new law. Observers predict that most of the 650 ISPs in Switzerland will not be able to afford costly upgrades like this and – except for the bigger market players – will have to close down.[12]

Federal department pushed to explain

In the first round of the usual consultations on new laws[13] between May and September 2010 the proposed BÜPF revisions were harshly criticised by most stakeholders from the business sector and civil society. The strongest concern was raised about the intended installation of Trojan horses on computers of suspects and the lengthening of the current data retention period from six to twelve months. (Under the contested data retention rules, ISPs are obliged to store comprehensive customer data to be delivered to security forces on demand). Another bone of contention is a new broad definition of "access providers", including all sorts of internet-related services. The broad resistance from various parts of society – including the right-wing Swiss Peoples Party (SVP/UDC), usually at the law and order front – caused some delays in the legislative procedure and pushed the Federal Department of Justice and Police into a crisis where they needed to explain their motives. Since the end of the consultation period, almost a year ago, there has been a remarkable silence.

Until recently: in early June 2011, the Federal Department of Justice and Police launched another consultation regarding a part-revision of the Ordinance on the Surveillance of Post and Telecommunications (VÜPF).[14] Observers are surprised that the Ordinance suddenly needs to be revised before the respective federal law (BÜPF) is passed – it normally happens the other way round. One of the official arguments for the hurry is that the Ordinance will allow Switzerland to sign the Council of Europe's Cybercrime Convention at the beginning of 2012. But critics surmise that an accelerated revision of the Ordinance may circumvent the legislative power of the Parliament without creating the required legislative basis for any new surveillance laws. And the recent VÜPF proposal still includes many of the strongly contested measures from the BÜPF: comprehensive state surveillance of internet traffic, lacking limits of monitoring options and areas, as well as too vaguely defined legitimate targets for surveillance (not only very serious crime or terrorism, as some suggest). The protection of privacy has also not been considered properly.[15] This has pushed some in the Swiss media to ask for a "pause for reflection."[16]

8 „Ablehnende Stellungnahme zum Entwurf BWIS II", press release, 29 September 2006. www.humanrights.ch/de/Schweiz/Inneres/Person/Sicherheit/idart_4576-content.html

9 „Überwachungswahn der Beamten in Bern", Tagesanzeiger, 19 August 2010. www.tagesanzeiger.ch/digital/internet/berwachungswahn-der-Beamten-in-Bern/story/12403271

10 Wikipedia, Secret Files Scandal. en.wikipedia.org/wiki/Secret_files_scandal

11 „Unter Druck der Amerikaner", Interview „Der Bund", April 2006. www.humanrights.ch/upload/pdf/060218_bund_staatsschutz_weber.pdf

12 Spitzel im Netz, Handelszeitung, 14 July 2011. www.handelszeitung.ch/unternehmen/spitzel-im-netz

13 Vernehmlassungen, Swiss Confederation website. www.admin.ch/dokumentation/gesetz/pc/index.html?lang=de

14 Revision des BÜPF und der VÜPF, Federal Department of Justice and Police website, August 2011. www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/info/2011/2011-08-120.html

15 Spitzel im Netz, Handelszeitung, 14 July 2011. www.handelszeitung.ch/unternehmen/spitzel-im-netz

16 Überwachung, Eine Denkpause ist nötig, Handelszeitung, 14 July 2011 (not available online).

Substantial privacy concerns

In his proposal regarding the BÜPF revision, the Federal Data Protection and Information Commissioner (FDPIC) found fault with the "too openly defined field of application of the law." Furthermore, the FDPIC considers the intended catalogue of criminal offences, in the Code of Criminal Procedure (StPO), as "too comprehensive regarding the placement of Trojan horses on computers and smartphones" because this offers "massive interference with the private life of people concerned." Besides telecommunications, all data on the computer, including private and personal data, can be monitored after the installation of the surveillance programmes. These concerns were not taken into consideration in the BÜPF consultation draft.

The draft law provides access to the information of monitored persons but not for their spouses or communication partners who are not part of the criminal procedure, but were affected by the surveillance and data storage. In his statement the Commissioner further referred to the German Constitutional Court judgement that data retention should be allowed only under certain conditions. In view of this, the planned prolongation of the data retention period to twelve months in Switzerland should be reassessed under aspects of proportionality.[17] According to other official sources, such as the Federal Department of Justice and Police, around 50 internet surveillances have been conducted against criminal organisations (involved in crimes such as blackmailing and money laundering) over the last years.[18] This figure does not offer much evidence for the state's demand for the widespread upgrade of surveillance capacities of Swiss access providers.

The biggest player on the Swiss telecom market, Swisscom and its competitor Sunrise, recently successfully sued the Federal Department of Justice and Police. In its verdict the Federal Administration Court approved the refusal of the two telecom providers to monitor the mobile internet traffic of suspects in police investigations. Costly investments in special devices would be needed for this purpose. And the provisions in law for such forced investments are missing. How the internet may be monitored is also not specified in the draft law nor in the Ordinance. The state ordering the surveillance was therefore judged "unlawful".[19]

Since the revelation of a second Secret Files Scandal in summer 2010, and similar incidents, the confidence of the public in security forces has notably decreased. A Swiss daily paper, under the headline "The Secret Files Scandal – a story of lies and deception", said the recent scandal is "not only a story of over-zealous spies and sluggish controllers but a chronicle of lies and deception – from the secret service up to the Federal Council." Regarding the continuous revision of the Federal Act on Measures for Safeguarding National Security (BWIS), a parliamentarian and member of the Social Democratic Party announced that "our side will only give hand to it [support the new legislation], if strong control mechanisms are granted."[20] Until now security matters are usually ab/used to increase the power and impact of secret and security services and law enforcement agencies.

Conclusions: A question of credibility and proportionality

As in other European countries, state security and cyber crime continue to be raised as worrying issues in the media and in public opinion. Any social or security issue, such as child pornography or paedophilia, the lack of privacy awareness among social networks users, or other current irritations and abuses in the digital age, give ground to the proponents of all sorts of new laws and protections, and to those who argue for more power and control of society by security forces.

Generally, human and civil rights concerns are raised by the usual suspects, such as civil society organisations, trade unions and left-wing parties, and do not find much support in other political circles. In the case of the BÜPF and VÜPF revisions, a broad alliance of different stakeholders in Swiss society has already shown resistance against the new surveillance laws. The row of unusual suspects ranges from access providers, various business associations and the right-wing Swiss People's Party (the Christian Democratic People's Party and the Liberal Party announced themselves indifferent in this matter). Swiss telecom and access providers almost unanimously refuse to be (mis)used as deputy sheriffs for state prosecutions. This broad political concern and alliance offer reason for hope that the planned surveillance act may not be applied.

17 FDPIC proposal on the revision of the BÜPF, 18th Annual Report 2010-11, point 1.4.9, June 2011. www.edoeb.admin.ch/dokumentation/00445/00509/01732/01753/index.html?lang=de

18 Swisscom kritisiert Schnüffelaufträge, Handelszeitung, 13 July 2011. www.handelszeitung.ch/unternehmen/swisscom-kritisiert-schnueffelauftraege

19 Swisscom kritisiert Schnüffelaufträge, Handelszeitung, 13 July 2011. www.handelszeitung.ch/unternehmen/swisscom-kritisiert-schnueffelauftraege

20 Die Fichenaffäre – eine Geschichte von Lug und Trug, Tagesanzeiger, 5 July 2010. www.tagesanzeiger.ch/schweiz/standard/Die-Fichen affaere--eine-Geschichte-von-Lug-und-Trug/story/16223362

The analysis of the Swiss human and civil rights situation in the information society shows that the country may be among the best candidates in terms of freedom of expression and access and openness principles, but that all sorts of security concerns systematically violate basic citizen rights – as in many other European countries where human rights are said to be fundamental and respected.

Action steps

- If the BÜPF should pass the legislative chambers, civil society networks and business associations may consider calling for a referendum to stop this law, in line with the Swiss tradition of direct democracy. The chances for success are not evident, even considering a broader political alliance, but it will prolong the public discourse on state surveillance and security measures undermining fundamental rights.
- Strengthen parliamentarian and public control over any new security and surveillance laws including ordinances.
- Establish an independent national human rights institution that complies with the principles relating to the status of national institutions for the promotion and protection of human rights (Paris Principles and Recommendation 6, UN Committee on Economic, Social and Cultural Rights).
- Provide more human rights education to parliamentarians (in line with Recommendation 21, UN Committee on Economic, Social and Cultural Rights).
- Expunge Article 293 of the Swiss Criminal Code which threatens media and other people with punishment when quoting official sources defined as "confidential" and in doing so contradicts the Federal Open Government Act. ■

Links of stakeholders – civil society and business actors

Humanrights.ch (MERS), Focus Switzerland
www.humanrights.ch/de/Schweiz/Inneres/Person/Sicherheit/index.html

Amnesty International, Swiss section
www.amnesty.ch/en?set_language=en&cl=en

Grundrechte.ch www.grundrechte.ch

Demokratische Juristinnen und Juristen der Schweiz
www.djs-jds.ch

Swiss Privacy Foundation www.privacyfoundation.ch

Digitale Gesellschaft www.digitale-gesellschaft.ch

Digitale Allmend blog.allmend.ch

Swiss Internet User Group (SIUG) www.siug.ch

ICT Switzerland www.ictswitzerland.ch

Information Security Society Switzerland (ISSS)
www.isss.ch

Swiss Telecommunications Association (asut)
www.asut.ch/content/content_renderer.php

GLOBAL INFORMATION SOCIETY WATCH 2011

In the year of the Arab uprisings **GLOBAL INFORMATION SOCIETY WATCH 2011** investigates how governments and internet and mobile phone companies are trying to restrict freedom online – and how citizens are responding to this using the very same technologies.

Everyone is familiar with the stories of Egypt and Tunisia. **GISWATCH** authors tell these and other lesser-known stories from more than 60 countries. Stories about:

PRISON CONDITIONS IN ARGENTINA Prisoners are using the internet to protest living conditions and demand respect for their rights.

TORTURE IN INDONESIA The torture of two West Papuan farmers was recorded on a mobile phone and leaked to the internet. The video spread to well-known human rights sites sparking public outrage and a formal investigation by the authorities.

THE TSUNAMI IN JAPAN Citizens used social media to share actionable information during the devastating tsunami, and in the aftermath online discussions contradicted misleading reports coming from state authorities.

GISWATCH also includes thematic reports and an introduction from Frank La Rue, UN special rapporteur.

GISWATCH 2011 is the fifth in a series of yearly reports that critically cover the state of the information society from the perspectives of civil society organisations across the world.

GISWATCH is a joint initiative of the Association for Progressive Communications (APC) and the Humanist Institute for Cooperation with Developing Countries (Hivos).

GLOBAL INFORMATION SOCIETY WATCH
2011 Report
www.GISWatch.org

ISBN 978-92-95096-13-4
9 789295 096134

APC

HIVOS