International Working Group
on Data Protection
in Telecommunications

Common Position on the detection of fraud in telecommunications

adopted at the 27th Meeting of the Working Group on 4-5 May 2000 in Rethymnon / Crete

The International Working Group on Data Protection in Telecommunications draws attention to the data protection issues related to the detection of telecommunications fraud, in particular concerning the processing of traffic data by telecommunications operators.

Fraud is specifically used here in the sense of 'fraudulent use of telecommunications services' rather than 'fraudulent activities by means of telecommunications networks (hacking etc.)'. The types of telecommunications fraud discussed here are detrimental to the telecommunications operators, as these deliver services which they are not, or only partly being paid for, resulting in loss of revenue.

The size of the fraud phenomenon, in terms of financial damage to operators is hard to estimate. Numbers quoted are 3-6% of revenue worldwide. It is clear that growing fraud levels must be a concern to many operators, especially since the margins on telecommunications services are dropping in the liberalised markets. There is a vested interest of telecom operators limiting this type of fraud.

General types of fraud

Two general types of fraud are:

Call sell operation/toll fraud. The reselling of calls to third persons without paying the operator for the calls. Several constructions are possible, often using 'phone-houses', dial-through constructions or mobile equipment.

Premium Rate Service Fraud. This includes several types of fraud with expensive special tariff numbers (typically 09-numbers). Sometimes the number is exploited in such a way that calls are being made, using fraudulent phones, to a revenue-generating number. A different approach is to have partners in crime connect phones, e.g. after business hours in offices, to such numbers. Another option is that people are, without being aware of this, being lured into making calls to expensive numbers. The fraudster collects the revenues from this activities.

Methods of committing fraud

The main ways of committing fraud are:

Subscriber fraud. A subscription is obtained through the regular subscription process under a false or stolen identity. It is also possible that employees of the telecom operator participate in this type of fraud, e.g. by deliberately skipping procedures to check a new subscriber's identity.

Surfing. This includes several forms of unauthorised use of facilities.

- Cloning of handsets. Identities, telephones or other attributes are being duplicated.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

- Calling card fraud. This includes theft of or fraud with PIN-codes and recharging cards.

- Misuse of hardware. This includes several ways to break into the telecommunications network.

Once this hacking has succeeded the network is used without paying for it. Access to the network can be gained through maintenance ports in telephone exchanges or PBXs, dial-in numbers, voice-mail systems etc.

- Teeing-in other subscriber' s line by physically connecting to the line.

Mobile fraud. Mobile communications open up several new forms of fraud. Specific types of fraud which are committed using mobile phones are the following. The simplest form is plain theft of mobile phones. Roaming fraud another form; expensive calls are being made from a foreign country, making use of the delay in billing these calls in the country where the phone is registered. Recharging or copying prepaid cards is also reported. Several types of fraud of connect-through services exist as well.

Detection of fraud: methods

Fighting fraud implies detection of fraud. In this section some indications will be given as to how fraud-detection works and which data are being used as input for the applied techniques.

Most data used for fraud detection are either Call Detail Records (CDRs) or billing data. CDRs form a collection of data sent over the network through the signalling system. These traffic data contain the calling and receiving number, time, duration and other data necessary for the communication. The billing system is the place where the CDRs are valued and the bills of individual customers are made up.

Fraud detection systems can be roughly grouped as follows:

- Simple analysis of reports based on traffic data (CDRs) and billing data. This means analysing the reports and searching for irregularities.

- Automated tools to analyse CDRs based on fixed pre-set rules. This can be done during the actual communication or afterwards. This offers more flexibility than the plain analysis, with the possibility to adapt rules. These systems are typical 'expert-systems'.

- Complex automated systems, with some capability to learn and create new detection rules itself. Techniques involved are neural networks, genetic algorithms and data warehousing/ data mining.

Data used for fraud detection

Several types of data are used as input for fraud detection. A non-limitative summary of the data involved in this process includes:

- High use

- Rising use

- Suspect use, such as suddenly increasing use of Premium Rate Services

- Long calls, e.g. longer than eight hours

- Suspect foreign destinations, which are known to fraud-sensitive

- Use of expensive services known to be fraud-sensitive

- User profiles; generally divided into several risk classes

- Individual calling patterns.

In order to 'learn', it is claimed that fraud detection systems have to assemble detailed data over long periods. In fact, when applying data mining and comparable techniques, the quality of the fraud detection is said to improve as time proceeds. This implies that the full history of subscriptions are being kept. As a rule, the more complex and adaptive the fraud detection system, the more data are being collected, and the longer these are kept for analysis.

Data protection aspects

Fraud detection brings several risks to privacy. Innocent people may be treated as potential fraudeurs, there is a risk of taking wrong decisions, the data processed for the purpose of fraud detection may be misused while the transfer and use of these data to third parties (police, secret services) might be beyond control of the operator.

Given the activities of telecommunications operators in fraud detection, what are the legal boundary conditions? Detection methods rely on the analysis of traffic data, which can in a general sense be considered as personal data. Processing of traffic data should therefore comply to privacy regulations.

Seen from the perspective of telecom operators, the wording in the applicable laws leaves room for interpretation as to which data they can legitimately collect, process and store. The same applies to the duration for which the data are being kept.

Recommendations of the IWGDPT:

1. In general , methods to limit financial risks likes prepaid systems, shortening of billing periods or guaranteed payments are to preferred to methods for afterwards monitoring or analysing personal behaviour.

2. The use of fraud detection systems should be limited to those circumstances where preventive measures to minimize the risks are demonstrated to have failed. No general justification can be given for the overall retention of traffic data for prolonged periods for the purpose of fraud detection.

3. Fraud detection systems come in many forms, and the data claimed to be necessary for the detection of fraud differ widely, dependent on the type of fraud and the technologies applied for detection. Each type of fraud should be dealt with in the way that is the least privacy invasive e.g. subscriber fraud should be limited by improving procedures to check the credentials of the subscriber.

4. In case fraud detection systems create automated decisions the data subject should be informed about that and be given means of redress.