

Revised postal and telecoms surveillance legislation

November 29 2017 | Contributed by [Walder Wyss](#)

[Revised Postal and Telecommunications Surveillance Act](#) [Scope of obligations](#) [Comment](#)

Revised Postal and Telecommunications Surveillance Act

On November 15 2017 the Federal Council announced that the revised Postal and Telecommunications Surveillance Act and its implementing ordinances will enter into force in March 2018. It also published the final text of the implementing ordinances. (1) This announcement is the final step in the revision process of this body of laws, which started in 2006.

The act, both in its present and revised form, applies to providers of postal or telecoms services. Through a dedicated postal and telecoms surveillance service, criminal prosecution authorities can obtain communications data collected by service providers. The dedicated service will play a greater role in the future, as it will be tasked with centralising all collected surveillance data.

The revised act clarifies, strengthens and broadens the powers of the criminal prosecution authorities when it comes to communications surveillance. More specifically, it seeks to prevent situations where criminal suspects could avoid surveillance by using new technologies, such as encrypted internet services. In doing so, it also creates a legal basis for the use of government spy software (so-called 'GovWare').

A key change introduced in the revision concerns the scope of the revised act. In fact, it will apply not only to providers of postal or telecoms services, but also to so-called 'derived communications services providers'. Derived communications services providers offer services which are based on telecoms services and enable one-way or multi-way communication. According to the Federal Council, providers that offer storage space for emails, hosting providers for email services, chat platforms, platforms that allow the exchange of documents, as well as providers of internet telephone services qualify as providers of derived communications services. The revised act also applies to:

- providers of internal telecoms networks;
- persons that enable third parties to access public telecoms networks; and
- professional resellers of SIM cards and similar means that enable access to a public telecoms network.

Scope of obligations

The exact scope of the obligations depends on the actor, it being understood that providers of postal or telecoms services and derived communications services providers with high economic relevance have the most extensive obligations under the act. In particular, they must:

- enable real-time and retroactive surveillance;
- interface with the processing system of the postal and telecoms surveillance service; and
- store marginal communications data for six months.

AUTHORS

[Jürg Schneider](#)



[Hugh Reeves](#)



The revision process has also involved various amendments to other laws, especially the Code of Criminal Procedure.

Comment

These various changes – in particular, insofar as they affect a broad range of actors which may fall under the qualification of derived communications services providers and the standardised information process – will call for businesses to check and adapt their practices and systems to ensure that they can comply with any communications surveillance request that they may receive, as well as other requirements of the revised surveillance legislation.

For further information on this topic please contact [Jürg Schneider](#) or [Hugh Reeves](#) at Walder Wyss Ltd by telephone (+41 58 658 58 58) or email (juerg.schneider@walderwyss.com or hugh.reeves@walderwyss.com). The Walder Wyss website can be accessed at www.walderwyss.com.

Endnotes

(1) The press release and relevant documentation is available in [German](#), [French](#) and [Italian](#).

The materials contained on this website are for general information purposes only and are subject to the [disclaimer](#).