Title: Switzerland puts its competitive advantage on the Internet at risk

Hardly a week goes by without new revelations from Edward Snowden. But while the revelations were widely discussed, the Government is undermining our privacy protections without much debate. That does not only threaten our privacy, it also makes us less competitive.

For many, the Internet has lost its innocence. We had just settled into this new, fascinating world, enjoyed unknown liberties and experimented with new forms of communication. Then we realized that shadowy figures are roaming the place. Since then, we are suspicious. Companies, too, are reconsidering. According to an Ernst & Young report, 93 % of companies worldwide intend to maintain or expand their investment in the area of cyber security over the next 12 months. And according to Peer 1, one of the leading cloud companies, one in four decision makers plans to withdraw its corporate data from the US as a result of surveillance activities.

Switzerland is ideally placed to benefit from these developments. For example, according to privacy and technology expert Sylvain Métille, the Swiss legal framework currently provides the best protection for email globally. It is also one of the few countries where legal persons enjoy privacy rights. The advantages are particularly obvious in comparison to the United States. Overall, Switzerland has the more solid legal processes and provides better legal remedies.

Mass data collections, which are routinely carried out in the US, are not possible in this country. All surveillance measures require strong suspicion, are clearly defined by law, and reviewed twice. In U.S. law, there are, if anything, only minimal legal checks. For example, the collection of metadata - e.g. the sender, recipient and title of an email - does not require suspicion and does not need to be related to ongoing investigations.

Perhaps the main concern of US law is the so-called 'extra-territorial jurisdiction'. American companies are legally obliged to give the authorities access to customer data - even if that data is located abroad, as some argue. But the problem is not limited to the US. The UK, France and other Western countries also have insufficient data protection regimes and Switzerland has a good chance to establish itself as a 'safe haven'' for Internet services. Local services are already observing growth, as Georg Greve, CEO of email provider Kolab Systems, confirms: "After the Snowden revelations last year, the interest in our services increased substantially." Franz Grüter, CEO of Swiss Cloud provider Green.ch, agrees: "Since last summer, we received a great number of inquiries for our services in Switzerland."

Is the Swiss internet industry at the beginning of a digital gold rush? Ironically, the country is about to give up this competitive advantage. Two new bills have the potential to greatly weaken Swiss privacy protections. The first bill would allow surveillance services to deploy Government spyware, essentially permitting bureaucrats to create secret "backdoors" to directly access your computer. Aside from the fact that this is deeply creepy, if the government can open this door, others could potentially enter it too. In addition to that, the bill would give the Government the possibility to use these measures to preserve vaguely defined "essential national interests", including "the protection of the economic and financial interests of Switzerland." It is unclear how these interests will be defined.

The other bill is limited to surveillance activities in criminal proceedings. Law enforcement agencies would have easier access to more extensive surveillance tools. The controversial Government

spyware could also be used in criminal proceeding to fight “particularly grave crimes”. Apparently, this includes theft, violation of public property and concealment of stolen goods. In addition to that, ISPs and telecom operator would have to systematically record metadata of all email, Internet and mobile phone connections for 12 months, which could be extended to include private chats forums, blogs and public wifi networks.

A broad coalition of consumer advocates, civil rights groups, the pirate party and the youth sections of all major political parties rejects the planned reform. Infrastructure providers such as Grüter are also concerned: "The new federal law would clearly go too far. It is as if one would preemptively collect the DNA profiles of all citizens."

The bill is currently under parliamentary review and the senate will shortly discuss Government spyware, which is the key element of the bill. One hopes that the upper house will appeal to Switzerland's traditional role as a global leader in privacy protections and reject the bill in its current form. This would not only protect our privacy, it would make us more competitive.