

GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

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



ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (APC)
AND HUMANIST INSTITUTE FOR COOPERATION WITH DEVELOPING COUNTRIES (Hivos)

ISBN: 978-92-95102-16-3

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

Creative Commons Attribution 3.0 Licence <creativecommons.org/licenses/by-nc/3.0/>

SWITZERLAND

“All eyes on you”



Communica-ch

Wolf Ludwig

www.comunica-ch.net

Introduction

As in various neighbouring countries, the Snowden revelations in early June 2013 caused increasing awareness and concerns in Switzerland about “Big Brother watching you” and surveillance by state authorities. While related discussions have been limited to few and informed circles in the country so far, the revelations have set a new landmark, with public opinion drifting somewhere between overload and resignation. However, the still ongoing revision of the Swiss Federal Act on the Surveillance of Post and Telecommunications (BÜPF) – a long-standing process – has gained broader public attention now and is more contested than ever before (see the Swiss country report from GISWatch 2011).¹ As in surrounding countries, widespread security considerations – mostly referring to terrorist threats or child pornography – are increasingly threatening and undermining principles of access and openness, as well as civil rights. Over the years, starting in May 2010, the federal government (Bundesrat) and its justice and police department are relentlessly pointing to the necessity of new technical means to combat crime and enhance law enforcement.² Such means, like Trojan horses on computers of suspects and the prolongation of the current data retention period from six to 12 months, are sold as “technological upgrades”, while providing “not more, but better surveillance”.

Policy and political background

In the first round of the usual consultations on new laws between May and September 2010, the suggested 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 prolongation of the current data retention period from six to 12 months. Under the contested data retention rules, internet service providers (ISPs) are obliged to store comprehensive customer data to be delivered to security forces on demand. Another bone of contention, besides privacy concerns, was 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 pulled the Federal Department of Justice and Police into a crisis of needing to explain its position.³ A year later, in November 2011, the Federal Council announced a revised version of the Ordinance on the Surveillance of Post and Telecommunications (VÜPF), which was to come into effect in January 2012. With the revised VÜPF, the government cunningly bypassed the contested BÜPF by introducing new surveillance measures at the ordinance level – such as prescriptions for telecom and service providers to monitor mobile and internet traffic.⁴

The BÜPF: Extending surveillance

At the time, critics surmised that this accelerated revision of the Ordinance actually circumvented the legislative power of the parliament, without creating the required legislative basis for any new surveillance laws by simply creating precedents. The Ordinance’s field of application was adjusted by including internet access providers alongside their telecom equivalents. These providers are obliged to secure infrastructure to facilitate surveillance and to implement new surveillance measures either by themselves or to task a third party to do this. Internet access providers were given a reprieve of 12 months for implementation.

1 Ludwig, W. (2011). Switzerland: Surveillance and security mania violating basic rights. In APC and Hivos, *Global Information Society Watch 2011: Internet rights and democratisation*. www.giswatch.org/en/country-report/freedom-expression/switzerland

2 Bundesamt für Justiz, Überwachung des Fernmeldeverkehrs, Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). www.ejpd.admin.ch/content/ejpd/de/home/themen/sicherheit/ref_gesetzgebung/ref_fernmeldeueberwachung.html

3 Ludwig, W. (2011). Op. cit.

4 Bundesamt für Justiz, Post- und Fernmeldeüberwachung: Klare und restriktive Rechtsgrundlagen, press release, November 2011. www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2011/2011-11-23.html

With the revised VÜPF the government announced an overhauled schedule for the ongoing revision of the BÜPF.⁵ Two years later, in February 2013, the Federal Council submitted its Memorandum (Botschaft) to the parliament regarding the BÜPF – a usual legislative procedure in the country. The purpose of the revision would be “to provide a clear and restrictive legal basis” for law enforcement and the use of GovWare for criminal procedures. This special software is used by police to monitor communication data such as sender, recipient, date, duration and ways of communication.

On the other hand, the new law did not allow the online investigations of computers or surveillance of spaces using cameras and microphones from infiltrated computers. The use of GovWare was supposed to be limited to “hard crimes” only, which justified covert investigations.

The government insisted on the prolongation of data retention from six to 12 months. According to the new law, surveillance by law enforcement bodies cannot be done in a preventive manner but only in the course of a criminal procedure. It must be ordered by public prosecutors and approved by court decision. Suspects may object to surveillance – if or whenever they get to know about it.

Compared to the VÜPF, the field of application in the revised BÜPF will be considerably extended: from telecom and internet access providers to service and hosting providers, chat forums and platforms, as well as all forms of other networks like hotels, hospitals, universities, public libraries and schools.⁶

Besides some modifications to the first contested draft (May 2010), its new version appears to various stakeholders like new wine in old wineskins – basically sticking to new surveillance techniques undermining civil rights and liberties. Critical voices did not become silent: in February 2014, Digital Society Switzerland, a small but active group specialised in net policy, together with six other civil society groupings including Member of Parliament Balthasar Glättli (Green Party), launched a complaint against data retention in Switzerland. The federal office in charge, the Service for Surveillance of Post and Telecommunication Traffic (ÜPF), rejected the complaint – as expected – by arguing that “high legal barriers would protect fundamental rights.” The complainants appealed to the Federal

Administrative Court.⁷ Meanwhile, in April 2014, the European Court of Justice (ECJ) declared the Data Retention Directive of the European Union “invalid” – a landmark ruling for many civil liberties groups all over Europe.⁸ The ECJ is backing key arguments of the Swiss complainants that existing practices for data retention “exceeded the limits imposed by compliance with the principle of proportionality” and calling it “a wide-ranging and particularly serious interference with the fundamental rights of respect for private life and of the protection of personal data.”⁹

Despite this revealing court ruling and broad opposition, the Swiss government and authorities drift between being unimpressed and stubborn. In March this year – just before the verdict – the Second Chamber of the Swiss Parliament (Ständerat), representing the cantons, gave its blessing to the BÜPF: 94% of the council’s members voted in favour, with only two votes against and four abstentions. Even some Ständeräte who had doubts caved in. Alexis Roussel, president of the Swiss Pirate Party, criticised the decision by concluding: “The Ständerat didn’t learn anything from the Snowden revelations.”¹⁰

Freedom or security – a common dilemma

However, parties and stakeholders opposing the planned BÜPF revision are broader than before. While most of the political parties (except the Greens) and the country’s political establishment of parliamentarians and party leaders support the new law or are indifferent at least, most of the party youngsters from all political spectrums have changed sides and joined the increasing ranks of opposition. Summer 2014 somehow looked like a showdown: at the end of May Switzerland saw its first net-political demonstration in front of the Federal Parliament in Bern, where several hundreds of people – digital natives mostly – expressed their common concerns against the BÜPF. They were supported by representatives from major business associations in the telecom and internet industry. Speakers from Asut, the Swiss Telecommunications Association, and Swico, the Association of ICT enterprises, besides others, expressed strong

5 Ibid.

6 Bundesamt für Justiz, Post- und Fernmeldeüberwachung: Klare und restriktive Rechtsgrundlagen, press release, February 2013. www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2013/2013-02-271.html

7 Steiger Legal, Urteil pro Vorratsdatenspeicherung in der Schweiz, July 2014. <https://www.steigerlegal.ch/2014/07/01/urteil-pro-vorratsdatenspeicherung-in-der-schweiz>

8 Court of Justice of the European Union, The Court of Justice declares the Data Retention Directive to be invalid, press release No 54/14, April 2014, curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

9 See footnote 7.

10 Ständerat segnet BÜPF-Revision ab, Computerworld.ch, March 2014. www.computerworld.ch/news/it-branche/artikel/staenderat-segnet-buepf-revision-ab-65429

reservations. Jean-Marc Hensch (Swico) welcomed the demonstrators: “Dear potential criminals, dear possible suspects” – referring to broad-scale surveillance and the storage of personal data without concrete facts supporting suspicion of a crime.¹¹ A speaker from the young social democrats (Juso) accused the Federal Council and his party elders of “historical amnesia”, pointing to the revelations of the second Secret Files Scandal in summer 2010 (and the early 1990s) or similar incidents that had shattered people’s confidence in its secret services before.¹²

The Federal Parliament (Nationalrat) was supposed to deal with the BÜPF bill in June, but the debate was postponed to its autumn or winter session. Observers predict more critical voices and substantial debates among parliamentarians, yet parliamentary opponents seem to be rather scarce. Ruedi Noser from the Liberal Party and a well-known ICT entrepreneur reflects: “Many MPs are not aware about the consequences of the BÜPF because they are digitally distant.” They obviously care more about banking secrecy than privacy. “I need to remind my party folks that privacy matters on the internet as well,” he said.¹³

Privacy as a privilege?

From the official side, it is Switzerland’s Data Protection and Information Commissioner Hanspeter Thür who expresses doubts about private and state actors that need to be better controlled whenever collecting data. “Consumers have almost no options any more to protect their private sphere – privacy becomes a privilege,” he feels.¹⁴ According to a recent study conducted in nine countries on behalf of the European Commission, public awareness and wariness about state surveillance is on the rise. The survey sample in Switzerland (75 to 90 people in all language regions) indicated that Swiss citizens are rather anxious about surveillance of the public for security reasons: 38% only were in favour of it (citizens are more critical in Germany only).¹⁵

A referendum on surveillance seems predictable

Political prognoses are usually difficult, depending on various factors (not only in Switzerland). However, if the contested BÜPF passes the Federal Parliament in the autumn or winter session (like the second Chamber Ständerat in March before) – which seems to be predictable – a referendum will be called for by various actors in the country. A Referendum Committee was already created at the end of May.¹⁶ Such referendums are instrumental to direct democracy and an essential part of the political system in Switzerland. Whenever the two Chambers of the Parliament pass a law, a public referendum can be announced and organised by any stakeholder groups in the country (usually political parties, unions, business or other associations or any initiatives). They usually create an alliance of opponents called a Referendum Committee. Such committees need to collect 40,000 signatures (practically, around 50,000 are necessary) from all over the country during a limited period of several months. Once this number is achieved, large packages of signatures are delivered – usually in a public action – to the Federal Chancellery in Bern. The office in charge will review and check the validity of the collected signatures before a referendum is officially approved. Upon approval of a referendum, the respective law is suspended until public voting – dates are fixed by the Federal Council in the course of the next federal voting schedule (usually in spring, summer or autumn every year).

The biggest challenge for any Referendum Committee is to organise broader alliances of supporters among opponents and to raise funds (a minimum of one million Swiss francs, roughly USD 110 million) for a voting campaign. In the given case of an anticipated Anti-BÜPF campaign, the prospects are not bad, with strong business actors on board (not only for money, but also for networking). Another decisive success factor for any such campaign is media coverage and support by influential media titles all over the country. As it looks now, the mixture of the Anti-BÜPF coalition is rather unique and heterogeneous, and has considerable potential to mobilise support from various spheres of Swiss society – particularly among youngsters and digital natives. However, a well-known risk factor is voting discipline – usually elder and conservative people use the opportunities of direct democracy while younger generations tend to abstain. And usually the level of participation in Swiss voting is rather

11 STOP BÜPF, Medienecho zur Stop-Büpf-Demo vom 31. Mai 2014 and Testimonials. stopbuepf.ch/medienecho-zur-stopbuepf-demo-vom-31-mai-2014

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

13 Überwachung: Der Streit um Staatstrojaner spaltet die Parteien, TagesWoche, July 2014. www.tageswoche.ch/de/2014_30/schweiz/664229

14 Datenschutz: „Privatsphäre wird zu einem Privileg“, Interview with the FDPIC, March 2014. www.nzz.ch/aktuell/schweiz/privatsphaere-wird-zu-einem-privileg-1.18256915

15 Schweizer lehnen Staatsüberwachung ab, NZZ am Sonntag, May 2014. www.nzz.ch/aktuell/schweiz/schweizer-lehnen-staatsueberwachung-ab-1.18309315

16 Ibid.

low, at around 50% or less. Nevertheless, an Anti-BÜPF campaign (depending on the final decision of the parliament) offers great opportunities for broader public discourse about state and other forms of surveillance in the digital age. The colourful coalition of critical voices and pronounced opponents of this law looks promising at least. What appears like a conflict of generations – digital natives versus immigrants – could be a next step into an open Swiss information society.¹⁷

Action steps

The topic of advancing the information society in Switzerland is so far mostly limited to some specialists, academia or a few informed circles. A high percentage of the population (close to 80%) use computers, mobile devices and the internet on a daily basis, but do not care so much about related issues, problems or challenges – as long as access to infrastructure and content is provided and everything works well. Even those using social networks

like Facebook, etc., generally do not care about privacy that much. Compared to Germany, net politics and related matters is still a playground for a few nerds, and media and internet literacy is often demanded but continuously underserved. More initiatives in this respect are needed on various levels of society (particularly schools). To work against the idea that “privacy becomes a privilege”, more awareness raising and discussion is needed – from the family up to the political levels (parties and parliament).

The anticipated Anti-BÜPF campaign (after the law is presumably adopted later this year) offers a great chance for broader public dispute and contestation on limits of state interference into and surveillance of private spheres. As the political establishment of the country has not yet arrived in the digital age, other parts of society – like the Anti-BÜPF coalition – need to step in and take the lead for an appropriate debate about the dangers and limits of surveillance.¹⁸

¹⁷ Petition STOP BÜPF, Nein zum Überwachungsstaat, July 2014. buepf.ch

¹⁸ Balthasar Glättli, Dossier BÜPF (13.025 Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs). www.balthasar-glaettli.ch/dossier/dossier-buepf-bundesgesetz-betreffend-die-ueberwachung-des-post-und-fernmeldeverkehrs