pre-print version – to appear in:

Privacy and Human Rights 2004.
An International Survey of Privacy Laws and Developments

edited by
– Electronic Privacy Information Center, Washington, DC, USA
– Privacy International, London, United Kingdom

The «Switzerland» chapter has been compiled by Christoph Müller in June 2004

Swiss Confederation (Switzerland)

Article 36(4) of the 1874 Constitution guaranteed, "[t]he inviolability of the secrecy of letters and telegrams." This Constitution was repealed and replaced by public referendum in April 1999. The new constitution, which entered into force on January 1, 2000, greatly expanded the older privacy protection provision. Article 13 of the Constitution now states: "All persons have the right to the respect of their private and family life, home, mail and telecommunications. All persons have the right to be protected against abuse of their personal data."[1]

Data Protection Laws
The Federal Data Protection Act of 1992 (*Loi fédérale sur la protection des données* or LPD) regulates personal information held by federal government and private bodies.[2] The Act requires that information be legally and fairly collected and places limits on its use and disclosure to third parties. Private companies must register if they regularly process sensitive data or transfer the data to third parties. Transfers to other nations must be registered and the recipient nation must have adequate laws. Individuals have a right of access to correct inaccurate information. Federal agencies must register their databases. There are criminal penalties for violations.

Almost each of the 26 Swiss Cantons (states) has a separate data protection law and its own data protection commissioner. However, as some cantons are rather small, some data protection commisioners are employed only by 10 percent of their working time for this purpose. In order to exchange opinions and to collaborate, the cantonal data protection officers have founded the association "DSB+CPD.CH" in March 2000. In 2003-2004, the association published a critical

1 *Constitution of Switzerland*, 1999, "Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999" (BV, SR 101), <http://www.admin.ch/ch/d/sr/c101.html>. In addition to the Constitution, every Federal law and regulation is available in an online directory. In this report, we generally link to the german versions ("*Systematische Rechtssammlung*" SR: <http://www.admin.ch/ch/d/sr/sr.html>). However, there are version avialable in French ("Recueil systématique du droit fédéral" (RS) <http://www.admin.ch/ch/f/rs/rs.html>) and in Italian ("*Raccolta sistematica del diritto federale*" <http://www.admin.ch/ch/i/rs/rs.html>).

2 *Bundesgesetz über den Datenschutz, DSG vom 19. Juni 1992 (Stand 2000)* (Swiss Data Protection Statute from June 19, 1992 (in the updated version of 2000), (DSG, SR 235.1), available in german at <http://www.admin.ch/ch/d/sr/c235_1.html> For an english translation see: <http://www.edsb.ch/e/gesetz/schweiz/index.htm> or <http://www.ics.uci.edu/~kobsa/privacy/switzerland.htm>.

opinion on the EPID project (see below), and in June 2004, a detailed list of web resources on computer security and "safer surfing."[3]

To date, the Federal Parliament is currently discussing a revision of the Data Protection Act, which in some parts provides better regulations, while at the same time proposing a major change in a new Article 17a. This Article allows federal authorities to create new data banks and to process personal data without previous regulation by the law, "if major public interest does not allow a postponement of data processing or if a testing phase is required." In these cases, the government only has to produce a regulation (decree).[4]
In June 1999, the European Union Data Protection Working Party determined that Swiss law was adequate under the European Union Directive.[5] In July 2000, the European Commission formally adopted this position, thereby approving all future transfers of all personal data transfers to Switzerland.[6] However, as long as the revision of the Data Protection Law is pending, Switzerland cannot formally ratify the Data Protection Protocol of the European Council.[7]

The LPD created the office of a Federal Data Protection Commissioner (the Commissioner, or EDSB .[8] The Commissioner maintains and publishes the Register for Data Files,[9] supervises federal government and private bodies, provides advice, issues recommendations and reports, and conducts investigations. The commissioner also consults with the private sector. The office publishes a detailed annual report,[10] as well as leaflets, summaries of press articles and critical statements, *e.g.*, on the medical tariffing system Tarmed (see below), on the telecom provider Orange SA collecting sensitive data of their employees, or on the governmental project to introduce a unique ID number for all Swiss residents (EPID).[11] Further, the office is advising governmental agencies on issues of data protection.

---

3 Association of Data Protection Commisionners <http://www.dsb-cpd.ch>. Brochure on "Safer Surfing" <http://www.dsb-cpd.ch/d/publikationen/broschuere_sicherheit_d.pdf>. Link list on "Safer Surfing": <http://www.datenschutz.ch/index/sichersurfen.htm?id=9254>.

4 *Eidgenössisches Justiz- und Polizeidepartement: Entwurf zur Teilrevision dess Bundesdatenschutzgesetzes*, (Federal Department of Justice and Police: Pre-draft for a Partial Revision of the Federal Data Protection Act), August 2001, available at <http://www.ofj.admin.ch/themen/datenschutz/vn-ber-d.pdf>. – A report by the controlling delegation of the National Council of the Federal Parliament (*Geschäftsprüfungskommission des Nationalrates* [GPK-N]) has been published in April 2004, together with a statement of the Government. See *Bericht der Geschäftsprüfungskommission des Nationalrates [GPK-N] vom 21. November 2003, sowie Stellungnahme des Bundesrates vom 24. März 2004,* in: Bundesblatt vom 06. April 2004 / Nr. 13 S. 1413 bzw. S. 1431: <http://www.admin.ch/ch/d/ff/2004/index0_13.html>. - While the National Council (*Nationalrat*) refused to discuss the project on March 3, 2004, (*i.e.*, to send it back to the commission for revision), the smaller chamber decided to discuss it. The consultation process is going on, without any decision being taken so far. (The National Council (*Nationalrat*) is the larger chamber of the Swiss Federal Parliament, representing the population, while the State Council (*Ständerat*) is the smaller chamber, representing the 26 *cantons*. Switzerland is governed by the collective Federal Council (*Bundesrat*), with seven members (ministers). Information about the political system in Switzerland can be found at <http://www.parlament.ch/e/homepage.htm>.

5 Data Protection Working Party – Article 19, Opinion 5/99 on the Level of Protection of Personal Data in Switzerland, June 7, 1999, available at <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp22fr.pdf>.

6 European Union, Press Release, *Commission Adopts Decisions Recognising Adequacy of Regimes in United States, Switzerland and Hungary*, July 27, 2000, available at <http://europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm>.

7 *Zusatzprotokoll zum Übereinkommen des Europarats zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten* (Série des traités européens STE Nr.108).

8 Homepage <http://www.edsb.ch/>.

9 According to official information by the EDSB office, there are approximately 1,200 individuals or companies registered, according to Article 11 of the Swiss Federal Act on Data Protection of June 19, 1992. E-mail from Eliane Schmid, EDSB office; to Cédric Laurant, Policy Counsel, Electronic Privacy Information Center (EPIC), July 8, 2004.

10 *Annual report*, nr. 11, published on July 5, 2004 <http://www.edsb.ch/d/doku/jahresberichte/tb11/index.htm> – The report is available in french as well on <http://www.edsb.ch/f/doku/jahresberichte/tb11/index.htm>

11 EPID means "*Einheitlicher Personenidentifikator*", *see* <http://www.edsb.ch/d/themen/weitere/epid/edsb-papier-epid_d.pdf> and "Register Would Give Everyone ID Number," New York Times, January 7, 2004. After protests, the EPID project has been revised in winter 2003-2004: instead of one unique ID number, it is now planned to introduce about six

Currently, there are 22 employees working for this office. However, the Federal Data Protection Commissioner has only limited possibilities for interventions: he can only submit "suggestions" (*Empfehlungen*), or ask the Data Protection Commission to review a case. Decisions of this commission can then be submitted to the Federal Court (*Bundesgericht*). The last decision of the Data Protection Commission published on its website dates back to August 29, 2003: The Commission decided that the pharmaceutical company Roche was not allowed to systematically take samples of the urine of their apprentices (*Lehrlinge*) in order to test them for the use of illegal drugs.[12] In 2000, Roche received a Swiss "Big Brother Award" for their testing of apprentices.[13]

Besides the Data Protection Act,[14] there are also legal protections for privacy in the Civil Code[15] and the Penal Code,[16] and special rules relating to workers' privacy from surveillance,[17] telecommunications information,[18] health care statistics,[19] professional confidentiality including medical and legal information,[20] medical research,[21] and identity cards.[22]

The identity card is machine-readable as is the new passport, which became effective on January 1, 2003. Banking records are protected by the Swiss Federal Banking Act of 1934. This Act was passed to guarantee strong protections for the privacy and confidentiality of bank customers. However, Switzerland has come under increasing pressure from the European Union and the Organization for Economic Cooperation and Development (OECD) to weaken these laws and provide greater access to bank records for the purposes of tax collection.

---

different ID numbers for different areas. In spring 2004, the law went into a second political consultation process. Traditionally, in Switzerland, new law projects are presented to the "interested public" for consultation (*Vernehmlassungsverfahren*, consultation process). This is mainly to prevent opposition to require a formal referendum on the bill.

12 "*Urteil der Eidgenössischen Datenschutzkommission vom 29. August 2003, Widerrechtliche Bearbeitung von Personendaten. Drogentests während der Lehre 68.68*": <http://www.vpb.admin.ch/deutsch/cont/aut/aut_1.2.3.5.html>. Members of the commission: <http://www.admin.ch/ch/d/cf/ko/index_111.html>

13 Big Brother Awards Switzerland, "Hall of Shame," <http://www.bigbrotherawards.ch/diverses/hallofshame>.

14 For an overview of legal regulations concerning Data Protection, *see* <http://www.admin.ch/ch/d/sr/23.html#235>.

15 Section 28 of the *Zivilgesetzbuch* (ZGB, SR 210), Civil Code, December 10, 1907, <http://www.admin.ch/ch/d/sr/c210.html>.

16 *Code pénal, Titre troisième: Infractions contre l'honneur et contre le domaine secret ou le domaine privé*, Art. 173-179. *Schweizerisches Strafgesetzbuch* (StGB) *vom 21. Dezember 1937* (SR 311.0) <http://www.admin.ch/ch/d/sr/c311_0.html>.

17 Section 328 of the *Obligationenrecht* (OR, SR 22) <http://www.admin.ch/ch/d/sr/22.html>, *Code of Obligations. See* International Labour Organization, Conditions of Work Digest, Volume 12, 1/1993.

18 *Fernmeldegesetz* (FMG, SR 784.10), available at <http://www.admin.ch/ch/d/sr/c784_10.html>, *Telecommunications Law* (LTC) of 30 April 1997.

19 *Office fédéral de la statistique*, *La protection des données dans la statistique médicale*, 1997 <http://www.admin.ch/bfs/stat_ch/ber14/statsant/ff1403c.htm>.

20 *Code pénal*, Art. 320-322, *Schweizerisches Strafgesetzbuch* vom 21. Dezember 1937 (StGB, SR 311.0) <http://www.admin.ch/ch/d/sr/c311_0.html>.

21 *Verordnung vom 14. Juni 1993 über die Offenbarung des Berufsgeheimnisses im Bereich der medizinischen Forschung* (VOBG, SR 235.154) <http://www.admin.ch/ch/d/sr/c235_154.html>, *Ordonnance du 14 juin 1993 concernant les autorisations de lever le secret professionnel en matière de recherche médicale (OALSP).*

22 *Bundesgesetz vom 22. Juni 2001 über die Ausweise für Schweizer Staatsangehörige* (Ausweisgesetz, AwG, SR 143.1) <http://www.admin.ch/ch/d/sr/c143_1.html>, and the corresponding regulation *Verordnung vom 20. September 2002 über die Ausweise für Schweizer Staatsangehörige* (Ausweisverordnung, VAwG, SR 143.11) <http://www.admin.ch/ch/d/sr/c143_11.html>, replacing the older *Ordonnance du 18 mai 1994 relative à la carte d'identité suisse*.

International cooperation against terrorism

Under the headlines of "fighting against terrorism" (especially after September 11, 2001), Switzerland expanded domestic surveillance, and established and strengthened collaboration agreements, especially with the US and the EU. On September 4, 2002, a secret "Operative Working Arrangement" has been signed, establishing a close "joint operative exchange of officers:"[23] Agents of both parties are permitted to work within their respective task forces against terrorism and thus to "have access to all information necessary to perform their task." Both signatory parties described their joint operation as an "outstanding cooperation." In autumn 2003, the Foreign Affairs Commission of the National Council criticized that the aggreement had never been submitted to the Parliament. In March 2004, a large majority of the National Council required that the Government submit the aggreement *ex post* to the Parliament. One specific focus in the cooperation between Switzerland and US intelligence authorities concerns the money flows. It brings into question the role of Swiss banks in "financing terrorists." After September 11, 2001, some banking organizations based in Switzerland have been put on a "black list" and their financial transfers have been closely investigated, and in some cases blocked.[24] On June 24, 2004, the Swiss Attorney General (*Bundesanwalt*) declared the end of the first step of the "9/11 investigations." He concluded that the Swiss Banks "did not play a major role" in financing the attacks. Still, some accounts of financing companies have been blocked, and some cases handed over to a federal investigative judge. At the end of the first step of the investigations, the Swiss Attorney General declared the end of the "Operative Working Arrangement."

In another type of cooperation, Switzerland is trying to find a common solution with the EU and the US with respect to passports and visas. In September 2003, the Swiss government commissioned a study on the feasibility of "upgrading" the Swiss passport with biometric identification tags. This should allow Swiss citizens to fulfill the requests introduced by the US government, requiring that from October 2004, every visitor without a visa would have to be able to present a passport with a biometric identity tag. The feasibility study should be presented during the summer of 2004.

Negotiations are ongoing on the issue of the disclosure of air travelers' data to US authorities. The immigration branch of the US Department of Homeland of Security requires large data sets from every passenger. This disclosure violates the Swiss Data Protection Law, which allows the transfer of data to another state only if the other nation has a similar data protection legislation, which is not the case of the US. Until now, the national airline company Swiss declares giving only limited data to US authorities. As negotiations are ongoing between the EU and the US on this issue, Switzerland seems to be waiting for an aggreement before joining in.[25]

---

[23] The "Arrangement" has been signed by the Swiss Attorney General (*Bundesanwalt*, General Federal Prosecutor), Mr. Valentin Roschacher for Switzerland, and by the US Attorney General John Ashcroft and US Deputy Secretary at the Department of Treasury, Kenneth Dam for the US. In June 2004, the Swiss newspaper "Facts" published a facsimile of the aggreement <http://www.facts.ch/dyn/magazin/schweiz/382176.html>.

[24] The Government has proposed new amendments in the criminal law to deal with "terrorist organizations" and "financing of terrorism" as well as for the ratification of the United Nations Convention against Terrorist Financing, *see* "*Lutte contre le terrorisme*," June 27, 2003, available at <http://www.ofj.admin.ch/themen/terror/intro-f.htm>.

[25] On May 28, 2004, the EU signed an aggreement with the US on the disclosure of PNR data. However, the European Parliament decided to present the case to the Court of Justice of the European Communities. As of the end of June 2004, no similar aggreement had officially been signed between Switzerland and the US.

Cooperation with the European Union

Switzerland is not a member of the EU, but has some special agreements with the EU. Some of these bilateral aggreements have been signed in 2000-2001. In May 2004, the government decided to sign another set of agreements ("Bilaterale II"). However, these contracts will probably have to be first approved by citizens by referendum.

The contracts include agreements on the mobility of persons (*Personenfreizügigkeit*). These agreements aim at shifting the borders between European nations to the external borders of Europe. Inside Europe, people may travel without the traditional border police control, while travellers from and to Europe will be confronted to strenghtened border controls. However, the national police forces will be allowed to execute "mobile controls" in the 30 km range along the borders, as well as in train stations, inside of trains and at airports. This means that all persons will *de facto* have to carry an ID document, which was not compulsory until now in Switzerland.[26]

An important part of the "Bilaterale II" bundle of agreements are the Schengen and Dublin conventions that the Swiss government decided to join but that the Parliament has not ratified yet. The Schengen Convention[27] would establish a close cooperation among police forces, in order to combat international "criminal tourism" (*Kriminaltourismus*). The core subject of this agreement is the Schengen Information System (SIS), a pan-European database that records personal information on people who have been arrested, migrants, and missing objects[28](*Fahndungsdatenbank*) by the national police forces. In the spring of 2004, SIS consisted of 10 million entries. In 2003, 1.2 million data sets concerned persons, but only 1.6 percent of these persons had been the subject of an international warrant. The large majority of files concerns persons from non-EU member states. The SIS database is not only a tool against crime, but also a tool for repression against immigration. SIS is operated by the EUROPOL, and by joining the Schengen agreement, Swiss police officers will have full online access to the SIS database. The Swiss Departement of Justice and Police (EJPD) calls the SIS "a revolutionary step for police work." Collaboration in the EUROPOL will be "faster and more efficient than with Interpol." Other parts of the Schengen Convention cover the cross-border observation by national police forces and the exchange of police officers.

The Dublin Convention, established in 1990, establishes a European cooperation agreement to process applications from asylum seekers. It will allow Switzerland to access "Eurodac", the pan-European database of fingerprints of asylum seekers and migrants.[29] According to the Dublin Convention, asylum requests are checked only by one EU member state whose decision becomes binding for all other member states.

There are several bilateral aggreements on police cooperation between Switzerland and many other nations in Europe, which expand the types of collaboration among law enforcement authorities. The Swiss Federal Police is, in this regard, exchanging to other countries.[30] Concrete collaboration has been tested in the case of international political and economic meetings, like the meeting of G8 in

---

[26] This rule is most likely against a decision by the Swiss Federal court of 1983, which held that identity controls are only allowed in case of a disruptive situation ("*situation troublée*"). *Bundesgerichtesentscheid* BGE 109 Ia 146 <http://www.polyreg.ch/bgeleitentscheide/Band_109_1983/BGE_109_IA_146.html>.

[27] <http://www.ejpd.admin.ch/d/dossiers/schengen/>.

[28] <http://www.fact-index.com/s/sc/schengen_information_system.html>.

[29] After a revision of the regulation *Verordnung über die Bearbeitung erkennungsdienstlicher Daten* by the Swiss Government on may 12, 2004, the Swiss border police is allowed to collect fingerprints of all persons they expect to be illegally trying to immigrate to Switzerland, and to store these data in the national data base AFIS, from June 1 2004 on The revision has to be regarded as a preparation for the joining of the Eurodac data base. See *Verordnung über die Bearbeitung erkennungsdienstlicher Daten vom 21. November 2001* (SR 361.3) <http://www.admin.ch/ch/d/sr/c361_3.html>.

[30] *E.g.*, in April 2002, the Swiss Government signed an aggreement with Europol on exchanging information as well as police agents. The Government promised to submit the aggreement to the parliament in a later stage.

Geneva in June 2003 and the meeting of the World Economic Forum in Davos in January 2004.It is most likely that Switzerland will ratify the Schengen and Dublin Conventions. However, nationalist-conservative parties, opposing the contracts, intend to organize a public referendum on this issue.

Police and Intelligence Agencies' activities

The Swiss Police system is traditionally strongly organized by the 26 *cantons*. Every canton has its own police force. However, in the last few years there have been substantial effort to build up a central "Federal Police" corps (Fedpol), based in Berne. This Fedpol has mainly investigative duties, including the "prevention" of crimes. Since 1994, there has been built up a Federal Criminal Police as well.[31] Most of the extension of this Fedpol has been done in order to "fight against organized crime and terrorism" (including "cybercrime," for which a specific task force has been established in 2003, the "Coordination Unit for Cybercrime Control" (CYCOS).[32] However, there are still some remarkable tensions between the Fedpol and cantonal Police forces.

Legally, the activities of the Fedpol are mainly based on the *Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit* (BWIS).[33] This law was enacted in July 1, 1998 as a follow-up of a scandal in the autumn of 1989, when members of a parliamentary investigative commission (the *Parlamentarische Untersuchungskommission*, or PUK) discovered huge databases of citizens in the premises of the Federal Police (the political police) and the Federal Prosecutor (*Bundesanwaltschaft*).[34]

The former Federal Police, now called the Service for Analysis and Prevention, is part of the Federal Office for Police Matters, which also includes the Federal Criminal Police. It hosts two data banks, including ISIS (the Information System for Internal Security), which replaced the old paper files of the federal police.[35] ISIS contains files on about 50,000 persons who are considered "terrorists," "violent extremists" or possible spies. Files are opened on "preventive" grounds, which means that no criminal investigation is required. However, data resulting from criminal investigations, and thus also from telephone surveillance, can be maintained for preventive purposes, even if the person is acquitted before a court. The other data bank is JANUS,[36] Most contained files of 62,500 persons in July 2001, Most of them being registered for alleged drug trafficking, since registration of consumers is not allowed. Files in JANUS can be created on the grounds of simple suspicion. The records on the

---

31 *Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes vom 7. Oktober 1994* (ZentG, SR 360) <http://www.admin.ch/ch/d/sr/c360.html>.

32 "Coordination Unit against Cybercrime" (CYCOS, KOBIK in German) <http://www.cybercrime.admin.ch/e/index.htm>.

33 *Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit vom 21. März 1997* (BWIS, SR 120) <http://www.admin.ch/ch/d/sr/c120.html>.

34 The Commission found about 900,000 folders, called "*Fichen*" (hence "*Fichenskandal*,"), most of whom were not suspected of having committed any offence. Most of the folders had to be destroyed since. At this time, there was no legal basis for the collection of these folders. In 1991 a citizens committee launched a popular initiative to abolish the political police. Surveillance should only be possible on the grounds of a criminal investigation. The vote on the initiative was postponed by the Government for years. In June 1998, nine years after the scandal 75 percent of the voters said no to the initiative. The Federal government had saved its political police, which since the beginning of the nineties had been completely modernized and, by July 1, 1998, received for the first time in history a legal basis with the Law on Measures for Maintaining Internal Security (BWIS).

35 ISIS: *Verordnung über das Staatsschutz-Informations-System (ISIS-Verordnung) vom 30. November 2001* (SR 120.3), <http://www.admin.ch/ch/d/sr/c120_3.html>.

36 *Verordnung über das Informationssystem der Bundeskriminalpolizei (JANUS-Verordnung) vom 30. November 2001 (Stand am 22. Januar 2002)* (SR 360.2) <http://www.admin.ch/ch/d/sr/c360_2.html>. JANUS is the fusion of three information systems which have been built up during the nineties, and had been maintained separately until 1998: DOSIS, which held data on investigations in drug trafficking; ISOK, the information system on "organized crime;" and FAMP which includes information about forged money, trafficking human beings (prostitution) and illicit pornography.

62,500 suspected targeted persons (*Stammpersonen*) also contain 116,500 references on third persons, which are not suspected.[37]

A revision of the BWIS is currently planned. The directors of the Federal Police and the Intelligence forces are demanding an extension of their capabilities, *e.g.*, to be allowed to spy inside private appartments or to tap telecommunications, even without the concrete suspicion of a crime.

On the legal basis of the BWIS, the government decreed a regulation which permits *and* compels all institutions "executing an official duty" to report any suspicion of a "terrorist activity" to the federal police.[38] These institutions include universities, hospitals, train carriers, etc. The regulation was first released in November 1 2001 in the aftermath of the attacks of September 11, 2001, to sunset after one year. It has then been extended for another year, and in November 2003 was extended for two more years.[39]

From January 1, 2005, the police will be officially allowed to operate undercover special agents.[40] The majority of the Parliament accepted a government's proposal, arguing that this would be "a necessary tool against organized crime", like terrorism and money laundering.

The Department of Justice and Police (EJPD) is preparing a new law including measures against racism, against so-called hooliganism, and against propaganda of violence.[41] The law is paving the way for establishing a centralized national database on so-called "hooligans" in the legal framework of the BWIS (see above), providing the basis for the exchange of data with other nations. The Government underlines that such a data base would be essential in view of the next European Football Championship, scheduled for 2008 in Switzerland and Austria. However, the term "hooliganism" would not be restricted to football fans since the law covers all kinds of "large public events," including political demonstrations.

In the context of the World Economic Forum in Davos in January 2004, police forces blocked the access to the mountain village and collected data on more than 1,000 peaceful demonstrators. According to a newspaper report in May 2004, the cantonal police transmitted the data to the Federal Police,[42] in order to cross-check it with the ISIS database. In January 2004, the cantonal police said that they would not transmit the collected data.[43] The World Economic Forum is a private event organized since 2000 in Davos, supported by large multinational companies, as well as by the Swiss Government.

---

37 Among them, 13,500 are so-called "contact persons;" 13,000 are telephone subscribers (with their names and addresses); and about 90,000 are telephone numbers with only fragmentary information to the respective persons (Conseil national *01-1068 – Question ordinaire de Dardel – Personnes enregistrées dans les systèmes de données JANUS et ISIS – Réponse du Conseil fédéral du 5 septembre 2001* <http://www.parlament.ch/afs/data/f/gesch/2001/f_gesch_20011068.htm>).

38 *Verordnung betreffend die Ausdehnung der Auskunftspflichten und des Melderechts von Behörden, Amtsstellen und Organisationen zur Gewährleistung der inneren und äusseren Sicherheit* (SR 120.1) <http://www.admin.ch/ch/d/sr/c120_1.html>.

39 In Switzerland, the citizens can demand a referendum on every law regarding domestic politics by collecting 50,000 signatures in the delay of 100 days – but they can not ask for a referendum in the case of a regulation (Verordnung, decree).

40 *Bundesgesetz über verdeckte Ermittlung* (BVE) vom 20. June 2003 (SR 312.8) <http://www.admin.ch/ch/d/sr/c312_8.html>.

41 *Bundesgesetz über Massnahmen gegen Rassismus, Hooliganismus und Gewaltpropaganda(Entwurf)* and press release <http://www.ejpd.admin.ch/doks/mm/2003/030212c-d.htm>.

42 "Service for Analysis and Prevention", DAP, *Dienst für Analyse und Prävention*, which is the political Swiss "preventive State Security Police", part of the Swiss Federal Police, ex-BUPO, *Bundespolizei*.

43 *See* Tages-Anzeiger, 11.6.2004, Wochenzeitung nr. 6, 5.1.2004 and nr. 17, 22.4.2004.

In April 2004, newspapers reported about a meeting of the "Club of Berne" in Berne on April 21, 2004. The Club members decided to continue their collaboration under the new name of the "Counter Terrorist Group/CTG." It was the first time that Swiss officials admitted its existence. According to different sources, the Club de Berne was founded in Berne in 1971 as a loose federation (*Zusammenschluss*) of national European intelligence service leaders. Today, the Club of Berne seems to consist of members of 27 nations. In 2002, the mysterious Club has been honored with a Swiss "Big Brother Award" in the category "lifetime award."[44]

Interception of telecommunications

Until the beginning of 2002, telephone tapping was governed by Article 179 *octies* of the Penal Code and corresponding regulations in the federal, the military and the cantonal Penal Procedure Codes.[45] Due to liberalization of the telecommunications sector by the 1997 Telecommunication Act, the government issued a regulation that established a specialized agency, *Le Service des Tâches Spéciales* (Special Services, or STS), within the Department of the Environment, Transport, Energy and Communications (UVEK), to administer wiretaps.[46] The STS now has the function of a being a link between the special services of the different private and state-owned telecommunications companies and the public prosecutors, who issue interception orders. Already under the previous regulation, every interception order had to be confirmed by a prosecution chamber of the federal court or by the cantonal high court.

From April 1, 2003 on, the Swiss telecom providers have to keep a log for six months of all communication traffic data,[47] to comply with the new Federal Law on the Surveillance of Mail and Telecommunications.[48] Implementation of this law will require that the respective telephone companies constantly track phones, and that they store the data collected. Whereas until 2003 interception was possible in all investigations relating to crimes and offences (crimes for which a prison sentence can be issued), the new law prohibits any preventive interception and provides, for the first time, for a catalogue of offenses. In the case of investigations on crimes and offences described in the catalogue, an instruction judge (*Untersuchungsrichter*), with the allowance of the prosecution chamber, can order providers to hand over the archived data. The same catalogue is relevant for real-time interception cases. In this case, a judge can compel a provider to install a direct connection of all telecommunications to the STS.[49]. In October 2003, the Law on the Surveillance of Mail and

---

44 <http://www.bigbrotherawards.ch/diverses/hallofshame>.

45 Articles 66-73, *Bundesgesetz vom 15. Juni 1934 über die Bundesstrafrechtspflege* (SR 312.0, Federal Criminal Procedure Code, *Procédure pénale fédérale*), <http://www.admin.ch/ch/d/sr/c312_0.html>, and: *Loi du 23 Mars 1979 sur la protection de la vie privée* (Law on the Protection of Privacy, March 23, 1979).

46 *Telecommunications Law* (LTC) of April 30, 1997. *Ordonnance du 1er décembre 1997 sur le service de surveillance de la correspondance postale et des télécommunications* (, December 1, 1997), available at *Ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication* (OSCPT), RS 780.11 from October 31, 2001, <www.admin.ch/ch/f/rs/c780_11.html>, in german Decree on the Monitoring of Mail Correspondence and Telecommunications. Until 2002, the technical procedures for wiretapping were carried out by a special service within former Telecom PTT (now Swisscom), the state monopoly company. The STS has been established in 2003 in order to technically establish a link between the requests of the judges and the data of the telecom providers. However, with the new system "Metamorphose" being introduced now, the DBA is also registering the requests in its own data base, keeping copies of the data for up to one year.

47 "Traffic data" means the technical data of the connections (*Kommunikationsranddaten*) sent by their customers by telephone, fax or the Internet. These data include the time, the sender and receiver's dial number, as well as – in the case of mobile phones – the geographical location.

48 *Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs* (BÜPF, SR 780.1) (*Loi fédérale sur la surveillance de la correspondance postale et des telecommunications*) <www.admin.ch/ch/f/rs/c780_1.html>, available at <www.admin.ch/ch/f/rs/c780_1.html> and its implementing decree, *Ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication* (OSCPT), RS 780.11 from October 31, 2001, available at <www.admin.ch/ch/f/rs/c780_11.html> (*Verordnung zur Überwachung des Post- und Fernmeldeverkehrs* (VÜPF, SR 780.11)), available at<http://www.admin.ch/ch/d/sr/c780_11.html>.

49 While at the beginning of the 1990s about 500 interception orders were issued annually, the number has continuously increased to about 2,000 orders since 1996 (2,138 cases). (Conseil National, Heures de Questions: Session d'hiver 1999,

Telecommunications was strengthened. In March 2003 already, the catalogue of criminal off,ences allowing interception -- chm: re-introduced, sorry for that) has been extended, introducing provisions combating against the "financing of terrorism."[50]

On October 21, 2003, the Federal Court decided in a unanimous vote that, in the case of wiretapping, the Federal Prosecutor has the duty to inform the persons observed after surveillance has been carried out, including information about the reasons of the monitoring.[51]

Prepaid mobile phone cards

In March 2003, the National Council (*Nationalrat*) passed a law which made it illegal to purchase cell phone SIM cards without providing personal information. The National Council followed in this point the decisions of the smaller chamber (*Ständerat*, or Council of States), that had already decided to pass such a law in December 2002, in the context of the UN Convention for the Suppression of the Financing of Terrorism.[52] In March 2004, the Swiss Attorney General (*Bundesanwalt* announced that tracking prepaid mobile phone cards (SIM cards) released by the Swiss telecom provider Swisscom helped the US intelligence find terrorists in Afghanistan.[53]

Réponse du Conseil fédéral concernant les écoutes téléphoniques (Answer by the Federal Council, Decembre 20, 1999) available at <http://www.parlament.ch/afs/data/f/gesch/1999/f_gesch_19993427.htm>.) To these orders, another 2,000 cases of disclosure of traffic data have to be added. Furthermore, Swiss authorities ordered 2,430 telephone taps in 2000 compared with 2,046 the previous year. More than a third of them were ordered in connection with a suspected breach in drugs law, an eighteen percent increase ("Phonetapping on the Increase," July 23, 2003, available at <http://www.swissinfo.org/sen/Swissinfo.html?siteSect=111&sid=1000096>) In 2002, lawful interception concerned 6,646 telephones, 2/3 of the mobile phones, that is 1,551 more than in 2001. Almost 3,000 real-time observations have been established in 2002. The tariff for lawful interceptions according to BÜPF has been changed for April 1, 2004. For Internet Service Providers, there are only two tariffs since then. One is for requests of past data from log files and it is CHF 538 flat (IP address, login number, email log). The other one is CHF 1,326 flat for real-time transmission of email messages. Since it is always a flat rate no matter how long the interception (or logs, up to six months) is, some suspect that law enforcement will always opt for maximum period just in case.

50 *See* <http://www.admin.ch/ch/d/as/2003/3043.pdf>.

51 Federal Court, BGE 8G.109/2003 of 21.10.2003, no publication. There have been numerous public revelations of illegal wiretapping. A 1993 inquiry found that phones used by journalists and ministers in the Swiss Parliament were tapped (Statewatch bulletin, Volume 3, Number 1, January-February 1993). The data protection commissioner also accused the Swisscom (Telecom PTT at that time), the state telephone company, of illegally wiretapping telephones. In February 1998, an agent for Israel's Mossad Secret Service was arrested by the Swiss authorities for attempting to tap the phone of a Lebanese immigrant whom he believed had links to the Hizbollah. On July 7, 2000 the Swiss court handed down a one year sentence to be suspended for two-years ("Swiss Court Hands Mossad Spy a Suspended One-year Sentence," Associated Press, July 10, 2000).

52 Topic *02.052 – Uno-Übereinkommen gegen Terrorismusfinanzierung und Bombenterrorismus* <http://www.parlament.ch/afs/data/d/gesch/2002/d_gesch_20020052.htm>. According to a New York Times report: "...following testimony from a Swiss federal prosecutor, Claude Nicati, that the Swisscom cards had become popular with Al [Q]aeda operatives." ("How Tiny Swiss Cellphone Chips Helped Track Global Terror Web," New York Times, March 4, 2004 <http://www.nytimes.com/2004/03/04/international/europe/04PHON.html?ex=1079384398&ei=1&en=efa2261f4a39d7e9>) . According to the telecom providers, more than two million prepaid SIM cards have been sold in Switzerland untill now. Approximately one third of all mobile phone customers in Switzerland are using a card of this type. In order to fulfil the new regulation, the Swiss government released a revision of the regulation VÜPF on June 23, 2004, forcing all Swiss telecom providers to sell their mobile SIM cards only if the customer provides a proof of their identity. This rule will come into force on August 1, 2004. According to telecom providers, aproximately 300,000 prepaid SIM cards have been sold anonymously since July 2002. For all these cards, the providers have to organize the registration _ex post_ by sending the customers a text message (SMS) asking them to register personally. If these customers fail to proof their identity, the providers will be compelled to block their SIM cards after October 31, 2004 (*See* Revision of the VÜPF, *Verordnung zur Überwachung des Post- und Fernmeldeverkehrs* (VÜPF, SR 780.11) <http://www.admin.ch/ch/d/sr/c780_11.html>, *Änderung vom 23. Juni 2004* <http://www.uvek.admin.ch/imperia/md/content/gs_uvek2/d/kommunikation/20.pdf>).

53 The New York Times wrote: "The investigation helped narrow the search for one of the most wanted men in the world, Khalid Shaikh Mohammed, who is accused of being the mastermind of the September 11 attacks." and explained, citing "a senior intelligence official based in Europe": "They thought these phones protected their anonymity, but they didn't (...) Even without personal information, the authorities were able to conduct routine monitoring of phone conversations." *See*Don Van Natta Jr. and Desmond Butler, "How Tiny Swiss Cellphone Chips Helped Track Global Terror Web," New York Times,

Electronic Warfare and Satellite telecom interception

In October 2003, the Swiss Government introduced a new regulation on electronic warfare.[54] The regulation allows the military forces to disrupt civilians' mobile phone communications and regulates radio interception, including the interception of satellite communications. Since the end of the 1990s, Switzerland is building up a system for satellite interception of the COMINT type (Communications Intelligence), similar to the UKUSA-"Echelon" system. The Swiss system, first called "Satos-3", then ONYX, started its operations in April 2000. All three operational sites are planned to be in operation by the end of 2005. Like the "Echelon" system, ONYX interception operates with software filtering the content of satellite communication for specific keywords.

In November 2003, the Controlling Delegation of the Federal Parliament (*Geschäftsprüfungsdelegation* or GPDel) released a detailed report on ONYX and presented some suggestions to improve the operational, as well as parlamentarian, controls over the system.[55] According to this report, ONYX and the UKUSA "Echelon" system are autonomous systems, without any technical interfaces. However, intelligence data is exchanged most probably on a case-by-case basis. ONYX is operated by a special agency of the Swiss Military forces, the Section for Electronic Warfare (EKF).[56] The Military Minister decides which governmental agencies are allowed to order ONYX interceptions. At this time, there are two agencies: The (military) Strategic Intelligence Agency (*Strategischer Nachrichtendienst*, or SND), responsible for foreign intelligence, and – to a minor degree – the (civil) Federal Police, responsible for domestic intelligence and "internal security" (*Dienst für Analyse und Prävention*, or DAP).[57] In the conclusion of their report, the GPDel suggests that the satellite interceptions ordered by the military SND should be precisely regulated by law.[58] Further, the GPDel urges the Swiss government to check the conformity of ONYX operations with the European Convention of Human Rights (ECHR), especially with its Article 8. Concerning domestic intelligence, the GPDel criticizes the absence of a law to regulate the competences of the Federal Police DAP. Finally, the Delegation urges for more transparency and for a political debate on

---

March 4, 2004 <http://www.nytimes.com/2004/03/04/international/europe/04PHON.html?ex=1079384398&ei=1&en=efa2261f4a39d7e9>).

54 *Verordnung vom 15. Oktober 2003 über die elektronische Kriegführung* (VEKF, SR 510.292), Inkrafttreten am 1. November 2003, <http://www.admin.ch/ch/d/sr/c510_292.html>. Art. 10 on "disturbing telecommunication". The regulation is based on the "Military Law" (*Militärgesetz* MG, SR 510.10), <http://www.admin.ch/ch/d/sr/c510_10.html>.

55 *Satellitenaufklärungssystem des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (Projekt "Onyx"). Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte vom 10. November 2003* <http://www.parlament.ch/ed-pa-gpd-onyx-d.pdf>. The report was also published in the official Bundesblatt on April 6, 2004 (p. 3, no. 1499) <http://www.admin.ch/ch/d/ff/2004/index0_13.html>.

56 *Abteilung Elektronische Kriegsführung*, EKF, which is a part of the "*Untergruppe Führungsunterstützung des Generalstabs*".

57 The third Swiss Intelligence Agency, the Air Force Intelligence Agency, can order interceptions by way of the SND. By ordering an interception, the agencies have to fix details of their orders, *e.g.*, the geographical area of the observation or a list of keywords. At the end of 2003, there have been 30 "contracts" (*Leistungsvereinbarungen*) established between the military SND and EKF, and one contract between the civil DAP and EKF. In other words: At this time, 92 percent of the ONYX operations were executed for the military SND, and eight percent for the civil DAP. The civil Police forces do not have direct access to the data collected for the military SND. An administrative "independent control group" has been established in October 2003 by the government to control the interception orders (UKI, *Unabhängige Kontrollinstanz*). ONYX is declared to be a tool for "foreign intelligence," not for "domestic intelligence." Therefore, the operating EKF is not allowed to transmit data concerning persons in Switzerland or Swiss citizens residing outside Switzerland to the military SND. Neither is EDK allowed to collect data concerning the Swiss "internal security" (*Innere Sicherheit*). However, this rule has been weeakened by beginning of 2004: If the EKF detects data concerning "internal security" "by coincidence" (*Zufallsfunde*), the agency is allowed to hand it over to the Federal Police (DAP), even if the data concerns Swiss residents. (Art. 5 Abs. 2 VEKF: "*Die EKF löscht grundsätzlich alle unabsichtlich erfassten und erkannten Informationen über inländische Kommunikationsteilnehmer. Sie kann solche Informationen jedoch bearbeiten und an den betreffenden Auftraggeber weiterleiten, soweit sie der Erfüllung des Auftrages dienen.*").

58 Today, the operations are fixed in the regulation only (VEKF, see above), but not in the "Military Law" (*Militärgesetz* MG, SR 510.10) <http://www.admin.ch/ch/d/sr/c510_10.html>.

Swiss satellite interception.[59] On March 24 2004, the Government welcomed the report of the GPDel and accepted to examine its [60] On July 6, 2004, the government presented its projects for funding military sites and infrastructures.[61]

DNA samples, biometry, and genetic screening

In July 2000, a regulation on the collection and storage of genetic profiles has been introduced, allowing the Swiss administration – by way of a new Agency called AFIS Services – to establish and operate a centralized data base with DNA profiles of persons and stains.[62] Data is collected by the Federal Office for Police since August 1, 2000. The regulation states that police forces are allowed to collect DNA samples only in case the offense committed is listed in a catalogue.[63] However, this catalogue does not only include crimes like murder, sexual offenses, life endangerment and rape, but also theft(*Diebstahl*).

All samples taken by the police are given a unique identifier, so that the name of the suspect is never disclosed to laboratory employees. The EDNA regulation is valid until December 2004. Afterwards, it will be replaced by a law which will not have any catalogue of offenses at all.[64]

In March 2004 the majority of the National Council decided to allow life insurance companies to review previous DNA analyses of persons in case they want to sign a contract with a life or a voluntary insurance company against invalidity. The law project still has to be approved by the smaller chamber (*Ständerat*).

Revision of the law on asylum

In May 2004, the National Council discussed a revision of the Law on Asylum.[65] The revision allows the collection of biometric data of immigrants and allows the police to transmit data of asylum seekers to their home nation, even before the request of the asylum seeker is decided upon. A minority in the National Council criticized the fact that this rule would bring asylum seekers and their relatives in danger. Despite the opposition, the National Council accepted the revision by 2/3 of the votes on May 5, 2004.

---

59 In spring 2004 the military intelligence services (SND, Strategischer Nachrichtendienst) published a booklet of 52 pages, however, without any news: <http://www.vbs.admin.ch/internet/gs/snd/d/nd_d.pdf>.

60 The answer was published on July 6, 2004 in the official Bundesblatt: "*Satellitenaufklärungssystem des Eidgenössischen Departementes für Verteidigung, Bevölkerungsschutz und Sport (Projekt 'Onyx'). Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte vom 10. November 2003. Stellungnahme des Bundesrates*" <http://www.admin.ch/ch/d/ff/2004/3115.pdf> in german; "*Système d'interception des communications par satellite du Département fédéral de la défense , de la protection de la population et des sports (projet 'Onyx'). Rapport de la Délégation des Commissions de gestion des Chambres fédérales du 10 novembre 2003*. Avis du Conseil fédéral <http://www.admin.ch/ch/f/ff/2004/2913.pdf>.

61 The report includes an additional amount of CHF 4.3 million for the ONYX site in Heimenschwand BE and CHF 1.2 million for the ONYX site at Leux VS. *Botschaft über Immobilien VBS (Immobilienbotschaft VBS 2005),* presented on 6 of July 2004 <http://www.admin.ch/ch/d/ff/2004/3215.pdf>.

62 *Verordnung über das DNA-Profil-Informationssystem* (EDNA, SR 361.1) <http://www.admin.ch/ch/d/sr/c361_1.html>.

63 EDNA, Article 5, for details on the procedure *see also* W.Bär, Adelgunde Kratzer & M. Strehler, "Swiss Federal DNA Profile Information System – EDNA," available at <http://www.promega.com/geneticidproc/ussymp12proc/abstracts/bar.pdf>.

64 *Bundesgesetz über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten oder vermissten Personen (DNA-Profil-Gesetz) – Entwurf*: <http://www.admin.ch/ch/d/ff/2003/4436.pdf>. *See* the discussion in the parliament (Nationalrat, Amtliches Bulletin, 20.06.03-08h00) <http://www.parlament.ch/ab/data/d/n/4619/86799/d_n_4619_86799_86951.htm>. In September 2002, the majority of the National Council decided, against the proposal of the preparing commission, not to include a catalogue in the new law on DNA profiles.

65 *Asylgesetzrevision*, *see* "Dossier Asylgesetz" of the Swiss Parliament and *"Sondersession 3.-5. Mai 2004: Überblick über die Entscheide des Nationalrats"* <http://www.parlament.ch/do-asylgesetz>.

Revision of the law on Foreigners

In May 2004, the National Council started the debate on the revision of the Law on Foreigners.[66] The larger chamber of the Federal Parliament decided to include biometric data in foreigners' identity documents. The law will also provide a definite legal basis for the Central Register of Foreigners, which now holds data on about 4.5 million persons. In order to avoid so-called "faked marriages" (*Scheinehen*), the law determines that marriage officers (*Zivilstandsbeamte*) will be allowed to investigate on the "honesty" of bi-national marriages. In June 2004, the National Council passed the Law, despite strong opposition in the parliamentary commission concerned.

Surveillance Cameras

After a pilot test in 2002-2003, the Swiss Federal Railway company SBB (now a private company, still owned by the state) announced a large project to install surveillance cameras in trains.[67] Until 2003, such surveillance was not allowed by law, neither was the operation of CCTV systems in train stations. In December 2003, a regulation was subsequently introduced, allowing the SBB to operate CCTV systems in train station, as well as inside trains.[68]

The city police of Zurich bought a new (mobile) camera system with capabilites for automatic car plate recognition (AFNES) to be operated in Zurich. It will be able to identify car plates and compare the results with the national data base RIPOL. With closer connections to EU justice and police agencies, Switzerland will most probably also gain direct access to European car plate data bases.

At the Zurich "Unique" airport, the cantonal Police of Zurich is testing a pilot system for automatic face recognition since the beginning of 2003. Officially, the Farec - Face Recognition system mainly aims at recognizing people trying to immigrate without identity documents. No results about the tests are available yet. The Zurich government is convinced that no explicit legal base is necessary for the tests. The data protection officier of the canton Zurich is quite skeptical about the usefulness of the system.[69]

Video surveillance is growing fast in Switzerland as well, as the cameras are getting smaller, cheaper and more sophisticated. This is especially true for the systems operated by private entities, such as shopkeepers or house owners. However, opposition against camera surveillance is growing as well: The committee of the Swiss "Big Brother Awards" has been organizing several "excursions" on the subject of surveillance cameras in Zurich and released a map locating the cameras in a city district of Zurich.[70] The Federal Data Protection Commissioner published a leaflet explaining the legal conditions for private individuals to operate video surveillance cameras.[71]

Private surveillance

Customer loyality programs (*Kundenbindungsprogramme*) are still expanding. According to the largest retail chain in Switzerland, Migros, more than one out of two households in Switzerland has a grocery shopping card. Data from the largest competitor, COOP, is similar. Smaller companies are also issuing their own cards. There is a growing risk that customers' databases are being merged, thus

---

66 *Ausländergesetzrevision*, Dossier: <http://www.parlament.ch/do-auslaendergesetz> and the *Bundesgesetz über die Ausländerinnen und Ausländer (AuG, Entwurf)* <http://www.admin.ch/ch/d/ff/2002/3851.pdf>.

67 *See* media release: <http://www.sbb.ch/gs/press/press_0303_d.htm#210303Kamera,berwachung>.

68 *Verordnung über die Videoüberwachung durch die Schweizerischen Bundesbahnen SBB (Videoüberwachungsverordnung SBB, VüV-SBB)* SR 742.147.2, <http://www.uvek.admin.ch/imperia/md/content/gs_uvek2/d/verkehr/schienenverkehr/vuev/1.pdf>, as well as the media release of the Departement UVEK, December 5, 2003: <http://www.uvek.admin.ch/dokumentation/medienmitteilungen/artikel/20031205/01748/index.html>.

69 *See, e.g.*, *Neue Zürcher Zeitung*, 23. August 2002, No. 194, at 37.

70 <http://www.bigbrotherawards.ch/kameras/>.

71 <http://www.edsb.ch/e/doku/merkblaetter/video.htm>.

providing increasingly detailed data profiles. As an example, in 2004, the second-largest Swiss retailer, COOP, has established a collaboration with the largest Swiss telecom provider Swisscom to share their respective "bonus points." Both companies stress that the exchange program consists only of aggregated data (*i.e.* bonus points), and that they did not exchange nor merge detailed information about specific customers.

The largest retailer, Migros, is involved in a research program on RFIDs (radio frequency identification tags) at the University of St. Gall, together with SAP and other software companies.[72] Until now, no large scale commercial use of RFID is known in Switzerland, with the exception of some ski lifts in mountain resort areas. Further, RFIDs are getting more and more used as access control devices by companies, libraries, schools, etc. In August 2002, the Swiss Federal Railway Company SBB decided to postpone their project of RFID-based contactless train tickets called "EasyRide". RFID chips have been used as identity tags at the UN "World Summit on Informations Society" (WSIS) in December 2003 in Geneva. The tags allowed to track the movements of the participants at the Summit.[73]

Insurance companies are interested in data about their customers. In summer 2003, the company "Winterthur" admitted that they used to keep secret data files on "risky customers," without informing the Federal Data Protection Commissioner, nor the customers, and thus not allowing their costumers to correct inaccurate data.[74] Further, according to media news in May 2004, some insurance companies are systematically using lie detectors (*Lügendetektoren*) in their call centers in order to detect if customers are lying when reporting their losses or damages (*Schäden*) without notifying them of this fact.

In a March 2004 revision of the Penal Code (*Strafgesetzbuch*), commercial companies are allowed to keep logs of phone conversations with their clients, even without their consent, for the purpose of securing evidence. However, they are not allowed to analyze this data for marketing purposes, nor to give this data to third parties.[75]

In the context of a large reorganization of the billing system of medical services provided by doctors and hospitals, the association of private health insurance companies (*Krankenkassen*), Santésuisse, is forcing the new tariff system Tarmed. According to this system, medical service providers have to include detailed ICD-10-Codes[76] in their bills, which are being handed over the insurance companies. By this system, the insurance companies get access to sensitive data about their customers. Although

---

72 Auto-ID Center at the University of St. Gall <http://www.m-lab.ch/>.

73 *See* press release, "The Physical Access Security to WSIS: A Privacy Threat for the Participants," December 12, 2003 <http://www.nodo50.org/wsis/>.

74 According to the Federal Law on Data Protection, every systematically organized database on personal data has to be registered at the Federal Data Protection Commissioner. (This rule may be abrogated in the current revision proposal). Further, the law states the right of everyone to get information about their personal data in the database, as well as the right to correct wrong data – with the exception of "secret data bases". In this case, the Federal Data Protection Commissioner has the duty to act as an intermediary. *See Bundesgesetz über den Datenschutz* (DSG, SR 235.1) vom 19. Juni 1992 (Stand am 3. Oktober 2000) <http://www.admin.ch/ch/d/sr/c235_1.html>. For an english translation *see* <http://www.ics.uci.edu/~kobsa/privacy/switzerland.htm> or <http://www.edsb.ch/e/gesetz/schweiz/index.htm>.

75 Presumably with the exception of giving away such data to investigating police forces, in the case that a judge ordered it. see: *Änderung des Art. 179 quinqies StGB, Abs. 1, Bst. b) vom 1. März 2004* (AS 2004 823). *Schweizerisches Strafgesetzbuch* (Code Penal) vom 21. Dezember 1937 (SR 311.0) <http://www.admin.ch/ch/d/sr/c311_0.html>, with the new article 179 quinqies: <http://www.admin.ch/ch/d/as/2004/823.pdf>.

76 IDC stands for International Code of Diseases. The International Statistical Classification of Diseases and Related Health Problems (commonly known by the abbreviation ICD) is published by the World Health Organization. It is currently in its tenth edition and is known as the ICD-10. *See* <http://www.yourencyclopedia.net/International_Code_of_Diseases>.

there have been critiques and protests by customers and doctors, as well as by Data Protection Commissioners, the Tarmed system is officially in operation since January 1, 2004.

The Swiss Football Association SFV (*Schweiz. Fussballverband SFV*) has been disclosing data about visitors of the European Football Championship "Euro 2004" in Portugal in May 2004.[77] For Switzerland, the SFV has been the exclusive seller of tickets for this championship. According to newspaper reports, the SFV informed the ticket buyers that they reserve the right to hand over the data of the visitors not only to the organizers of the "Euro 2004" (including UEFA, the Union of European Football Associations), but also to other parties – even for commercial purposes, which raises the likelihood of the constitution of large databases of football fans.

--> ## new subtitle, ??
In some cantons, the data protection law is at the same time a "Freedom of Information Law" (*Öffentlichkeitsgesetz*), and the data protection officer has the duties of a Freedom of Information Protection Officer as well. According to such laws, all official documents should be publicly available and citizens have a legal right to receive information - except if a document is declared as confidential. Other cantons and the Confederation are preparing a similar law..[78] However, the first consultations among interested parties are revealing considerable opposition, *e.g.* in the canton of Zurich

Switzerland is a member of the Council of Europe (CoE) and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108) in 1997.[79] Switzerland has also signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.[80] In November 2001, Switzerland signed, but has not ratified, the CoE Convention on Cybercrime.[81] It is a member of the Organization for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

---

77 Christian Maurer, "*Datenschutz: Gelbe Karte fuer Fussballverband*," *SonntagsZeitung*, February 1, 2004.

78 For the Confederation, see the proposal *Botschaft zum Bundesgesetz über die Öffentlichkeit der Verwaltung (Öffentlichkeitsgesetz, BGÖ)* <http://www.ofec.admin.ch/themen/oeffprinzip/bot-d.pdf>.

79 "*Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Abgeschlossen in Strassburg am 28. Januar 1981. Von der Bundesversammlung genehmigt am 5. Juni 1997. Schweizerische Ratifikationsurkunde hinterlegt am 2. Oktober 1997. Für die Schweiz in Kraft getreten am 1. Februar 1998*" (Übersetzung des französischen Originaltextes, Translation of the original in french, RO 2002 2847). SR 0.235.1) <http://www.admin.ch/ch/d/as/2002/2847.pdf>, Signed October 2, 1997; ratified October 2, 1997; entered into force February 1, 1998.

80 EMRK, signed in Rome on November 4, 1950, accepted by the parliament on October 3, 1974, ratified on November 28, 1974 <http://www.admin.ch/ch/d/sr/0_101/index.html>.

81 Signed November 23, 2001.