The scope of application of the recently introduced Federal Act on the Surveillance of Post and Telecommunications in Switzerland

Lukas Stocker (left) and Dr Jan Kleiner[1] (right)
Bär & Karrer
Zürich

Introduction

On 1 March 2018, the fully revised Federal Act on the Surveillance of Post and Telecommunications (FASPT) entered into force in Switzerland. According to the Federal Council of Switzerland, the main objective of this new act is to ensure that necessary surveillance of (postal and) telecommunications traffic will also be possible in the future and not be prevented by the introduction of new technologies (such as encrypted internet telephony). The intention is therefore not to surveil more, but to be able to surveil better.

The present article focuses on whether the aforementioned purpose, the surveillance of telecommunications traffic by use of new technologies, can indeed be achieved by the current wording of the new FASPT and how possible challenges are addressed, particularly by the competent surveillance authority, the Post and Telecommunications Surveillance Service (PTSS). The article focuses on telecommunication services. Postal services will thus not be addressed.

FASPT: Scope of Application

In order to be a so-called "person obliged to cooperate" (POC) under the FASPT, providers of (new) communication services must be covered by the personal as well as territorial scope of application of the new act. Questions may arise in relation to both of these aspects.

Personal Scope of Application

As regards the personal scope of application, under the old FASPT, only providers which were considered telecommunications services provider (TSP) were considered POC. In this respect, a company is qualified as a TSP in case it procures, as the responsible party, the transportation of telecommunication (information-technology) traffic for third parties. In other words, a TSP is a natural or legal person who transmits or arranges to transmit information using telecommunications techniques for Swiss third parties and assumes responsibility for the provision of the promised service in respect of these third parties within the framework of a contractual relationship.

As a result, the term TSP covered mostly typical telecommunications networks and network operators. However, it failed to cover so-called "over-the-top" (OTT) service providers, which provide telecommunications services over the internet, and thus without transmitting by themselves (or being the responsible party to do so) the data by means of telecommunications techniques.

To include such OTT and similar service providers, a new type of provider obliged to cooperate was introduced in the FASPT: so-called "provider of derived communication services" (PDCS). This term covers providers of one-way and multipath communication, such as providers that allow documents to be uploaded, providers of storage space for e-mails, hosting providers, cloud services, as well as multi-way communication services, which allow communication between users, such as chat platforms and peer-to-peer internet telephone service providers.

As will be addressed further below, PDCS only have limited obligations under the FASPT. However, what must be added is that providers of derived communication services with high economic relevance (annual turnover in Switzerland of more than CHF 100 million together with more than 5000 participants and/or entities that have received more than 100 requests for information within the last 12 months) are obliged to comply with the same (complete) obligations as TSPs.

> THE LIMITED SCOPE OF TERRITORIAL APPLICABILITY REFLECTS A DILEMMA OF THE SWISS SURVEILLANCE AUTHORITIES

Territorial Scope of Application

In addition to the personal scope of application, a provider must fall within the territorial

scope of application in order to be a POC under the FASPT.

In principle, the FASPT is applicable to providers of telecommunication services in Switzerland, in accordance with the so-called principle of territoriality of Swiss public administrative law. As a result, and according to the prevailing Swiss legal doctrine as well as case law, a provider is subject to the FASPT if it is legally domiciled or if it owns infrastructure in Switzerland. Further, even if the provider (or any of its subsidiaries) has its legal domicile in Switzerland, it cannot be required to provide the Swiss surveillance authority (PTSS) with requested data, as long as the relevant data of Swiss customers is not stored/managed by such Swiss entity, but *e.g.* located on servers abroad, to which the Swiss (subsidiary) company has no access.

Dilemma of Swiss surveillance authorities

The limited scope of territorial applicability reflects a dilemma of the Swiss surveillance authorities, because most of the PDCS, which provide telecoms services by the use of "new technologies", such as OTT service providers, are domiciled outside of Switzerland and have their data stored and, respectively, managed by non-Swiss companies.

What is more, even in case a PDCS is subject to the territorial scope of the FASPT, it must be noted again that PDCS are typically subject only to limited surveillance obligations, unless they are considered having a high economic relevance. In essence, PDCS do not have to carry out the surveillance themselves, but only have to tolerate it (in case surveillance is ordered). For this purpose, PDCS have to grant access to their facilities and must provide the information necessary for the surveillance. Finally, PDCS must edit the marginal data available to them; however, there is no obligation to collect such marginal data.

On the contrary, TSPs are required, amongst others, to provide, upon request, the following information to the surveillance authorities: (i) the telecommunications' traffic (call content, such as text data, audio, pictures etc.) of the person under (real time) surveillance; (ii) personal information (name, date of birth, address and, if known, occupation of the user), the addressing elements and the type of services; and (iii) so-called marginal data (or intercept related information, such as time, duration and location) of the person under surveillance.

In an attempt to address this dilemma, the Swiss surveillance authority PTSS published on 16 April 2019 an information sheet on TSPs and PSCSs[2], which is intended to serve as a guide for service providers in order to determine whether they are subject to the FASPT, and if yes, which category of POC, notably TSP or PSCS, they belong to.

According to this information sheet, certain OTT services such as communication services for the transmission of voice, text, images, sound, video or a combination thereof, e-mail, instant messaging, messaging services and communication services in social media, shall be considered as telecommunications services, independently on whether such services are offered together with the underlying connectivity. In other words, the PTSS is of the view that certain OTT services provider shall be treated as TSPs, although they do not procure, as the responsible party, connectivity, i.e. the transmission of information, for Swiss third parties.

Furthermore, the PTSS is of the view that jurisdiction (i.e. the territorial scope of application) is fulfilled not only in case the service provider has its registered office in Switzerland or the service provider has a subsidiary in Switzerland that controls, by law or on a factual basis, communications and/or data storage. Rather, the PTSS is of the view that service providers are subject to the FASPT too, which provide services to persons in Switzerland or services that are specifically targeted for Swiss people.

With this information sheet, the PTSS seems to try to extent the scope of application of the FASPT, presumably to address the shortcomings – from a surveillance perspective –, which the wording of the FASPT as well as the current legal practice seem to produce. By following the position of the PTSS, most of the OTT services provide would most likely be subject to the FASPT as a TSP, which would mean they would be obliged to cooperate with Swiss surveillance orders to the fullest extent possible.

However, the position of the PTSS has been subject to criticism. Indeed, they seem to be in contradiction to previous case law of the competent courts. What is more, the basis of argumentation of PTSS's position appears to be rather weak. From a legal perspective, the clear wording of the applicable laws, notably the FASPT and the Swiss Telecommunications Act (TCA), the qualification as a TSP requires that the provider is in fact responsible for the connectivity, by either transmitting by itself or arranging to transmit information using telecommunications techniques, towards its contractual partner, notably, a Swiss end-customer.

Likewise, Swiss legal doctrine and case law is clear that in line with the applicable principle of territoriality, it is not sufficient if a service provider offers or provides its services to persons in Switzerland in order to be obliged to cooperate with Swiss surveillance duties. Such provider must have, in addition, its seat in Switzerland or a have a Swiss subsidiary, which has access to the relevant data.

There is no case law known to us of the Swiss Federal Tribunal, which would address PTSS's positions, which it recently made public with its information sheet on TSPs and PSCSs. However, it is expected that the positions of PTSS, at least the rather controversial ones, will be subject to court proceedings in the near future. It will be interesting to see how the courts will address the issues raised regarding the scope of applicability of the FASPT.

1 Lukas Stocker is an Associate in the Telecommunication, Media, Entertainment and Sport Practice of Bär & Karrer, Switzerland; Dr. Jan Kleiner is a Partner in the same practice group.
2 The information sheet can be accessed with the following link: https://www.li.admin.ch/sites/default/files/2019-04/04_2019_Merkblatt_FDA_AAKD_EN.pdf