

Germany: Bundestag allows police access to private PINs and passwords

Johann Müller
11 April 2013

Last month, the combined votes of the governing parties and the Social Democratic Party (SPD) enabled the German federal parliament (Bundestag) to legislate amendments to the Telecommunications Act. These changes effectively expand access to so-called inventory data.

Paragraph 113 of the Act deals with the retrieval of private user data managed by access providers such as mobile phone operators and Internet service providers (ISPs). Inventory data can be an important tool in the monitoring of telecommunications networks, because it affords direct access to the subscriber connection ports of individuals.

Early last year, parts of the text of the relevant paragraph were declared unconstitutional by the Federal Constitutional Court, because they violated the individual's fundamental right to "informational self-determination" (i.e., the protection of personal data). The court had given the legislature until June 2013 to create new regulations in line with the constitution. In particular, the judges ruled that the obligation of access providers to supply information about access security codes, such as passwords and personal identification numbers (PINs), failed to meet the requirements of the principle of due proportionality.

They also regarded the current practice of acquiring IP addresses to access information about users as a violation of the principle of the secrecy in telecommunications. They objected that, when assigning an address to the owner of a communication port, providers also cannot avoid sifting through that owner's call detail records.

The revised law now essentially aims to legally safeguard the parts of the inventory data legislation criticised by the Federal Constitutional Court. In other words, the legal framework has been extended to

legitimise a practice that was previously regarded as illegal.

With respect to the obligations of the access providers, ISPs with more than 100,000 customers are now required to maintain a "secure electronic interface" in order to minimise the time needed for certain agencies to retrieve information. Each request for information will have to be officially reviewed by a responsible specialist, but this would not preclude abuse of the system in practice.

Judicial authorisation is currently required only when access security codes are specifically requested by the police. Requests for such data by intelligence agencies must be approved by a parliamentary control commission. As in the past, access to all other inventory data can be had by police and the secret service without judicial authorisation.

To counter inadequate legal provision in the assigning of IP addresses to users, the procedure was explicitly declared legal as the consequence of changes made in the regulation of telecommunications secrecy. The only limitation on access arises from the requirement that a request to use an IP address must be made for a specific time. It is difficult to imagine how such a request could be placed in advance, since the same IP address is usually assigned to several users in the course of the high rate of allocations typically made over a long period of time. In the case of requests for access codes or an IP, the person whose data has been accessed is supposed to be notified of the fact some time later. But this in turn applies only when such notification would not thwart the aim of the search.

A commentator from the *Die Zeit* newspaper tersely summed up the intentionally abstruse wording of the new rules. The law means, "that police and intelligence services will in the future be allowed to obtain

extremely personal information about mobile phone users, and do so with the press of a button and without having to face any major legal hurdles”.

The innocuous sounding term, “inventory data”, should not detract from the fact that the issue involves direct access to people’s private lives. “Not only names, addresses and bank account details will be sent to the police. But also the PINs of the mobile phones, and passwords blocking e-mail inboxes and accessing services like Dropbox and dynamic IP addresses”, warned *Die Zeit* .

The parliamentary factions of both the Greens and the Left Party voted against the amendments. The opposition of the Greens is grossly cynical in view of the fact that they had joined with their SPD partners in the ruling coalition of the time to pass the original version of the law that was later declared unconstitutional in 2004.

Interior ministry spokesman stressed that the new regulations would not authorise an extension of the powers of the police and intelligence agencies. They also confirmed that the current practice, which was previously illegal, has now been legitimised.

However, the obligation of access providers to set up an interface for requests for information can only be seen as preparation for the massive expansion of access to inventory data. This in turn will facilitate the mass retrieval of data on the part of the police and intelligence services.

In recent years, measures undertaken by many governments to combat social unrest and riots have been aimed at monitoring, controlling and tampering with telecommunication channels such as the Internet and mobile phone communications. Access to the Internet in Egypt and Syria was temporarily cut off, and mobile phone networks were blocked during demonstrations to counteract the proliferation of calls and messages.

During and after the revolt in the UK in the summer of 2011, young people were sentenced to long prison terms, after their Facebook entries were accessed, evaluated and deemed criminally offensive. The British police monitored social networks and messaging services, and negotiated with access providers to overcome usage restrictions (see, “What do the repressive measures imposed in the UK portend?”).

The police in Germany also scanned mobile phone

data, incurred during a demonstration and obtained over wide areas. The adopted law on access to inventory data legalises and facilitates such monitoring. It exposes the determination of the government and SPD opposition to restrict democratic rights and upgrade the security apparatus in order to prepare for future class struggles.



To contact the WSW and the Socialist Equality Party visit:

wsws.org/contact