

Das Metanetz – Anatomie des modernen Überwachungsstaats

Während EU-weit die Richtlinie der verpflichtenden Speicherung von Verkehrsdaten aus Telefonie und Internet ["Data Retention"] umgesetzt wird, zeigen zwei aktuelle Überwachungsskandale in der EU, wie einfach die existierenden, technischen Überwachungsszenarien von Staatsorganen zu missbrauchen sind. Permanente Rasterfahndung in den Kommunikationsdaten aller Bürger ist das herausragende Feature des europäischen Überwachungsstaats der nahen Zukunft.

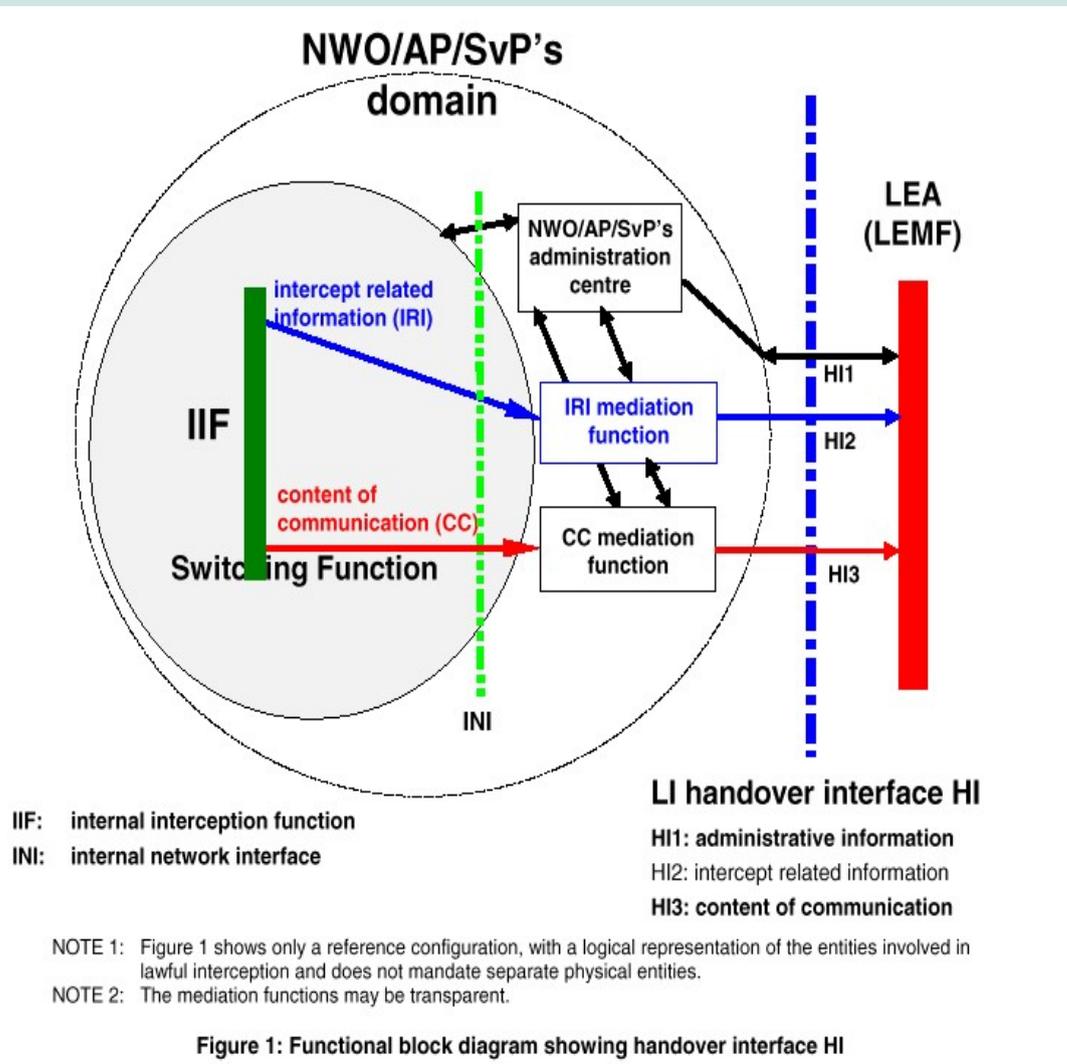
Linz, Ars Electronica 2007 09 06

Abriss der EU-weiten Überwachungsstandardisierung

- 1995 Ein EU-Ministerratsbeschluss passiert den Fischereiausschuss
- 1996 Arbeit an den Überwachungsstandards im European Telecom Standards Institute beginnt
- 1998/99 ein EU-Aufreger namens ENFOPOL
- 1999 Jahre vor Fertigstellung der UMTS-Netze ist der erste UMTS-Überwachungsstandard fertig

ETSI ES 201 671 Schema der Überwachungsschnittstelle

- LEA = Law Enforcement agency
- HI1 Anfrage LEA
- HI2 Verkehrsdaten
- HI3 Call Content
- Strichpunktierte Linien - Grenze zwischen Rechts- und Polizeistaat



Die neue Schnittstelle für “Vorratsdaten” alias “Data Retention”

- Das Technische Komitee ETSI TC LI [Lawful Interception] setzt die EU-Richtlinie um.
- Das Pflichtenheft [Requirements] stammt vom holländischen Geheimdienst PIDS.
- Das deutsche Bundesamt für Verfassungsschutz, das britische Home Office/MI5, Verisign, das FBI, die israelischen Spezialfirmen Verint und Nice als weitere Beteiligte an einem Standard, der die Kommunikationsdaten aller EU-Normalbürger betrifft.

Telecom Italia: Massives Data-Mining in Kunden-Verkehrsdaten

- Februar 2006 Data Warehouse Population Platform der TI analysiert 20 Millionen Verkehrsdatensätze pro Stunde. Gesamt: 3 Milliarden Datensätze.
- Das RADAR genannte System der TI ist eine Eigenkonstruktion aus Oracle-Datenbanken- und -Software und Data-Mining-Tools. Aufgabe: Früherkennung von Betrug und Abwanderung [Churn]
- Juli 2006: Vodafone Italia klagt TI wegen unzulässigem Datamining in Verkehrsdaten und Abwerbung von Kunden.

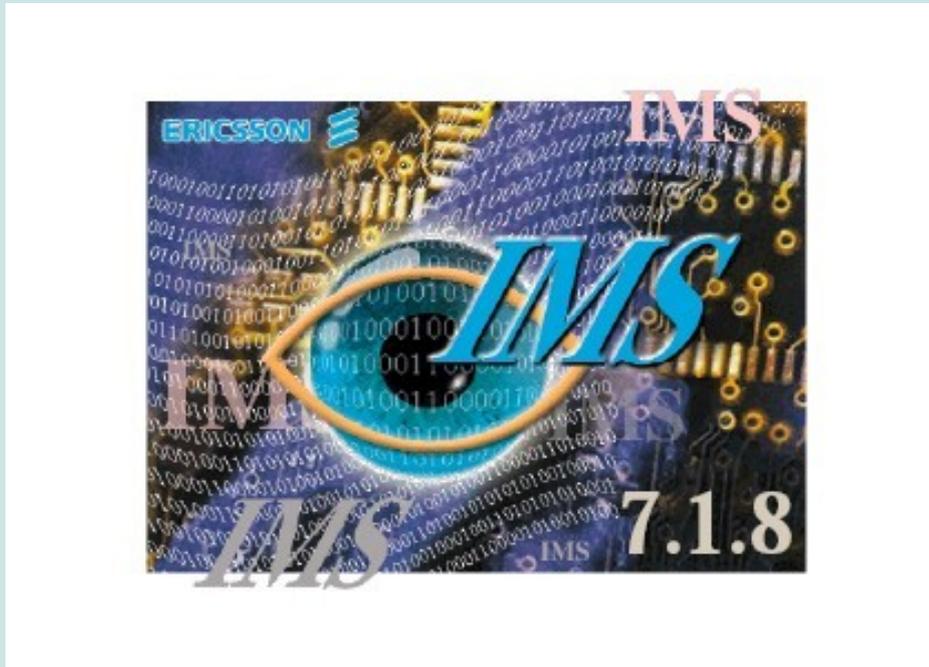
Mafiajäger, CIA-Renditions, Verkehrsdaten und der Tod

- 2003/4 Ex-Mafiajäger Adamo Bove liefert als Sicherheitschef der Telecom Italia Mobile Verkehrsdaten, die zur Anklage gegen zwei Dutzend CIA-Mitarbeiter wegen Verschleppung eines Imams nach Ägypten führen.
- Frühjahr 2006 Bove untersucht Lücken im TI-Sicherheitsystem: RADAR hat eine Hintertür.
- Juli 2006 Bove stürzt in Neapel von einer Brücke, der Vizechef des Militärgeheimdienstes SISMI wird verhaftet.

Zwischenbilanz des Skandals in der Telecom Italia

- September 2006 Boves Vorgänger als TI-Sicherheitschef, Giovanni Tavaroli, wird des systematischen Missbrauchs der ETSI-Schnittstellen beschuldigt: Illegaler Datenhandel und Erpressung.
- Die Verkehrsdatensätze wurden über eine eigene Agentur verkauft, auch auf Bestellung.
- Januar 2007 : Zwei Dutzend Telekomtechniker, Polizisten und SISMI-Agenten sind in Haft. 14 Millionen Euro beschlagnahmt.

Vodafone Hellas: Schnittstelle gehackt, Sicherheitschef erhängt gefunden



- März 2005 Nach Problemen im Netz von Vodafone Hellas finden Techniker des Ausrüsters Ericsson, dass die ETSI-Schnittstelle “gehackt” wurde.
- Zwei Tage später wird Netzwerksicherheitschef Kostas Tsalikidis erhängt aufgefunden.

Fakten zum Abhörskandal in Athen

- Premier Kostas Karamanlis und sein Kabinett wurden monatelang abgehört.
- Eine Software unbekannter Herkunft aktivierte am ETSI-Interface illegal Ericssons Überwachungssuite IMS. Programmiersprache PLEX, 6500 Zeilen mit “Rootkit” Funktion.
- Ericsson vor Gericht: Vodafone hat auf Verlangen des britischen Geheimdiensts MI6 agiert.
- Dezember 2005 MI6 Stationsleiter in Athen enttarnt, 76 Millionen Euro Strafe für Vodafone.

Die Spuren zurück ins ETSI

- Der Skandal in Athen flog durch eine Kollision von Überwachungsprotokollen am ETSI-Interface auf.
- In der AG 3GPP SA LI treffen Techniker von Vodafone , Ericsson und Home Office/MI5 und FBI regelmäßig zusammen.
- April 2006 brachte der Ericsson-Techniker in 3GPP SA LI dazu einen - siehe oben – Protokoll-Änderungsantrag ein.
- In Italien wurde die “Live”-Schnittstelle vom obersten Lawful-Interception-Verantwortlichen missbraucht.

Was beide Fälle gemeinsam haben

- Involvierung von nationalen Militärgeheimdiensten und CIA bzw. MI6.
- Missbrauch der ETSI-Überwachungsschnittstelle zum illegalen Mitschnitt von Telefongesprächen.
- Die Sicherheitschefs in den kompromittierten Netzen enden durch Selbstmord, die Angehörigen zweifeln.
- Zusammenhang mit “Anti-Terror-Maßnahmen”. In Italien waren es CIA-Entführungen, in GR wurde dem MI6 und dem griechischen Geheimdienst EYP vorgeworfen, Pakistanis gefoltert zu haben.

Was all das für die EU-weite “Vorratsdatenspeicherung” bedeutet

- Durch die den Telekoms vorgeschriebene Bereithaltung genau definierter Verkehrsdatensätze im System wird Data-Mining für “Staatsicherheitsagenturen” weitaus einfacher.
- Analog zu den Angriffen auf das “Live-Interface” ES 201 671 wird es systematische Attacken von Geheimdiensten auf das neue Interface und damit auf historische Verkehrsdaten geben.

Das Metanetz – Anatomie des modernen Überwachungsstaats

Das Überwachungsszenario in den Telefonienetzen der nahen Zukunft wird eine permanente Rasterfahndung nach Kommunikationsmustern sein, die über das Data-Retention-Interface als Routine über die Kommunikationsdaten aller Bürger läuft.

Bei Alarm wird die Überwachungsschnittstelle nach ES 201 671 automatisch aktiviert und die Kommunikation live aufgezeichnet.

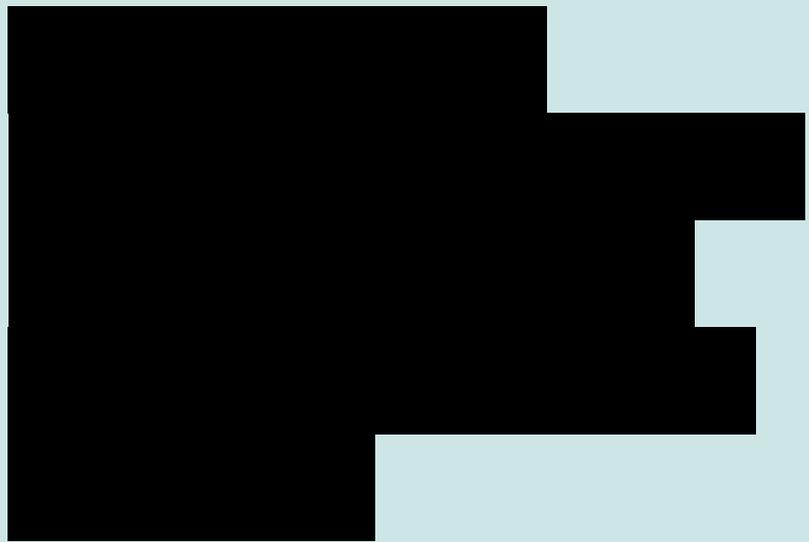
Tod an der Überwachungsschnittstelle

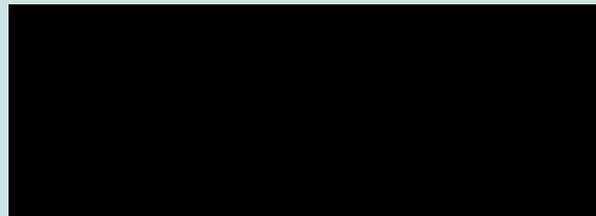


- 
Netzwerkarchitekt
von Vodafone Hellas,
im Januar 2005
erhängt aufgefunden.
- Seine Angehörigen
sind überzeugt, dass
 ermordet
wurde.

Tod an der Überwachungsschnittstelle



- 

- 

keinen
Abschiedsbrief.

Das Metanetz – Anatomie des modernen Überwachungsstaats

2007 - Who is next?

erich.moechel@orf.at