Erich Moechel

Data Retention, Surveillance Interfaces and Death

While data retention (the mandatory storage of detailed records of telephone calls and Internet traffic) is currently being implemented throughout the EU, two recent surveillance scandals illustrate just how simple it is to abuse the technical surveillance scenarios of intelligence agencies. At the surveillance interfaces of the telecommunications networks, the number of deaths involving network security directors is starting to mount up. So, for starters, here's a brief rundown of modern government surveillance practices from the perspective of the telecommunications sector.

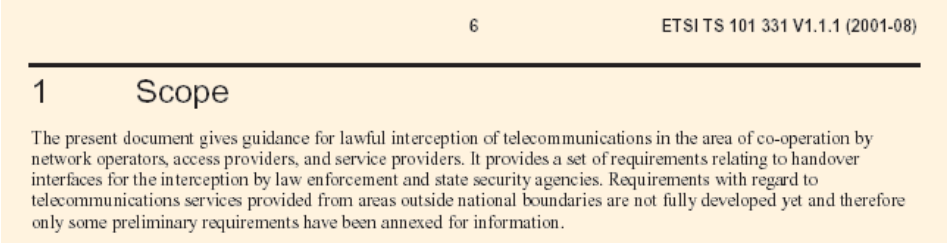
Fall 2007—all across Europe, existing legislation for the protection of data privacy is being turned on its head. What had been forbidden heretofore throughout the EU-namely, long-term storage of so-called traffic data from telecommunications networks and the Internet—is about to become mandatory.

The obligation to store call detail records—i.e. who talked to whom; when, where and how they did so—as mandated in the EU's *Data Retention Directive*—is the highpoint to date of a development that has been making shockingly undeviating progress since 1995 through the European communications landscape.

As soon as the quantity of assembled data reaches a certain critical mass, it's automatically processed by special software applications which generate complete communications profiles that are so revealing that they make conventional wiretapping superfluous in most cases. The mandatory retention of call detail records for every telephone line within the EU, which will go into effect this fall, will result in the availability of a set of data containing details of all communications within a timeframe of six months to two years.

The EU Council of Justice and Home Affairs Ministers got the ball rolling on January 17, 1995 in requiring telecommunications providers to cooperate in the surveillance efforts of law enforcement agencies. This "written procedure" was quickly and quietly passed through the Fisheries Committee; EU delegates were not notified until November 1996, when the decision was published in the official journal of the EU. By that point, technical implementation had long since begun in the European Telecom Standards Institute (ETSI).

All relevant documents that have been released by the ETSI since 1996 refer to this *Council resolution on the lawful interception of telecommunications* 96/C 329/01, the only resolution on this subject to date.



6 ETSI TS 101 331 V1.1.1 (2001-08)

1 Scope

The present document gives guidance for lawful interception of telecommunications in the area of co-operation by network operators, access providers, and service providers. It provides a set of requirements relating to handover interfaces for the interception by law enforcement and state security agencies. Requirements with regard to telecommunications services provided from areas outside national boundaries are not fully developed yet and therefore only some preliminary requirements have been annexed for information.

Specifications Sheet-Key Passage: Excerpt from one of the specifications sheets for lawful interception: "Requirements of law enforcement agencies". Mention of "government intelligence agencies" is hidden away in a single sentence in the introductory section entitled "Scope."

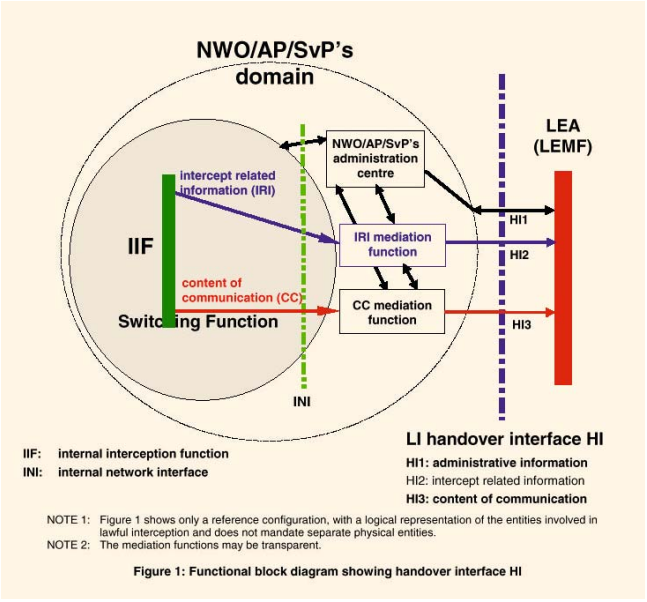


Figure 1: Functional block diagram showing handover interface HI

ETSI ES 201 671. The model of the live surveillance interface consists of three channels: queries are received via HI1, and the network operator provides the intercept-related information (IRI) to the law enforcement agency (LEA) via HI2. HI3 copies the audio data of a telephone conversation if needed. The broken (dashed) line approximately demarcates the separation between a state founded on the rule of law and a police state. These interfaces, which are built into all European telecommunications networks, must be able to deliver data to at least three LEAs simultaneously. There is a strict technological provision in force here: agencies conducting parallel surveillance operations must not be able to notice the activities of the other agencies. In this way, intelligence agencies protect themselves from data traffic analysis on a global basis.

Since its inception, a considerable expenditure of effort has gone into this: ETSI working groups have produced approximately 150 papers detailing technical requirements, specifications and standards regulating how data are to be captured from all sorts of networks. In order for this data traffic to function among different networks, there have to be a standardized interface and protocols that specify in which order these data are sent to the interface. Standards have also been developed that specify the way in which the data is delivered to law enforcement agencies.

Already in 1999, and thus years before the first UMTS networks went into operation, the technical details were established as to the points in the UMTS network at which Internet traffic and MMS would be intercepted.

Following the pattern of live surveillance standards (ETSI ES 201 671 and related regulations), a data retention interface is now being standardized. Telecommunications companies and mobile service providers must maintain in their systems detailed traffic records about all customers and, upon request, deliver them via dedicated interface to law enforcement agencies.

So far, so legal. The fact that the key positions on these surveillance standards committees are occupied by intelligence agency personnel, and that technicians from these agencies' private sector suppliers are playing along certainly provides food for thought.

Whoever controls these surveillance interfaces doesn't just have civil society's current forms of telecommunications in their sights. An assessment of the historical data sets of any telephone line invariably delivers an incredibly precise reflection of a private individual's social milieu or a company's business activities. No one knows that better than intelligence agency bureaucrats; after all, analysis of communications traffic has been part of their espionage repertoire for over a century.

Thus, the level of commitment to data retention is high. The so-called reporter responsible for the EU's data retention specifications sheet is a specialist on the staff of the intelligence agency of the Netherlands, PIDS (Platform Interceptie, Decryptie en Signaalanalyse).

Germany's Federal Office for the Protection of the Constitution, in turn, formulated the body of rules regulating how the data sets are to be delivered via the interface. The secretary and numerous staff members have been provided by the British Home Office. Among the private sector associates actively involved in this effort is Verisign, a firm with very close ties to the US military-electronic complex, which is also represented in the ETSI by a former high-ranking FBI agent who was responsible for implementing telephone surveillance in the United States.

Other sponsors of the data retention interface are the Israeli telecommunications surveillance

specialists Verint and Nice. Both firms grew up in the shadow of Israel's military-electronic complex; both firms' assortments of products speak for themselves.
These specialists are working together with technicians from telecommunications companies, mobile service providers and their suppliers to prepare the technical setup that will make it possible to create detailed communications profiles of all telephone users in the EU. Of course, as we are constantly being assured, the sole purpose of all this is to combat dangerous criminals, and its use is purely a police matter that will require a writ signed by a judge.
The facts of the matter are quite different. The overwhelming majority of the standardization documents are indeed addressed explicitly to law enforcement agencies, but the respective specification sheets on which these standards are based explicitly formulate the needs of law enforcement and intelligence agencies.
How important access to the surveillance interfaces actually is to the above-mentioned agencies is something that the network security directors of Vodafone's Greek subsidiary and Telecom Italia got an up-close-and-personal taste of in 2005 and 2006.
When the details of a wiretapping scandal involving Vodafone Hellas first began to leak out in spring 2005, the company's network security director was found hanged. In July 2006, the security director of Telecom Italia jumped from a bridge as details began to come out about Europe's worst-ever case of abuse of telecommunications traffic data. Among the two dozen people arrested were Telecom Italia's former chief of security, the assistant director of SISMI, the country's military intelligence agency, high-ranking police officials and Telecom technicians.
What they abused was pretty much every sort of abusable data that could be obtained from a landline and cell phone network including Internet connectivity. Data-mining of the call detail records was carried on in grand style, despite the fact that, according to the data protection standards then in effect throughout the EU, this data should have been deleted long before.
The data sets were sold by an in-house marketing agency; the company also accepted commissions, such as storing and analyzing the call records and online activities of celebrities. The ETSI surveillance interfaces were abused in order to tap telephone conversations, transcripts of which then appeared in newspapers.
The ETSI interface in the network of Vodafone Hellas was used to systematically bug the cell phone conversations of Greek Prime Minister Kostas Karamanlis and his cabinet. The scandal broke when technicians working for the Swedish telecommunications supplier Ericsson discovered software in the Vodafone network that didn't belong there.
They had activated the surveillance interface for lawful interception in the Athens headquarters of the Vodafone network. Instead of being provided to law enforcement agencies, though, the conversations of Greek cabinet ministers were automatically routed like a conference call to a prepaid-card cellphone. Greek courts were unable to find out who controlled it. What they did establish, however, was that, over the previous two years, the Greek government had called in special investigators from the British Home Office and the FBI to track down the ominous November 17 terror organization. Investigators questioned above all government officials specialized in telephone traffic data.
In the ETSI's lawful interception working group 3GPP SA LI, specialists from the British Home Office, the FBI, Vodafone and Ericsson—thus, actually all the parties involved in the Greek case—are working together with Germany's Federal Office for the Protection of the Constitution and other organizations to develop new surveillance rules for new mobile services. At the moment, lawful interception of MMS is standardized, as is WLAN roaming for cell phones. A surveillance norm for Internet TV is also in the offing.

Translated from German by Mel Greenwald