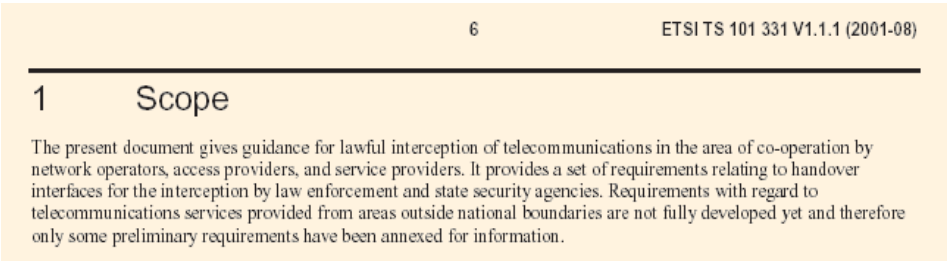
Erich Moechel

Data-Retention, Überwachungsschnittstellen und der Tod

Während EU-weit gerade die Einführung der verpflichtenden Speicherung von Verkehrsdaten aus Telefonienetzen und dem Internet *(data retention)* umgesetzt wird, zeigen zwei Überwachungsskandale, wie einfach die technischen Überwachungsszenarien von Geheimdiensten zu missbrauchen sind. An den Überwachungsschnittstellen der Telekomnetze häufen sich die Todesfälle von Netzwerk-Sicherheitschefs. Kurzer Abriss des modernen Überwachungsstaats aus der Perspektive des Telekomsektors.

Herbst 2007. Quer durch Europa werden die bestehenden Datenschutzgesetze auf den Kopf gestellt. Was bis dahin EU-weit verboten war, nämlich die dauerhafte Speicherung von sogenannten Verkehrsdaten aus Telefonienetzen und dem Internet, wird nunmehr Pflicht.
Die durch die EU-Richtlinie zur Vorratsdatenspeicherung *(Data Retention Directive)* verordnete Speicherpflicht für Verkehrsdaten – also wer mit wann wo wie kommuniziert hat – ist nur der vorläufige Höhepunkt einer Entwicklung, die sich seit 1995 mit erschreckender Geradlinigkeit durch die europäischen Kommunikationsgesellschaften zieht. Sobald nämlich eine kritische Menge vorhanden ist, lassen sich aus den Verkehrsdaten mit speziellen Software-Anwendungen auf Knopfdruck komplette Kommunikationsprofile erstellen. Die wiederum sind so aufschlussreich, dass sich herkömmliches Abhören in den meisten Fällen erübrigt. Mit der nun eingeführten Speicherpflicht wird ab Herbst für jeden Telefonanschluss innerhalb der EU ein Datensatz mit allen Kommunikationen im Zeitraum von sechs Monaten bis zwei Jahren „vorrätig" sein.
Den Auftakt dazu setzte der Rat der Innen-und Justizminister am 17. Januar 1995 mit der Kernaussage, die Telekoms haben die Anforderungen der Strafverfolger (Law Enforcement Agencies) zur technischen Bereitstellung von Überwachungs-Andockpunkten zu erfüllen. Die Entscheidung ging als „beschlossene Sache" durch den Fischerei-Ausschuss, die EU-Parlamentarier erhielten erst im November 1996 Kenntnis davon, als der Beschluss im offiziellen Journal der EU publiziert wurde. Da hatte die Umsetzung auf technischer Ebene im European Telecom Standards Institute (ETSI) längst begonnen.
Auf diesen Ratsbeschluss über das „gesetzmäßige Abfangen von Telekommunikation" *(Council Resolution on the Lawful Interception of Telecommunications 96/C 329/01)* – den einzigen bisher zum Thema – berufen sich alle einschlägigen Dokumente aus dem ETSI, die seit 1996 erstellt wurden.



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.

Pflichtenheft Schlüsselpassage: Ausriss aus einem der Pflichtenhefte für Lawful Interception: „Requirements of law enforcement agencies". Die „Staatssicherheitsdienste" sind in einem Satz im einleitenden „Scope" (Geltungsbereich) versteckt.

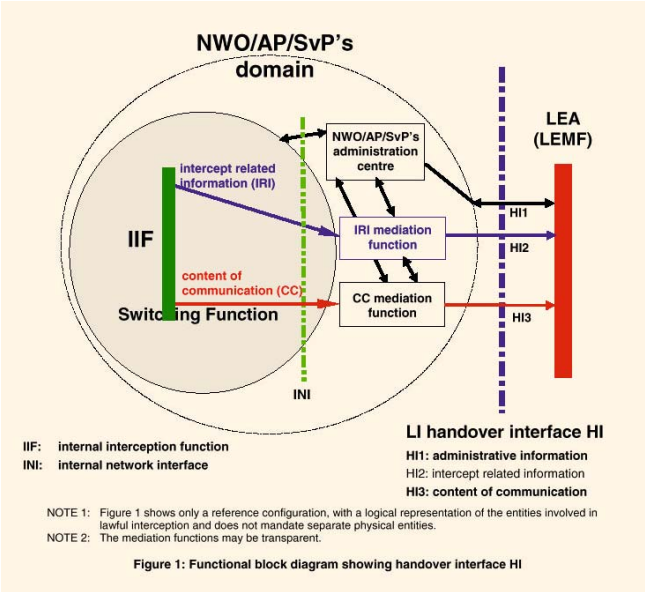


Figure 1: Functional block diagram showing handover interface HI

ETSI ES 201 671. Das Modell der Live-Überwachungsschnittstelle besteht aus drei Kanälen: Über HI1 wird angefragt, der Netzbetreiber spielt dann über HI2 die Verkehrsdaten *(Intercept Related Information IRI)* an die Law Enforcement Agency (LEA) weiter. HI3 kopiert die Audiodaten eines Telefonats bei Bedarf. Die strichlierte Linie markiert in etwa die Trennung von Rechts- und Polizeistaat. Diese Schnittstellen, die in allen europäischen Telefonienetzen eingebaut sind, müssen mindestens drei LEAs parallel mit Daten bedienen können. Strikte technische Auflage dabei: Parallel überwachende Agencies dürfen von den wechselweisen Aktivitäten nichts bemerken. So schützen sich die Geheimdienste nämlich weltweit vor Verkehrsanalysen.

Mit erheblichem Aufwand wurden von ETSI-Arbeitsgruppen bis dato um die 150 Pflichtenhefte, technische Spezifikationen und Standards erstellt, wie Daten aus Netzen aller Art abzugreifen sind. Dafür, dass dieser Datenverkehr netzüberschreitend funktioniert, bedarf es einer normierten Schnittstelle und Protokollen, die festlegen, in welcher Reihenfolge diese Verkehrsdaten an der Schnittstelle ankommen. Ebenso genormt ist, wie der Datenabtransport an Law Enforcement, also an die Strafverfolger, durchgeführt wird.

Bereits 1999, also Jahre bevor die ersten UMTS-Netze in Betrieb gingen, wurde technisch detailliert festgelegt, an welchen Punkten im UMTS-Netz Internetverkehr und MMS abgegriffen werden.

Nach dem Muster des „Live"-Überwachungsstandards (ETSI ES 201 671 und Anverwandte) wird nun eine Schnittstelle zum Abzapfen historischer Daten standardisiert, das Data Retention Interface. Telekoms und Mobilfunker müssen von allen Anschlüssen detaillierte Verkehrsdatensätze in den Systemen halten und sie auf Anfrage über die Schnittstelle auf Standleitungen an Law Enforcement, also an Polizei und Justiz, überspielen.

So weit, so rechtsstaatlich. Dass die Schlüsselpositionen bei dieser Überwachungs-Standardisiererei allerdings von Geheimdienstpersonal besetzt sind und Techniker von Geheimdienst-Zulieferern mitwirken, sollte zu denken geben.

Wer diese Überwachungs-Andockpunkte kontrolliert, hat nicht nur die aktuellen Telekommunikationen der Zivilgesellschaft im Blick. Eine Auswertung der historischen Datensätze jedes Telefonanschlusses bildet das soziale Umfeld einer Person oder die Geschäftstätigkeit einer Firma in der Regel verblüffend genau ab. Das wissen die Nachrichtendienst-Bürokraten am besten, zumal in dieser Branche „Verkehrsanalysen" von Kommunikationsverkehr seit gut einem Jahrhundert zum Handwerk gehören. Dementsprechend ist man bei Data Retention engagiert. Ein „Berichterstatter" – also Betreuer – für das Data-Retention-Pflichtenheft ist ein Spezialist des niederländischen Geheimdienstes PIDS (Platform Interceptie, Decryptie en Signaalanalyse). Das deutsche Bundesamt für Verfassungsschutz wiederum formuliert das Regelwerk, wie die Datensätze von der Schnittstelle abzutransportieren sind. Das britische Home Office stellt nicht nur den Sekretär, sondern ist auch personell stark vertreten. Zu den aktiven Beiträgern gehört auch die mit dem militärisch-elektronischen Komplex der USA eng verbundene Firma Verisign. Die wird im

ETSI durch einen hochrangigen Ex-FBI-Mann repräsentiert, der davor für die Umsetzung der Telefonüberwachung in den USA zuständig war. Weitere Sponsoren der Vorratsdaten-Schnittstelle sind die israelischen Telekom-Überwachungsspezialisten Verint und Nice. Beide Firmen sind im Schatten des militärischen-elektronischen Komplexes Israels groß geworden, beider Sortiment an Produkten spricht für sich.

Diese Spezialisten bereiten zusammen mit Technikern der Telekoms und Mobilfunker und deren Ausrüstern jenes technische Set-Up vor, das die Erstellung von detaillierten Kommunikationsprofilen aller EU-Telefoniebenutzer ermöglicht. Selbstverständlich diene das alles nur der Verfolgung schwerer Verbrechen und sei eine reine Polizeiangelegenheit, samt Beschluss eines ordentlichen Gerichts wird stets versichert.

Die Realität sieht anders aus. In der Tat ist zwar die Masse der Standardisierungsdokumente explizit an Law Enforcement (= Strafverfolger), also an die Polizei, adressiert. Die den Standards jeweils zu Grunde liegenden, Pflichtenhefte formulieren jedoch explizit die Bedürfnisse von „Strafverfolgern und Staatssicherheitsagenturen".

Wie wichtig gerade Letztgenannten der Zugang zu den Überwachungsschnittstellen ist, das haben die Netzwerk-Sicherheitschefs von Vodafone Griechenland und der Telecom Italia 2005 und 2006 am eigenen Leib erfahren. Als der Abhörskandal bei Vodafone in Griechenland im Frühjahr 2005 aufzufliegen begann, wurde der Netzwerk-Sicherheitschef von Vodafone Hellas erhängt aufgefunden. Im Juli 2006 stürzte der Sicherheitschef der Telecom Italia von einer Brücke, nachdem der größte in Europa bisher bekannt gewordene Fall des Missbrauchs von Telekom-Verkehrsdaten losbrach. Unter den zwei Dutzend Verhafteten befindet sich der ehemalige Sicherheitschef der Telecom Italia ebenso wie der stellvertretende Chef des Militärgeheimdienstes SISMI. Unter den restlichen Verhafteten sind ebenso viele ranghohe Carabinieri wie Telekom-Techniker. Missbraucht wurde so ziemlich alles, was sich in einem Telefonie- und Mobilfunk-Netz samt Internet-Connectivity an Daten missbrauchen lässt. In besonders großem Stil wurde Data-Mining in Verkehrsdaten betrieben, die nach den damals noch gültigen EU-weiten Datenschutzstandards eigentlich längst hätten gelöscht sein müssen. Die Datensätze wurden über eine eigene Agentur verkauft, Aufträge nahm man ebenso an, wie Telefonie- und Internet-Verkehrsdaten von Prominenten auf Vorrat gespeichert und analysiert wurden. Die ETSI-Überwachungs-Interfaces wurden missbraucht, um Telefonate mitzuschneiden, deren Abschriften dann in den Tageszeitungen auftauchten.

Im Netz von Vodafone Hellas wurde die ETSI-Schnittstelle dazu benutzt, um die Mobiltelefone des griechischen Premiers Kostas Karamanlis und seines Kabinetts systematisch abzuhören. Der Skandal flog auf, als Techniker des schwedischen Telekom-Ausrüsters Ericsson im Vodafone-Netz eine Software fanden, die dort nicht hingehörte. Sie aktivierte nämlich die Überwachungsschnittstelle für Lawful Interception in der Zentrale des Vodafone-Netzes In Athen. Den Telefonaten des griechischen Kabinetts wurden wie in einer Konferenzschaltung Wertkartenhandys zugeschaltet. Wer diese kontrollierte, konnten die Gerichte nicht mehr feststellen. Sicher ist, dass die griechische Regierung in den beiden Jahren davor Spezialermittler vom britischen Home Office sowie vom FBI ins Land geholt hatte, um die ominöse Terrorgruppe 17. November aufzuspüren. Gefragt waren vor allem auf Telefonie-Verkehrsdaten spezialisierte Beamte.

In der ETSI-Arbeitsgruppe 3GPP SA LI (LI = Lawful Interception) aber erarbeiten die Spezialisten des britischen Home Office, des FBI, von Vodafone und Ericsson – also eigentlich alle im obigen Fall Involvierte – mit dem deutschen Bundesverfassungsschutz und Co neue Überwachungsregeln für neue mobile Dienste. Im Moment wird Lawful Interception vom MMS standardisiert sowie WLAN-Roaming für Handys, auch eine Überwachungsnorm für Internet-TV ist in Vorbereitung.