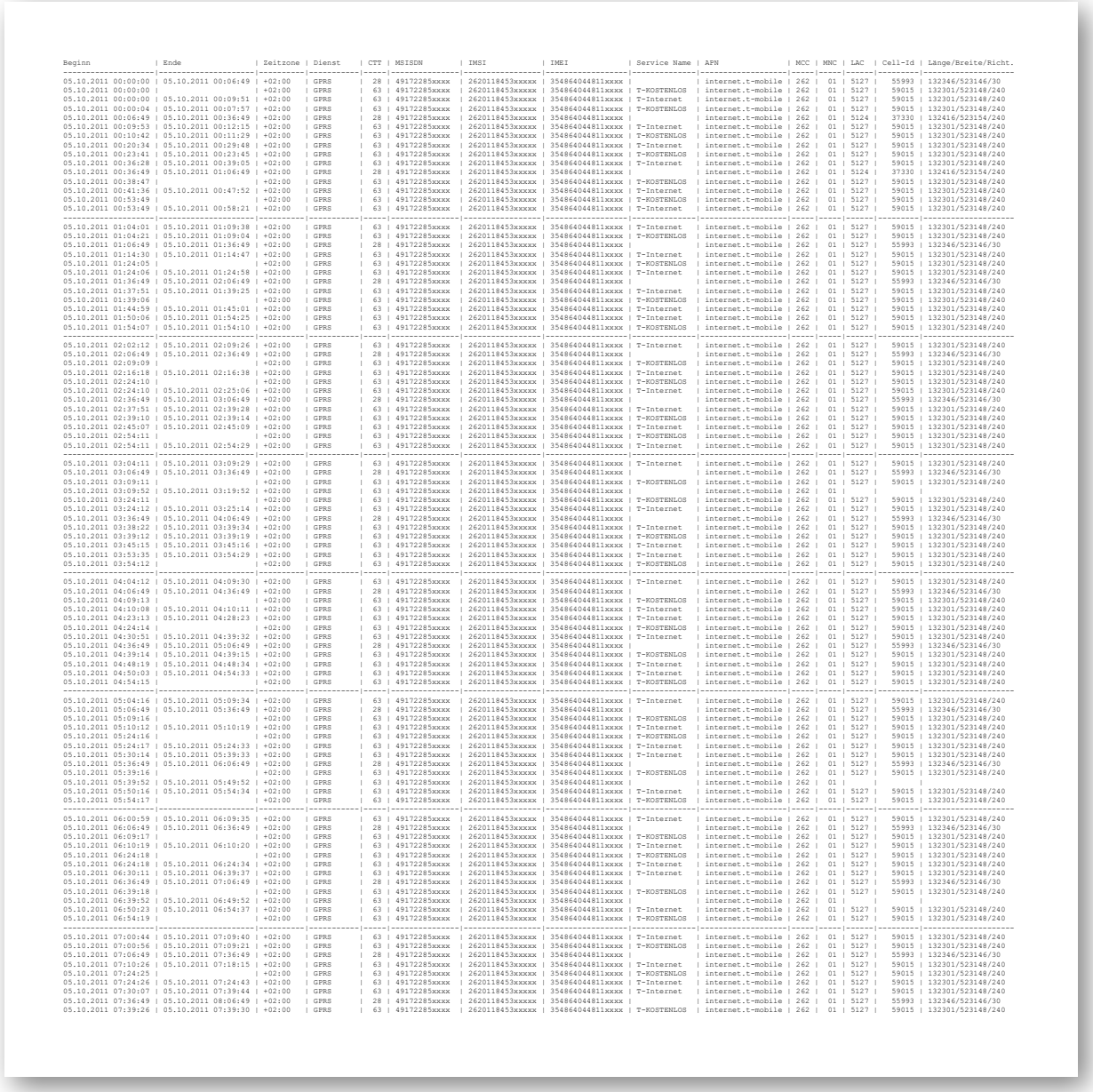
Big Brother Is Watching You

Was die Visualisierung von Vorratsdaten verrät

Handout zum Vortrag auf der „Domain pulse“ vom 14. Februar 2012

von Michael Kreil



Beginn	Ende	Zeitzone	Dienst	CTT	MSISDN	IMSI	IMEI	Service Name	APN	MCC	MNC	LAC	Cell-Id	Länge/Breite/Richt.
05.10.2011 00:00:00	05.10.2011 00:06:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 00:00:00		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 00:00:00	05.10.2011 00:09:51	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 00:00:04	05.10.2011 00:07:57	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 00:06:49	05.10.2011 00:36:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5124	37330	132416/523154/240
05.10.2011 00:09:53	05.10.2011 00:12:15	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 00:10:42	05.10.2011 00:11:29	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 00:20:34	05.10.2011 00:29:48	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 00:23:41	05.10.2011 00:23:45	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 00:36:28	05.10.2011 00:39:05	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 00:36:49	05.10.2011 01:06:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5124	37330	132416/523154/240
05.10.2011 00:38:47		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 00:41:36	05.10.2011 00:47:52	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 00:53:49		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 00:53:49	05.10.2011 00:58:21	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 01:04:01	05.10.2011 01:09:38	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 01:04:21	05.10.2011 01:09:04	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 01:06:49	05.10.2011 01:36:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 01:14:30	05.10.2011 01:14:47	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 01:24:05		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 01:24:06	05.10.2011 01:24:58	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 01:36:49	05.10.2011 02:06:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 01:37:51	05.10.2011 01:39:25	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 01:39:06		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 01:44:59	05.10.2011 01:45:01	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 01:50:06	05.10.2011 01:54:25	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 01:54:07	05.10.2011 01:54:10	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 02:02:12	05.10.2011 02:09:26	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 02:06:49	05.10.2011 02:36:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 02:09:09		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 02:16:18	05.10.2011 02:16:38	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 02:24:10		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 02:24:10	05.10.2011 02:25:06	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 02:36:49	05.10.2011 03:06:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 02:37:51	05.10.2011 02:39:28	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 02:39:10	05.10.2011 02:39:14	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 02:45:07	05.10.2011 02:45:09	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 02:54:11		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 02:54:11	05.10.2011 02:54:29	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 03:04:11	05.10.2011 03:09:29	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 03:06:49	05.10.2011 03:36:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 03:09:11		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 03:09:52	05.10.2011 03:19:52	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01			
05.10.2011 03:24:11		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 03:24:12	05.10.2011 03:25:14	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 03:36:49	05.10.2011 04:06:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 03:38:22	05.10.2011 03:39:34	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 03:39:12	05.10.2011 03:39:19	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 03:45:15	05.10.2011 03:45:16	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 03:53:35	05.10.2011 03:54:29	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 03:54:12		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 04:04:12	05.10.2011 04:09:30	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 04:06:49	05.10.2011 04:36:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 04:09:13		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 04:10:08	05.10.2011 04:10:11	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 04:23:13	05.10.2011 04:28:23	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 04:24:14		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 04:30:51	05.10.2011 04:39:32	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 04:36:49	05.10.2011 05:06:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 04:39:14	05.10.2011 04:39:15	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 04:48:19	05.10.2011 04:48:34	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 04:50:03	05.10.2011 04:54:33	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 04:54:15		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 05:04:16	05.10.2011 05:09:34	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 05:06:49	05.10.2011 05:36:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 05:09:16		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 05:10:12	05.10.2011 05:10:19	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 05:24:16		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 05:24:17	05.10.2011 05:24:33	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 05:30:14	05.10.2011 05:39:33	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 05:49:52	05.10.2011 06:06:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 05:39:16		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 05:39:52	05.10.2011 05:49:52	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01			
05.10.2011 05:50:16	05.10.2011 05:54:34	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 05:54:17		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 06:00:59	05.10.2011 06:09:35	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 06:06:49	05.10.2011 06:36:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 06:09:17		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 06:10:19	05.10.2011 06:10:20	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 06:24:18		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 06:24:18	05.10.2011 06:24:34	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 06:30:11	05.10.2011 06:39:37	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 06:36:49	05.10.2011 07:06:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 06:39:18		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 06:39:52	05.10.2011 06:49:52	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01			
05.10.2011 06:50:23	05.10.2011 06:54:37	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 06:54:19		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 07:00:44	05.10.2011 07:09:40	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 07:00:56	05.10.2011 07:09:21	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 07:06:49	05.10.2011 07:36:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 07:10:26	05.10.2011 07:18:15	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 07:24:25		+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 07:24:26	05.10.2011 07:24:43	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 07:30:07	05.10.2011 07:39:44	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-Internet	internet.t-mobile	262	01	5127	59015	132301/523148/240
05.10.2011 07:36:49	05.10.2011 08:06:49	+02:00	GPRS	28	49172285xxxx	262011845xxxxx	354864044811xxxx		internet.t-mobile	262	01	5127	55993	132346/523146/30
05.10.2011 07:39:26	05.10.2011 07:39:30	+02:00	GPRS	63	49172285xxxx	262011845xxxxx	354864044811xxxx	T-KOSTENLOS	internet.t-mobile	262	01	5127	59015	132301/523148/240

Daten wie in der Tabelle links scheinen auf den ersten Blick langweilig zu sein. Unzählige Einträge, endlose Reihen, alles voller Zahlen und mit Abkürzungen, die keiner kennt. Solche Tabellen sind jedoch nur die bekannteste und zugleich ineffizienteste Darstellungsform von Daten.

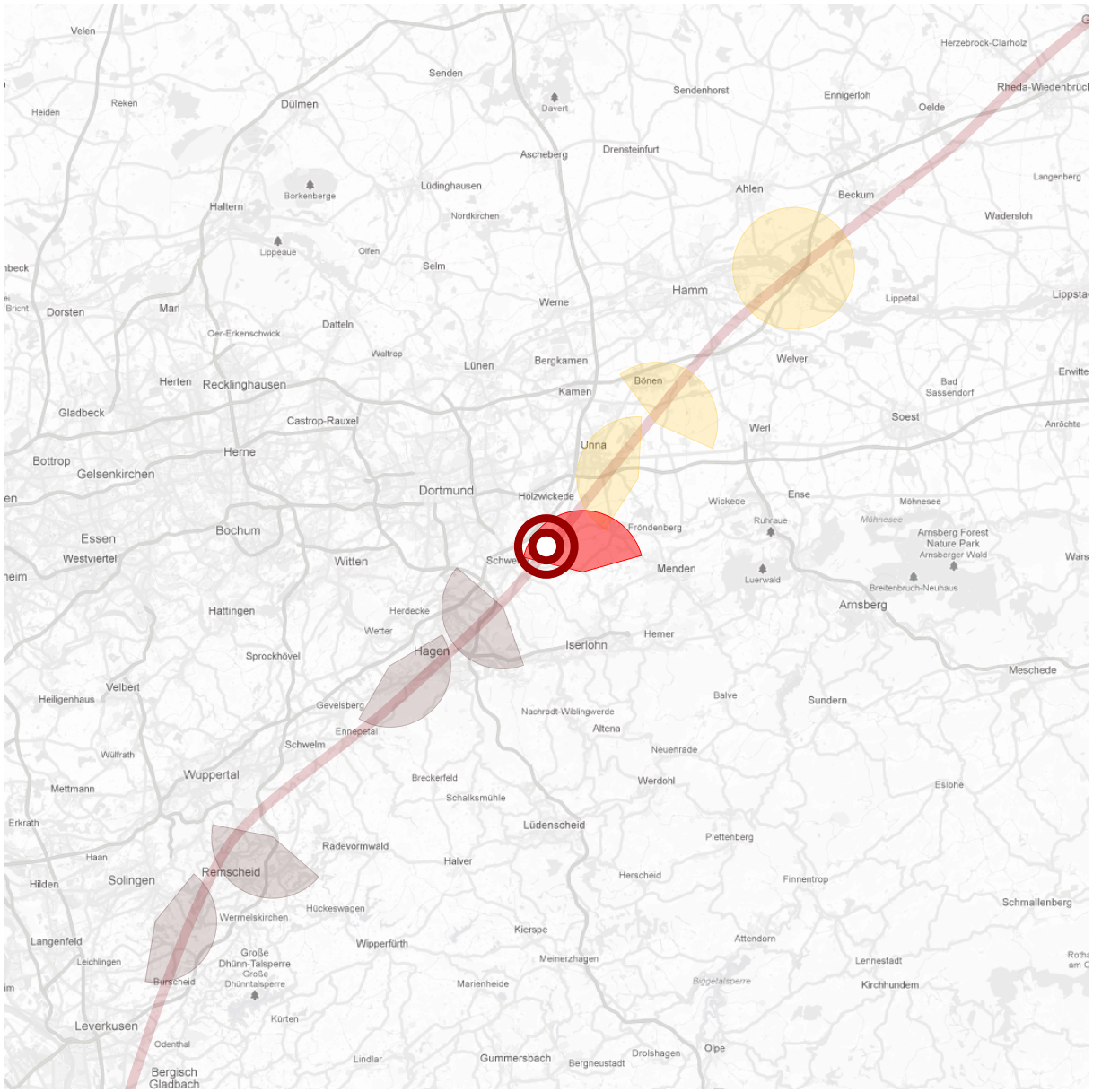
Tatsächlich ist es äußerst spannend zu schauen, welche Informationen sich hinter diesen Daten verbergen. Das langweilige Äußere täuscht darüber hinweg, dass all diese Zahlen und Abkürzungen eine Bedeutung haben – sowohl einzeln, aber auch in ihrer Kombination.

Es erinnert stark an ein Puzzle-Spiel mit tausend Teilen: Jedes Puzzle-Teil zeigt nur einen winzigen Ausschnitt. Erst wenn die Teile richtig zusammen gesetzt werden, ergibt sich ein Gesamtbild.

Bei einem handelsüblichen Puzzle-Spiel hat der Hersteller das fertige Bild bereits festgelegt. Welches Gesamtbild sich aus tausenden von Zahlen ergibt, weiß man jedoch erst, wenn man versucht, die Teile zusammen zu setzen.

Dabei gilt: Um so umfangreicher die Datenmenge ist, also um so mehr „Daten-Puzzle-Teile“ vorliegen, um so lückenloser und detailreicher ist das Gesamtbild.

Eine besonders umfangreiche Menge an Daten, die uns in ihrem Ausmaß und Detailreichtum sehr überraschte, waren die Vorratsdaten von Malte Spitz.



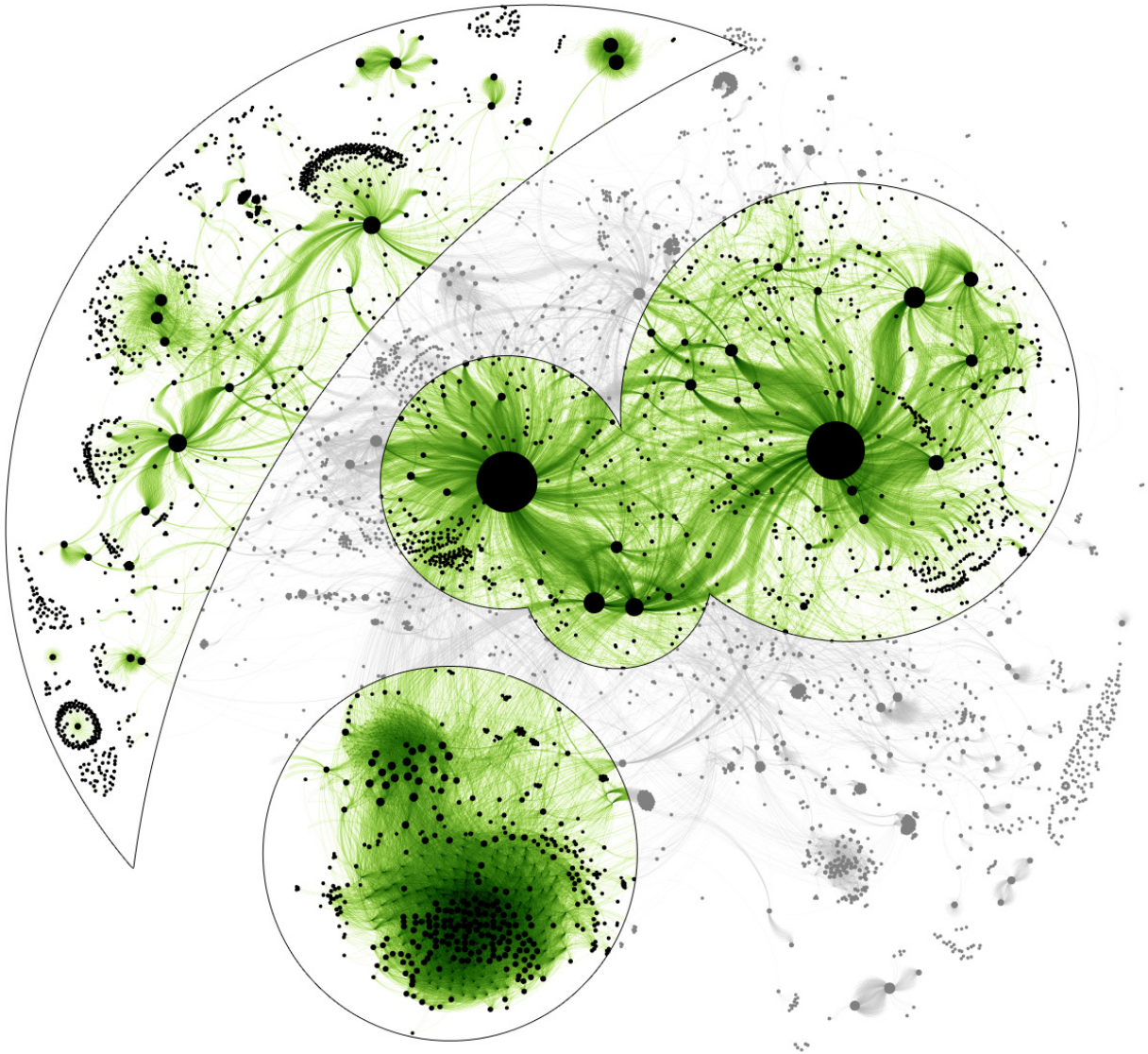
In diesen Vorratsdaten werden Daten des eigenen Handys gespeichert. Dabei werden Angaben erfasst, wann und wie lange man ins Internet gegangen ist, wann und wie lange man telefoniert hat, und mit welchem Mobilfunk-Sendemasten man verbunden war.

Der Grünen-Politiker Malte Spitz hatte 2009 die Deutsche Telekom verklagt und die Herausgabe seiner Vorratsdaten gefordert.Die Deutsche Telekom übergab ihm seine Daten als Excel-Tabelle mit knapp 36.000 Zeilen. Darin waren alle Vorgänge seines Handys der letzten sechs Monaten erfasst (von August 2009 bis Februar 2010).

Besonders interessant an den Vorratsdaten von Malte Spitz waren die Angaben, wann und mit welchen Mobilfunk-Sendemasten sein Handy verbunden war. Daraus ließ sich der Aufenthaltsort von Malte Spitz berechnen … und das fast lückenlos über einen Zeitraum von 6 Monaten.

Damit konnten wir uns erstmals ein Bild von der Vorratsdatenspeicherung machen. Zum ersten Mal wurde bewusst, wie viele Informationen in den Vorratsdaten stecken und welches Missbrauchspotential sich daraus ergibt.

Dabei haben wir noch nicht einmal die kompletten „Verkehrsdaten“ betrachtet. Dahinter verbergen sich ja nicht nur die eigenen Aufenthaltsorte.

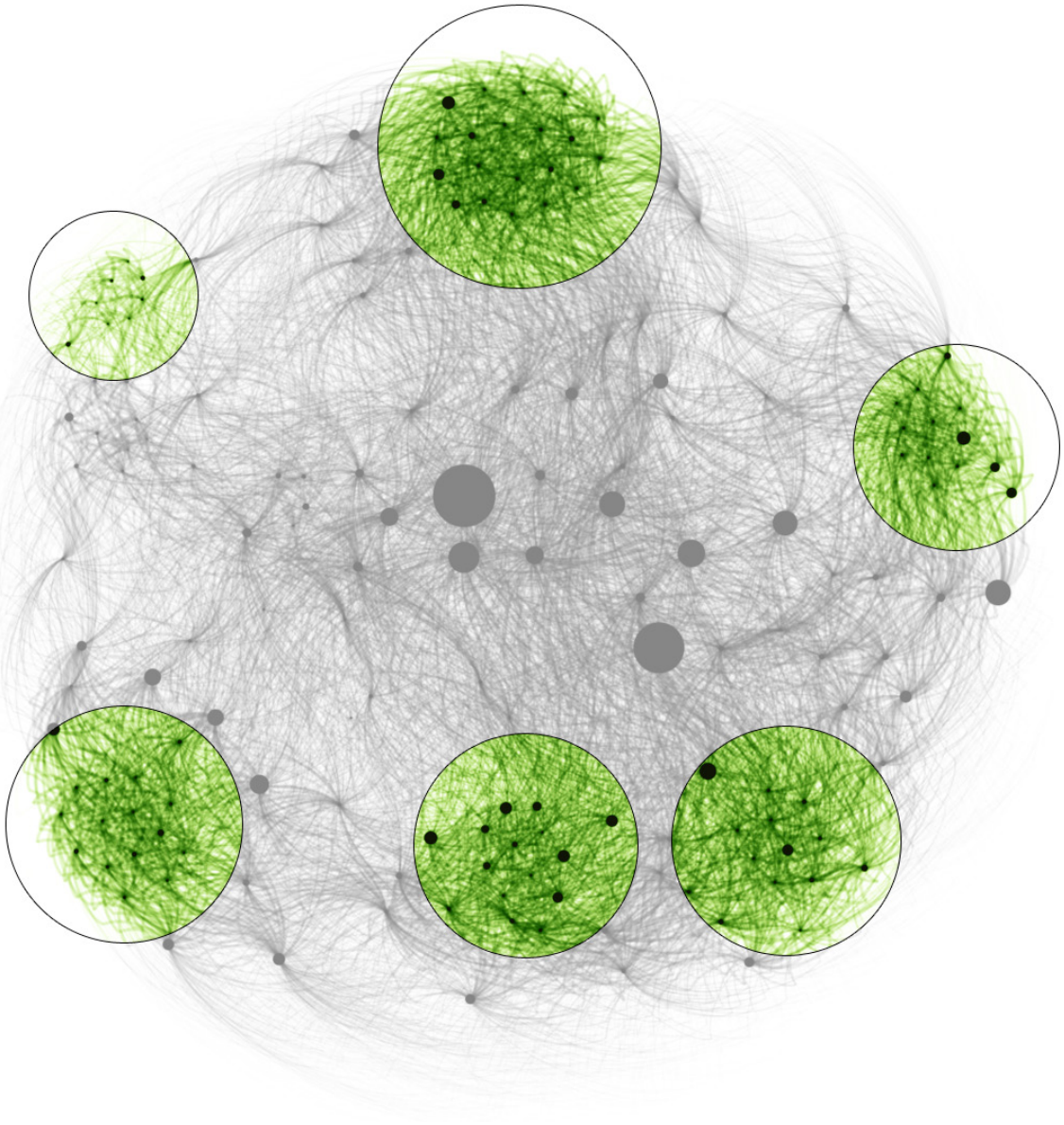


In den „Verkehrsdaten“ werden auch Verbindungsdaten gespeichert, also z.B. wann Sie mit wem und wie lange telefoniert haben. Dazu mal ein kleines Experiment:

Links ist eine Visualisierung meines E-Mailverkehrs der letzten sechs Jahre zu sehen. Die knapp 4.000 schwarzen Punkte sind die E-Mail-Adressen und die grünen Linien dazwischen zeigen die Intensität, mit der die entsprechenden E-Mail-Adressen miteinander kommuniziert haben. Insgesamt sind so 22.000 E-Mails dargestellt.

Der große schwarze Punkt mitte links ist dabei meine private E-Mailadresse, der große rechts meine Geschäftsadresse. Davon ausgehend, lassen sich verschiedenen Kommunikationsnetzwerke ausmachen. So stehen die Punkte um meinen privaten E-Mailaccount für meinen Freundeskreis. Etwas weiter rechts ist dagegen der Kreis des geschäftlichen E-Mailverkehrs. Unten links ist dann der Verein sichtbar, in dem ich Mitglied bin. Dort wird vorranging über Rundmails kommuniziert, die an hunderte Adressen geschickt werden. Die Wolke am linken Rand sind schließlich abonnierte Newsletter und Benachrichtungs-Mails

So, oder zumindest so ähnlich, würde auch Ihr E-Mailverkehr aussehen. Auch in Ihrer Kommunikation könnte man Gruppen finden. Man würde sehen können, wer Ihre Kollegen sind, Ihrer Freunde, wer zu Ihrer Familie gehört und in welchen Vereinen und Verbänden Sie aktiv sind.



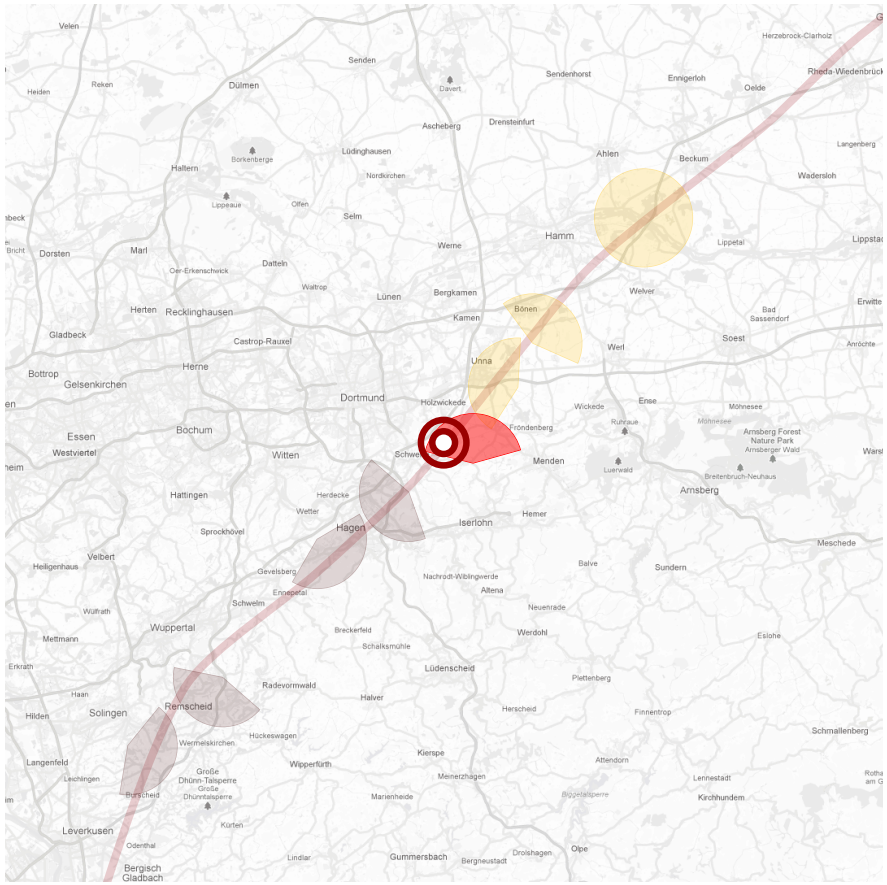
Das geht nicht nur mit dem E-Mail-Verkehr, sondern auch mit anderen Kommunikationsformen. Hier sieht man noch einmal die Vorratsdaten von Malte Spitzs Handy. Diesmal sind sie auch als Netzwerk dargestellt, das sich aus seinem Kommunikationsverhalten berechnen lässt.

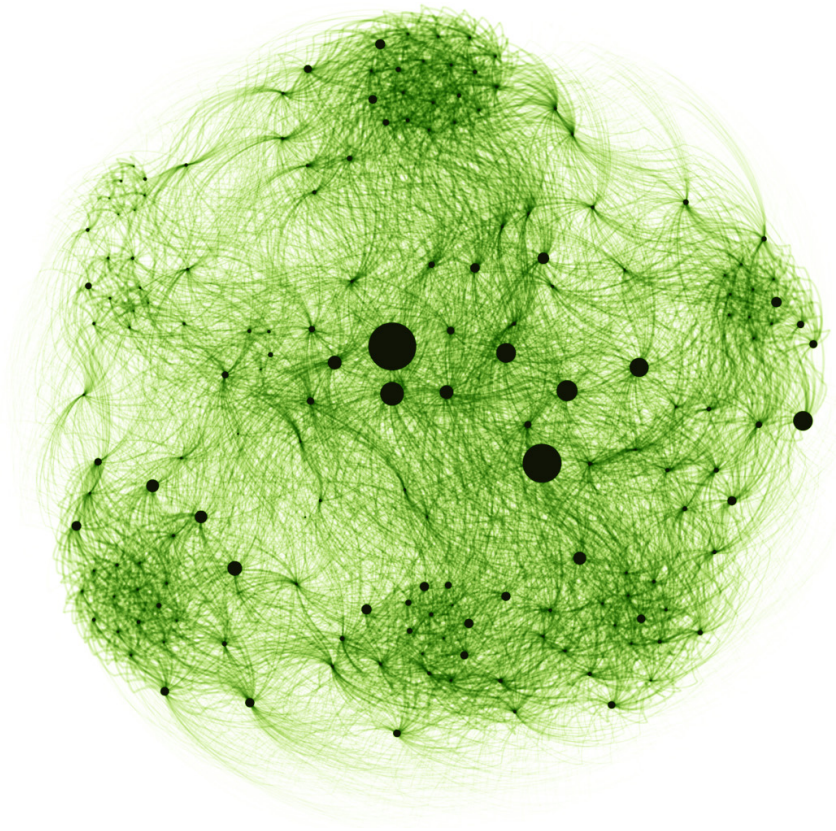
Solche Netzwerke nennt man auch „soziale Netzwerke“. Sie bilden Ihr persönliches, soziales Umfeld ab.

Um solch eine sozialen Netzwerk zu berechnen, muss man nur beobachten, wer mit wem kommuniziert. Die Inhalte der Kommunikation müssen dafür nicht aufgezeichnet werden. Es genügen bereits Uhrzeit, Dauer und eindeutige Personenidentifikationen wie z.B. Telefonnummern.

Das bereits daraus auf das soziale Umfeld geschlossen werden kann, scheint überraschend. Wenn man jedoch länger darüber nachdenkt, ist es eigentlich ganz logisch:

Wenn man nur lange genug beobachtet, wie eine Person mit ihrem soziale Umfeld interagiert, kann man auch auf Ihr soziales Umfeld schließen!





Offensichtlich enthalten Vorratsdaten nicht nur technische Informationen über Mobilfunkgeräte, Aus diesen Daten lassen sich auch viele Informationen über deren Besitzer ermitteln, und zwar viel mehr Informationen, als es der erste Eindruck vermuten lässt.

Aus den verwendeten Mobilfunkzellen lässt sich ein komplettes Bewegungsprofil des Besitzer berechnen. Und die Kommunikationsdaten, die einen großen Teil unserer täglichen, zwischenmenschliche Interaktion erfassen, zeigen auch unser soziales Umfeld.

Was sich damit aus den Vorratsdaten erkennen lässt, was deren Erfassung für Möglichkeiten bietet und welches Missbrauchspotential sich draus ergibt, soll nun anhand von drei möglichen Begebenheiten gezeigt werden?.

In unserem ersten Beispiel denken wir uns eine Person mit besonderer gesellschaftlicher Verantwortung. Es könnte sich beispielsweise um einen Diplomaten, eine Bundestagsabgeordnete oder einen Vorstandsvorsitzenden eines großen Unternehmens handeln.

Nehmen wir einmal an, dass diese Person eines Tages eine Festnetz-Telefonnummer anruft, die zu einer Suchtberatungsstelle gehört. Am darauffolgenden Donnerstag betritt die Person die Funkzelle der Suchtberatungsstelle zum ersten Mal, um dann wöchentlich jeden Donnerstag kurz vor 17:00 Uhr dort zu erscheinen.

Offensichtlich hat die Person einen wöchentlichen Termin bei einer Suchtberatungsstelle. Das ist eine Information, die ganz klar zur Privatsphäre der Person gehört.

Aber nicht nur das. Zusätzlich sind Suchtberatungsstellen durch eine Schweigepflicht geschützt. Ihre Daten, z.B. welche Personen sie betreuen und beraten, unterliegen einem besonderen Schutz. Solch eine Schweigepflicht kann aber nicht mehr greifen, wenn die Kommunikation und die Aufenthaltsorte einer Person in den Vorratsdaten gespeichert werden.

Denken wir uns nun ein zweites, komplexeres Beispiel:

Ein Geschäftsmann oder Politiker kontaktiert telefonisch erst eine Urologie und sucht sie dann später auf.

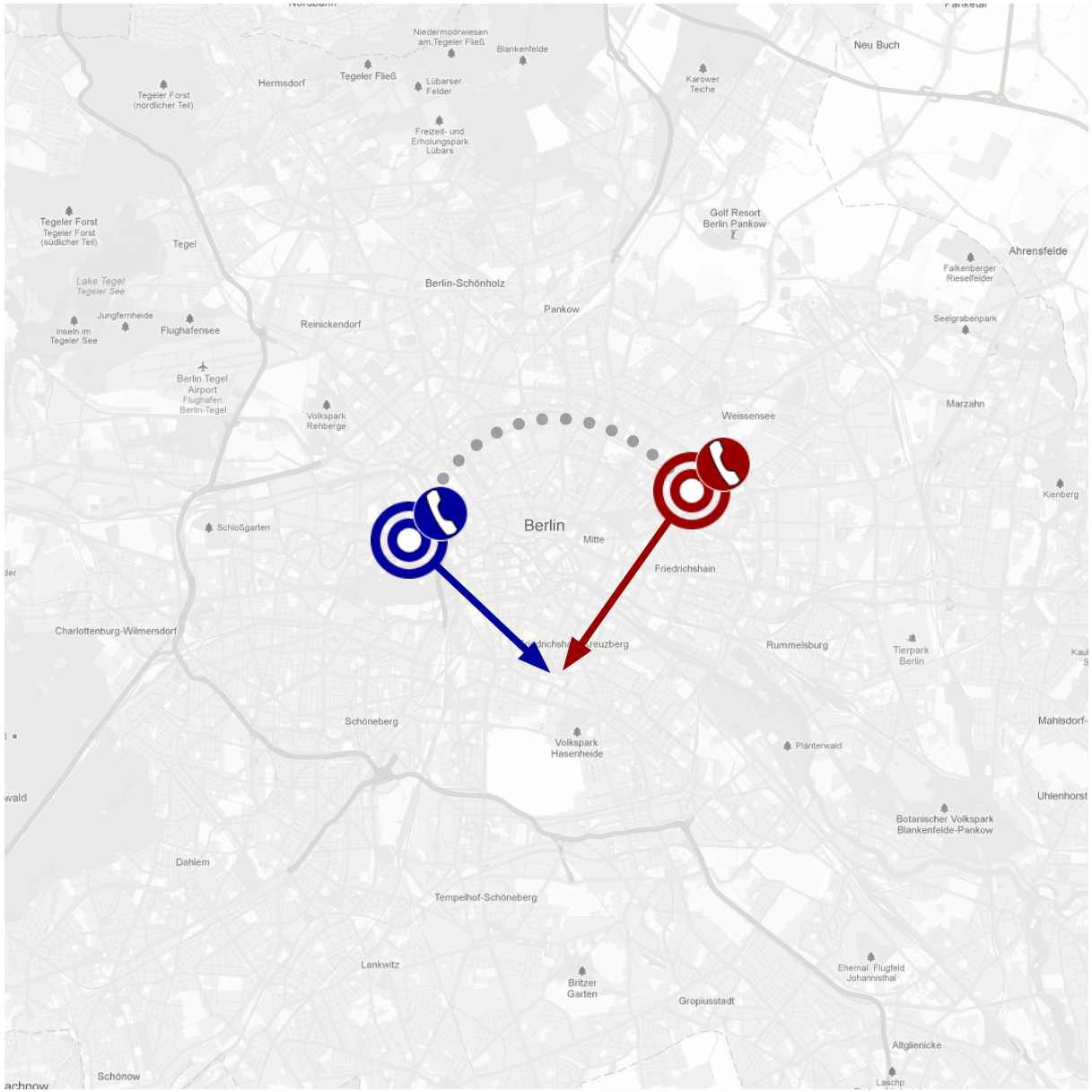
Am darauffolgenden Tage kontaktiert und besucht er eine Radiologiepraxis, um direkt danach wieder sich bei der Urologie einzufinden.

Tage später besucht er dann eine Chirurgie, die sich auf die Entfernung von Krebstumoren spezialisiert hat. Um dann regelmäßig sowohl wieder die Urologie, als auch einen Psychologen zu besuchen.

All das wird genau mit Positions- und Kommunikationsdaten mitprotokolliert, selbst, dass er einen Termin ausfallen lässt.

Jede einzelne dieser Informationen unterliegt eigentlich der ärztlichen Schweigepflicht – zusammen genommen wird aber auch dem Letzten klar, dass der Betroffene mit hoher Wahrscheinlichkeit an Prostatakrebs erkrankt ist. Dazu kommt: Wer in die Vorratsdaten schaut, weiß auch über den Verlauf der Krankheit bescheid, z.B. dadurch, dass erst eine Radiologie und anschließend doch eine Chirurgie aufgesucht wurde.

All diese sensiblen Daten sind bisher Ärzten und ihren Patienten vorbehalten. Durch die Speicherung von Vorratsdaten wird dieses Vertrauensverhältnis jedoch ausgehebelt.



Schließlich das dritte Szenario: Ein Beamter der Bundespolizei kontaktiert per Telefon eine Journalistin einer bekannten Tageszeitung. Kurze Zeit später bewegen sich beide in Richtung Stadtzentrum, um dann für 2 Stunden gemeinsam in einer Mobilfunkzelle zu verbringen.

Zwei Tage später erscheint dann in der Tageszeitung ein Artikel mit kompromittierenden Details über diese Bundesbehörde.

Kann die Journalistin ihren Informanten noch schützen? Nein, denn Vorratsdaten höhlen das Berufsgeheimnis aus! Ob Diplomaten, Bundestagsabgeordnete, Journalistinnen, Ärzte, Rechtsanwälte … der Schutz ihrer Mandanten und Patienten ist nicht mehr möglich.

Aber nicht nur einzelne Berufsgruppen sind betroffen, sondern jeder Bürger, jedes Unternehmen und ebenso der gesamte Staatsapparat! Was bedeutet es, wenn die Kommunikation und Aufenthaltsorte jedes Beamten gespeichert werden? Jedes Polizisten, Staatsanwaltes, Richters, Diplomaten, Abgeordneten, Ministers – ja selbst die Daten der Kanzlerin werden erfasst!

Dabei stellt sich unweigerlich die Frage: Wenn diese Daten solch eine Brisanz haben, sind sie dann auch sicher?

26.05.2008

Projekt „Clipper"

Jahrelang soll die Telekom im ganz großen Stil Journalisten, eigene Manager und Aufsichtsräte bespitzelt haben. Durch ein ominöses Fax aufgerüttelt, verspricht der neue Vorstandschef René Obermann nun rückhaltlose Aufklärung. Die Staatsanwaltschaft prüft bereits.

Vielleicht wäre sie nie ans Tageslicht gekommen. Diese „unappetitliche Geschichte", wie ein hochrangiger Telekom-Mann am Freitag vergangener Woche murmelte. Diese absurde Melange aus ganz viel Wirtschaftskrimi und einer ordentlichen Portion Macht und Größenwahn, einem Schuss Paranoia, komplett demontierter Mitbestimmung und missachteter Pressefreiheit.

Wie gesagt: Vielleicht wäre der ganze Vorgang in den Akten der Deutschen Telekom AG verschwunden. Aber dann musste ja auch noch das leidige Geld dazukommen. Und vor allem dieses Fax, das vor rund vier Wochen in der Bonner Zentrale landete wie ein dröhnendes Echo aus einer anderen, einer früheren, einer vergangenen Unternehmensära. Man konnte das Schreiben an den Chefsyndikus als unverhohlene Drohung deuten. Immerhin heißt es am Ende des dreiseitigen Papiers, das dem SPIEGEL vorliegt: „Unterschätzen Sie nicht mein Aggressionspotential und meine Leidensfähigkeit."

Zumindest war es eine Abrechnung in zweierlei Sinn: Der Telekom-Top-Jurist wurde vom Chef einer Berliner Beratungsfirma aufgefordert, sich schleunigst mit ihm in Verbindung zu setzen. Ziel: „Eine geregelte, gegen Indiskretionen gesicherte Beendigung unserer Geschäftsbeziehung."

Zugleich zog das Schreiben quasi einen Schlussstrich unter Aktionen, die über einen langen Zeitraum nur einem Zweck gedient haben sollen: deutsche Wirtschaftsjournalisten sowie Aufsichtsräte und auch Top-Manager des Konzerns und ihre telefonischen Kontakte zueinander auszuspähen.

...

2008 wurde durch einen Spiegel-Artikel bekannt, dass Vorstand und Aufsichtsrat der Deutschen Telekom AG Untersuchungen anordneten, um interne Lecks aufzudecken. Die Untersuchungen, womit die Abteilung „Konzernsicherheit" beauftragt wurde, beinhalteten offenbar auch illegale Aktivitäten, wie die Bespitzelung von Aufsichtsräten, eines Vorstandsmitglieds, Angehörigen und Mitarbeitern von Betriebsräten, „aber auch dem Konzernbereich nicht zuzuordnende Dritte", wie zum Beispiel Journalisten oder Ver.di-Chef Bsirske.

Nach einem Anfang November 2008 veröffentlichten vorläufigen Zwischenbericht der Bonner Staatsanwaltschaft wurden mindestens 55 Menschen „in den Jahren 2005 und 2006 nach den heute vorliegenden Erkenntnissen" ausgespäht. Dabei wurden hunderttausende Verbindungsdaten illegal beschafft und von der Firma Network Deutschland ausgewertet, um herauszufinden, welche Telekom-Mitarbeiter mit welchen Journalisten gesprochen hatten.

Die Süddeutsche Zeitung berichtete am 30. Mai 2008, dass die Bespitzelungen durch die Telekom noch deutlich weiter gegangen sein sollen. So sollen auch mit einer speziellen Software über das Mobilfunknetz Bewegungsprofile von einzelnen Personen erstellt worden sein.

(Quelle: de.wikipedia.org)

Dies ist leider nur ein Beispiel von vielen. In großen Organisationen mit tausenden von Mitarbeitern lässt sich der korrekte Umgang mit vertraulichen Daten nie einhundertprozentig sicherstellen. Insbesondere, wenn Unternehmen, Abteilungen oder einzelne Mitarbeiter unter großem Druck stehen, werden Fehlentscheidung getroffen und Befugnisse überschritten.

Nun, da Telekommunikationsunternehmen dazu gezwungen wurden, besonders umfangreich und besonders detailliert Informationen über die Bevölkerung zu sammeln, hat sich mit Sicherheit eins erhöht: das Missbrauchspotential.

Wie sieht es mit der IT-Sicherheit aus?

18.02.2011 **Netzwelt-Ticker: Hacker kaperten kanadische Regierungsrechner**

03.04.2011 **Datenraub: Hacker legt Kundenadressen von US-Großbank offen**

27.04.2011 **Hackerangriff: 75 Millionen Sony-Kundendaten gestohlen**

03.05.2011 **Sicherheitsrisiko: Hacker konnten Daten von 100 Millionen Sony-Kunden kopieren**

07.05.2011 **Datenlecks: Sony-Kundendaten zeitweise im Web abrufbar**

03.06.2011 **„Ein Kinderspiel": Hacker stehlen erneut Sony-Kundendaten**

08.07.2011 **Cyber-Attacke: Hacker klauen Daten von Zoll-Server**

12.07.2011 **Anonymous-Angriff: Hacker feiern Diebstahl Zehntausender militärischer Zugangsdaten**

14.07.2011 **Cyberangriff: Hacker erbeuten Tausende Pentagon-Geheimdaten**

21.07.2011 **Netzwelt-Ticker: Hacker verziert bundesregierung.de mit Katzen-Content**

25.07.2011 **Österreichs GEZ: Anonymous-Hacker klauen über 200.000 Kundendaten**

12.10.2011 **93.000 geknackte Konten: Neuer Hacker-Angriff auf Sony**

25.10.2011 **Meldeverzeichnis veröffentlicht: Spektakulärer Datenklau erregt Israel**

Dies ist eine kleine Auswahl der bekanntesten Sicherheitsdesaster des Jahres 2011.

Sony war offensichtlich das beliebteste Ziel von Hackerangriffen. Es ist jedoch erschreckend, wie ein internationales Technologie-Unternehmen beim Schutz von persönlichen Kundendaten, insbesondere den Millionen von brisanten Kreditkarten-Informationen, wiederholt und nachhaltig versagen kann. Und obwohl nun Kunden- und Kreditkarten-Daten veröffentlich wurde, gab es für Sony bis heute keine nennenswerten Konsequenzen.

Neben Sony wurden auch zahlreiche nicht private Institutionen Ziel von Hackerangriffen. So teilte die Österreichische GEZ mit, ihr seien insgesamt 214‘000 Datensätze gestohlen worden, davon 96‘000 mit Kontodaten.

Besonders spektakulär ist der Datenklau beim israelischen Einwohnermeldeamt. Hier hatte ein früherer Mitarbeiter die Daten aller Israelischen Einwohner an ein Unternehmen verkauft. Später sind diese Daten im Internet aufgetaucht.

08.07.2011

Hacker klauen Daten von Zoll-Server

Jetzt wurde auch eine deutsche Ermittlungsbehörde Opfer eines Hackerangriffs: Unbekannte haben brisantes Material von mindestens einem Zoll-Rechner entwendet, die Daten wurden im Web veröffentlicht.

Hamburg/Berlin - Die Unbekannten haben mindestens ein Ziel erreicht: Aufmerksamkeit. In der Nacht zum Freitag veröffentlichte eine Hackergruppe namens NN-Crew im Web Datensätze, die angeblich von Servern von Ermittlungsbehörden entwendet wurden und detaillierte Informationen zu Überwachungseinsätzen der Behörden enthalten.

Nach Informationen von SPIEGEL ONLINE haben die Unbekannten Material von einem Server einer Zollbehörde entwendet. Eine Sprecherin der Bundespolizei bestätigt: „Nach derzeitigen Feststellungen stammen die veröffentlichten Daten von einem Zoll-eigenen Server, auf den anscheinend auch Informationen der Bundespolizei zur Anwendung des Zielverfolgungssystems Patras für die Weiterverteilung im Zollbereich kopiert wurden." [...]

Bei Patras handelt es sich den veröffentlichten Dokumenten zufolge um ein System zur Auswertung von Positionsdaten, die zum Beispiel GPS-Peilsender an den Fahrzeugen überwachter Personen per Mobilfunk übermitteln. Die Bundespolizei hat den Patras-Server vorläufig abgeschaltet und alle Nutzer gewarnt.

Bewegungsprofile aus dem gesamten Bundesgebiet

Unter den veröffentlichten Daten finden sich Bewegungsprofile aus dem gesamten Bundesgebiet. Die einzelnen Datensätze sind in Ordnern sortiert, die die Namen unterschiedlicher Polizeistellen tragen. Darunter finden sich gemeinsame Ermittlungsgruppen der Landespolizeien, der Bundespolizei und des Zolls zur Rauschgiftbekämpfung, auch Zollfahndungsämter und mobile Einsatzkommandos sind betroffen.

Die einzelnen Datensätze enthalten Positionsprotokolle, die laut den Dokumenten in den Jahren 2009 und 2010 aufgezeichnet worden sind. [...]

Von welchen Geräten die Daten aufgezeichnet worden sind, lässt sich nur auf Basis der parallel von der NN-Crew veröffentlichten Dokumente vermuten. Powerpoint-Präsentationen und Handbücher beschreiben, wie Überwachungstechnik installiert und gepflegt werden kann. Die beschriebenen Geräte werden demnach an Fahrzeugen angebracht, ermitteln über GPS-Signale die Position und übermitteln diese per Mobilfunk. [...]

Aus den veröffentlichten Dokumenten geht hervor, dass die gesammelten Positionsdaten zur Auswertung auf einen oder mehrere Server geladen wurden. [...]

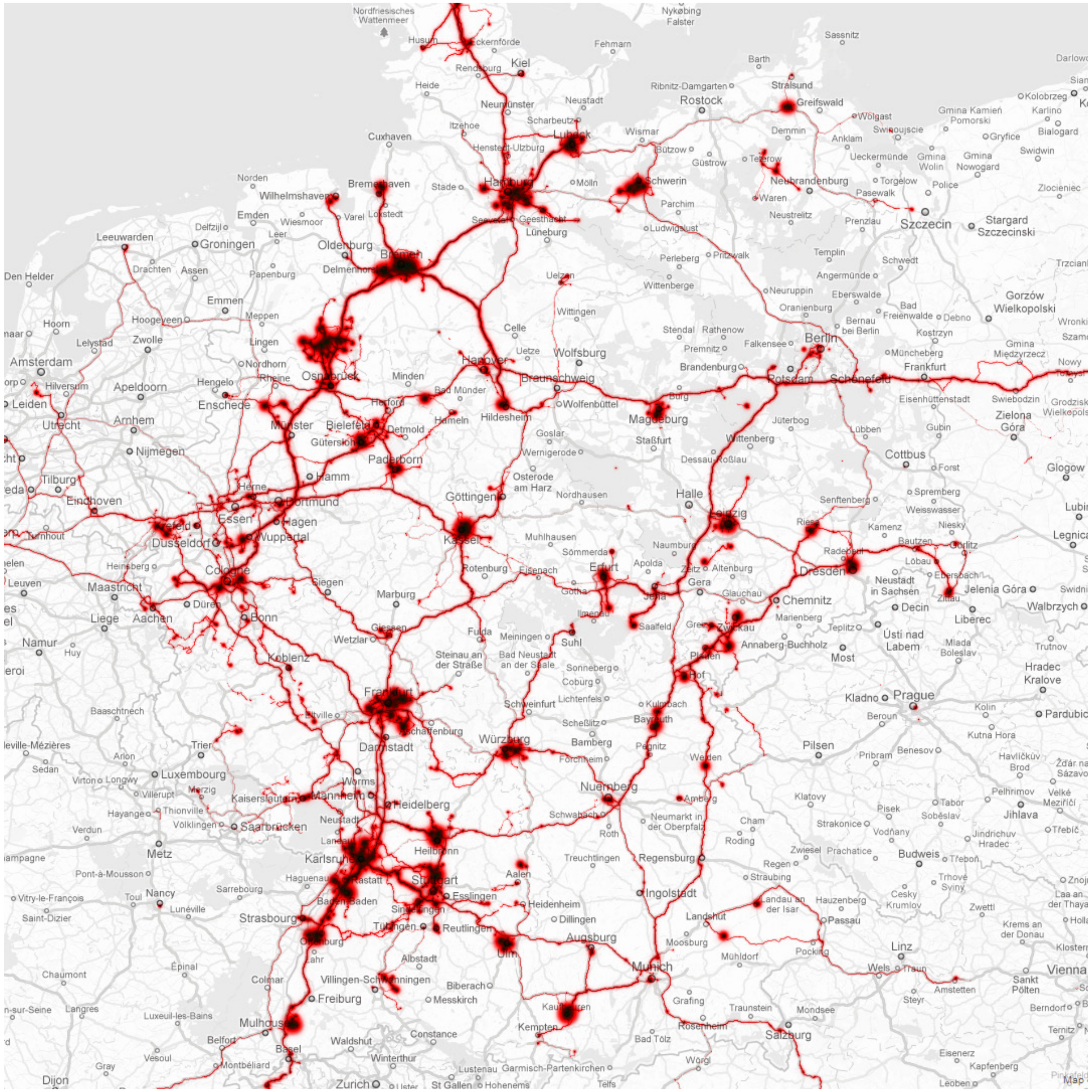
So etwas kann auch in Deutschland passieren.

Im Juli 2011 wurde bekannt, dass ein gemeinsamer Server des Deutschen Zolls und der Bundespolizei gehackt und alle Daten veröffentlicht wurde. Später zeigte sich, dass es sich bei dem Server um einen Rechner des Patras-Systems handelt.

Patras ist ein System, dass Geoinformationen von sogenannten GPS-Trackern sammelt. Einfach ausgedrückt laufen hier die Daten von Peilsendern zusammen, die verdächtigen Personen z.B. am Fahrzeug befestigt werden. Diese Sender schicken dann in regelmäßigen Zeitabständen, teilweise im 10-Sekunden-Takt, ihre Position an den Zentralcomputer, wo sie ausgewertet werden können.

Mit diesem System lassen sich verdächtige Personen genau verfolgen. Man kann nicht nur sehen, wo und wie schnell die Personen sich mit ihrem Auto bewegen, sondern auch, wann und wo sie parken.

Schaut man sich die Daten genauer an, erkennt man schnell, wo diese Personen wohnen und arbeiten, da sie üblicher Weise tagsüber in der Nähe des Arbeitsplatzes und nachts in unmittelbarer Nähe ihrer Wohnung parken. Beobachtet man dieses Verhalten über mehrere Monate, kann man die Identität der Personen ermitteln.



Der Patras-Server enthielt Informationen von fast 100 Peilsendern. Insgesamt über 4 Millionen Datensätze zeigen genau, wann sich die Verdächtigen wo befunden haben.

Nochmals: Diese brisanten Bewegungsdaten liegen frei im Internet. Jeder kann darauf zugreifen! Jeder kann die Wohnorte der verdächtigen Personen ermitteln.

Ob die Überwachung jeder einzelnen verdächtigten Person gerechtfertigt war, und ob sich unter diesen Personen auch unschuldige Mitbürger befunden haben, ist ebenfalls bis heute nicht geklärt.

Wie konnten diese brisanten, personenbezogenen Daten ins Internet gelangen? Wurden der Deutsche Zoll und die Bundespolizei Opfer eines schweren Hackerangriffs? War das ein Fall von schwerer, organisierter Kriminalität?

Nein! Es war banale Inkompetenz!

08.01.2012

Fieser Gruß an den neugierigen Papa

Ein spektakulärer Hackerangriff auf die Bundespolizei geht nach SPIEGEL-Informationen offenbar auf ein kompliziertes Vater-Tochter-Verhältnis zurück. Kölner Fahnder ermitteln gegen einen hohen Beamten der Bundespolizei aus Frankfurt am Main.

Der Mann hatte seiner Tochter einen Trojaner auf den Rechner gespielt, um ihr Treiben im Internet zu überwachen. Die Tochter hatte allerdings einen Freund aus der Hackerszene, dem die Spionage auffiel.

Um es dem neugierigen Vater heimzuzahlen, drang der Hacker in dessen Computer ein. Dort sah er, dass der Polizist dienstliche Mails an seinen Privatrechner umgeleitet hatte. Das ebnete dem Hacker den Weg ins Innere der Bundespolizei. Als Folge des Angriffs musste der „Patras"-Server abgeschaltet werden, über den die Polizei Verdächtige observiert.

Bundesinnenminister Hans-Peter Friedrich (CSU) erklärte die Computersicherheit zur Chefsache. Im Netz beanspruchten mehrere Hacker den Ruhm für die Aktion. Vielleicht zu Recht: Der Server wurde zweimal geknackt.

„Ein Beamter der Bundespolizei ließ seine Tochter mit einem Trojaner überwachen!"

Vielleicht hat er dabei gegen seine Tochter sogar den umstrittenen Staatstrojaner eingesetzt?

„Der Freund der Tochter drang daraufhin in den Privatrechner des Vaters ein und erlangte Zugriff auf interne E-Mails der Bundespolizei, die der Beamte auf seinen Rechner umgeleitet hat!"

Ganz offensichtlich war das kein schwerer Hackerangriff einer internationalen, kriminellen Vereinigungen, sondern die Kombination eines Familienstreits und die Anmaßung und Inkompetenz eines Polizeibeamten!

Auszug aus der Wikipedia:

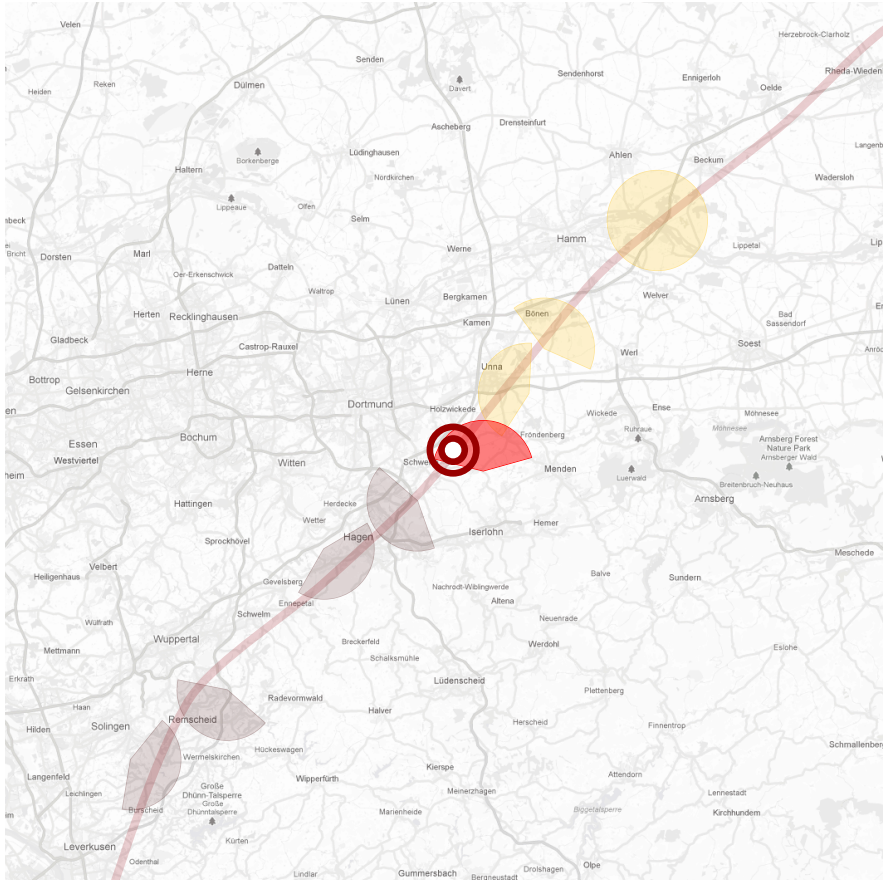
> **Facepalm** (englisch face = ‚Gesicht' und englisch palm = ‚Handfläche') ist ein Begriff des Internetjargons. Hierbei wird die physische Geste beschrieben, in der eine Hand Teile des Gesichts bedeckt. Damit sollen verschiedene Gefühle (Fassungslosigkeit, Scham, Verlegenheit, Skepsis, Frustration, Ekel oder Unglück) ausgedrückt werden. Es entspricht der Redewendung „die Hände vors Gesicht schlagen".

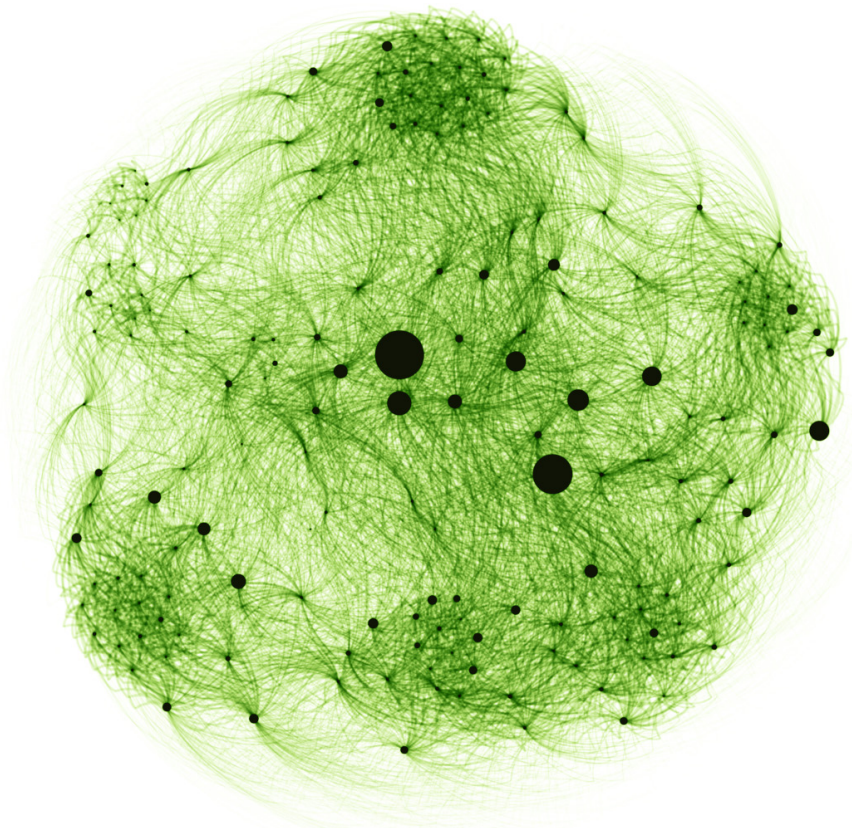
Mit diesen zahlreichen Beispielen und Zeitungsartikeln will ich weder der Telekom, der Bundespolizei, noch anderen Institutionen ihre Daseinsberechtigung absprechen. Nein, wir brauchen diese Institutionen. Und ich hoffe im Interesse aller, dass diese Vorfälle lückenlos aufgeklärt und entsprechende Konsequenzen daraus gezogen werden.

Was aber all diese Beispiele zeigen: In diesen Institutionen stehen Computer, die niemals hundertprozentig sicher sein können und deshalb jederzeit gehackt werden können. Und in diesen Institutionen, ob privat oder staatliche, arbeiten Menschen, die beabsichtigt oder unbeabsichtig Fehler machen.

Das ist nichts Ungewöhnliches. Es passieren immer Fehler, nur gibt es Dinge, bei dem keine Fehler passieren dürfen!

Wenn der Staat gemeinsam mit privaten Unternehmen unsere Mobilfunkdaten überwachen lässt, wenn von jedem Handy-Nutzer ein Bewegungs- und Kommunikationsprofil angelegt wird, wenn sowohl 10-jährige Schülerinnen, als auch jedes Regierungsmitglied davon betroffen ist, dann dürfen mit diesen Daten keine Fehler passieren!





Das Urteil des Bundesverfassungsgerichts am 2. März 2010 erklärte das deutsche Gesetz zur Vorratsdatenspeicherung für verfassungswidrig. Und obwohl durch das Urteil die staatliche Pflicht zur Vorratsdatenspeicherung entfallen ist, sammeln alle großen Telekommunikationsanbieter weiter. Sie sammeln sogar mehr Daten als zuvor, denn erst mit der Einführung der Vorratsdatenspeicherung werden z.B. auch Bewegungsprofile erfasst.

Diese brisante Daten dürfen nicht in die falschen Hände gelangen. Das muss unter allen Umständen verhindert werden. Zusätzliche Sicherungsmaßnahmen reichen dafür nicht aus, denn es liegt in der Natur der elektronischen Daten, dass sie jederzeit unbemerkt kopiert werden können. Die einzige Möglichkeit, den Missbrauch der Daten zuverlässig zu verhindern, ist diese Daten erst gar nicht zu erheben. Hier besteht für den Gesetzgeber dringender Handlungsbedarf!

Alle beschriebenen Szenarien von überwachten Bundestagsabgeordneten, Richtern, Anwälten, Ärzten und Journalisten sind in der Geschichte unseres Landes bereits in der einen oder anderen Form eingetreten. Durch die Vorratsdatenspeicherung, also die Speicherung von Verkehrsdaten z.B. von Handys, entsteht jedoch ein völlig neues Missbrauchspotential. Jeder Bundesbürger lässt sich nun per Mausklick nachverfolgen und überwachen.

Da sowohl Mitarbeiter bei den Telekommunikationsanbietern als auch bei Polizeibehörden Zugriff auf diese Daten haben, lässt sich der Missbrauch nicht kontrollieren.

Wenn private Unternehmen Zugriff auf Bewegungs- und Kommunikationsprofile ihrer Kunden haben, also auch ihrer Vorstands-, Aufsichtsrats- und Gewerkschaftsmitglieder, von Politikern, die vielleicht entgegen der privatwirtschaftlichen Interessen des Konzerns agieren, oder Richter, die Verfahren gegen den Konzern verhandeln – dann sind das hochkritische Situationen.

Ebenso problematisch ist es, wenn die Polizeibehörden Zugriff auf solch private Daten haben. Wenn die Exekutive die Bewegung jedes Richters und jedes Regierungsmitglieds überwachen kann, dann ist die Gewaltenteilung in Gefahr. Wenn in einer Notsituation die Exekutive frei dreht, ist sie nicht mehr einzudämmen. Im Ausnahmezustande stellt das Missbrauchspotential der Vorratsdaten eine Gefahr für unsere Demokratie dar.

Diese Szenarien sich schon längst nicht mehr Teil einer theoretische Debatte, sondern bereits Realität. Diese Daten werden weiterhin erhoben und die Polizei hat weiterhin Zugriff darauf.

Wenn ihr eingeschaltetes Mobilfunktelefon gerade neben ihnen liegt, existiert vermutlich bereits ein Eintrag für Sie, dass Sie sich genau jetzt hier befinden.

Jede Kurznachricht, jeder E-Mail-Abruf und jedes Telefonat, dass Sie heute getätigt haben, wurde mitprotokolliert.

Falls sie bei diesem Gedanken ein mulmiges Gefühl bekommen, können Sie sich auf den folgenden Webseiten weiter über die Vorratsdatenspeicherung informieren:

Der Vortrag auf der Domain pulse
vom 14. Februar 2012:
http://www.domainpulse.de/de/programm#unit3888

ZEIT ONLINE
„Was Vorratsdaten über uns verraten“
http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz

Arbeitskreis Vorratsdatenspeicherung:
http://www.vorratsdatenspeicherung.de

Netzpolitik.org
http://netzpolitik.org/tag/vorratsdatenspeicherung/

Digitale Gesellschaft
http://digitalegesellschaft.de/portfolio-items/vorratsdatenspeicherung/