SWITCHcert Security Report

July 2014

I. Swiss monitoring law facing opposition

When the Council of States looked at the revision of the Swiss Federal Mail and Telecommunications Monitoring Act (BÜPF) on 19 March this year, there was broad agreement on the need for the legal framework for criminal prosecution to be brought up to date with developments in modern information technology. The view was that the planned extension of the data retention period from 6 to 12 months and the use of so-called «government trojans» to monitor suspects were therefore to be approved. The Council of States passed the BÜPF by 30 votes to 2, with four abstentions. The next step will be for the matter to be put before the other chamber of Switzerland's parliament, the National Council, in the autumn.

In the meantime, opposition has begun to mount from various sources. The criticisms focus on the proportionality and effectiveness of the envisaged measures. «I know of no cases where a serious offence could not be prevented or solved due to the currently applicable period.» said Federal Data Protection and Information Commissioner Hanspeter Thür, for example, commenting on the extension of the data retention period in an interview in the NZZ newspaper.

Furthermore, many questions have apparently still to be adequately clarified: Which offences is the use of the spyware to be permitted for? For example, will aggravated theft or criminal damage be sufficiently serious? How can it be ensured that no data are added to or changed on a computer monitored by «GovWare»? What form is the duty to cooperate to take in practice in the case of smaller (WLAN) providers?

A further group of critics categorically rejects any extension of surveillance by the state, citing the fundamental right to privacy as a core element of a democratic society. In this regard, historian Nathalie Baumann asked: «What sort of self-image does a state have if it has around a quarter of its citizens under surveillance?» Here she was referring to the Secret Files Scandal dating back to 1989, and bemoaned the lack of a wider discussion of this issue across society.

This debate could now take place. A cross-party referendum committee set up at the end of May plans to oppose the revision of the BÜPF should the law be passed by the National Council without any amendments. The committee is broadly based, with representatives from the youth wings of all parties except the CVP, and also from Swico, the ICT industry association in Switzerland.

Meanwhile, the federal government is planning to invest CHF 91 million in the modernization and development of the monitoring of mail and telecommunications traffic through to 2021. A media release issued by the Federal Department of Justice and Police (FDJP) on 1 July 2014 essentially said that where it is a matter of solving serious crimes or searching for people in need, intervening in fundamental rights by analysing telephone or mail traffic is justified. The FDJP added that there is a strong public interest in this. Furthermore, legislators had restricted the use of stored data by imposing high legal barriers.

This is also the crux of the FDJP's rationale in rejecting submissions by six members of Digital Society Switzerland against the extension of the data retention period. Although the latter welcomed the recognition of the fact that data retention represents a serious infringement of fundamental rights, they nonetheless plan to challenge the rejection, taking the case as far as the European Court for Human Rights (ECHR) if necessary.

Meanwhile, on 8 April 2014, the European Court of Justice (ECJ) ruled that the EU directive on data retention is invalid, stating that it «interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data.»

Read more here:

http://www.srf.ch/news/schweiz/session/staenderat-votiert-fuer-schnueffel-software

http://www.nzz.ch/aktuell/schweiz/privatsphaere-wird-zu-einem-privileg-1.18256915

http://www.netzwoche.ch/News/2014/03/25/Georg-bitte-lies-diese-Karte-nicht.aspx

http://www.inside-it.ch/articles/36499

http://www.inside-it.ch/articles/36172

http://www.nzz.ch/aktuell/schweiz/angst-vor-dem-schnueffelstaat-1.18313578

http://www.netzwoche.ch/de-CH/News/2014/06/02/Bund-will-weitere-91-Millionen-fuer-Ueberwachung-aufwenden.aspx

http://www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2014/2014-07-01.html

https://www.digitale-gesellschaft.ch/2014/02/21/digitale-gesellschaft-erhebt-beschwerde-gegen-vorratsdatenspeicherung/

http://www.steigerlegal.ch/2014/07/01/urteil-pro-vorratsdatenspeicherung-in-der-schweiz/

http://www.zeit.de/digital/datenschutz/2014-04/vorratsdatenspeicherung-europaeischer-gerichtshof-eugh

II. Facebook users as guinea pigs

It’s no secret that users of the social networking site Facebook pay for it with their data. Users have also accepted the fact that Facebook determines which of the messages from their friends are shown on their personal newsfeed, or timeline, and which aren’t. After all, Facebook always endeavours to ensure that we only see what we’re really interested in: delivering an improved user experience.
At the beginning of June, however, a study was published in the scientific magazine PNAS which showed that in January 2012, Facebook submitted hundreds of thousands of its users to an involuntary experiment. As part of a scientific study, the timelines of 310 000 users were manipulated for a week. For half of this group, Facebook reduced the number of posts with positive emotional content, and for the other half the negative content. A further 310 000 test subjects had their timelines left unchanged to act as a control group. The study examined the impact the manipulation had on the mood and posting behaviour of the users. The result: Facebook can influence the mood of users in either direction, albeit only to a minor extent.

The publication of the study unleashed a wave of indignation towards Facebook. The primary criticism is that Facebook misused its users as guinea pigs without obtaining their prior consent. Now there are some smart people saying that «data use for research» is covered under the Data Use Policy. But even smarter people have discovered that this clause was only inserted four months after the study was conducted. Furthermore, «data use for research» does not include users having to serve as guinea pigs without being asked. Adam Kramer, the Facebook man who led the study, posted the following statement on Facebook on 29 June 2014: «The reason we did this research is because we care about the emotional impact of Facebook and the people that use our product. [...] The goal of all of our research at Facebook is to learn how to provide a better service.» In other words, an improved user experience.

According to a report in «The Register», the UK data watchdog is now investigating the matter and considering taking action against the social media platform. The US group EPIC (Electronic Privacy Information Center) has also submitted a complaint to the supervisory authority, the FTC. What impact this has had on Mark Zuckerberg's mood is not known.

Read more here:

http://www.businessinsider.com/how-the-facebook-news-feed-works-2014-2

http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/der-facebook-boersengang/facebook-manipuliert-nutzer-gefuehle-fuer-eine-studie-13016744.html

http://www.pnas.org/content/111/24/8788.full

http://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/

https://www.facebook.com/akramer/posts/10152987150867796

http://www.theregister.co.uk/2014/07/01/uk_and_irish_data_watchdogs_wade_in_on_facebook_messin_with_your_head_scandal/

III. Cyber attacks on our minds

When we hear of cyber war, we mostly think of things like highly specialised computer viruses, manipulated industrial plants, and denial-of-service attacks on critical systems. Less well known are the armies of trolls-for-hire, who deliberately shape the mood in social media communities and the comments sections of news portals.

According to a report in the Süddeutsche Zeitung, there is for example a company in St. Petersburg with around 600 staff whose primary task is to manipulate opinion on the Internet in line with the interests of the Russian government. The costs translate into around USD 1 million – a month. These manipulations are not restricted to Russian-speaking media, and instead focus above all on English-language sites as well.

According to Süddeutsche Zeitung, a group of hackers is supposed to have gained access to the email account of a key employee of the St. Petersburg-based agency and published more than 800 emails at the end of May. These reveal a picture of how «organised trolls» operate: First, English-language Internet media are systematically analysed by categories such as the age distribution of the users, the times of daily peak activity, and the political stance of the readers.

The trolls-for-hire then receive precise instructions on how to place comments on the corresponding forums. Themes, key words and criteria are clearly specified. The trolls are paid by performance, and their daily target is 50 comments on news portals and 50 tweets, while also administer six Facebook pages.

But other intelligence services are also using social networks for their own propaganda purposes. For example, until autumn 2012 the Americans ran a Twitter-like platform for Cuba aimed at provoking unrest there. And since last year, the British secret service is said to have had a special unit called the Joint Threat Research Intelligence Group, with at least 150 staff working on manipulating opinion and engaging in strategic discrediting on social media.

In his presentation to this year's «re:publica» media convention in Berlin entitled «There is no democracy without media literacy», Jaroslaw Lipszyc highlighted comprehensive media literacy as being the only means of defence in times of information wars.

A further recent example showed just how important it is to have a deliberate and discerning approach to dealing with the media. At the end of June, a spate of deliberately misleading information on Facebook and in e-mails unleashed major panic among bank customers in Bulgaria. The posts stated the deposits held by clients with a Bulgarian bank were no longer secure. This prompted a run on the bank, with thousands clearing their accounts. In the space of a single day, some EUR 400 million was withdrawn from the bank, which was quickly forced to close all its counters. Bulgaria's central bank regards this as a systematic attempt to destabilise the country by attacking the banking system.

Read more here:

http://www.sueddeutsche.de/politik/propaganda-aus-russland-putins-trolle-1.1997470

http://www.nzz.ch/international/putins-internetpiraten-1.18324628

http://www.faz.net/aktuell/snowden-dokumente-wie-man-die-oeffentlichkeit-infiziert-12881233.html

http://re-publica.de/session/there-no-democracy-without-media-literacy

http://futurezone.at/digital-life/falschmeldung-auf-facebook-verursacht-bankenansturm/72.895.325

http://in.reuters.com/article/2014/06/27/bulgaria-banks-idINL6N0P81SG20140627

http://news.yahoo.com/white-house-defends-cuban-twitter-stir-unrest-222510641.html

https://netzpolitik.org/2014/neues-aus-der-jtrig-abteilung-von-gchq/

IV. What happened to TrueCrypt?

The news hit like a bombshell: on 28 May 2014, an announcement out of the blue on the official website of TrueCrypt – a widely used, open source encryption software recognised as being secure – stated that development had been ended and the software was potentially insecure. Instead of the original website content, all that remained was a recommendation on how to migrate encrypted data to Microsoft's BitLocker solution.

Initially, it all seemed like a defacement hack. However, only a limited version of the software was available on Sourceforge – and this was certified with the developers' valid signing key. Given that the TrueCrypt website has not since been restored, the hack theory no longer has any credence. There has also been no information seeking to clarify matters from the team of developers, who largely work anonymously.

This has naturally spawned a whole range of theories connecting the events to the intelligence services. Some creative observers have discovered that the initial letters of the warning posted in red by the developers on the homepage – «Using TrueCrypt is not secure as it may contain unfixed security issues» – reads «utinsaimcusi». This can be broken down into the Latin phrase «uti nsa im cu si», which when entered into Google Translate comes out as: «If I wish to use the NSA.»

Researchers focused their interest on the security of TrueCrypt a year prior to this in the wake of the Snowden revelations. Donations were gathered, and the Open Crypto Audit Project (OCAP) was set up to examine the software in detail. In March, phase one of the audit revealed that TrueCrypt did not contain any backdoors, but had various weak points. The OCAP team has in the meantime posted the last full version (7.1a) on the web, and is endeavouring to find a successor solution for the software.

TrueCrypt still enjoys a good reputation among security professionals. That is by no means the case for all encryption products. «Most commercial encryption products are junk», was a recent tweet from cryptography professor Matthew Green, one of the most respected independent experts in the field.

Read more here:

http://truecrypt.sourceforge.net/

http://grahamcluley.com/2014/06/truecrypt-hidden-message/

http://opencryptoaudit.org/

http://www.heise.de/security/meldung/TrueCrypt-geprueft-Keine-Backdoor-laxe-Programmierstandards-2170398.html

http://www.nzz.ch/aktuell/digital/truecrypt-71a-download-open-crypto-audit-project-ocap-1.18319652

https://github.com/AuditProject/truecrypt-verified-mirror

https://twitter.com/matthew_d_green/status/478956352237076480

The Clipboard: Interesting presentations, articles and videos

According to a new court ruling, if served with valid warrant from a US authority, US firms must hand over data even if they are stored on servers outside the US:

http://www.nzz.ch/wirtschaft/wirtschafts-und-finanzportal/europaeische-datenwolken-als-beliebte-loesung-1.18308010

In a two-part blog post, Bryce Boland and Greg Day from Fireeye examine how to get a handle on the business case and ROI aspects of IT security measures:

http://www.fireeye.com/blog/corporate/2014/07/economics-of-security-part-i-translating-information-security-risks-to-business-risk.html

In a blog post and white paper, Symantec reported on the hacker group «Dragonfly» alias «Energetic Bear», which currently has its sights set on the western energy industry:

http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf

The SWITCHcert Security Report was written by Frank Herberg.

It does not reflect the opinions of SWITCH but is instead a summary of articles published in various media. SWITCH accepts no liability for the content or opinions contained in the Security Report or for its correctness.

News from SWITCH: For staffing reasons, the SWITCHcert Security Report will be taking a summer break in August. The next report will be published in September. As always, we will keep you up-to-date with the most important security issues at securityblog.switch.ch.