Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Annual Report 2020

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

Are you one of the millions of people in Switzerland that use WhatsApp, Signal or Threema? If so, then it may only be a few minutes since you last encrypted or decrypted a message. This is because these messaging apps convert every message into encrypted text before it is sent and only transform it back into plain text when it reaches the recipient's device.

Cryptographic methods are as old as written communication itself. But with the spread of the internet and ever more powerful mobile terminal devices, encryption technologies have become more important, to the point that it is now difficult to imagine everyday life without them – businesses would not be able to protect their trade secrets, law firms would not be able to safeguard client confidentiality and none of us would be able to make digital payments.

The PTSS also relies on cryptographic algorithms as our confidential communication with police forces, public prosecutors, compulsory measures courts and telecommunications service providers is routinely encrypted.

However, as a service provider to law enforcement authorities, we are also confronted with the challenges of encryption. When suspected offenders use a service with end-to-end encryption, the state measures for telecommunications surveillance come up against technical limitations.

"As a service provider to law enforcement authorities, we are also confronted with the challenges of encryption."

New approaches to telecommunications surveillance are therefore called for. One promising approach is the analysis of metadata. Metadata does not relate to the content of a message, but provides information about its context; for example it documents whom a suspect contacted and from where.

In this year's annual report, we show how law enforcement services and the Federal Intelligence Service use metadata to glean information from encrypted content. A public prosecutor, an investigator and a representative of a telecommunications service provider offer insights into the future of telecommunications surveillance.

The digital transformation of society cannot be halted or reversed. Metadata analysis is an attempt to develop new solutions in areas that we can control.

This fundamentally optimistic attitude is in keeping with my inclinations as a person and manager. I am always confident that something good can come of a situation even if it initially looks less than promising. The way all the staff at the PTSS responded to the outbreak of the coronavirus pandemic has shown me that I am not entirely wrong.

State-of-the-art infrastructure is one thing; the willingness of employees to switch to this completely new situation within a few days so as to do all of their work from home without any loss of quality or time is something else.

Let me put it this way: post and telecommunications surveillance has been guaranteed in Switzerland at all times throughout the pandemic. What's more, the results of a survey of law enforcement agencies showed consistently high satisfaction with the quality and availability of our services.

And this is all thanks to our staff. Their willingness to make the best of a unique situation is what allowed us to make a success of 2020.

René Koch
Head of PTSS

01

OVERVIEW

■ Telecommunications service providers (TSPs) include mobile communications, telephone, email and internet providers such as Swisscom, Sunrise, Salt and UPC.

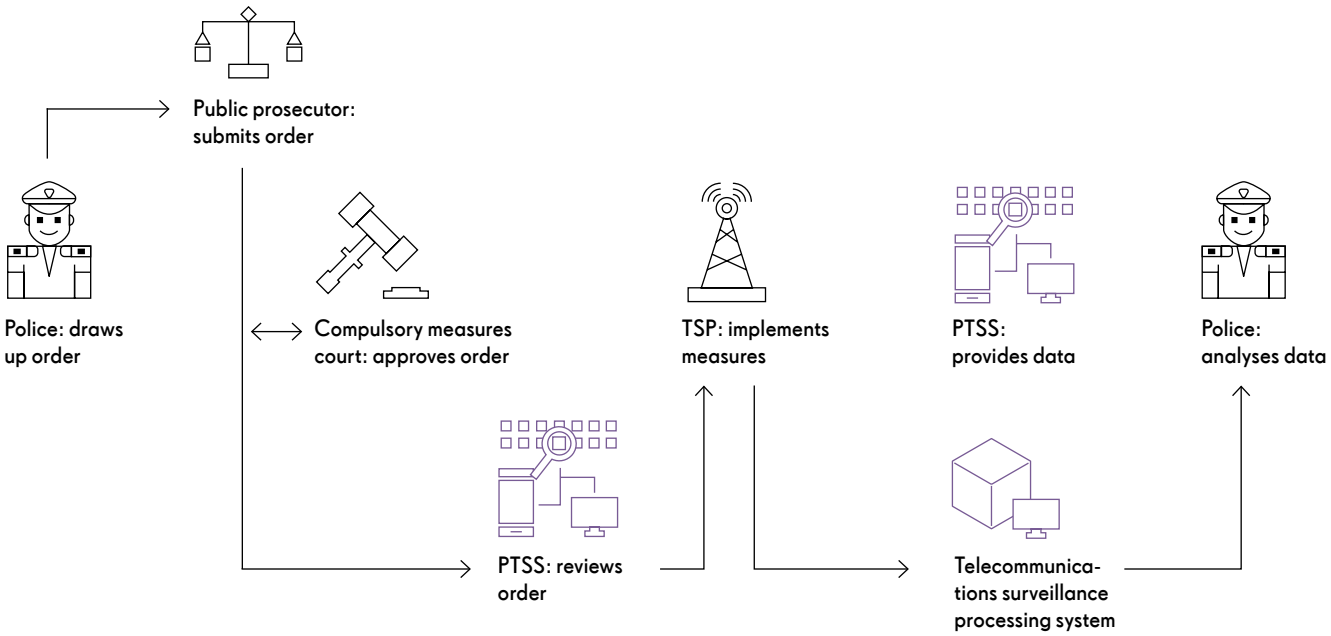
The PTSS: an overview

When investigating serious crime, the federal and cantonal law enforcement authorities can order measures to monitor 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 authorities make 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 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). The revised Federal Act on the Surveillance of Post and Telecommunications (SPTA) and the associated implementing ordinances gave the service a clear, up-to-date legal framework. It is now 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, Alexandre Suter (Head of the Provider Management Division), Jean-Louis Biberstein (Head of the Surveillance Management Division) and Nils Güggi (Head of the Legal Affairs and Controlling Division)

Provider Management

The 23 staff of the Provider Management Division are responsible for creating and keeping up to date 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 establishes whether the TSPs are able to monitor their telecommunications services and provide information and data as required.

Under the SPTA, TSPs must at all times, be able to monitor the services they offer and to provide the associated data and information, unless they are legally exempted from the obligation to do so.

The Provider Management Division's Special Case Team develops tailor-made solutions for TSPs that are not themselves able to implement surveillance measures, or who are not legally re-

quired 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.

The staff also manage relations with more than 700 providers, advise them on technical and legal matters and issues related to 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/5G networks.

Surveillance Management

The 19 members of the Surveillance Management Division handle the PTSS's interaction with the prosecution authorities and the Federal Intelligence Service (FIS). The team advises the police forces and public prosecution services on all legal, technical, organisational and administrative matters relating to postal and telecommunications surveillance.

The staff deal with the surveillance orders, which they check for completeness before passing them on to the TSPs. The team ensures that the prosecution authorities receive the data the TSPs subsequently deliver. Surveillance management also includes drawing up invoices for the prosecution authorities and the FIS and making payments to the TSPs.

Along with the IT operator, the team is responsible for incident and problem management regarding detected or suspected IT errors. It is involved in the development of new applications and provides internal and external first- and second-level support.

The Surveillance Management team also runs training sessions for the prosecution authorities and the FIS. Outside office hours, it provides a duty service with the technical support of 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 computers, smartphones and other terminal devices. This has consequences for telecommunications surveillance as the technical interface between the PTSS's processing system and the several hundred TSPs needs to be constantly adapted.

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

In addition to its responsibility for IT projects, the team of 15 draws up the legal framework necessary to ensure that surveillance is correctly conducted. This safeguards the public's right to privacy and is a key requirement in ensuring the data gathered can be used in court.

This largely involves adapting ordinances to reflect the latest technological changes. For example, the departmental ordinance on conducting surveillance in post and telecommunications services (VD-ÜPF) is revised each year and amended if necessary.

The Legal Affairs and Controlling Division also deals with financial management, reporting and public relations. The staff respond to scores of media enquiries each year and are available to respond to queries 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 Administrative Criminal Proceedings Division has had the authority to prosecute anyone failing to fulfil their legal obligations in connection with the surveillance of post and telecommunications.

The two persons of the Administrative Criminal Proceedings Division investigate complaints, establish the facts, carry out the legal analysis and, if necessary, punish these transgressions. 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 2020

January

Outbreak of the coronavirus pandemic
A new virus causing respiratory illness is discovered in Wuhan. On 23 January, China cancels all major events marking the Chinese New Year. The pandemic and its consequences will occupy the PTSS for the whole of 2020.

March

New standards for the surveillance of 5G services
The Federal Department of Justice and Police (FDJP) brings the revised Ordinance on the Implementation of Post and Telecommunications Surveillance (OI-PTS) into force on 1 March. This legislation introduces standards for the surveillance of 5G mobile services. The ordinance amendments particularly concern technical interface requirements for the provision of information, real-time surveillance and metadata via the PTSS's new system components.

Mandatory remote working for all employees
From 16 March, all PTSS staff are told to work from home. Exceptions can be made if a line manager considers that someone needs to be onsite for operational reasons.

Training sessions fall victim to the pandemic
The PTSS runs regular training sessions for law enforcement authorities but due to the epidemiological situation, all sessions have to be suspended from March 2020.

April

Transparency towards the public
The opendata.swiss portal, operated by the Federal Statistical Office (FSO), offers easy and secure access to federal, cantonal and communal public data. The PTSS has also featured on opendata.swiss since 23 April 2020, providing figures on surveillance measures conducted since 2011.

May

The Federal Administrative Court issues its judgment on the Threema instant messaging service

Threema GmbH, which is based in the canton of Schwyz, operates a platform that allows customers to send and receive end-to-end encrypted text messages, photos, videos and voice messages. In the legal dispute over a decision issued by the PTSS, the Federal Administrative Court rules on 19 May that Threema should be classified as a provider of derived communication services (PDCS) rather than a telecommunications service provider (TSP).

July

More flexible searches for simple and complex information

Because TSPs have upgraded their systems, from 1 July, law enforcement services have the option of transmitting 'IR_FLEX' type requests. Four types of information requests can now be submitted with search criteria which tolerate errors and identify phonetic matches, e. g. between the surnames Mühler and Müller.

Simple information is now free of charge

Simple information comprises basic information on telecommunications connections. For years, law enforcement authorities had to pay CHF 9 for a simple information request. Since 1 July 2020, this information has been provided free of charge. This also simplifies billing and paying those bills. However, telecommunication service providers will continue to be paid CHF 3 for every response. To offset the revenue shortfall, various surveillance measures will become more expensive (see article "New fee regulations at the PTSS" on page 26).

The PTSS publishes its 2019 Annual Report

The PTSS publishes an annual report for the second time. The report, which is published in four languages, provides the facts and figures on the PTSS's activities. It also offers an insight into the PTSS's work with law enforcement authorities and service providers.

August

Partial revision of the SPTA through the 'collective dispatch'

On 26 August, the Federal Council approves the "Federal Act on administrative simplification and relief of the Federal Budget" which also concerns the Federal Act on the Surveillance of Post and Telecommunications (SPTA). The partial revision of the SPTA seeks to simplify the financing of post and telecommunications surveillance. In future, it should be possible for the authorities ordering measures to contribute to the cost of post and telecommunications surveillance measures at a flat rate.

September

Mobile localisation within the framework of the PCTA

On 25 September, the Swiss parliament adopts the Federal Act on Police Counterterrorism Measures (PCTA). The new category of mobile localisation necessitates amendments to the PTSS ordinances. The PTSS legislative team is already working on implementation.

November

Media reports on the topic of encryption

There is intense debate about the encryption of messaging services across the European Union. SRF Radio investigates the topic here in Switzerland and approaches the FDJP and the Federal Intelligence Service (FIS) with questions. The PTSS's response is broadcast on the current-affairs radio programme Echo der Zeit on 17 November.

New version of the RDC enters pilot phase

The PTSS has been working on the Telecommunications Surveillance Programme, since early 2015. The first stage is completed on 24 November, with the Retained Data Component (RDC) going into operation with visualisation and grouping functions following the introduction of components for order management and information requests. The RDC stores the retroactive data supplied by telecommunications service providers, and supports the work of investigators with its new functions.

Satisfaction with the PTSS

The Post and Telecommunications Surveillance Service supports the work of the law enforcement authorities and the FIS. Surveying the satisfaction of these target groups and using feedback to determine where improvements can be made is one of the PTSS's priorities. Analysis of the 2020 customer satisfaction survey shows that performance ratings improved – in some cases significantly – compared with the 2018 survey. Respondents rated staff competence and reliability particularly highly, which in this exceptional year is especially worth highlighting.

02

BACKGROUND

Who contacted whom, when, for how long and from where

How metadata becomes evidence

In order for the PTSS to obtain suspects' metadata and to provide it to law enforcement authorities, an order from a public prosecutor and its approval from a court are required. The new version of the Retained Data Component (RDC), which entered the pilot phase in 2020 with its visualisation and grouping functions, speeds up the transmission of this data, improve its readability and thus enhance the efficiency of law enforcement.

Police officers were faced with a trail of destruction when they arrived at the scene on the A9 motorway north of Lausanne. First, they discovered a row of three burned-out cars, then a few kilometres further – at the La Sarraz motorway exit – they found a security van, also burned out. It later transpired that the perpetrators had made the armoured security vans stop, forced the occupants to get out by beating them and threatening them with Kalashnikovs, and subsequently fled with the stolen cash.

The crime occurred on 23 August 2019 at 3 a.m.. Over a year later, in early October 2020, French police arrested seven suspects. Then, around a month later, came the next police operation: near Lyon and in the canton of Vaud, police arrested 13 people suspected of attacking a security van in the same manner near Mont-sur-Lausanne. They are all awaiting trial.

The breakthrough in the investigation came primarily from a series of antenna searches. Staff from the *Brigade d'analyse des traces technologiques* BATT (Digital forensics team) at the Vaud cantonal police force had been analysing which mobile phones were logged in before, during and after the crime in certain mobile radio cells. Julien Cartier, head of BATT, talks of intensive telecommunications surveillance work.

The legal framework for analysing telecommunications activities is set out in the Federal Act on the Surveillance of Post and Telecommunications (SPTA). It requires providers of telecommunications services that operate in Switzerland to retain all users' communication data for six months. Meanwhile, Articles 269 and 273 of the Swiss Criminal Procedure Code set out the conditions under which law enforcement authorities can collect and use the data stored by providers in criminal proceedings.

Only if the courts approve

The surveillance of telecommunications is a serious encroachment on fundamental rights. This is why authorisation must be granted by one of the cantonal compulsory measures courts, which also have the power to order pre-trial detention, for example. If there is a public prosecutor's order that must be approved by the compulsory measures court, the PTSS requests the data from providers and passes it on to the law enforcement authorities.

Metadata: an explanation

The metadata collected for the purposes of retroactive surveillance and to identify the perpetrators of crimes committed via the internet is known as Retained Data. The Federal Act on Post and Telecommunications Surveillance (SPTA) uses the wording 'retained metadata'. The metadata from telecommunications traffic is the data that shows with whom, when, for how long and from where the person under surveillance is or has been in connection with, as well as the technical details of the connection (Art. 8 let. b SPTA). As the surveillance of past telecommunications is known as retroactive surveillance, the alternative term 'metadata of telecommunications from past communications' also exists.

The Vaud cantonal police do not keep any statistics on how often metadata analysis has been instrumental in solving crimes. "That would be pure number juggling," says Julien Cartier. He never loses sight of the bigger picture though: retroactive telecommunications surveillance sharpens the focus of police investigations by firming up existing suspicions or exonerating suspects.

Twenty years ago, after studying forensics, Julien Cartier joined his team at the Criminal Investigation Department in the Canton of Vaud. In that time, he has witnessed how metadata analysis on subscribers, on their locations and on the technical characteristics of connections has steadily gained importance.

On the one hand this is because data traffic in mobile networks practically doubles every few months, which makes analysis more fruitful but also more labour-intensive; and on the other, it is because it is becoming more and more difficult for the law enforcement authorities to catch criminals 'red-handed' using real-time surveillance. The reason behind this is technical, but in simple terms is to do with increasing levels of encryption.

It started with Edward Snowden

Remember that back in summer 2012, Edward Snowden revealed how easy it was for his employer – the National Security Agency (NSA) – to wiretap the PCs and smartphones of unsuspecting users. The hardware, software and telecoms industries responded and have since invested large sums in new cryptographic processes to encrypt phone calls, emails, chats, websites and communications from apps.

This also benefits criminals. What's more, as Julien Cartier explains, habitual offenders and their accomplices are occasionally involved in the technological developments. Back in the summer of 2020, the EncroChat case, in which French and Dutch investigators reported that they had managed to infiltrate an end-to-end encrypted communication platform, made headlines all over the world. Hundreds of the platform's users had been arrested by that point, accused of crimes ranging from drugs and arms trafficking to murder.

It was sophisticated tools that finally allowed the law enforcement authorities to decipher the flow of messages on EncroChat, but it was the digital clues that the crypto network had left in the mobile networks that gave it away.

"The great thing about metadata is that it can't be concealed or manipulated, and this benefits law enforcement authorities," explains Julien Cartier. The international community of experts in Lawful Interception agree that improved metadata analysis can at least partly offset the increasing difficulties with real-time surveillance.

In summer 2020, investigators reported that they had infiltrated an end-to-end encrypted communication platform.

The BATT carries out just over 1,000 retroactive surveillances every year. There is little variation in the figures. That said, 2020 was a special year for Julien Cartier's ten-strong team as they accessed the new visualisation and grouping function of the Retained Data Component (RDC) online for the first time on 23 November.

The RDC is one of four components in the PTSS's central processing system, which since 2014 has been completely overhauled and adapted to reflect the latest technical standards (in other words, 5G). The pilot test of the RDC involving selected cantonal police forces got

under way in November 2020 and work has since been done on rolling it out as standard.

"The RDC has allowed us to significantly improve the quality of our services," says project manager, Manfred Beyeler. He explains that data transfer from providers to the PTSS and from the PTSS to the law enforcement authorities is now considerably faster. What used to take several days is now done in minutes. This makes metadata analysis a handy tool, even in investigations where there is enormous time pressure, e. g. in a kidnapping.

Philipp Umbricht is chief public prosecutor in the canton of Aargau. His investigators are also among the pilot users of the new RDC. Besides the rapid transmission, he praises the standardised data formats that comply with the guidelines of the European Telecommunications Standards Institute. He explains that the readability of the data has significantly improved, leaving investigators more time to concentrate on their core operations.

A smartphone generates 30,000 records

There is plenty to do; an average smartphone leaves around 5,000 data points on mobile networks every month. If investigators were to analyse a smartphone's digital trails from a six-month period, they would be dealing with no fewer than 30,000 records. "Picking out leads from this amount of data is time-consuming," says Philipp Umbricht.

Certain grouping and filter functions are installed in the new RDC. In addition, investigators from cantonal police forces and fedpol work with software tools like those used in large industrial and service companies. These business intelligence tools allow patterns to be identified in large volumes of data.

In a narcotics case, for example, it may transpire that the suspect always sent text messages to certain recipients on the same days. If the police then establish that the messages in question were always sent away from the suspect's place of residence, it is reasonable to assume that the individual under surveillance was contacting suppliers or buyers.

"We compile typical movement profiles for suspects," says Philipp Umbricht. To do so, the specialists from the Aargau cantonal police also tap alternative data sources. Using traffic cameras or credit cards, social media platforms or loyalty programmes, our digital infrastructure generates virtually uninterrupted digital clues, which can be relevant to law enforcement authorities.

The loyalty points accumulated with a supermarket chain, for example, indicate where someone was buying their everyday items during the period in question. From this, conclusions can be drawn about the individuals' main place

Continued on page 20

What used to take several days is now done in minutes thanks to digital interfaces.

Weighing up the benefits

The retention of metadata is not without its critics here in Switzerland. An appeal filed by Swiss NGO the Digital Society is pending before the European Court of Human Rights.

For Nils Güggi, head of the Legal Affairs and Controlling Division at the PTSS, there can be no contesting the fact that the surveillance of metadata is an encroachment on the right to privacy enshrined in the Swiss Federal Constitution, but on the other hand, he believes there is a public interest in bringing the perpetrators of serious crimes to justice.

Under Article 36 of the Federal Constitution, the retention of metadata is therefore permissible, Güggi says. This interpretation underpins the Federal Act on the Surveillance of Post and Telecommunications and the associated ordinances.

NGO the Digital Society (die Digitale Gesellschaft) has a different view. This non-profit organisation says it is committed to protecting citizens and consumers in the digital age. It argues that the storage of metadata means that everyone in Switzerland is being kept under surveillance 24/7 without reason or suspicion.

In 2014, the Digital Society submitted a request to the PTSS for the blanket deletion of this data. The PTSS rejected the request, so the Digital Society took the case to the Federal Administrative Court, which also rejected its appeal, as did the Federal Supreme Court. In 2018, the Digital Society finally took the case to the European Court of Human Rights (ECHR), where it is still pending.

While the ECHR generally attaches great importance to privacy protection, Nils Güggi is optimistic that it will approve the retention of metadata in Switzerland.

He refers in particular to two features of current practice: first, that any analysis of metadata must be approved by a compulsory measures court, and second, that the providers' user data is made available via the PTSS's processing system. This guarantees that the authorities can only access the data if access has been authorised.

of residence. If the evidence matches the results of localisation using metadata, another piece of the puzzle falls into place. If there are discrepancies, the suspects will have some interesting questions to answer.

Philipp Umbricht and his colleagues at the public prosecutor's office in the canton of Aargau conducted 42,000 criminal proceedings in 2020. In the same period, the Aargau compulsory measures court approved 21 real-time surveillance operations and 125 retroactive surveillance operations.

Amateur and professional criminals

According to Umbricht, about half of surveillance cases concern people who draw suspicion upon themselves while going through an emotionally difficult time. Umbricht refers to them as compulsive laypeople. They pay little attention to their communication behaviour, which means that retroactive surveillance can relatively quickly uncover incriminating or exculpatory evidence.

The other half require more investigative effort. Cycling fan Umbricht calls them the 'elite amateur' delinquents. These people are professionally or at least habitually involved in fraudulent schemes or in dealing in prohibited goods, such as narcotics, medicines or artworks. As they are aware of how revealing metadata is, they are particularly eager to communicate anonymously.

The easiest way to send emails or messages, browse the internet or call incognito is to use prepaid SIM cards that are unregistered, falsely registered or registered to straw men. They are a real headache for law enforcement authorities as tracing them back to an individual is time-consuming and costly. While registration of prepaid cards has been mandatory in Switzerland since 2004, the law enforcement authorities estimate that there are still several hundred thousand in circulation, and they are actively traded in criminal circles.

Unregistered prepaid cards are actively traded in criminal circles.

Prepaid mobiles were also used in the security van attacks in Vaud. In addition, the law enforcement authorities discovered an elaborate digital concealment system, which led them to believe that the perpetrators were involved with a gang of internationally networked serious offenders.

As the criminal proceedings are still under way, the head of the BATT is not able to give any details. All he will say is that "they didn't make it easy for us." For Julien Cartier, the fact that the case has resulted in arrests and that individuals have been charged is not merely a professional success. He also sees it as a signal to the criminal underworld that "if we deploy the right resources, we're always one step ahead of offenders."

"Data volumes are growing rapidly."

Hubert Wagner
Lawful Interception Officer at Swisscom

You ensure that Swisscom – a company with over 16,000 employees – is able to provide information and conduct surveillance in accordance with the SPTA at all times. What resources do you have at your disposal to do so?
We don't communicate our costs, but it is no secret that we have eleven staff members working to guarantee 24/7 operations. I also allocate a lot of internal engineering assignments. So, as you can tell, our costs are significant. As these are only partly reimbursed, it's important to note that cooperation in telecommunications surveillance is not a business for providers like us, but a legal obligation.

You are responsible for both real-time surveillance and retroactive surveillance at Swisscom. What's the difference?
Real-time surveillance requires expertise in networks. Meanwhile, our staff in Zurich and Bern who are responsible for the storage of metadata (retroactive surveillance) are IT specialists with expertise in databases and Lawful Interception.

Staying on the topic of metadata, what sort of volumes are we talking about?
The volume of data in our networks is growing rapidly. Between 2017 and 2020 alone, it rose from 267 to 556 million terabytes. At the end of 2020, we had 0.5 petabytes of metadata. That's about half a billion megabytes.

How do you locate the datasets requested by the PTSS with the urgency that is sometimes required?
All metadata is archived in a structured manner by time period. Email data is stored separately from information on telephone calls and SMS. When an enquiry is received for a specific time period, the system knows relatively precisely where the data can be found.

Lawful Interception is a highly specialised business. What software tools do you work with?
The basic technology is an open-source platform that we can customise and upgrade. On top of that, we have applications to manage day-to-day operations which we wrote ourselves based on the framework of a Swiss provider.

You deal with the PTSS around the clock. How do you respond if a foreign entity wants to utilise Swisscom customers' metadata?
In that case we would advise them to follow the legal procedure. If we didn't, we'd be in breach of telecommunications confidentiality.

Ready in fifteen minutes

Responsible for advice and technical support: Niko Lukic from Surveillance Management.

At night, the phone is always within reach by his bed with the ringtone on maximum volume.

Serious crimes are committed and people go missing every day in Switzerland. The public is usually informed through a media alert set up on a device, a common practice for users of the smartphone generation. However, for employees of the Surveillance Management Division like Niko Lukic, these alerts have a special meaning because when he's on duty and law enforcement services require the communication data of missing persons or suspects for their investigations, he has a direct part to play.

The PTSS is contacted by investigators from cantonal police forces, as well as public prosecutors and staff at compulsory measures courts. Niko Lukic has worked in the Surveillance Management Division at the PTSS for over ten years.

Orders to the Special Case Team

Lukic and his seven colleagues make up the PTSS contact point for the law enforcement authorities. He forwards routine requests to providers at the click of a mouse. Other assignments take longer, e. g. when sending a Special Case Team to a small telecoms provider that is not able to provide the data for real-time surveillance.

Investigators are often dependent on his expert advice because of the complexities involved. Sometimes they ask for technical support and other times "we work together to come up with the ideal approach."

Every seven weeks, Niko Lukic carries one of the PTSS's two on-call mobile phones for seven days and seven nights. At night the phone is always within reach by his bed with the ringtone on maximum volume. "On average, the alarm goes off twice a night," says Lukic. The rules state that he has to deal with the matter within 15 minutes.

When a family member goes missing, everyone knows that you have to expect the worst. Now, rapid localisation determines whether the missing person can be helped.

Lukic explains that during missions, the trusted routines kick in, and that you only really think about the people behind the measures when things have calmed down. "At the peak of the coronavirus pandemic in November and December," he says, "it was hard, as we had a suicide attempt virtually every night."

"Correct, clear and complete"

The PTSS guarantees the legally compliant surveillance of post and telecommunications. It is also involved in developing the legal framework. Lawyer Daniela Siegrist is a member of the four-person team that translates technical changes in the telecoms sector into legislation.

Ms Siegrist, as we all know from our civic education classes, Parliament passes acts and the government enacts the associated ordinances. What is the PTSS's role?
It is the Federal Administration's role to put forward concrete proposals for new legal provisions in all of the various and sometimes extremely complex dossiers. The PTSS in its field of telecommunications surveillance is no exception. The one thing that is special about the PTSS is that we are a small unit with only 60 employees but we perform the same tasks as the large federal offices.

The PTSS is a product of the liberalisation of the telecommunications market over 20 years ago, but it has only been jointly responsible for legislating in this area since the last complete revision of the Federal Act on the Surveillance of Post and Telecommunications (SPTA). Why is that?
The increasing prevalence of internet-enabled mobile phones in the noughties once again sped up technological development in the telecoms industry as more and more people were regularly using apps and VoIP platforms. In view of this trend, it was felt that future legislative projects would require technical expertise that could most easily be collected where the action takes place, so here within the PTSS itself. Since then, we have had a legislative team with four members.

The last revision of the SPTA and its ordinances came into force in March 2018. In the 2020 reporting year, you were once again working on a package of amendments to four individual ordinances. Why were these revisions needed?
There is no single, uniform trigger for the revision of an ordinance. A potential reason may be issues raised in the National Council or Council of States. We prepare the Federal Council's opinion and, depending on what the Federal Assembly decides, we take action. A second reason to revise the SPTA or its ordinances are amend-

ments to other acts or ordinances with implications for surveillance. On 13 June 2021, the Federal Act on Police Counterterrorism Measures will be put to a national referendum. One of the things the Act provides for is the localisation of persons presenting a threat to public safety. If the law is approved, we will have to specify in the SPTA regulations how the corresponding measures will be implemented.

To what extent do law enforcement authorities and telecommunications service providers (TSPs) influence legislation?
The answer to this question takes us back to the technical dynamics of the telecoms industry. In a world without inventors, engineers and innovations, the PTSS could limit itself to receiving the requests from the law enforcement authorities and issuing relevant orders to the TSPs, but the fact is that the TSPs are constantly redesigning and developing their infrastructures. This is why it is often the case that existing regulations can no longer be satisfactorily applied in practice, or that technology offers unprecedented possibilities which require new provisions to be created on the basis of the SPTA.

Which specific technical innovations are you most concerned about at the moment?
The introduction of the 5G standard to mobile networks represents a huge challenge. 5G renders some previous forms of surveillance impossible and makes others possible. The law enforcement authorities are impacted by these new possibilities and would like to see the ordinances adapted as soon as possible so that they can benefit from them.

The provision or export of user data involves time and effort for the TSPs, which currently number around 780. How willing are they to keep implementing new regulations?
There is indeed a certain conflict between the right of TSPs to pursue private commercial activities freely and the public interest in effective law enforcement. The PTSS acts as an intermediary in this area. In terms of legislation, this means that when amending ordinances, we always weigh

up whether the changes could result in an additional burden for the TSPs. What's more, we also propose changes that simplify existing processes and therefore reduce effort for the TSPs.

Staff at the PTSS deal with law enforcement authorities and TSPs literally around the clock. Is there even time in the stress of day-to-day operations to discuss fundamental concerns that could have legal implications?
Our lawyer colleagues in Surveillance Management and Provider Management systematically log the incoming suggestions and complaints. The concerns of stakeholder groups form part of a roadmap; this basically means that we have an internal list that describes and evaluates these concerns.

How do you go about drafting an article or an ordinance?
First of all, we need a preliminary draft. At this stage, we lawyers work a bit like writers or journalists in search for inspiration. Once we have an initial draft, we discuss it in a small group in order to get a final version. The final text must meet all the requirements and be as clear as possible.

How closely do you work with the technical team at the PTSS during this phase?
As a very first port of call, we have a technician in the legislative team. He is an engineer with training in law. When we have to deal with highly technical aspects, we also confer with other colleagues.

How much do you lawyers actually know about network technology and IT?
Lawyers also need a certain affinity for technology and IT. If we have already done a bit of pro-

New fee regulations at the PTSS

More than 260,000 pieces of information, some simple and others far more complex, were supplied to law enforcement services in 2020. Until the middle of the year, each individual request was subject to a charge and had to be billed.
In November 2017, the Federal Council had mandated the PTSS to set up a working group to look at ways of simplifying the billing of telecommunications surveillance.
Following several workshops, the working group proposed retaining the existing individual billing model, but reducing administrative costs by making requests regarding users of IP addresses or telephone numbers free of charge. As the PTSS previously charged CHF 9 for this simple information and providers were still to be paid CHF 3 for each answer, this regulation meant an annual revenue shortfall of CHF 1.4 million for the PTSS and thus also for the federal budget. The working group therefore recommended increasing fees for retroactive and real-time surveillance. The working group's suggestions were incorporated in a partial revision of the Ordinance on Fees and Payments for Postal and Telecommunications Surveillance, which was approved by the Federal Council on 20 May 2020 and came into force on 1 July. Since then, authorities entitled to do so can request simple information free of charge, while providers will continue to be paid CHF 3 per answer.

gramming in our spare time, that helps to better understand the complex interrelationships.

What happens to a draft text once the legislative team gives it the thumbs up?
It then goes to the management team, who critically review it. When the editing work is complete, the proposal is put out for office consultation. Once the comments of the various federal offices have been incorporated, the Federal Council opens up the consultation at our request. All interested parties – in particular the law enforcement authorities and the TSPs – have the opportunity to comment on the proposal. The draft is then put back out for office consultation and finally it's back to the Federal Council, which has to approve the text.

That sounds rather time-consuming …
It is a lengthy process. The number of those involved keeps growing. Fortunately for us, the Federal Chancellery provides guidance and recommendations for legislative projects in the Federal Administration. The 'red folder' contains lists of addresses, boilerplates and various style sheets. For example, if an explanatory report exceeds 30 pages, a table of contents is required.

Telecommunications surveillance measures affect the right to privacy. How has the legislator ensured that data protection is given due consideration in the development of telecommunications surveillance?
The SPTA attaches great importance to the protection of privacy. That already places tight restrictions on the scope for legal drafting where ordinances are concerned. What's more, every proposed ordinance revision is also examined by the Federal Data Protection and Information Commissioner.

At what point in the legislative process can ordinary citizens have their say?
Our consultation documents together with the details of contact persons are fully accessible on the Federal Chancellery's website. Any person or organisation can submit comments or criticism on our proposals within the statutory period.

"Finally, it's the Federal Council's turn again: it approves the ordinance."

Daniela Siegrist

03

FACTS AND FIGURES

Reasons for surveillance

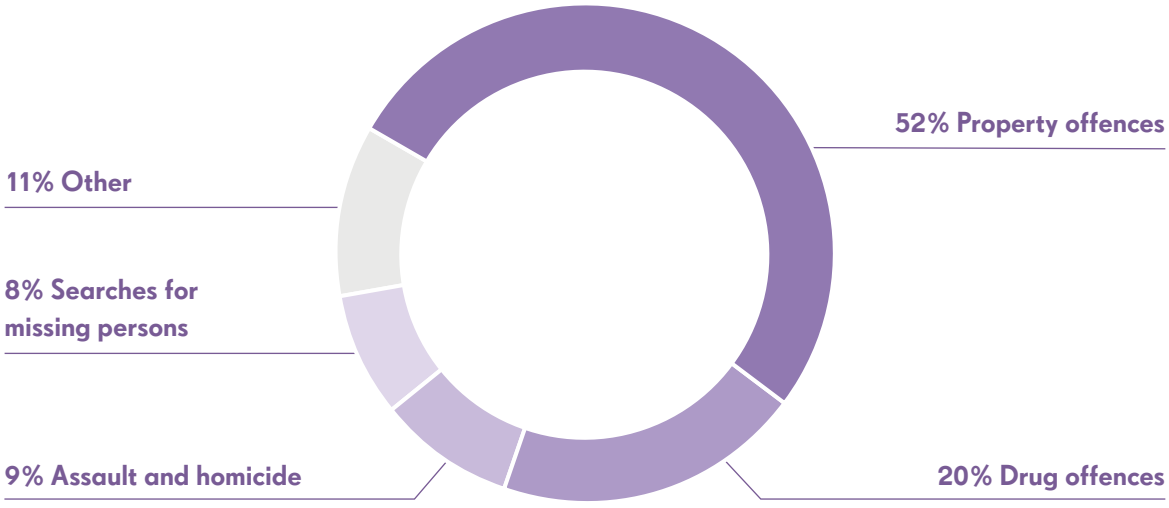
According to police crime statistics, 523,062 offences were reported in Switzerland in 2020. Telecommunications surveillance was used as an investigative measure 9,085 times, a comparatively low figure.

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 (52%). In second place, at 20%, were serious narcotics cases, with assault and homicide cases in third place, at 9%.

Telecommunications surveillance can also be used to search for missing persons. In 2020, these searches accounted for 8% of all cases, coming in in fourth 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).

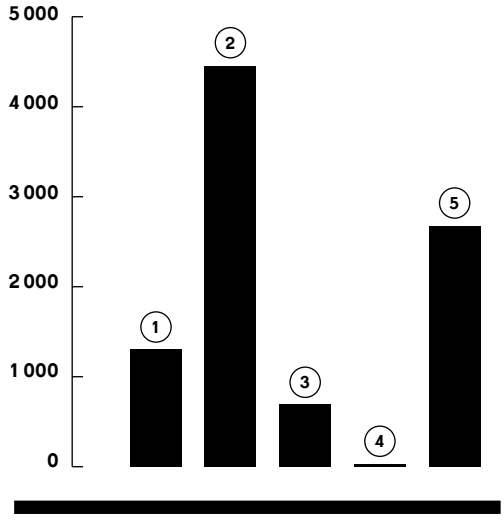
Searches for missing persons (3)
The purpose of these searches is to locate and rescue people, such as injured hikers or missing children.

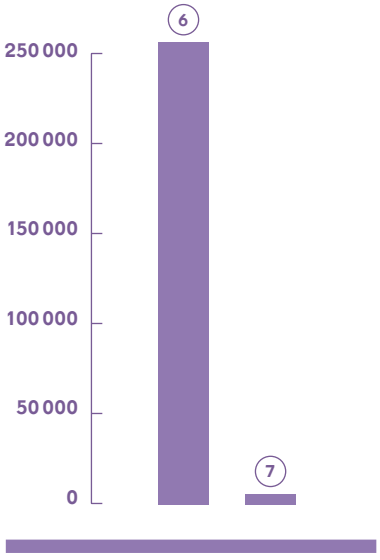
Searches for convicted persons (4)
A criminal search enables law enforcement services to locate the whereabouts of people on whom a custodial sentence has been imposed or against whom a measure involving deprivation of liberty has been ordered in a legally binding and enforceable judgment.

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.

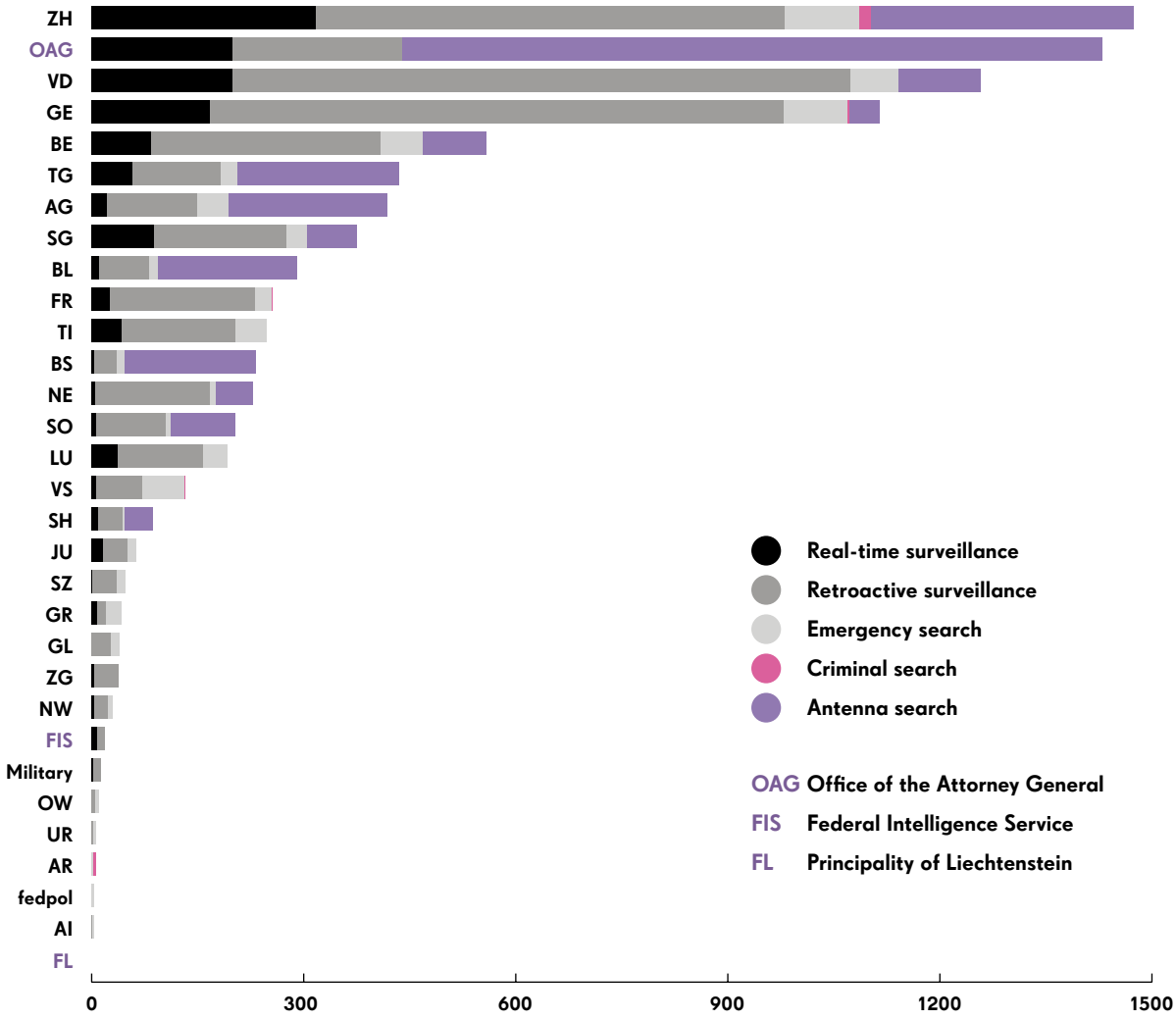
Simple information (6)
Simple information includes basic information on telecommunication connections, for example who the subscriber of a particular telephone number or IP address is.

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



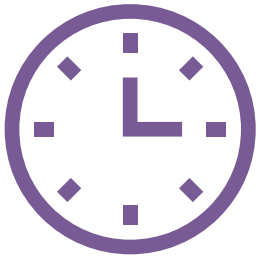
Cases and assignments

When the prosecution authorities or the Federal Intelligence Service open a new file, this is known as a case. In the course of the investigation, it may be appropriate to conduct telecommunications surveillance. If the authorities take the required measures, it is rare that they submit only a single surveillance order to the PTSS. Even searching for a missing person often requires multiple tracking measures for different times. When the law enforcement agencies conduct antenna searches, this can involve a large number of assignments in a single case. There are three reasons for this: in Switzerland, almost every point in a populated area is covered by several mobile radio antennas belonging to different providers. In addition, there may be public WLAN access points. Secondly, the law limits antenna searches to a maximum of two hours for data protection reasons, which means that several separate searches may be required, especially when it is not known precisely when a crime was committed. And thirdly, a provider's radio cells can overlap at particularly busy locations, such as railway stations. In 2020, the PTSS carried out over 2,500 antenna search assignments, spread over just 26 cases.

Number of enquiries from the public

23

Number of on-call assignments



724

Registered users processing system

WMC 5500
Warrant Management Component (assignment management)

IRC 2600
Information Request Component (information)

RDC 1900
Retained Data Component (retroactive surveillance)

ISS 2500
Interception System Switzerland (real-time surveillance)

Number of Special Cases

185

(See p. 8/9, Provider Management)

PTSS financial performance in CHF

Total revenue
12.9m

Total expenditure
32.3m

Federal contribution
19.4m

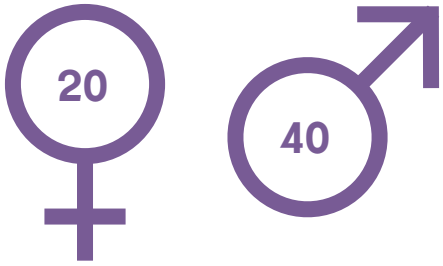
Number of media enquiries

21

Number of employees

60

Numbers of women / men



Average age

44

First language

63% German

7% Italian

23% French

7% Other

Age distribution

20 to 29
12%

30 to 39
22%

40 to 49
27%

50 to 59
36%

60 to 69
3%

“If we deploy the right resources, we’re always one step ahead of offenders.”

Julien Cartier, Head of Brigade d’analyse des traces technologiques (BATT) at the Vaud cantonal police

Publication details

Concept: PTSS
Editing: PTSS
Collaboration: JNB Journalistenbüro, Lucerne
Realisation: Schön & Berger, Zurich
Printing: Druckerei Ruch, Ittigen
Photos: Lia Lüthi, Barbara Hesse
Font: Minion Pro, Drescher Grotesk
Paper: Z-Offset
Language versions: English, German, French and Italian
Copyright: PTSS
Further information: www.li.admin.ch
Publication: July 2021

■

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
Fellerstrasse 15
3003 Bern