Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP
Post and Telecommunications Surveillance Service PTSS

Annual Report 2022
PTSS

■

Telecommunications surveillance must be viewed in its global context. English is the standard language used at international conferences, in international bodies and in the telecommunications industry itself. The English term Lawful Interception (LI) is now also widely used here in Switzerland. The Post and Telecommunications Surveillance Service adopted the use of the standard terminology in 2010. Since then, it has had its own website, at:

www.li.admin.ch

Dear reader

Any implementation of a measure involving the surveillance of post and telecommunications constitutes a serious infringement on the fundamental rights of the person concerned. Interventions affecting these constitutionally protected rights must be expressly provided for by legislation. The specific execution of a given measure is governed in detail by the implementing ordinances. Moreover, each surveillance measure must be approved by a court.

Or to put it as clearly as possible: There can be no gap whatsoever between the legal basis for a measure and its execution by the PTSS.

Telecommunications technology is developing at an exponential rate, offering more and more new services and possibilities for communication. The technical, organisational, and administrative framework of telecommunications surveillance must be adjusted regularly to keep pace with this development. These adjustments are led by the PTSS, with the involvement of law enforcement agencies and telecommunications service providers.

Even though telecommunications surveillance is changing rapidly, our legal mandate remains the same: ensuring effective law enforcement. One of the tools we have at our disposal for this purpose is our Special Cases Team.

"Even though telecommunications surveillance is changing rapidly, our legal mandate remains the same: ensuring effective law enforcement."

On the basis of a court order, this mobile unit can carry out surveillance measures at all telecommunications service providers operating in Switzerland. Starting on page 15, you can read about how a special operation like this works and how our experts are deployed to set up surveillance infrastructure on site.

For me personally, that article reminded me of when I joined the service 15 years ago. At the time, the PTSS had to rely on external partners to handle special cases. As a trained telecommunications technician and engineer, it was clear to me that this model would become obsolete in the face of rapid technological change. That is why the PTSS has increasingly developed its own competencies in all its areas of activity since 2010. This allows the PTSS to meet the challenges in its complex and highly specialised environment.

I hope you enjoy reading this report.

René Koch
Head of PTSS (until May 2023)

01

OVERVIEW

■ Telecommunications service providers include mobile, telephone, email, and internet service providers such as Swisscom, Sunrise, and Salt.

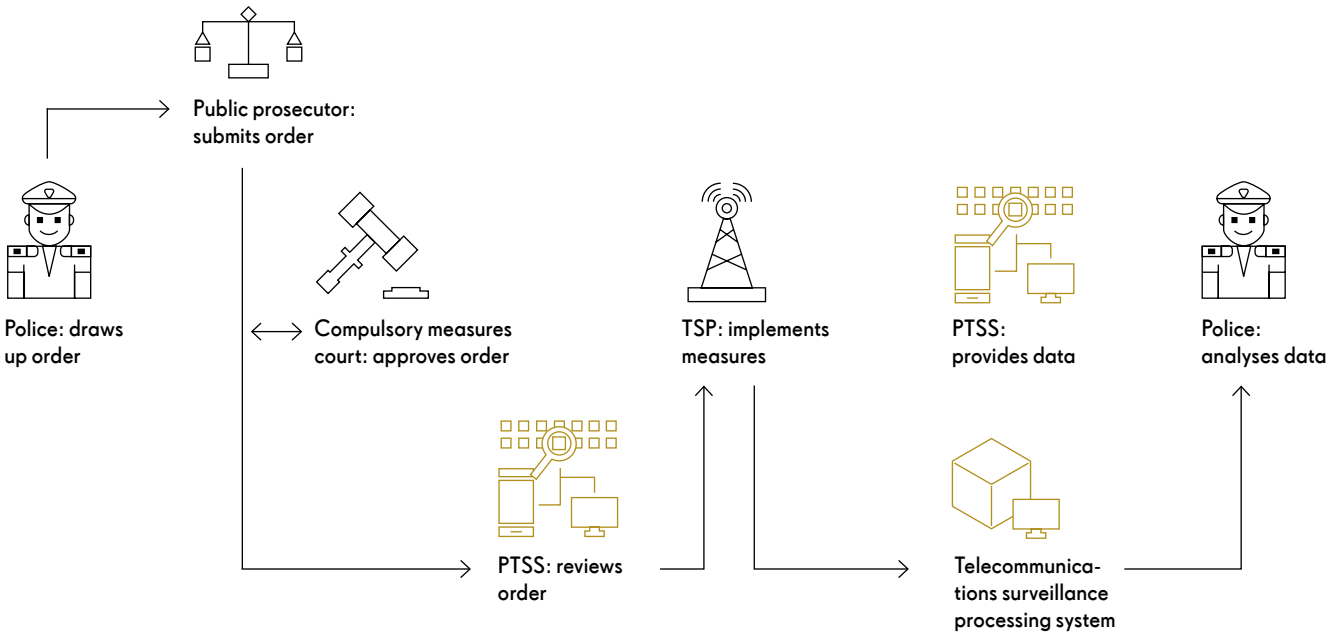
The PTSS: an overview

When investigating serious crimes, the federal and cantonal law enforcement authorities can order measures to conduct surveillance of postal and telecommunications activity. Since 1 January 1998, the Post and Telecommunications Surveillance Service (PTSS) has been responsible for carrying out these measures; it also ensures that the applicable legislation is observed. The law enforcement authorities or the Federal Intelligence Service (FIS) submit a request for data to the PTSS, which then obtains the data from the telecommunications service providers (TSPs); this is then passed on to investigators for analysis.

Neither crime nor modern telecommunications recognise geographical boundaries, so international cooperation plays an essential role in the fight against crime. The PTSS works to promote international standardisation and the exchange of knowledge and information with our counterparts abroad.

The PTSS is responsible for implementation of post and telecommunications surveillance. The PTSS acts independently and autonomously and is not subject to directives from other authorities. It is affiliated for administrative purposes to the IT Service Centre of the Federal Department of Justice and Police (ISC-FDJP). It is organised into four divisions.

The surveillance process



The four divisions

The PTSS management team (from left to right): René Koch (Head of the PTSS and of the Administrative Criminal Proceedings Division), Jean-Louis Biberstein (Head of the Legal Affairs and Controlling Division and Deputy Head of the PTSS), Alexandre Suter (Head of the Provider Management Division) and Michael Galliker (Head of the Surveillance Management Division)

Provider Management

The 22 staff of the Provider Management Division are responsible for creating and updating the technical specifications that the TSPs are required to observe when providing data to the PTSS. They are also responsible for the compliance procedure, in which the PTSS assesses whether the TSPs are able to conduct surveillance and provide information and data as required.

Under the Federal Act on the Surveillance of Post and Telecommunications (SPTA), TSPs must at all times be able to conduct surveillance of the services they offer and to provide the associated data and information, unless they have legally obtained an exemption from the obligation to do so.

The Provider Management Division's Special Cases Team develops tailor-made solutions for TSPs that are not themselves able to implement surveillance measures, or who are not legally required to do so. The team is therefore involved when, for example, a small provider such as a local cable network or hotel is required to conduct surveillance activities. See also the Special Cases article on page 15.

The staff also manage relationships with more than 900 providers, advise them on technical and legal matters, and issue related orders and decisions within the scope of their supervisory authority.

A team of four is responsible for ensuring the smooth functioning of the applications of the data processing system.

Furthermore, the Provider Management experts help to develop new applications and are active on a number of national and international standardisation committees, for example for the development and implementation of interface specifications for 4G and 5G networks.

Surveillance Management

The 17 members of the Surveillance Management Division are responsible for ensuring smooth interactions of the PTSS with law enforcement and the FIS.

The team advises police forces, public prosecution services, compulsory measures courts, and the FIS on all legal, technical, organisational and administrative matters relating to postal and telecommunications surveillance.

Staff receive surveillance orders, which they subject to a formal check before passing them on to the TSPs. The team ensures that the law enforcement authorities receive the data the TSPs subsequently deliver. Surveillance management also includes drawing up invoices for the law enforcement authorities and the FIS and making compensation payments to the TSPs.

The team is the central point of contact when there are problems with the processing system or users experience other difficulties, and it is involved in the development of new applications.

The Surveillance Management team also runs training sessions for users.

Outside office hours, it provides a duty service with technical support mainly from the Provider Management Division. This means the PTSS is available round the clock.

Legal Affairs and Controlling

Information and Communication Technology (ICT) is one of the most innovative sectors in the economy. It regularly introduces new standards, launching new services for increasingly powerful terminal devices. This has consequences for telecommunications surveillance, given that the technical interface between the PTSS's processing system and the several hundred TSPs needs to be constantly adapted.

Together with their colleagues from Provider Management, the specialists in the Legal Affairs and Controlling Division ensure that it is always possible to conduct telecommunications surveillance, even in a highly dynamic technological environment. The division is responsible for planning and managing all IT projects critical to the PTSS's mandate.

In addition to its responsibility for ensuring proper execution of IT projects, the team of 16 draws up the legal framework necessary to ensure that telecommunications surveillance is correctly conducted.

In many cases, this involves adapting ordinances to reflect the latest technological changes. For example, the departmental ordinance on conducting surveillance in post and telecommunications services is revised periodically and amended if necessary.

The Legal Affairs and Controlling Division also deals with financial management, reporting, and public relations. The staff respond to media enquiries and are available to answer questions from the general public.

Administrative Criminal Proceedings

The SPTA and the associated implementing ordinances give the PTSS additional tasks, one of which is to conduct administrative criminal proceedings. An independent chief investigator has duties similar to that of a public prosecutor.

Since March 2018, the PTSS has had the authority to prosecute anyone failing to fulfil their legal obligations in connection with the surveillance of post and telecommunications.

The two staff members of the Administrative Criminal Proceedings Division investigate complaints, establish the facts, carry out legal analyses and, if necessary, punish these contraventions. The director of proceedings can order coercive measures such as seizures and searches, as well as conduct interrogations.

When the proceedings are complete, the PTSS issues orders and decisions on penalties or orders to dismiss proceedings.

A look back at 2022

January

SLDT launch for users
The SLDT (secure large data transfer) solution permits large amounts of data to be transmitted electronically and securely to users. This makes it possible to avoid sending data carriers by post in certain cases. The first police organisations have successfully tested SLDT together with the PTSS, and users are now being granted access step by step.

February

Training resumes, albeit only on a small scale
After a long interruption due to the pandemic, the first on-site training sessions are being held again. The online training material developed during the pandemic is still available and will be further expanded.

March

Entry into force of the legal basis for analysis functions
On 11 March 2022, the Federal Council decided that the legal basis for the analysis function would enter into force on 1 May 2022. These amendments (Art. 7 and 8 SPTA) create the explicit legal basis to analyse telecommunications surveillance data in the processing system of the PTSS.

April

'La Suisse sous couverture' web series
On 25 April 2022, RTS announced the release of the second season of the 'La Suisse sous couverture' web series. The series includes a segment on the surveillance system of the PTSS. This 12-minute documentary is available at the following link: https://www.youtube.com/watch?v=k-fJ2lQ1aok8.

May

Proposal to the Federal Council 'Telecommunications surveillance: Additional personnel and financial resources for the PTSS and the ISC-FDJP'
The aim of the Telecommunications Surveillance Programme* is to replace and further develop the PTSS processing system. This programme, initiated in 2015, will be concluded in 2024. The PTSS will then take over responsibility for new components and related tasks from the programme organisation. The proposal aims to ensure that the PTSS has the necessary resources for these purposes. The proposal was discussed and adopted by the Federal Council on 4 May 2022.

Revision of the implementing ordinances (especially adjustments concerning 5G)
The consultation on the partial revisions of the four implementing ordinances for the Federal Act on the Surveillance of Post and Telecommunications (SPTA) ended on 23 May 2022. The PTSS received 68 responses as part of this consultation. The draft ordinances were modified on the basis of these submissions.

June

Federal Act on Police Measures to Combat Terrorism
The Federal Act on Police Measures to Combat Terrorism (PMCT) provides for various preventive police measures. It entered into force on 1 June 2022. The Act includes amendments to the SPTA. In particular, the measures include a new type of surveillance for mobile localisation.

July

First PTSS newsletter for law enforcement authorities
The first newsletter for users of the PTSS processing system was prepared and published in July 2022. It contains practical information on the daily work relating to telecommunications surveillance. The plan is for the newsletter to be published roughly twice a year.

* More information is available at www.li.admin.ch > Themes > Telecommunications Surveillance Programme

September

Preparations for the reorganisation of the PTSS
The PTSS was mandated to carry out a reorganisation. The goal is to optimise task fulfilment within the current organisational legal framework. Several workshops were held in the second half of 2022 for this purpose. The new organisation will be implemented effective 1 May 2023.

October

2022 customer satisfaction survey
Every two years, the PTSS conducts a customer satisfaction survey among the organisations benefitting from its services. According to the survey, satisfaction remains high. On a scale from 1 (very dissatisfied) to 6 (very satisfied), the following scores were achieved:
Overall satisfaction of evaluating authorities: Improvement from **4.7** to **4.9**
Overall satisfaction of ordering authorities: Improvement from **4.6** to **4.9**
Overall satisfaction of approving authorities: Decline from **5.7** to **5.5**

December

Ordinance on the Financing of Post and Telecommunications Surveillance: Office consultation concluded
The draft ordinance provides for the introduction of flat rates. The goal is to simplify the current financing and invoicing system and, at the same time, to increase the cost recovery ratio of the PTSS. The office consultation was concluded on 28 November 2022. A consultation procedure will follow in the first half of 2022. Entry into force is planned for 1 January 2024.

02

BACKGROUND

Mobile, flexible, and competent

A team for special missions

Small telecommunications service providers – such as local WLAN and cable network operators – can be exempted from the legal obligation to conduct surveillance. If suspicious actions occur in their networks and a court-approved surveillance decision has been made, the Special Cases Team of the PTSS takes over.

Eichenweg 3 in Zollikofen, campus of the Federal Administration. Two members of the Special Cases Team load cargo boxes with tools, cables, connectors, and electronic components. Using a goods lift, they bring the material into the delivery area.

The team leader is already waiting for them. A minivan stands ready. After loading, the adhesive with the logo of the Swiss Confederation is pulled off the door of the minivan, and then they're off. "No one should see from far away that we're coming," says the man at the wheel.

His boss takes the passenger seat. He is an internationally recognised specialist in lawful interception (LI). With a degree in computer science, he has worked for international telecommunications providers and network operators. After several assignments as an external LI expert, he joined the PTSS on a permanent basis in 2012. He has headed the team since 2017.

His speciality is data conversion, which is the core mission of the Special Cases Team: converting locally acquired data into the relevant standards of the European Telecommunications Standards Institute (ETSI).

Last year, about 10,000 surveillance measures took place in Switzerland – the vast majority in the networks of the major TSPs. Market leaders such as Swisscom, but also Sunrise and Salt, are required by law to be able to intercept data in their networks and transfer it in the prescribed formats to the PTSS processing system.

The SPTA defines different categories of entities obliged to collaborate: those who must actively implement the surveillance measures and those who must only tolerate them. The main concern here is proportionality. Medium-sized and small businesses that are not subject to a large number of surveillance measures should not have to make the investments necessary for that purpose. They are not required to build up their own LI competencies: They only have to tolerate that surveillance takes place. "The actual work – establishing the ability to conduct surveillance – is then carried out by our Special Cases Team," says Alexandre Suter, Head of Provider Management at the PTSS.

He estimates that more than 1,000 companies throughout Switzerland may be affected by special cases. These range from hotels that offer their guests free WLAN to internet access providers and providers of smartphone apps.

Since the revised SPTA entered into effect in March 2018, the Provider Management division has carried out special case assignments at about 40 companies. And each year, five to ten

Once the legal circumstances have been clarified, the technical discussion starts.

more providers – or individual clients of those providers – are targeted by law enforcement.

"Our work begins with a telephone call to the provider's LI officer," the team leader explains. Once contact has been established, the parties involved exchange critical information about target connections and devices via encrypted email.

Once the legal circumstances have been clarified, the Special Cases Team begins discussing the technical implementation. These discussions can be short (if a surveillance has already taken place) or longer (if this is the first time a provider is involved in a special case).

The extreme heterogeneity of telecommunications infrastructures requires special attention. Each provider relies on different software and hardware suppliers. Moreover, many providers run several system generations in parallel. The team must be prepared for countless combinations of terminals, connectors, and protocols. The team leader recalls: "Once, a network component that we absolutely needed was only available in Spain."

The minivan has reached its destination – a data centre in the greater Zurich area. An employee lets the team in. Outside, the sun is shining; inside, the server racks are blinking. Additional light comes from a few ceiling lights. The server farms are humming and the cooling systems are hissing.

"For years now, telephone and data traffic has been handled almost without exception in the cloud," the team leader explains. If unambig-

uous address elements are available for a suspicious person, the Special Cases Team's operations mainly take place in data centres like this one. Heading farther field – say, to the premises of a local cable network operator – is only necessary if the team has to be close to the target for technical reasons.

The team looks for a spot between the server cabinets and sets up. The Special Cases Team has brought the hardware required for the surveillance activity. The equipment is procured from manufacturers who also supply the law enforcement and intelligence services of other countries. Sometimes, however, the standard tools reach their limits. Then the operation follows a twin-track approach:

While one part of the team sets up surveillance on site, their colleagues back at the office develop a case-specific software solution. As soon as the server is online, connectivity tests

begin. Thanks to these tests, software changes can be uploaded up to the last minute.

One of the provider's specialists is available in the background. He answers questions that arise during the course of the operation. "Normally, cooperation is good," says the team leader. Exceptions prove the rule: Sometimes, a provider may offer passive resistance and only wants to allow the PTSS to do their job after consulting with a lawyer. In very rare cases – when the provider wants to prevent physical access to its infrastructure – PTSS Provider Management is forced to call in police support.

Software changes can be uploaded up to the last minute.

The motives of recalcitrant providers are often unclear. The PTSS does not even enter into contact with providers which are suspected by law enforcement of being close to the target persons. "In such cases, we take an alternative route to get at the target," the head of the Special Cases Team explains. He does not reveal what happens specifically when a provider's infrastructure cannot be accessed. "But one thing is certain: We always find a way."

Special case operations are generally about real-time surveillance. For the team, this means that the job is only complete when current communications data can be transmitted immediately and without interference to the PTSS processing system.

By about 3pm, the surveillance operation is ready. The team packs up its equipment and loads it back in the minivan. What stays behind at the provider is an inconspicuous box. This is the special case server that intercepts the suspect's data and voice traffic.

Now, it's up to the investigators and public prosecutors.

The big rebuild

The real-time surveillance component of the telecommunications surveillance processing system is being replaced. In the summer of 2021, implementation work began on the Federal Lawful Interception Core Component (FLICC).

When senior prosecutor Urs Hubmann uses the abbreviation IOC, he does not mean the International Olympic Committee, but rather Italian Organised Crime. "Italian organised crime is currently one of the great threats to our internal security."

The 65-year-old lawyer has headed the Office of the Public Prosecutor II (OPP II) of the Canton of Zurich since 2011. OPP II deals in particular with crimes that are not reported, but rather investigated on the basis of police suspicion. The aim is to use covert coercive measures to create an evidentiary basis that allows suspects to be brought to justice.

"Italian organised crime is currently one of the great threats to our internal security."

Urs Hubmann, Senior Prosecutor, Canton of Zurich

Aggravated robbery, drug and human trafficking

The focus is on cases of organised crime and serious gang crime. Offences range from aggravated robbery to qualified drug trafficking, human trafficking, serious cases of money laundering, and qualified cybercrime.

OPP II has a full toolbox at its disposal for investigating these crimes. In addition to the use of undercover investigators, the analysis of financial transactions, and the placement of microphones and cameras, tools also include the surveillance of telecommunications, whether retroactively or in real time.

Real-time surveillance allows investigators to track where the target is moving and what they are currently discussing with their conversation partner. In 2022 OPP II of the Canton of Zurich conducted more than 200 real-time surveillances, corresponding to about 20 % of the total number in Switzerland.

In technical terms, surveillance is performed using the Interception System Schweiz (ISS), the real-time component of the PTSS's telecommunications surveillance processing system. "The platform was acquired in 2013 and is showing its age," Ernesto Ruggiano says. Ruggiano is the project manager at the PTSS responsible for replacing ISS with the new Federal Lawful Interception Core Component (FLICC). The project was launched five years ago. The implementation phase began in the summer of 2021.

OPP II would rather have FLICC up and running today than tomorrow. The main reason is the technical development in the telecommu-

nications industry. ISS is simply not designed for telecommunications surveillance in light of today's state of technology, in particular the 5G mobile communications standard. "This means it takes a lot of time and effort to evaluate even a single surveillance session, such as a short telephone call," says Urs Hubmann.

What also complicates surveillance is a shift in communication behaviour. Even criminals spend a lot of time talking about irrelevant things. This means the flood of data investigators have to sift through is enormous.

Real-time surveillance of voice communications and text messages is scheduled to be available by mid-2023. This will be followed by integration of internet data and email surveillance and, finally, what could be called interior finishing, namely integration of new advanced functionalities.

Visualisation and automatic transcription

Examples of these advanced features include clear visualisation of the surveillance results, automatic transcription of voice messages with the option of translation, or evaluation of more precise localisations of devices under surveillance. "FLICC allows us to establish real-time surveillance as a modern, easy-to-use, and efficient investigation tool," says Ernesto Ruggiano.

Between 2016 and 2022, the number of real-time surveillances nationwide fell from 2,800 to just over 1,200. This fall is due not least to the fact that proceedings in which real-time surveillance serves as evidence are becoming increasingly complex and require more specialised knowledge. FLICC aims to change this.

Experts agree that high investigatory pressure keeps organised and serious gang crime from taking root in society. In particular, rigorous investigation and prosecution of the relevant criminal offences prevents gangs from carrying out their internal conflicts in public and from harming bystanders in violent confrontations.

"Excessive violence on the streets is still rare in Switzerland," says Hubmann. "We absolutely have to make sure it stays that way."

"We are establishing real-time surveillance as a modern and efficient investigation tool."

Ernesto Ruggiano, FLICC Project Manager, PTSS

“Switzerland is an attractive target.”

Tracking down spies, terrorists, and cyberattackers: Jürg Bühler is Deputy Director of the Federal Intelligence Service.*

Are you an avid newspaper reader, Mr Bühler?
Not especially. But in principle, all content published by domestic and foreign newspapers may contain information that is of use to an intelligence service. We refer to this as open source information, which the FIS systematically collects and evaluates. This gives me a good overview of the most important news items.

From what other sources does the Federal Intelligence Service (FIS) obtain information?
There are quite a lot. In principle, we can collect relevant information from all administrative offices of the federal government and the cantons. Via cooperation with the cantons, this is also true of the communes.

That still doesn't sound very exciting …
We also work with human intelligence, which means human sources recruited by our case officers. Case officers maintain contact with persons who have access to information that is important for the fulfilment of the FIS's mission. Case officers correspond quite closely to the public's image of a 'secret agent'. Finally, other sources of information are our international partner services and the cantonal intelligence services.

How many case officers are employed by the FIS?
We provide that information only to our supervisory bodies.

The counterpart to human intelligence is signals intelligence. What is that?
Signals intelligence is reconnaissance through technically generated signals, usually from communications equipment. This also includes radio reconnaissance of signals from abroad or from satellites in space. We also use cable reconnaissance: under certain conditions, we can intercept cross-border data flows and evaluate them according to search terms covered by our legal mandates; these may include certain names, projects, or address elements in telecommunications such as telephone numbers.

* The interview with Jürg Bühler was conducted in December 2021, before the start of the war in Ukraine.

This leads us to the topic of lawful interception (LI) and the PTSS. How important is telecommunications surveillance for the work of the Federal Intelligence Service?
It provides us with information that would otherwise be unavailable to us. In 2022, the FIS conducted two operations involving the use of such intelligence-gathering measures requiring authorisation. One related to counterterrorism, and the other to prohibited intelligence activities.

A total of 10,250 telecommunications surveillances took place in Switzerland in 2022. Of that number, 95 were ordered by the FIS. Why so few?
The legal requirements for the FIS's use of surveillance measures are very strict. The FIS has to request authorisation from the Federal Administrative Court to conduct any LI measure. If the court approves the measure, it must be released by the head of the DDPS, who must first obtain the opinions of the heads of the FDFA and the FDJP. We cannot initiate the measure before it has been approved.

One of the founding fathers of the PTSS

Jürg Bühler has been a member of the management board of the Federal Intelligence Service (FIS) since it was set up in 2010. His police and intelligence activities in the service of the Swiss Confederation date back to the 1990s, however. He was around in the days of the Swiss Posts, Telephones and Telegraphs (PTT) monopoly, when telecommunications surveillance was still performed by the separate district directorates: "Surveillance was mostly performed by female specialists who listened in with headphones and recorded the relevant conversations." Liberalisation of the telecommunications industry presented lawmakers with a twofold challenge: Firstly, they had to set out the surveillance obligations of the new, private providers; secondly, they had to create a provider-neutral service for the sovereign task of telecommunications surveillance. Bühler, now 58-years-old, was then head of forensic police investigations at the Federal Police: "In a national working group, we developed proposals together with the legal service of Telecom PTT for a surveillance service operated by the federal government." The result was the Special Tasks Service (STS), which took up its work on 1 January 1998. Exactly ten years later, the STS moved from DETEC to the FDJP. Since then, it has been operating under its current name, PTSS.

“Qualified cyberattacks almost invariably take place across borders.”

Jürg Bühler, FIS Deputy Director

Even if there is a suspicion that Switzerland’s national security is at risk?
That’s a prerequisite anyway that must be met before we can apply any such measure. As part of the response to the secret files scandal in the 1990s, lawmakers deliberately curtailed the leeway of the former domestic intelligence service. Until the Intelligence Service Act entered into force in September 2017, we were prohibited from engaging in domestic telecommunications surveillance. Since then, we have been making use of this possibility, albeit to a much lesser extent than opponents of the Act feared at the time. This is documented in the statistics we publish each year.

The key responsibilities of the FIS include counterespionage. Who spies in Switzerland?
We estimate that several thousand foreign intelligence officers operate in Switzerland on a permanent basis. About a quarter of the staff of the diplomatic missions of certain countries – I don’t want to name any names – is engaged in intelligence tasks.

Is Switzerland that important to foreign powers?
Switzerland is a high-tech country and accordingly an attractive target for economic espionage. Moreover, Geneva is home to a large number of UN bodies. As the host state of international organisations, we have a responsibility to prevent political espionage against third parties on our territory. This means that the FIS also collects and evaluates information suggesting that a government acts against non-governmental organisations, ethnic minorities, or opposition groups within Switzerland.

Let’s look at counterterrorism, which gave rise to three out of four telecommunications surveillance measures last year. What is the FIS’s focus?
The focus is currently on the ‘Islamic State’.

What groups of persons pose a threat?
In Switzerland, the threat emanates from individuals radicalised here who have been inspired by jihadist propaganda and by personal contacts, but increasingly also from persons for whom radicalisation and violence are linked to personal crises or psychological problems. Both groups can carry out spontaneous attacks, mainly on soft targets. Even more of a threat are terrorists from

abroad who have orders to carry out targeted attacks. We can see that these two groups cooperate to some extent: Terrorists from abroad recruit amateurs within Switzerland in order to train them.

Probably the most prominent threats to our national security are perceived to be cyberattacks against public facilities such as hospitals or the power supply. In your assessment, is this perception correct?
The number of computer-assisted attacks on military and civilian targets is steadily increasing worldwide. They pose a significant threat to Switzerland as well, given its highly digitalised infrastructure.

Is the FIS prepared for threats from cyberspace?
Our cyber division is responsible for detecting and preventing attacks against the computer systems of critical infrastructures at an early stage. You have to bear in mind, however, that the legal basis for our activities entered into force more than five years ago. During the parliamentary debates leading up to the popular vote in the autumn of 2016, the threat from cyberspace still seemed manageable. Parliament and the population gave clear priority to protecting privacy. This means that before engaging in surveillance of suspicious activities – whether using GovWare or via the PTSS – we have to show that there is a direct and serious threat to national security. But that is precisely what causes problems.

Why?
Because qualified attacks almost invariably take place across borders. The last stop of a cyberattack before it is launched is nearly always beyond Switzerland's borders. This means: Cyberattacks for which infrastructures in Switzerland are misused are directed against facilities abroad, which means they do not constitute a direct threat to Switzerland within the meaning of the law. But from the perspective of defending against threats, reconnaissance in these cases is nevertheless important to protect Switzerland against attacks as well.

How do the intelligence services of our neighbouring countries deal with cross-border attacks?
We are surrounded by countries governed by the rule of law. There as well, the concept of 'national threat' is comparatively narrow. Consequently, some of these countries likewise do not have a legal basis for detecting and thwarting any preparations for attacks on targets in Switzerland. This is a structural problem that attackers can specifically exploit. The problem must therefore be addressed at both the national and international levels.

Has Switzerland already taken steps in this direction?
The Intelligence Services Act is currently being revised. The plan is to include threats to important international security interests as grounds for the use of intelligence-gathering measures that require authorisation. This would also expand our options when combating cyberattacks.

03

FACTS AND FIGURES

Reasons for surveillance

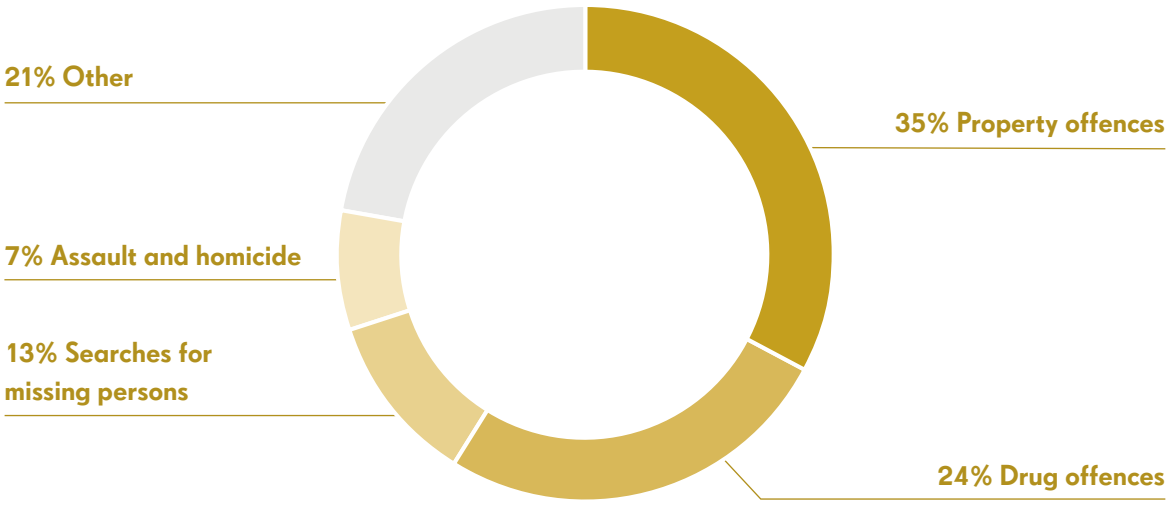
According to police crime statistics, 549,404 offences were reported in Switzerland in 2022. Telecommunications surveillance was used as an investigative measure 10,253 times, a comparatively low figure.

It is worth noting that several surveillance orders may result from one offence or one procurement measure requiring authorisation. For example, both the landline and several mobile phones belonging to a suspected offender can be monitored. Furthermore, the same mobile phone number is often the subject of various obligations to cooperate in surveillance, in order to be able to cover all roaming cases. The number of persons actually under surveillance is therefore noticeably lower than the number of surveillance measures ordered.

Surveillance measures were most often used to investigate property offences, e.g. theft and fraud (35%). In second place, at 24%, were serious narcotics cases, with assault and homicide cases in fourth place, at 7%.

Telecommunications surveillance can also be used to search for missing persons. In 2022, these searches accounted for 13% of all cases, coming in in third place.

You can find further information on our statistics at:
www.li.admin.ch/en/stats



Definition and number of surveillance measures and types of information

Real-time surveillance (1)
Real-time surveillance is the simultaneous, slightly delayed or repeated transmission of post or telecommunications data to the law enforcement services over the processing system.

Retroactive surveillance (2)
Retroactive surveillance involves, in particular, the inspection of telephone records (who called whom, when and for how long).

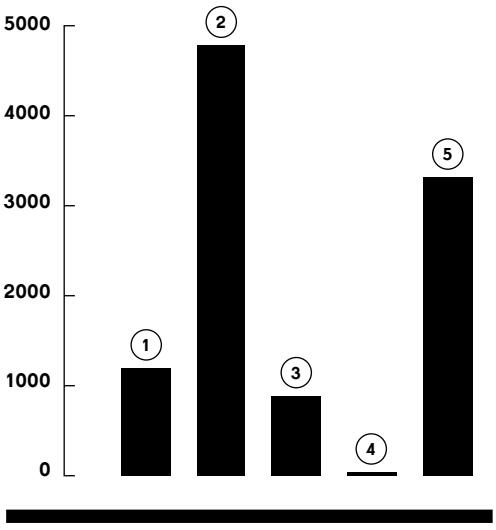
Searches for missing persons (3)
The purpose of these searches is to locate and rescue people, such as injured hikers or missing children.

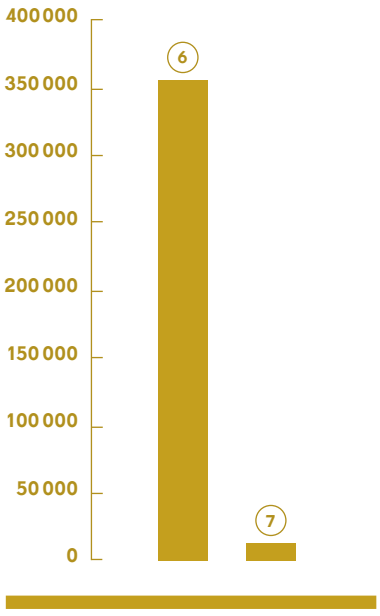
Searches for convicted persons (4)
A criminal search enables law enforcement services to locate the whereabouts of people on whom a custodial sentence has been imposed or against whom a measure involving deprivation of liberty has been ordered in a legally binding and enforceable judgment.

Antenna search (5)
An antenna search involves a mobile radio cell or a public WLAN access point. It registers all communication, attempts at communication and network access within a specific time frame.

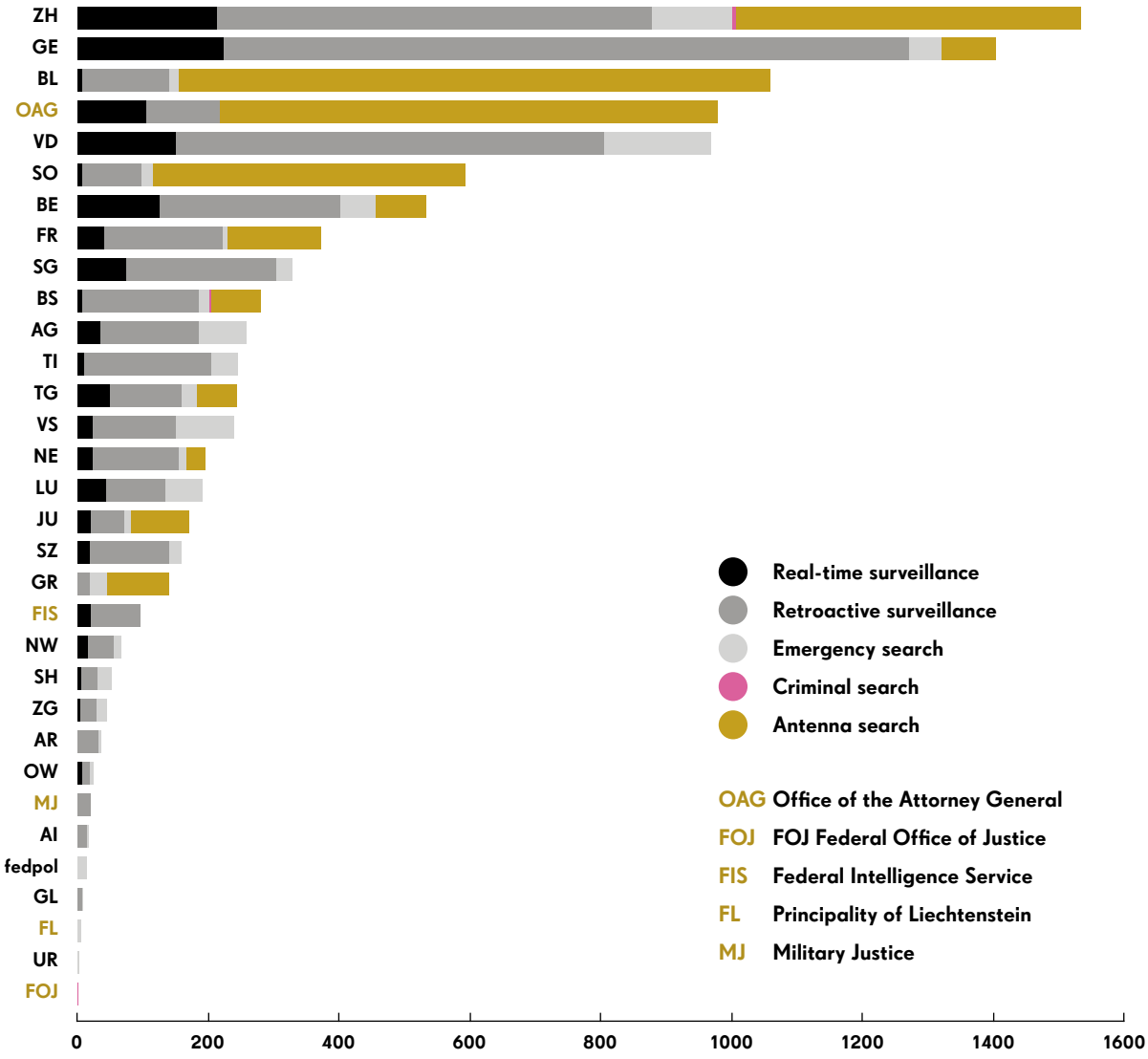
Simple information (6)
Simple information includes basic information on telecommunication connections, for example who the subscriber of a particular telephone number or IP address is.

Complex information (7)
Complex information provides more detailed information on telecommunications connections, including copies of contracts and identity documents.





Mandates from the federal government, cantons and Liechtenstein

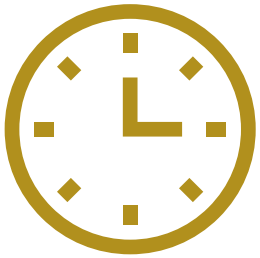


Surveillance orders of the Federal Office of Justice
The Federal Act on the Surveillance of Post and Telecommunications (SPTA) provides for surveillance not only for criminal proceedings that are ongoing in Switzerland. Corresponding measures can also be carried out in the execution of a request for mutual legal assistance submitted by foreign authorities. The Federal Office of Justice (FOJ) is responsible for mutual assistance cases.

Number of enquiries from the public

24

Number of on-call assignments



870

Registered users processing system

WMC 2400
Warrant Management Component

IRC 4300
Information Request Component

RDC 2200
Retained Data Component (retroactive surveillance)

ISS 2450
Interception System Schweiz (real-time surveillance)

Number of Special Cases

83

(See p. 8/9, Provider Management and p. 15 – 19 "A team for special missions")

Number of media enquiries

21

PTSS financial performance in CHF

Total revenue
12.4m

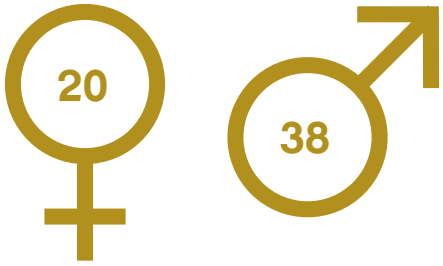
Total expenditure
31.7m

Federal contribution
19.3m

Number of employees

58

Numbers of women / men



Average age

46.5

First language

67% German

6.4% Italian

24.5% French

2.1% Other

Age distribution

20 to 29
10%

30 to 39
19%

40 to 49
26%

50 to 59
40%

60 to 69
5%

“The actual work, namely establishing the ability to conduct surveil-lance, is carried out by our Special Cases Team.”

Alexandre Suter, Head of the Provider Management Division

Publication details

Concept: PTSS
Editing: PTSS
Collaboration: JNB Journalistenbüro, Lucerne
Realisation: Schön & Berger, Zurich
Printing: Druckerei Ruch, Ittigen
Photos: Lia Lüthi, Barbara Hesse, David Kelly
Font: Minion Pro, Drescher Grotesk
Paper: Z-Offset
Language: German, French, Italian and English

■

In the interests of legibility and comprehension, we have refrained from using complex technical and legal terms. We have also tried to use gender-neutral language where possible.

Federal Department of Justice and Police FDJP
Post and Telecommunications Surveillance Service PTSS
3003 Bern