



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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



Annual Report 2023

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

	Editorial by the management team	4
01	Overview	
	The PTSS: an overview	7
	Main events in 2023	11
02	Background	
	The principles of surveillance in Switzerland	15
	From the prosecutor's order to the PTSS	
	In the service of our users	18
	An interview with Valentin Murariu, Head of Requirements Management, and Fatima Ghobrini	
	How investigators catch the criminals	20
	Tom Bader and Adrian Durrer from the Lucerne Police give an insight into their work.	
	Standardisation – “We're working on the future.”	23
	From requirements to standards	
03	Facts and figures	
	Surveillance measures in detail	27
	Our staff, their tasks and our finances	30



The PTSS management team (from left to right): Jean-Louis Biberstein, Michael Galliker, Alexandre Suter, Tobias Beljean

Dear reader

The legal framework for telecommunications surveillance has to be regularly updated to take account of the ever-evolving nature of telecommunications technology. In November 2023, the Federal Council amended the implementing ordinances to the Federal Act on the Surveillance of Post and Telecommunications (SPTA), to prevent any gaps in surveillance following the introduction of 5G. In this annual report, you will find out more about international standardisation, which is also reflected in telecommunications surveillance legislation. The relevant article is on page 23.

Another milestone last year was the Federal Council's decision to introduce a new

financing ordinance with effect from 1 January 2024. Until the end of 2023, telecommunications surveillances were billed to the cantons on a case-by-case basis. Moreover, around 70 % of surveillance services were funded by the federal government, although it used only 10 % of these services for itself. The new financing ordinance greatly simplifies the invoicing system by introducing annual flat rates for the cantons. The rates are such that the cantons now bear around 75 % of the cost of surveillance services.

The PTSS's processing system also has to keep pace with developments in telecommunications. The Telecommunications Surveillance Programme improves the quality of surveillance

“The PTSS reorganisation has provided an important foundation for the adoption and further development of the new IT applications.”

of the various communication channels (mobile telephony, internet, etc.). It is intended to ensure that the needs of prosecution authorities in the context of telecommunications surveillance can continue to be fully met in accordance with legal requirements. We reached a key milestone in this regard last year, with the new real-time surveillance component FLICC successfully entering the productive pilot phase in August 2023.

The Telecommunications Surveillance Programme is expected to be concluded by mid-2024. Its activities will then be taken over by PTSS. The preparatory work for this already got under way last year. The PTSS reorganisation has provided an important foundation for the adoption and further development of the new IT applications. In undertaking the reorganisation, we

have made sure that the needs of our customers can be systematically recorded and taken into account even after the programme organisation is disbanded. For more on this subject, check out the interview with the new Requirements Management Team on page 28.

2023 also saw a change in personnel as René Koch, who was instrumental in the development of the PTSS for many years, decided to take on a new professional challenge. We would like to thank him for his major contribution to telecommunications surveillance in Switzerland. His successor, Daniela Schär, took up her new role on the 1st February 2024. A profile of the incoming PTSS head can be found on page 13.

We hope you enjoy reading this report.

Tobias Beljean
Interim Head of the PTSS



Jean-Louis Biberstein
Deputy Head of the PTSS, Head of the
Legal Affairs and Controlling Division



Michael Galliker
Head of the Surveillance Management
Division



Alexandre Suter
Head of the Provider Management Division



01

OVERVIEW

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

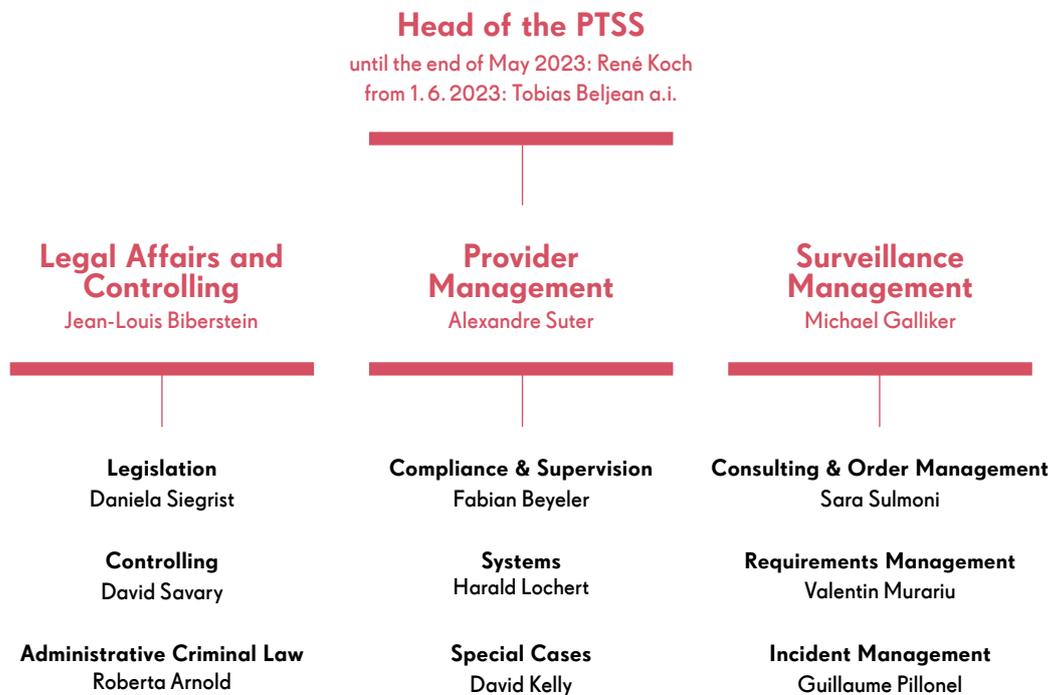
The PTSS: an overview

When investigating serious offences, the federal and cantonal law enforcement authorities can order measures to conduct surveillance of postal and telecommunications activity. Since the 1st September 2017, the Federal Intelligence Service (FIS) has also been authorised to order surveillance measures from the Post and Telecommunications Surveillance Service (PTSS) in case of a threat to Switzerland's internal or external security. Since the 1st January 1998, the PTSS has been responsible for carrying out these measures in a legally compliant manner and in accordance with the rule of law. The authorities make a request for data to the PTSS, which obtains the data from the telecommunications service providers (TSPs); this is then passed on to investigators for analysis. The service also ensures that the applicable legislation is observed and that the public's fundamental right to privacy is protected.

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).

Neither crime nor modern telecommunications recognise territorial borders, 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 organised into three divisions, each of which is now divided into three teams.



Legal Affairs and Controlling

The **Legal Affairs and Controlling Division** is responsible for the legal and operational framework of the PTSS's work. The team is tasked with drawing up the necessary legal framework to ensure that telecommunications surveillance is correctly conducted. This safeguards the public's right to privacy and is a key requirement in ensuring that the data gathered can be used in court. The Legal Affairs and Controlling Division is split into three teams: Legislation, Controlling and Administrative Criminal Proceedings.

The **Legislation Team** is responsible for the entire legislative process at the PTSS. This includes implementing legislative projects for all ordinances relating to postal and telecommunications surveillance. For example, the FDJP Ordinance on the Implementation of Post and Telecommunications Surveillance (OI-PTS) is reviewed periodically and amended if necessary. In many cases, this involves adapting ordinances to reflect the latest technological changes. This team is also responsible for representing Switzerland and participating in national and international standardisation bodies, as well as political affairs in collaboration with the General Secretariat. In addition, it provides in-house advice and support

in all proceedings involving the administration of justice. Staff respond to media enquiries and handle requests for information from the public. Training administration is now also the responsibility of the Legislation Team.

The **Controlling Team** performs cross-cutting functions for the PTSS, including financial management, controlling and reporting. It issues invoices to law enforcement authorities and the FIS and makes compensation payments to TSPs. Legal project support as well as risk and process management also fall within the team's remit. This team also includes the information security officer and the data protection officer for the organisational unit.

The **Administrative Criminal Proceedings Team** exercises the PTSS's administrative criminal law competences and conducts proceedings on behalf of the service. In so doing, it acts independently and is not subject to directives from other authorities.

Provider Management

The **Provider Management Division** is responsible for all matters relating to cooperation between the PTSS and entities obliged to cooperate (providers, in particular TSPs). The division has supervisory authority over the latter and responsibility for the processing system, including all PTSS applications. Its staff also manage relationships with some 1,000 providers, advise them on technical and legal matters, and issue related orders and decisions within the scope of their supervisory authority. The division's remit also includes sharing information and knowledge with other organisations in Switzerland and abroad. The Provider Management Division is

split into three teams: Compliance and Supervision, Special Cases and Systems.

The **Compliance and Supervision Team** is responsible for maintaining relations with persons and entities obliged to cooperate. This includes advising them on legal, technical, organisational and administrative matters. Under the 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 are legally exempted from the obligation to do so. The Compliance and Supervision Team verifies this capability to carry out surveillance and provide information (known as the "compliance assessment procedure"). The team also exercises the PTSS's supervisory authority over those required to cooperate with it.

For TSPs that are not themselves able or legally required to do so, the Provider Management Division develops and operates tailor-made solutions for implementing surveillance measures. These cases are handled by the **Special Cases Team**. It is involved when, for example, a small provider such as a local cable network operator or a hotel is required to conduct surveillance activities. This team is responsible for developing and operating all customised and complex surveillance measures. Within this framework, it also manages operational projects for the PTSS.

The **Systems Team** is tasked with ensuring the smooth functioning of data processing system applications. It oversees the operation and further development of components. Supplier, test and release management is also part of its remit.

Surveillance Management

The **Surveillance Management Division** handles the PTSS's interaction with law enforcement authorities and the FIS. It takes care of operational business, specifically order processing, consulting and incident management. Together with the IT Service Centre ISC-FDJP, its staff are the single point of contact in case of problems with the processing system or other difficulties experienced by users. This division is also involved in the development of new applications. The Surveillance Management Division is split into three teams: Consulting and Order Management, Requirements Management and Incident Management.

The **Consulting and Order Management Team** advises police forces, public prosecution services, compulsory measures courts and the FIS on legal, technical, organisational and administrative matters. It examines, processes and monitors surveillance orders, emergency searches and searches for wanted persons. Staff receive surveillance orders, which they subject to a formal check before passing them on to the TSPs. They then ensure that law enforcement authorities receive the data supplied by the TSPs. The team also processes requests for information.

The **Requirements Management Team** is responsible for the further development of the telecommunications surveillance processing system. It ensures that the system is adapted to the changing requirements of users and to changes in processing and analysis capabilities. With its expertise, the team supports the planning and steering of all mission-critical IT projects. It is also responsible for project management and architecture in connection with brand-new initiatives.

The **Incident Management Team** deals with problems affecting data transmission in operational business. It also offers technical advice in complex cases.

Outside office hours, Surveillance Management provides standby cover with the technical support of the Provider Management Division in particular. As such, the PTSS is available around the clock.

A look back at 2023

January

Procedure before the ECHR

On the 23rd January 2023, the Federal Office of Justice (FOJ) received the PTSS's opinion for the response to the European Court of Human Rights (ECHR) in the case of Glättli and others (Digitale Gesellschaft) v. Switzerland. This concerns the question of whether six-month data retention in Switzerland is permissible.

February

Consultation opened on the PTSS financing ordinance

On the 22nd February 2023, the Federal Council opened the consultation on the Ordinance on the Financing of Post and Telecommunications Surveillance (FO-PTS). The draft ordinance provides for the introduction of flat rates. The goal is to simplify the previous financing and invoicing system while increasing the percentage of costs recovered by the PTSS.

March

First SPTO revision – adaptation to technical innovations (5G)

The office consultation on the first partial revision of the Ordinance on the Surveillance of Post and Telecommunications (SPTO) began on the 24th March 2023. The aim is to adapt telecommunications surveillance to developments in technology.

April

Publication of 2022 annual statistics

The annual statistics for 2022 and related press release were published on the 28th April 2023. The statistics can be found at www.li.admin.ch/en/stats.



May

PTSS reorganisation

The reorganisation of the PTSS was implemented on the 1st May 2023. The main aim of the reorganisation was to structure the PTSS in such a way that it can better serve the interests of its various partners, in particular the prosecution authorities and the Federal Intelligence Service. Another goal was to enable the PTSS to take over the tasks assigned to it after the end of the Telecommunications Surveillance Programme (see box on page 19).

June

Au revoir René!

René Koch left the PTSS at the end of May 2023 after heading up the service for 15 years. We would like to thank him for his tireless commitment and dedicated service. Tobias Beljean took over as interim head on the 1st June.

July

Annual Report 2022 available online

The PTSS Annual Report 2022 was published on Friday 28th July 2023.

August

FLICC 1.0 productive pilot

The productive pilot of FLICC 1.0, the PTSS's new modular component for real-time surveillance, was launched on the 21st August 2023.

September

New Data Protection Act

The new Data Protection Act came into force on the 1st September 2023. The regulations governing the telecommunications surveillance processing system were also updated.

New PTSS head

In late September 2023, staff were informed that Daniela Schär would take over as head of the PTSS on the 1st February 2024.

October

Report in response to postulate 19.4031

by Albert Vitali

The Federal Council considers the Federal Act on the Surveillance of Post and Telecommunications Traffic (SPTA) to be sufficiently SME-friendly, with only some action needed at ordinance level. This is highlighted in the report 'Für ein verhältnismässiges Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs' (For a proportionate Federal Act on the Surveillance of Post and Telecommunications), which the Federal Council adopted at its meeting on 18 October 2023 in response to Albert Vitali's postulate 19.4031. The report states that the categorisation of companies subject to a duty to cooperate should be stipulated at ordinance level.





New PTSS head

Daniela Schär was deputy head of the Legal Data Processing Unit at the Federal Office of Justice (FOJ) and last year served as interim head of that unit and of the Swiss Criminal Records Unit. Prior to this, she was for several years the overall project manager for the 'NewVOSTRA criminal records information system' project and managed up to 35 employees in various roles at the FOJ.

Daniela has many years of leadership experience as well as extensive experience in project management, procurement under the WTO Government Procurement Agreement and in the implementation and supporting of departmental affairs. Before that, she worked in several other FOJ departments. Among other things, she reorganised the Swiss Criminal Records Unit and led various organisational and interdisciplinary projects for several years as an assistant to the Deputy Director of Central Services.

Daniela has a degree in information science. She also gained an Executive Master of Public Administration (eMPA Unibe) at the University of Bern in 2017.

She is also a certified senior project manager of the International Project Management Association (IPMA), Level B.

Daniela is 38 years old. She is married and lives in Burgdorf. In her free time, she enjoys cycling around Switzerland and, when the weather is less good, cooking up a feast for family and friends.

November

FO-PTS and first partial revision of SPTO (5G): entry into force on 01.01.2024

At its meeting on the 15th November 2023, the Federal Council decided to bring the FO-PTS into force on the 1st January 2024. The new ordinance provides for flat rates, which will reduce the administrative burden for all parties involved.

Another three SPTA implementing ordinances were updated to reflect technological developments, including 5G. These also come into force on the 1st January 2024. The aim is to avoid gaps in telecommunications surveillance, enable more precise positioning and continue to ensure effective prosecution.

02

BACKGROUND

The principles of surveillance in Switzerland

When we hear the word “surveillance”, alarm bells automatically start ringing. And rightly so, because surveillance, regardless of the context in which it takes place, is an invasion of privacy.

In Switzerland, privacy is protected as a fundamental right in the constitution. As such, it is an essential right vis-à-vis the state that is guaranteed to everyone at all times. In certain cases, however, the law states that this fundamental right of an individual may be curtailed for the general good by means of the surveillance of post or telecommunications (‘surveillance’). Because Switzerland is a state governed by the rule of law, any encroachment on fundamental rights as serious as surveillance is only possible within a strictly controlled framework. The Post and Telecommunications Surveillance Service (PTSS) ensures that surveillance can be carried out in Switzerland. However, it is also the guarantor vis-à-vis the public that surveillance is conducted in accordance with the law.

Every criminal investigation is triggered by an offence that has been committed. The prosecution authorities, including public prosecutors and the police, need to investigate in order to solve these crimes and track down the perpetrators. Surveillance is a tool that prosecution authorities are authorised to use as part of their investigations. However, this tool may only be deployed for serious offences. The circumstances that can give rise to surveillance are listed exhaustively in the Swiss Criminal Procedure Code (CrimPC). Surveillance is not permitted in the case of non-serious offences.

In the course of the investigation, suspicion falls on one or more individuals. In order for surveillance to be used, the suspicion against the person or persons concerned must be demons-

The PTSS guarantees the population that surveillance in Switzerland fulfils the legal requirements.

trably substantiated. In other words, there must be a probability bordering on certainty that they were involved in the offence.

As noted above, surveillance is a very serious encroachment on fundamental rights. This tool is therefore only to be used as a last resort. The prosecution authorities must prove that they have already deployed all other less invasive means without success or that the investigation would be disproportionately prolonged or even rendered impossible without surveillance. This subsidiarity is an indispensable prerequisite for surveillance.

If all of the above requirements are met, a public prosecutor must be convinced that surveillance is actually necessary and appropriate in the investigation in question. When this is the case, they will order the PTSS to place the suspected persons under surveillance.

As soon as the PTSS receives the surveillance order from the public prosecutor's office, it undertakes a formal examination. Among other things, it considers whether the authority is authorised to order surveillance, whether the offence in question corresponds to the list of criminal offences in the Criminal Procedure Code, and whether the surveillance measure ordered is permissible. In other words, it checks all the formal legal requirements that an order for surveillance must fulfil under the legal framework. If there are any unanswered questions, the PTSS will contact the public prosecutor concerned.

The PTSS is not a judicial authority. Its remit does not therefore include examining the proportionality of surveillance. This review must be carried out by a compulsory measures court for each individual surveillance taking into ac-

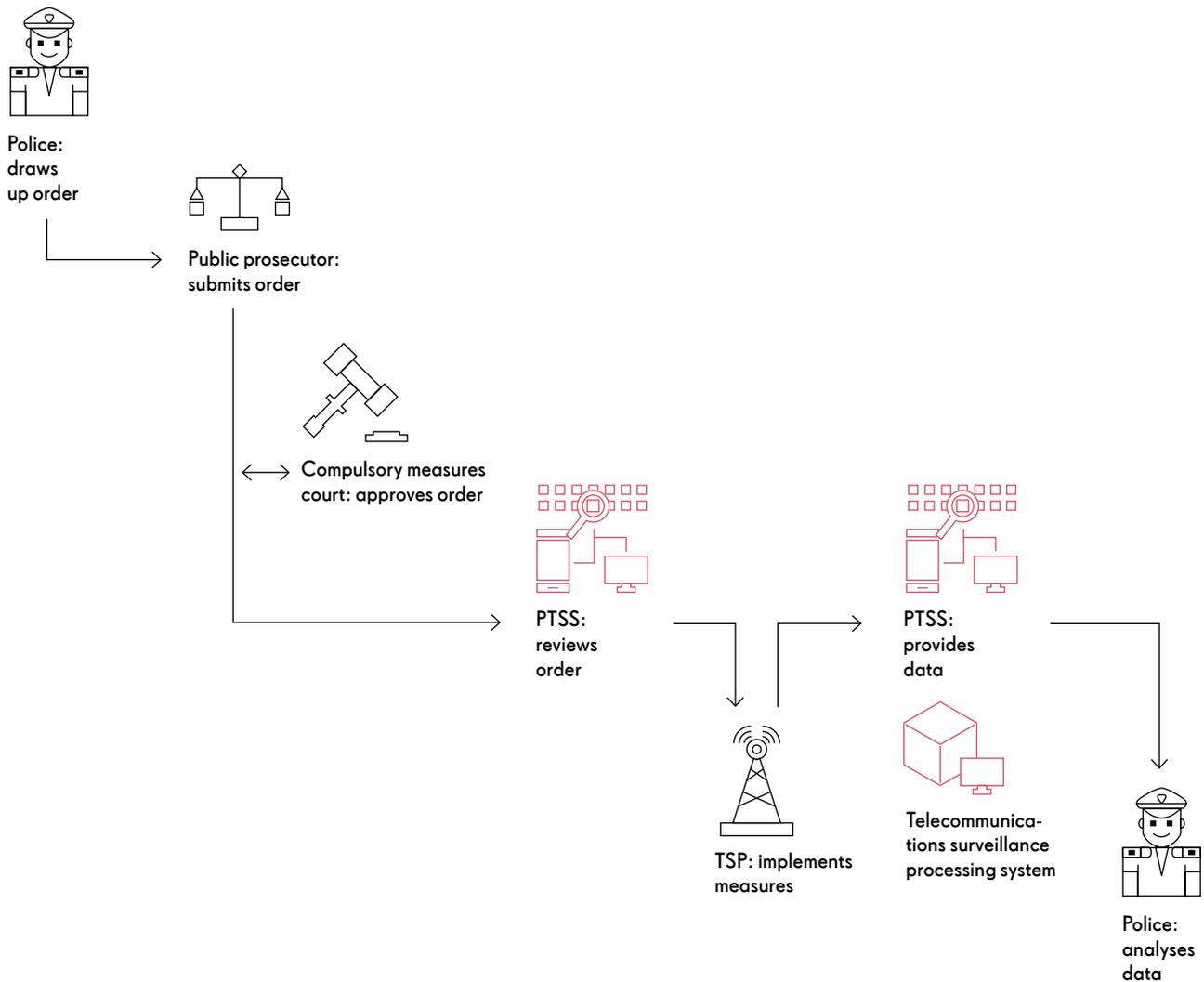
count the specificities of each case. If the judges are convinced on the basis of the available files in the investigation concerned that the surveillance ordered is proportionate and in compliance with the law, they will authorise it. The competent compulsory measures court also imposes the necessary measures to protect persons subject to professional secrecy (e.g. doctors, lawyers).

Only if all the above requirements are met can the ordered surveillance be carried out and

can the data obtained from it be used as incriminating or exculpatory evidence in criminal proceedings.

The public prosecutor issuing the order, the PTSS, and the competent compulsory measures court are therefore the three authorities that together bear responsibility for every surveillance carried out in Switzerland under the Criminal Procedure Code.

The surveillance process



In the service of our users

As part of the reorganisation of the PTSS, a new team was set up in 2023. Its remit includes requirements management, architecture and project management. The team therefore ensures that user needs are taken into account in the development of the PTSS processing system. It is headed up by Valentin Murariu, who is also the delegated project sponsor within the Telecommunications Surveillance Programme.

Mr Murariu, could you tell us the reasons that led to the creation of your team?

The formation of the Requirements Management Team reflects the PTSS's desire to get closer to its customers and their needs. We've created new roles with the aim of offering our customers a single point of contact for managing their requirements. This enables us to maintain a close relationship with our users and respond effectively to their requests. Also, by establishing a cross-team forum, we're putting in place a platform for better inhouse communication between projects.

What does the day-to-day work of your team members involve?

My team is responsible for receiving, studying and, where viable, implementing users' requests relating to the components of our system. Consequently, our day-to-day work is organised around our customers' requirements.

In practical terms, user requests are assessed by engineers for their feasibility and necessity. Once approved by the engineers, the requests are processed by the architects with a view to being integrated into the system.

Our Project Management Office aims to facilitate coordination between teams by provi-

ding a forum for exchange between the different teams working on a given project.

Our components are primarily used by criminal investigation departments, so on the client side, my team is mainly in contact with investigators specialising in surveillance.

We want to communicate as directly as possible with our customers and are constantly seeking to improve our performance in this area. To this end, we're in the process of optimising existing exchange platforms and establishing new channels for even faster contact, tailored to our customers' needs.

What kind of profiles do you look for to carry out these tasks?

When setting up my team, I mainly looked for people with extensive experience in requirements management, excellent listening skills and adaptability, and a strong customer focus. Another key criterion is the ability to communicate in Switzerland's various languages in order to facilitate interaction with all our contacts.



Fatima Ghobrini during a presentation

Fatima Ghobrini is a requirements engineer in Valentin Murariu's team.

Ms Ghobrini, you're a member of the Requirements Management Team. Could you tell us about your role?

I'm responsible for gathering, analysing and defining customer needs and expectations. Several times per week, we organise what we call 'early adopters' meetings, where our users can present their requests to us. By working closely with our clients, whether they be prosecutors or members of the police or the Federal Intelligence Service (FIS), we're able to gain a thorough understanding of their needs.

I mainly deal with the French-speaking cantons.

Can you give us a concrete example?

One example that springs to mind is a recent project we carried out with a French-speaking canton. Users were having difficulties with the user interface of our FLICC component, which they found non-intuitive and not effective in meeting their specific needs. By organising dedicated workshops with them, I was able not only to un-

derstand their needs, but also to gather their suggestions for improvement.

Following these discussions, we designed a tailor-made interface. As well as improving the operational efficiency of users in that canton, the initiative has provided a model for developments for other cantons.

For me, this example epitomises the impact of our close collaboration: by actively listening and responding in a targeted way to specific needs, we've been able not only to enhance the user experience, but also to strengthen the trust and partnership between the cantons concerned and our service.

The processing system is renewed

'Development and operation of the telecommunications surveillance processing system and of the police information systems of the Swiss Confederation' is a project to update the processing system of the PTSS and fedpol's police information systems to reflect the technical developments of recent years and to meet the requirements of future technologies.

Programme start date 1. 1. 2016

Programme end date (scheduled) 30. 6. 2024

Guarantee credits CHF 110.5 million

Milestones 2023

- Go-live of FLICC 1.0 pilot (real-time surveillance) in August 2023
- Go-live of KasewareCH (investigation system) in September 2023
- Implementation of long-term data storage on the various processing system components
- Upgrading of three components: IRC (Information Request Component), RDC (Retained Data Component) and WMC (Warrant Management Component)

Online fraud

How investigators catch the criminals

Many fraudsters exploit the online mail-order business for their nefarious activities. Surveillance often helps to convict these criminals. We talked to Tom Bader and Adrian Durrer from the Lucerne Police to find out how they use PTSS surveillance measures in their investigations.

Imagine someone asks you for your surname, first name and date of birth on the pretext of working out your star sign and ascendant. They might go on to ask for your address and then embark on a seemingly innocent conversation about city neighbourhoods. You think nothing of it and chat away merrily.

Soon afterwards, you start receiving bills for things you supposedly ordered online. You know nothing about it and complain, but to no avail: the damage is done and you are barred from ordering anything on account in future.

What happened? Your new acquaintance has posed as you on the internet and purchased items in your name. All that's needed to do this is your full name and date of birth, and in some cases your address.

Online shopping may be convenient, but it also enables this kind of scam. What's more, even if you are careful, don't reveal your date of birth and don't share your address with complete strangers, your data may have been leaked and sold on the dark web. In an interview with the PTSS, cyber investigators Adrian Durrer and Tom Bader from the Lucerne Police describe two such cases.

Night-time at the parcel pick-up point

Over an extended period, a number of individuals get charged for goods that they supposedly bought in an online store. In fact, they never made any such purchases. Someone else had ordered the items in their name, had the parcels redirected to a pick-up point and then collected them at night.

The police later analyse CCTV footage from the parcel collection points at the times when the packages were retrieved, but all they can see is a hooded figure, which doesn't get them very far with their investigation.

“We can't order surveillance on the slightest suspicion of fraud.”

Adrian Durrer, Lucerne Police



Lucerne police investigators analysing data in FLICC

One of the packages contains an iPhone. Every mobile phone carries a unique 15-digit IMEI serial number that allows it to be identified anywhere in the world. The online retailer that dispatched the iPhone reports the IMEI of the purchased device to the police. This is where the PTSS comes in to play: a simple information request reveals two telephone numbers and names linked to use of the iPhone.

An order for retroactive surveillance of the two phone numbers is also submitted to the PTSS. The location of one of the numbers exactly matches the time when the hooded figure was captured on CCTV at a parcel collection point. Bingo! The individual in question is arrested and almost a hundred cases are solved.

“It’s often at the interface between cyberspace and real life that we make headway,” says IT investigator Tom Bader, who was involved in the case. “But we have to be lucky to land such a

“Each case is new and you have to approach it with an open mind like a beginner.”

Tom Bader, Lucerne Police





“Fraudsters are very quick to exploit technical and economic innovations.”

Adrian Durrer, Lucerne Police

direct hit, where someone has the stolen iPhone in their pocket and uses it with their own SIM card. Most of the time, it's more like a jigsaw puzzle that we have to put together piece by piece. But when we succeed, it's obviously a huge sense of achievement.”

It would not be feasible to order surveillance in every case of suspected fraud, explains Bader's colleague Adrian Durrer. Consequently, all requests for surveillance must be backed up by solid evidence. Scammers are rarely one-off offenders, so surveillance usually opens doors that lead to many more cases being solved.

A suspicious rucksack

During a police check at an illegal gambling club, a person is found with a rucksack full of electronic devices, false identity documents and lists of addresses. The individual concerned has previous convictions: their last prison sentence was for ordering packages in other people's names, intercepting them and selling them on.

■ Retroactive postal surveillance (parcels): In Switzerland, every parcel sent is registered and photographed. Retroactive postal surveillance allows an authority to view a list of all parcels sent to an address in a particular period. It must be authorised by a compulsory measures court.

The police submit an order to the PTSS for retroactive postal surveillance of the addresses. The details are compared with data held by the residents' registration office and only the false addresses are subject to surveillance. This reveals dozens of packages that the suspect has ordered in other names, which provides enough evidence for a conviction.

One particularly brazen element in this case is that some of the addresses were taken from the court documents from the previous conviction, which the individual had asked to look at based on their right to inspect the case documents.

Fraudsters are very quick to exploit technical and economic innovations, explains Durrer. It is therefore important that the police can investigate quickly and easily.

“When you've been in the job for a long time, you often think you've seen it all,” says Bader. “But experience can also be a hindrance. Every case is new and you have to approach it with an open mind like a beginner. Very few scammers make the same mistake twice.”

Standardisation

“We’re working on the future.” From requirements to standards.

The globally interconnected nature of mobile communications brings with it a host of challenges. Amongst other things, standards enabling cooperation between providers, authorities and the judiciary need to be developed. Jean-Pascal Chavanne is responsible for standardisation at the PTSS. Together with a colleague, he represents Switzerland’s interests in the field of telecommunications surveillance in a number of standards organisations.

Anyone travelling from Geneva to St Gallen 150 years ago would have had to adjust their watch more than once. Many towns and cities had their own time, measured by the sun: when the sun was at its highest, that meant it was twelve noon. Between Geneva and St Gallen, the difference was around a quarter of an hour.

With the arrival of the railways, heralding much faster travel, local times became a massive administrative headache, as timetables suddenly had to be adjusted to different time zones. In 1894, the Federal Council finally decided to adopt Central European Time. This was an early example of international standardisation.

Standards are particularly important in the case of innovative technologies. Without international standards governing the width of railway tracks, trains would be unable to travel from one country to another. And without standardised mobile networks, it would not be possible to receive data on a mobile phone abroad.

Introducing an international standard is far from simple, as the different power sockets around the world go to show. As a rule, standards

are not specifications issued by centralised bodies, but are developed within the community of interest. If a standard does eventually become established, it often saves time, money and resources. However, achieving this outcome takes a great deal of diplomacy, skill, technical understanding and in-depth work.

Many towns had their own time, measured by the sun.



3GPP Meeting in Toulouse, August 2023

Weighing up the solutions

For the PTSS, standards are particularly necessary for lawful interception (LI) to enable the exchange of data between providers, the administration and the judiciary. Jean-Pascal Chavanne is one of the PTSS staff members responsible for negotiating standards. The trained engineer has worked at the PTSS for the past 12 years. He represents Switzerland on LI-related issues in the international cooperation forum for mobile telecommunications standards, 3GPP. In a global network, it is not worthwhile for Switzerland to have specific and customised solutions of its own. Standards organisations are not decision-making bodies but rather platforms for discussing priorities, problems and solutions linked to the latest technological advances. Many meetings are required with representatives of various groups before a standard is declared as such. Chavanne

“I get to see how the world of telecommunications is developing and be right there at the forefront.”

Jean-Pascal Chavanne

says he has not yet seen a single vote at the 3GPP plenary meetings. Everything, he adds, is based on consensus, which is reached through lively discussion.

When it comes to standards, mobile operators have different requirements than the PTSS, for example. Chavanne used to work for Swisscom and so is familiar with both sides. The fact that he – like many other PTSS employees – has a good understanding of private-sector needs and working practices has enabled the PTSS to build up additional trust among mobile service providers.

The ultimate outcome of this work is the several hundred page Annex 1 to the Ordinance on the Implementation of Post and Telecommunications Surveillance (OI-PTS), which sets out the technical specifications for surveillance. “A telecommunications standard is often not just a single solution but a proposal of four or five possibilities,” says Chavanne. Determining the best option for Swiss implementation is not always easy. For example, the police and the military use the Swiss coordinates system (LV95). However, LV95 is only applicable in Switzerland. The solution defined in Annex 1 of the OI-PTS, the World Geodetic System 1984 (WGS84), also applies abroad and is used, for example, in the context of GPS. A great deal of consideration is needed to decide on the best standard for Swiss use, notes Chavanne.

Right at the forefront

Chavanne says he has been very lucky with his career. “I find this topic so interesting, it’s almost like a hobby. I get to see how the world of telecommunications is developing and be right there at the forefront. You could say we’re working on the future.”

In recent years, 3GPP has been discussing in particular the transition to the new 5G mobile communications standard, which is significantly more complex than its predecessors. As many standards are still undergoing technical development by providers, some subjects are off-limits in public meetings as they cannot be discussed in front of rivals. In such situations, and also in difficult negotiations, a lot can be achieved in coffee

breaks, one-to-one conversations and closed meetings.

Chavanne explains that much of the work done is pioneering. Switzerland, for example, was one of the first countries to be involved in a reshaping of the standard for the transmission of surveillance orders. In cooperation with the United Kingdom and the Netherlands, ideas were first collected, then presented at rapporteur’s meetings, and feedback was incorporated. By the time the standard was presented and adopted at the plenary session, everybody had to have been convinced of its merits as there was no time for any further feedback.

One of the issues currently on the agenda is the increasing interconnectedness of the automotive industry. For example, how can a licence plate number or vehicle number be linked to a SIM card? This would require the development of a standard encompassing car manufacturers, public authorities and mobile providers. And now, after five years in which the switch to 5G has been the main topic in standards organisations, the next standard, 6G, is already on the horizon.

03

FACTS AND FIGURES

Reasons for surveillance

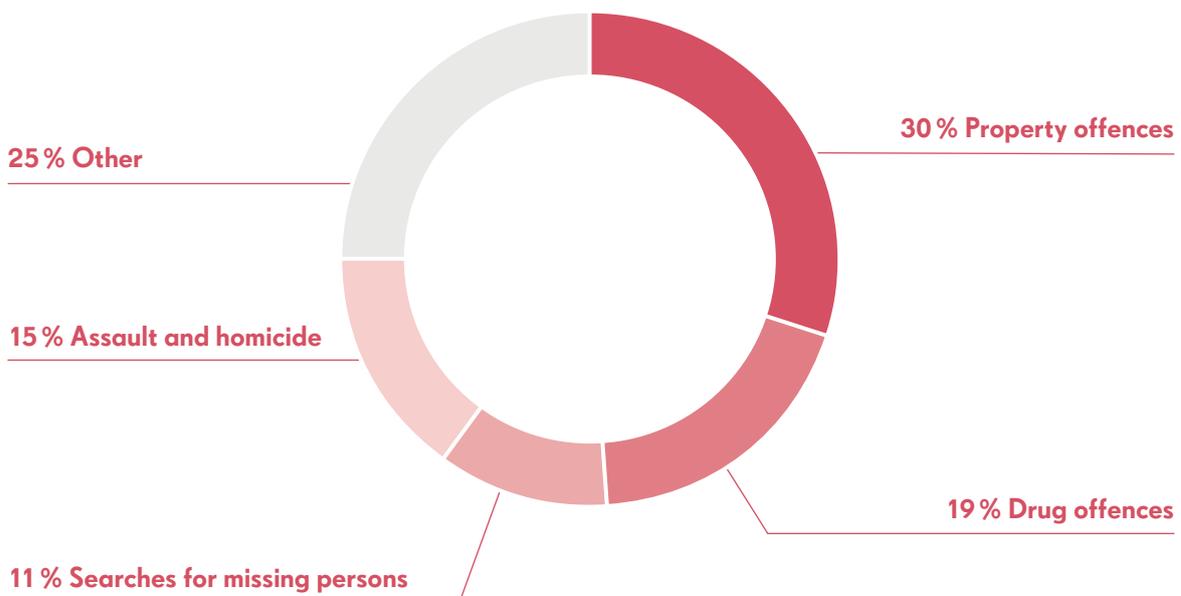
According to police crime statistics, about 500,000 offences are reported in Switzerland every year. Telecommunications surveillance was used as an investigative measure 9,428 times in 2023, a comparatively low figure.

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 not-

ceably lower than the number of surveillance measures ordered. Surveillance measures were most often used to investigate property offences, e.g. theft and fraud (30%). In second place, at 19%, were serious narcotics cases, with assault and homicide cases in third place, at 15%. Telecommunications surveillance can also be used to search for missing persons. In 2023, these searches accounted for 11% of all cases, ranking fourth.

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 includes data on who has been in contact with whom, when, how, for how long and from where, for a maximum period of six months in the past.

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

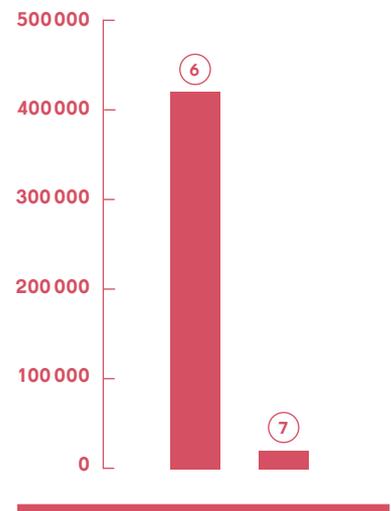
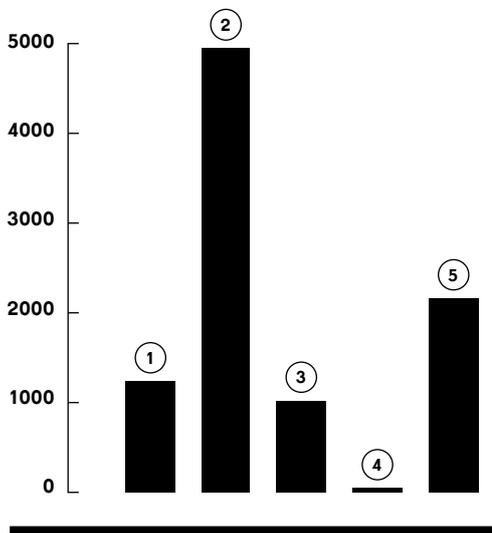
An antenna search includes the retroactive surveillance of all communications, communication attempts and network accesses that have taken place at a specific location via specific mobile radio cells or a specific public WLAN access during a given period of time.

Simple information ⑥

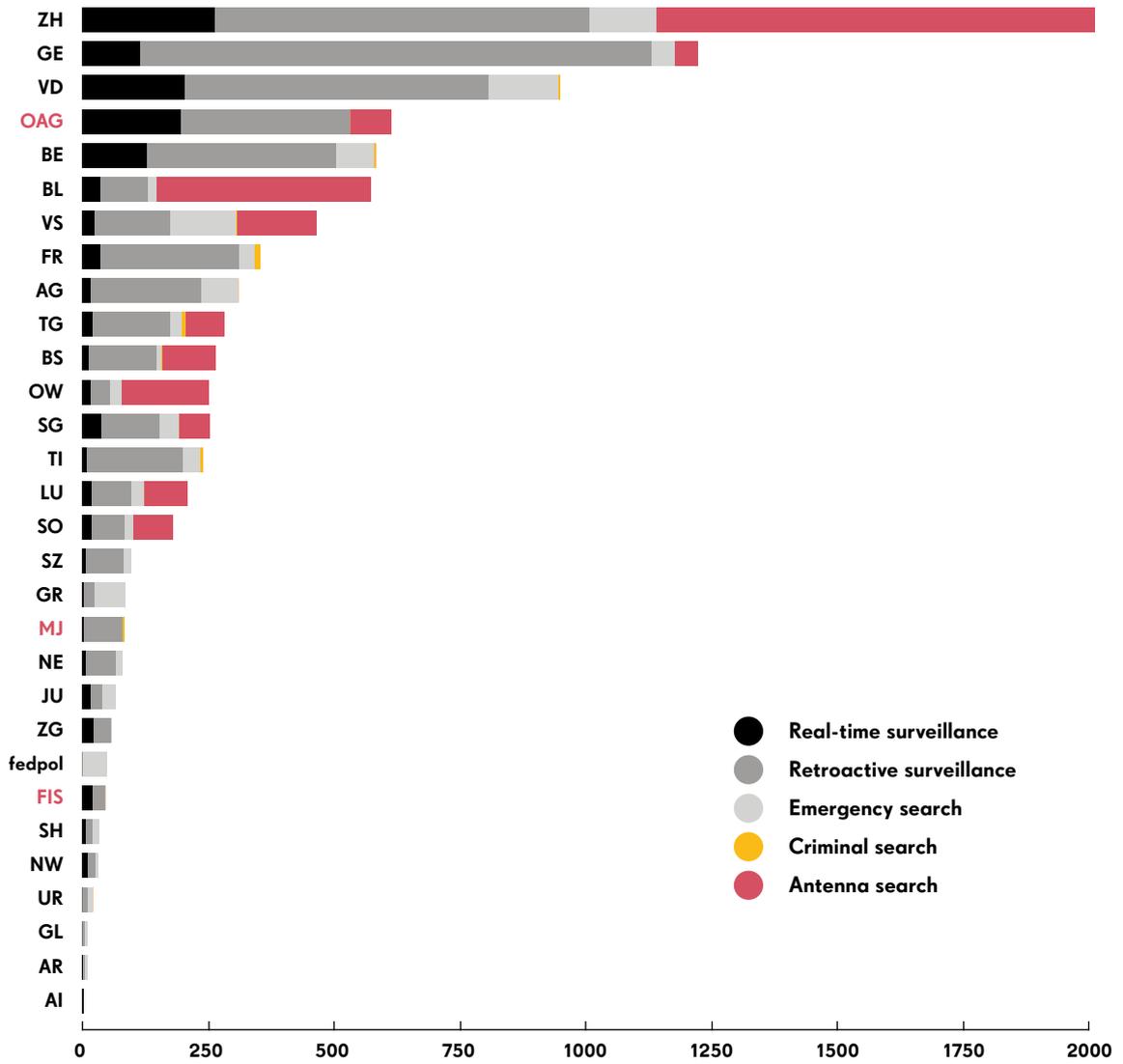
Simple information includes basic information on telecommunication connections, for example who the subscriber of a particular telephone number or IP address is.

Complex information ⑦

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



Mandates from the federal government and cantons



OAG Office of the Attorney General
 MJ Military Justice
 FIS Federal Intelligence Service

Number of enquiries from the public

22 

Registered users processing system

WMC **3400**

Warrant Management Component

IRC **4900**

Information Request Component

RDC **2200**

Retained Data Component

ISS **2450**

Interception System Schweiz

Number of media enquiries

5

Number of on-call assignments

1009 

Number of Special Cases

44

(See p. 9, Provider Management, Special Cases Team)

PTSS financial performance in CHF

Total revenue

12,8

Total expenditure

36,1

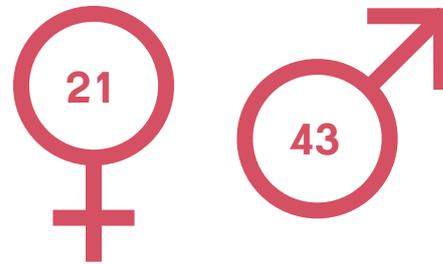
Federal contribution

23,3

Number of employees

64

Numbers of women / men



Average age

45,8

Age distribution

20 to 29

7,8%

30 to 39

21,9%

40 to 49

21,9%

50 to 59

42,2%

60 to 69

6,3%

First language

67,2% German	1,6% Italian
29,7% French	1,6% Other

“Surveillance can only be used for serious offences.”

Jean Louis Biberstein, Deputy Head of the PTSS, Head of the Legal Affairs and Controlling Division

Impressum

Editing: PTSS

Realisation: Schön & Berger, Zurich

Printing: Druckerei Ruch, Ittigen

Photos: Cover: Martial Trezzini / Keystone;

p. 4, 13, 19: Media und Event Services

(MS-AMC-MES) FOITT;

p. 21: Lucerne Police; p. 24: 3GPP

Illustrations: p. 21, 22: Bianca Litscher, Lucerne

Font: Minion Pro, Drescher Grotesk

Paper: Z-Offset

Language: German, French, Italian and English

© PTSS, April 2024



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

