burckhardt

Katia Favre • David Känzig

January 3, 2012

Ordinance on Lawful Interception Revised Entry into Force on January 1st, 2012, Twelve Month Transition Period for Internet Access Providers

Basel
burckhardt AG
Steinentorstrasse 23,
Postfach 258,
CH-4010 Basel

Zürich
burckhardt AG
Usteristrasse 12,
Postfach 1172,
CH-8021 Zürich

burckhardtlaw.com

Thouvenin Rechtsanwälte
Klausstrasse 33
CH-8034 Zürich

Phone +41 44 421 45 45
Fax +41 44 421 45 00
E-mail info@thouvenin.com

www.thouvenin.com

Telecommunication Newsletter Switzerland

Ordinance on Lawful Interception Revised Entry into Force on January 1st, 2012, Twelve Month Transition Period for Internet Access Providers

The Ordinance on Lawful Interception (the "**Ordinance**") has been revised and will enter into effect on January 1st, 2012. The necessity of this revision was undisputed. The revision was accelerated by two recent decisions of the Federal Administrative Court, which found the imposition of the lawful interception obligation for internet over broad band and mobile devices to be without a sufficient legal basis. The major focus of the recent revision of the Ordinance concerns the interception of data transmitted over Internet.

Incumbent providers
According to the first draft of the Ordinance, all providers of internet services, which would have included provider of chat, blog or social media services or operators of private networks would have been subject to the lawful interception obligation. Due to the broad criticism that has been raised by internet providers during the consultation process, the application has now been narrowed to *internet access* service providers.

Internet access service providers must either intercept the data themselves or contractually delegate the interception to a third party. Therefore, Internet access providers do not necessarily have to buy the equipment or implement measures to intercept data themselves provided the interception obligation is assured through third party service providers.

Interception of Internet Services Data
The Ordinance also clarifies which data have to be intercepted by defining (i) the Internet access, (ii) the applications and (iii) the data subject to interception. The Internet access has been broadly defined. The Ordinance lists dial-up access to a network access server, broad band access, access through mobile packet data technologies (e.g. GPRS or LTE), wireless access (e.g. Wi-Fi, Wimax or WLL) and even other access through OSI layer 2 or 3.

Similarly, nearly all applications seem to fall under the scope of the Ordinance, as it enumerates in a generic way synchronic and asynchronic mail services (such as instant messaging and e-mail) as well as telecommunication services based on digital media (including VoIP, Audio and Video). The kind of data to be intercepted is described in a similar way as the ones that had to be intercepted under the current Ordinance.

Interception of Telephone Services Data
Under the revised Ordinance, the providers of mobile telephony services have to provide the Surveillance Authority with location data such as the cell ID and location identification regarding the antennas, even where no communication was established.

Missing Clarification between Internet and Telephony Services
The Ordinance, unfortunately, does not clarify which services have to be qualified as telephony services or as Internet services. The Surveillance Authority obviously bases the distinction on the customer perception, according to which VoIP through a regular telephone falls under telephony services whereas VoIP services through a computer is qualified as Internet services. With the convergence, however, this distinction will become more and more opaque.

Catch All Clause
Further, the Ordinance contains a catch all clause, according to which the Surveillance Authority may request from the telecommunications service providers all relevant interfaces permitting the Surveillance Authority to have access to data even if the particular interception case has not been explicitly

specified in the Ordinance. This catch all clause is the response to the two recent decisions of the Federal Administrative Court, which found insufficient legal basis for the interception ordered by the competent authority. It is, however, not undisputed, whether the catch all clause suffices.

Territorial Scope of Application
The territorial scope of application has been clarified in the Ordinance: All mobile devices transmitting data over a Swiss telecommunications service provider, irrespective of the location of the device, of the country code or of the network is subject to lawful interception. During the consultation procedure, the Internet access providers have indicated that it might not be possible for them to intercept data originating from services provided abroad or from services installed by the customers themselves.

Entry into Force
The Ordinance enters into force on January 1st, 2012; Internet Service Providers have a twelve month transition period to implement lawful interception.

Publication of Technical, Organizational and Administrative Requirements
The two decisions of the federal administrative court regarding lack of sufficient legal basis also lead the Surveillance Authority to publish its technical, organizational and administrative requirements, which Can be found under
https://www.li.admin.ch/en/index.html.

Ordinance on Costs
Together with the Ordinance on lawful interception, the Ordinance on costs has been revised and which clarifies which services will be compensated and the amount of the compensation.

Expected Revision
The revision of the Ordinance can be understood as a quick patch until the current revision of the Lawful Interception Act is passed by the Parliament. It is expected that also the Lawful Interception Ordinance will have to be revised again at that point in time.

January 3, 2012

Katia Favre and David Känzig