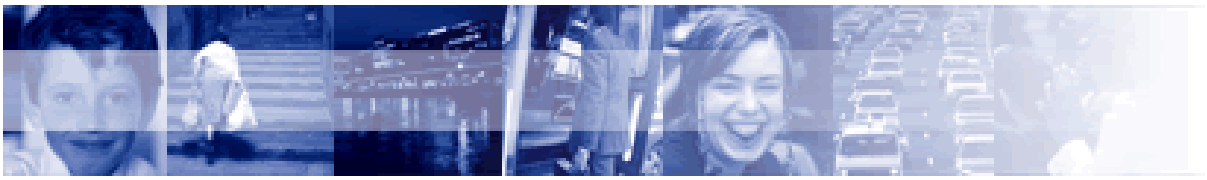
PRISE
privacy security

Security Research

PASR

Preparatory Action on the enhancement of the European industrial potential in the field of Security research



Grant Agreement no. 108600
Supporting activity acronym: PRISE

Activity full name:
Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies

Activity type: Supporting Activity

Annexes to D 5.2 Austrian report - Interview meeting about security technologies and privacy

Start date of Activity: 1 February 2006 Duration: 28 month

Author(s): Johann Čas, Institute of Technology Assessment

Supporting Activity Co-ordinator
Johann Čas,
Institute of Technology Assessment, Austrian Academy of Sciences
Strohgasse 45, A-1030 Vienna, Austria
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

Partners

Institute of Technology Assessment,
Vienna, Austria
Contact: Johann Čas
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

The Danish Board of Technology,
Copenhagen, Denmark
Contact: Lars Klüver
LK@Tekno.dk
www.tekno.dk

The Norwegian Board of Technology,
Oslo, Norway
Contact: Christine Hafskjold
christine.hafskjold@teknologiradet.no
www.teknologiradet.no

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
Kiel, Germany
Contact: Marit Hansen
LD10@datenschutzzentrum.de
www.datenschutzzentrum.de

Table of Contents **page**

Annex 1 Participants background

As of 1st of July the registered participants represented the following categories according to the selection matrix. The 27 persons fitting perfectly into the selection matrix, were supplemented by seven additional participants in a way to fill existing gaps as much as possible. Nevertheless younger and male persons were slightly underrepresented.

	18 – 34 years			35 – 54 years			55 + years		
Men	1	3	1	3	3	1	2	1	0
Women	1	2	0	2	2	3	2	3	4
	L	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**

Table 1: Registered participants as of 1st of July

On the day before the interview meeting all registered participants were contacted by phone in order to remind them and to check the actual number of participants. As a very large number of participants could not be reached or withdraw their declaration of intention, another round of quick recruitment had to be started. This process embraced mainly persons who expressed interest in the first round of recruitment, but were not selected, because already sufficient numbers were available for the respective category. A further requirement for the last-minute recruitment was the availability of an e-mail address in order to be able to send the background material.

	18 – 34 years			35 – 54 years			55 + years		
Men	0	1	1	0	0	4	1	0	0
Women	0	0	0	0	0	2	1	4	3
	L	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**

Table 2: Participants of Austrian Interview Meeting on the 12th of July

In the resulting list of participants there is a considerable overrepresentation of female, older and better educated persons. In view of the extremely high rate of cancellations and non-appearance the recruiting company contacted all persons who did not show up in order to ask for the reason for this decision. Whereas several factors were named or detected that contributed to the low participation rate (season and time of the event, weather conditions at that day, timing of recruitment, remuneration in the form of voucher etc.), a decisive motivation for cancellation appeared to be the extent of the provided background material and complexity of involved issues which may have overcharged specifically persons with low education and may have raised doubts about having enough knowledge to participate in the discussion.

Annex 2 Program of the interview meeting (German)

Ablaufplan Interview-Meeting 12.6.2007

Von	Bis	Beschreibung
17:45	18:05	Registrierung
18:05	18:15	Begrüßung und Einführung
18:15	18:45	Einführung Technik und Fragen
18:45	18:55	Bedienen am Büffet
18:55	19:00	Zurück in den Klubraum und Austeilen der Fragebögen
19:00	20:00	Ausfüllen der Fragebögen Fragen, Abgabe Kontrolle
20:00		Abgabe der letzten Fragebögen, Kontrolle
20:00	21:00	Gruppeninterviews in den jeweiligen Räumen
21:00		Ausgabe der Gutscheine, Fahrtkostenabrechnung, Getränke und Buffet

Annex 3 Material send to the participants

3.1 Text invitation letter

Sehr geehrte …,

herzlichen Dank dafür, dass Sie die Einladung zu einer Gruppendiskussion zum Thema Privatsphäre und Sicherheitstechnologien angenommen haben und mit uns Ihre Ansichten und Meinung dazu diskutieren wollen. Sie unterstützen damit unsere Forschungen zu einem sehr wichtigen Thema und helfen uns dabei, die Standpunkte von Bürgerinnen und Bürgern bei unserer Arbeit berücksichtigen zu können.

Beigelegt finden Sie Szenarien, in denen die Erfahrungen und Gedanken zu Sicherheitstechnologien von zwei erfundenen Personen beschrieben werden. **Bitte lesen Sie diese Szenarien unbedingt vor dem Treffen durch.** In diesen Geschichten werden sowohl die Probleme als auch die Technologien beschrieben, über die wir Sie befragen und die wir mit Ihnen diskutieren wollen.

Zusätzlich haben wir für Sie noch Informationen zum Hintergrund und Ablauf des Treffens sowie eine kurze Beschreibung des Projekts beigelegt, in dessen Rahmen dieses Treffen organisiert wird.

Wir freuen uns schon sehr, Sie am 12. Juni persönlich in Wien begrüßen zu dürfen. Hier die genaue Zeit und der Ort des Treffens:

Dienstag, den 12. Juni 2007, von 18 bis 21 Uhr

im Clubraum der

Österreichischen Akademie der Wissenschaften

Dr. Ignaz Seipel-Platz 2

1010 Wien

Mit freundlichen Grüßen

3.2 Text information letter

Informationen zum Interview -Treffen

Warum Privatsphäre und Sicherheitstechnologien?
Man mag sich dessen oft nicht bewusst sein, aber es werden immer mehr Informationen über unsere Aktivitäten in unterschiedlichen Situationen gesammelt und gespeichert. Beispielsweise wenn man eine E-Mail versendet oder empfängt, wenn man von einer Kamera am Bahnhof gefilmt wird oder wenn man etwa mit einer Bankomat- oder Kreditkarte bezahlt. Dies ist eine Folge von fortgeschrittenen Sicherheitstechnologien. Diese Technologien können unser Sicherheitsgefühl erhöhen, indem sie zur Verhütung oder Aufklärung von Verbrechen oder Terrorismus beitragen und sie können auch unser tägliches Leben einfacher gestalten.

Diese Entwicklungen bei den Sicherheitstechnologien können aber auch problematisch sein. Wie können wir ein Gleichgewicht zwischen einem sicheren und einfacheren täglichen Leben einerseits und der Gefahr von Verletzungen der Privatsphäre, ungerechtfertigten Beschuldigungen und dem Missbrauch persönlicher Daten andererseits finden? Dies ist das Dilemma, das wir gerne mit Ihnen diskutieren würden.

Warum gerade ich?
Entwicklungen bei Sicherheitstechnologien werden Einfluss auf jeden von uns haben. Es ist daher wichtig, die Standpunkte jener Personen zu berücksichtigen, die in Zukunft mit diesen Technologien leben werden - Sie gehören dazu!

Was ist ein Interview-Treffen?
Das Treffen ist ein zwangloses Zusammenkommen nach der Arbeit und wird etwa drei Stunden dauern. Sie werden etwa 30 weiteren Teilnehmerinnen und Teilnehmern mit unterschiedlichem Hintergrund begegnen; keiner von ihnen wird besondere Kenntnisse im Bereich Sicherheitstechnologien besitzen. Ein Experte wird das Spannungsfeld zwischen Privatsphäre und Sicherheitstechnologien vorstellen und es wird die Möglichkeit geben, Fragen zu stellen. Im Anschluss werden Sie gebeten, einen Fragebogen auszufüllen. Abschließend werden Szenarien zu zukünftigen Sicherheitstechnologien unter Anleitung professioneller Interviewer in kleineren Gruppen diskutiert.

Die Teilnahme ist kostenlos und wir werden eventuelle Fahrtkosten (mit öffentlichen Verkehrsmitteln) ersetzen. Während des Treffens wird es die Möglichkeit geben, an einem Buffet Getränke und Speisen zu sich zu nehmen. Als Zeichen der Anerkennung werden Sie zudem ein kleines Geschenk erhalten.

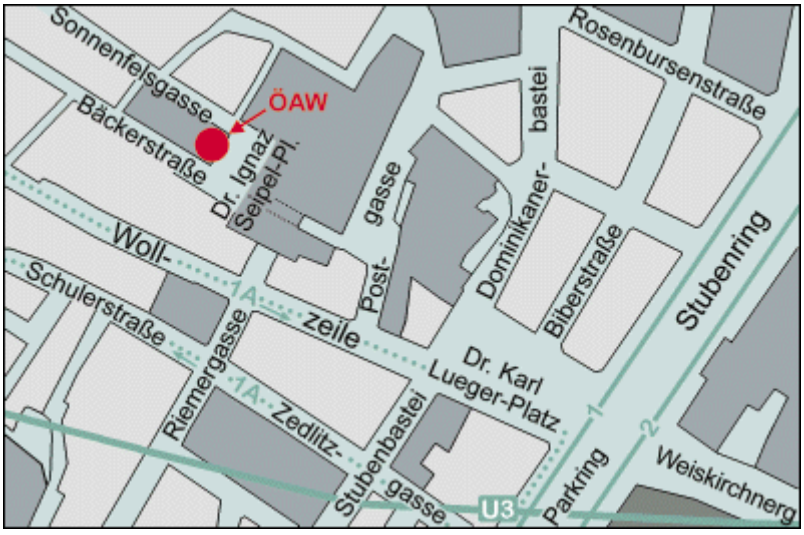
Während des Treffens möchten wir Ihre Diskussionsbeiträge aufzeichnen; alle Ihre Beiträge werden nach dem Treffen anonymisiert werden.

Was ist der Anlass?
Das Interview-Treffen ist ein wichtiger Teil des EU-Projekts PRISE. Dieses Forschungsprojekt wird von vier Institutionen in Österreich, Dänemark, Deutschland und Norwegen durchgeführt. All diese Einrichtungen haben große Erfahrung in der Einschätzung und Bewertung neuer Technologien. Die Interview-Treffen werden in Österreich, Dänemark, Deutschland, Norwegen, Spanien und Ungarn durchgeführt.

Das Ergebnis des PRISE-Projekts werden Empfehlungen für die zukünftige Entwicklung von Sicherheitstechnologien in der Europäischen Union sein. Die bei den Treffen vertretenen Standpunkte werden ein wesentliches Element im Projekt darstellen.

Mehr Informationen über PRISE können Sie der beigefügten Kurzbeschreibung entnehmen. Sie können auch die Projekthomepage unter http://prise.oeaw.ac.at besuchen (diese Informationen sind allerdings nur in Englisch vorhanden)..

Wo findet das Interview-Treffen statt?
Das Interview-Treffen findet in der Wiener Innenstadt (1. Bezirk) im Clubraum der Akademie der Wissenschaften,
Dr. Ignaz Seipel-Platz 2 statt:
Nächstgelegene U-Bahnstation: U3, Stubentor, Ausgang Wollzeile



Kontakt
Falls Sie irgendwelche Fragen oder Anmerkungen haben, wenden Sie sich bitte an:

Johann Čas
Institut fuer Technikfolgen-Abschaetzung
Strohgasse 45/3.Stock
A-1030 Wien

Tel.: +43 (0) 1 51 581 - 6581
Fax: +43 (0) 1 710 98 83
e-mail: jcas@oeaw.ac.at

3.3 Scenarios in German – Austrian version

Welche Meinung haben Sie zu Sicherheitstechnologien? Szenarien als Stoff zur Diskussionsanregung

Im Folgenden möchten wir Ihnen Geschichten von zwei Menschen - Carla und Peter - erzählen. Wir werden Ihre Begegnungen mit unterschiedlichen Sicherheitstechnologien und Maßnahmen beschreiben, und dabei ihre Gedanken und Ideen dazu erfahren. Um die Szenarien allgemein anwendbar zu machen, haben wir es vermieden, bestimmte Länder, Städte oder Flughäfen als Beispiele zu nennen. Stattdessen haben wir versucht zu zeigen, wie unterschiedliche Länder - und Sicherheitsbehörden - unterschiedliche Ansätze beim Einsatz von Sicherheitstechnologien gewählt haben. Die Szenen spielen sich in nicht allzu ferner Zukunft ab, um auch die Nutzung von einigen Sicherheitstechnologien oder gesetzlichen Bestimmungen zeigen zu können, die bisher noch nicht umgesetzt wurden.
Wir hoffen, dass die Geschichten dieser beiden Personen Sie dazu anregen werden, über Sicherheit und den Schutz der Privatsphäre und Ihr Verhältnis zu diesen beiden Grundwerten nachzudenken.

Carla ist 62 Jahre alt. Sie hat ihr ganzes Leben gerne als Lehrerin gearbeitet, aber nun überlegt sie sich, in Pension zu gehen. Alles wird so technisch in diesen Tagen! Und auch die Kinder scheinen lauter zu sein als zuvor. Vielleicht wird sie einfach nur alt? Diese Woche wird sie sich darüber aber nicht den Kopf zerbrechen. Es ist der Beginn der Sommerferien und sie wird ihren Sohn, der in einem Nachbarland wohnt, besuchen.

Carla nimmt die U-Bahn, um zum Bahnhof zu fahren. Sie hat vorher ihre Universal-Fahrkarte aufgeladen. Sie verwendet diese zum Bezahlen ihrer Fahrten, indem sie sie vor ein Lesegerät beim Zugang zur U-Bahn hält. Die Universal-Fahrkarte aus Plastik enthält einen kleinen Chip. In ihm ist gespeichert, wie viele Fahrten noch als Restguthaben vorhanden sind. Carla hat sich für eine so genannte anonyme Universalkarte entschieden. Sie weiß, dass die aufgeladenen Beträge verloren sind, wenn sie die Karte verliert; und es ist schon ein kleiner zusätzlicher Aufwand, eine eigene Karte dafür zu verwenden. Die normale Universal-Fahrkarte ist natürlich in die Mobiltelefone oder die neuartigen mobilen Multifunktionsgeräte des jeweiligen Besitzers integriert. Man muss es nur mit sich tragen und sich mit einem Fingerabdruck ausweisen, um alle Verkehrsmittel benutzen zu können.

Carla kann sich nicht helfen, aber sie empfindet es als unangenehm, Fingerabdrücke zu verwenden, um sich auszuweisen. Sie merkt, dass es die Jungen heute überhaupt nicht zu kümmern scheint, aber für sie wird es immer mit Verbrechern und Verhaftungen in Verbindung stehen. „Es ist schlimm genug, sich ausweisen und seinen Fingerabdruck hergeben zu müssen, wenn man ins Ausland reist, denkt sie sich. Sie möchte dies keinesfalls öfter tun, als unbedingt notwendig!

Biometrische Verfahren
Biometrische Verfahren identifizieren Personen automatisch aufgrund ihrer biologischen Merkmale oder ihres Verhaltens. Biometrische Verfahren können verwendet werden, um Zugang zu Gebäuden oder zu Information (Computern, Daten) zu kontrollieren. Die am häufigsten gebrauchten Verfahren nutzen Fingerabdrücke oder Gesichtsmerkmale.
Der Vorgang, bei dem die biometrischen Merkmale einer Person mit den gespeicherten Daten verglichen wird, wird „matching“ genannt. Dieser Vergleich ergibt eine bestimmte Punkteanzahl. Ob eine Person akzeptiert oder abgelehnt wird, hängt davon ab, ob dieser Wert eine bestimmte Schwelle überschreitet.
Biometrische Merkmale können in Form des Originals oder als so genannte „Templates“

gespeichert werden Das Template ist ein reduzierter digitaler Datensatz, der aus dem Original errechnet wird. Aus Datenschutzgründen wird empfohlen, nur das Template zu speichern und das Original zu löschen. Bei öffentlichen Systemen und Strafverfolgungsbehörden werden jedoch oft auch die Originalabbildungen aufbewahrt, etwa bei biometrischen Reisepässen oder Gesichtserkennungssystemen.

Wir können zwischen *Identifikation* und *Verifikation* unterscheiden. Bei der Identifikation geht es darum, herauszufinden, wer eine Person ist, indem ihre Merkmale mit allen in einer Datenbank gespeicherten Templates verglichen werden. Bei der Verifikation werden nur die Merkmale einer Person mit den über sie gespeicherten Werten verglichen; hier geht es darum, sicherzustellen, dass eine Person wirklich diejenige ist, als die sie sich ausgibt.

Eine Herausforderung für biometrische Systeme im Allgemeinen ist es, eine Balance zwischen der False Acceptance Rate (FAR) und False Rejection Rate (FRR) zu finden. Von falscher Annahme (oder falsch positiv) spricht man, wenn ein System eine Person fälschlicherweise identifiziert. Wenn das System hingegen eine registrierte Person nicht identifiziert, dann spricht man von, falscher Ablehnung (oder falsch negativ).

Einer der wesentlichen Vorteile von biometrischen Verfahren ist, dass ein starker Bezug zur jeweiligen Person vorhanden ist. Biometrische Verfahren ermöglichen bessere Zugangskontrollen und Identitätsdiebstahl wird viel schwieriger, wenn persönliche Daten an die biometrischen Merkmale der Person gebunden sind. Dies ist auch der größte Nachteil biometrischer Systeme. Ist ein Satz von biometrischen Daten einmal geknackt, so ist er für immer verloren.

Peter ist 32 Jahre alt. Er arbeitet als Vertreter für ein Autohaus. Heute steht er früh auf, um zu einer Automobilmesse in Mitteleuropa zu reisen. Er duscht sich schnell, nimmt seine Tasche und steigt dann in sein Auto, um zum Flughafen zu fahren. Wie üblich ist er zu spät dran, da er aber für den Quick-Check-In registriert ist, sollte es kein Problem geben. Beim Quick-Check-In erspart man sich das ganze Theater mit dem Herzeigen seines Reisepasses und mit der Überprüfung, ob man ein gesuchter Verbrecher ist und natürlich auch die ganzen rigorosen Sicherheitsüberprüfungen. Man muss sich nur einmal einer sehr gründlichen Überprüfung und Registrierung unterziehen und zustimmen, dass alle Daten am Flughafen gespeichert werden. Im Gegenzug kann man das ganze normale Check-In Verfahren umgehen und sich nur mehr am Eingang biometrisch verifizieren lassen.

Peter muss an seinen Kollegen denken, für den seiner Meinung nach der Schutz der Privatsphäre zu einer fixen Idee geworden ist. Er behauptet, dass es schon jetzt zu viel Überwachung in der Gesellschaft gibt, und er akzeptiert nicht einmal Cookies auf seinem Computer! Sogar die Google Toolbar hat er deinstalliert - niemand tut das! Wenn es wahr wäre, dass amerikanische Behörden diese Daten nutzen, um Beziehungsnetze herauszufinden und nach verdächtigen Profilen zu suchen, dann wäre das doch bestimmt allgemein bekannt? Wahrscheinlich ist er schon ein paar Stunden früher aufgestanden und steht nun in der Menschenschlange vor der Sicherheitsüberprüfung. Nun gut, er hat es ja so gewollt! Peter hofft nur, dass es sein Kollege schafft, rechtzeitig durch die Sicherheitskontrollen zu kommen, damit sie noch einmal ihre Präsentation durchgehen können, bevor sie ins Flugzeug einsteigen müssen.

- o -

Carla kommt am Hauptbahnhof an. Wie in der U-Bahn gibt es auch hier überall Kameras. Bildschirme und Lautsprecher wiederholen Sicherheitswarnungen, bis sie niemand mehr bewusst wahrnimmt: "Abgestellte Taschen werden von den Sicherheitskräften entfernt!“ oder „Ihr Gesicht wird automatisch mit jenen von bekannten Terroristen verglichen!" Über die zweite Meldung gab es vor einigen Jahren eine Debatte. Die meisten Länder geben nicht bekannt, dass sie Gesichter erfassen und mit unterschiedlichen Datenbanken abgleichen; und es wurde vorgeschlagen, dass man es auch hier nicht tun sollte. Aber die Regierung war sich

einig, dass die Leute grundsätzlich wissen sollten, wann und wo sie überprüft werden. "Das ist besonders wichtig, wenn man selbst nicht mehr feststellen kann, ob Kameras installiert sind oder nicht" denkt sich Carla. Sie hat gehört, dass es Länder geben soll, wo auch E-Mails und Telefongespräche auf verdächtige Wörter und Sätze überprüft werden. „Aber das kann bestimmt nur ein Gerücht sein!“

Carla fühlt, dass ihr der ganze Lärm in den Kopf steigt und steuert auf die *stille Zone* zu. Sie muss ihre Identitätskarte herzeigen, ehe sie eintreten kann, aber nachdem sie erst einmal drinnen ist, entspannte sie sich. „Keine Kameras, keine Mobiltelefone, keine Computer, keine störenden Warnungen! Es sollte wirklich mehr solche technikfreie Zonen geben!“ denkt sie sich.

Es ist nicht so, dass sie nicht an Kameras gewöhnt wäre. Schließlich gibt es sie schon seit langer Zeit, aber sie scheinen in letzter Zeit immer aufdringlicher zu werden. Nachdem man begonnen hatte, sowohl Gesichtserkennungssoftware als auch Programme zum Erkennen verdächtigen Verhaltens einzusetzen, fühlt sie sich mehr beobachtet und überwacht als zuvor: „Bewege ich mich jetzt wie eine Terroristin?“ Wie peinlich wäre es, etwas zu tun, das die Antiterrorpolizei veranlassen könnte, sie aufzugreifen und zu überprüfen! Um fair zu sein, dies ist ihr noch nie tatsächlich passiert, aber sie kann nicht anders, als darüber nachzudenken, wenn sie von Kameras umgeben ist.

Und, wie die meisten Leute, kennt sie jemanden, der tatsächlich verdächtigt wurde, ein Terrorist zu sein. Als diese Sicherheitstechnologien eingeführt wurden, gab es viele Probleme mit Gesichts-erkennungssystemen. Und weil die Politik die Möglichkeit und den damit verbundenen Skandal vermeiden wollte, dass eine Person auf den Fahndungslisten unerkannt durch die Kontrolle schlüpft, war das Ergebnis eine große Anzahl von Fehlalarmen (*falsch Positive).*

Einer ihrer Kollegen, dessen Eltern aus dem Iran stammen, wurde mit einem Terroristen verwechselt. Er empfand diese Verwechslung als sehr demütigend. Und sie kann das auch gut verstehen, wenn er sagt: „Wenn man von Antiterroreinheiten in kugelsicheren Westen festgenommen wird und aussieht wie ich, sehen dich die Leute danach mit anderen Augen an -, selbst wenn man mit einer Entschuldigung wieder freigelassen wird.“ Carla weiß, dass er für eine Weile danach Orte mit Videoüberwachung mied, insbesondere wenn er mit seinen Kindern unterwegs war.

In jüngster Zeit haben mehr und mehr Personen die Legitimität und Wirksamkeit der Videoüberwachung bezweifelt. In einigen Stadtteilen haben sie mit Versuchen begonnen, anstelle von Überwachungskameras eine bessere und hellere Straßenbeleuchtung zu installieren. Offensichtlich mit guten Ergebnissen!

- o -

Da er in einem Autohaus arbeitet, kann Peter immer die neuesten Modelle fahren. Das Auto, das er im Moment benutzt, ist mit neuester Technik ausgestattet: einem Galileo Satellitennavigationssystem,

Videoüberwachung

Von Videoüberwachung mit *aktiven Kameras* spricht man, wenn die Person, die die Vorgänge am Monitor beobachtet, die Kamera durch Bewegen oder Zoomen steuern kann, um einer Person oder einer sich abzeichnenden problematischen Situation folgen zu können. Aktive Kameras können mit automatisierten visuellen Überwachungsprogrammen kombiniert werden, die komplizierte Verfahren verwenden, um verdächtiges Verhalten zu erkennen oder Personen anhand von in Datenbanken gespeicherten Fotos zu identifizieren.

Passive Kameras: Diese Kameras zeichnen auf, was in einer bestimmten Stelle (zum Beispiel in einem Kiosk) geschieht. Die Aufzeichnungen werden nur dann betrachtet, wenn es besondere Vorfälle gibt, etwa einen Raub, Kampf usw.

Während die früheren Videoüberwachungs-systeme analoge Technik nutzten, werden sie zunehmend durch digitale Systeme ersetzt. Mit diesen Systemen kann man schneller nach bestimmten Ereignissen suchen oder verdächtige Personen mit Hilfe von vorhandenen Datenbanken identifizieren. Es besteht aber die Sorge, dass digitale Aufzeichnungen auch leichter manipuliert werden können.

Automatische Gesichtserkennung
Bei automatischen Gesichtserkennungssystemen wird das Gesicht einer Person automatisch erfasst und mit in einer Datenbank gespeicherten Informationen zur Identifikation oder Zugangskontrolle verglichen. Solche Systeme werden normalerweise verwendet, um sicherzustellen, dass eine Person beispielsweise nicht auf einer Liste von bekannten Verbrechern oder Terroristen ist.

Automatische Kennzeichenerfassung
Diese Systeme werten die von Videokameras erfassten Nummerntafeln aus und vergleichen sie mit einer Datenbank. Systeme zur Kennzeichenerkennung werden in mehreren Ländern eingesetzt. Hauptsächlich werden sie verwendet, um Mautvergehen oder Geschwindigkeitsübertretungen zu verfolgen, aber sie werden auch verwendet, um gestohlene Fahrzeuge zu identifizieren.

automatischem Notruf über das eCall-System und eine Reihe von weiteren Fahrzeugsicherheitssystemen. Peter weiß nicht einmal genau, was diese alles können. Das eCall-System ist jetzt in alle neuen Autos standardmäßig eingebaut, und es soll automatisch einen Notruf absetzen, wenn das Auto in einen Unfall verwickelt ist. Weil es das Galileo-System nutzt, kennt es die genaue Position des Autos.

In den letzten Jahren hat es viele Vorschläge gegeben, dieses System auch für andere Zwecke zu verwenden. Nach einem versuchten Terrorangriff in Berlin stahlen die Terroristen ein Auto und flüchteten damit durch Deutschland. Es zeigte sich, dass das System verwendet werden konnte, um Autos aufzuspüren und sogar zu stoppen! Da das gestohlene Auto ein teures Modell mit dem neuesten Stand an Antidiebstahlstechnik war, konnte es einfach mit einem über Satelliten ausgestrahlten Befehl gestoppt werden. Die Terroristen konnten festgenommen werden; danach beschlossen die EU-Mitgliedsstaaten, dass diese Systeme auch von der Polizei für die Verfolgung von Verbrechern und verdächtigen Terroristen verwendet werden können.

Nach genauen Untersuchungen, wie viele Verkehrstote man vermeiden könnte, wenn die Lenker die Geschwindigkeitsbegrenzungen einhalten würden, wurde vorgeschlagen, in Fahrzeugsicherheitssysteme auch eine automatische Geschwindigkeitskontrolle einzubauen. Dieses Modul kann die jeweils erlaubte Höchstgeschwindigkeit mit dem tatsächlich gefahrenen Tempo vergleichen. Der ursprüngliche Vorschlag ging so weit, dass ein Chip im Motor dafür sorgen sollte, dass kein Auto schneller als die erlaubte Höchstgeschwindigkeit fahren kann. Nach heftigen Protesten von Seiten der Automobilindustrie und von Automobilclubs wurde davon abgesehen. Im Moment ist das System so eingestellt, dass jedes Mal wenn ein Auto zu schnell fährt, ein Anruf an die Zentrale der Verkehrspolizei erfolgt, und die Geldstrafe automatisch vom Bankkonto des Autoeigentümers abgebucht wird.

Peter steigt aufs Gaspedal. Noch sind nicht alle Straßenabschnitte vom System erfasst. Er hat eine Liste der freien Strecken heruntergeladen und in sein Navigationssystem eingespeichert. Er bekommt jedes Mal, wenn er auf einer unkontrollierten Strecke unterwegs ist, ein Signal. Er wird auch gewarnt, wenn er sich wieder an Geschwindigkeitsbegrenzungen halten muss. "Es ist gut, dass Überwachung auch in umgekehrter Weise funktioniert", denkt er sich.

Peter kommt am Flughafen an. Das Nummernschild seines Autos ist schon im System gespeichert und sein Auto wird automatisch registriert, wenn er in das

Technologien zur Ortung
Es ist möglich, die ungefähre Position von Mobiltelefonen aus den Koordinaten der nächstgelegenen Funkstationen zu berechnen.
Für eine genauere Ortung werden satellitenbasierte Systeme genutzt:
GPS ist das derzeit vorhandene System, die Abkürzung steht für *Global Positioning System*. Es besteht aus 24 Satelliten, die die Erde umkreisen. Mit den Signalen von drei Satelliten kann man den Längen- und Breitengrad des GPS-Empfängers bestimmen, mittels vier Satelliten kann man auch die Höhe berechnen.
Das zukünftige System heißt *Galileo* und wird 30 Satelliten umfassen, die genaueste Orts- und Zeitinformationen für Benutzer am Boden und

in der Luft bieten werden. Es soll im Jahr 2010 betriebsbereit sein. Es wird genauer als das GPS-System sein, und soll auch innerhalb von Gebäuden funktionieren.

eCall

Das eCall-System soll in Autos eingesetzt werden. Das Gerät enthält Sensoren, die es nach einem Unfall aktivieren. Es löst einen automatischen Notruf aus und übermittelt Information über die Zeit, den genauen Standort und das betroffene Fahrzeug.

Das Gerät wird nicht permanent mit einem mobilen Datenübertragungsnetz verbunden sein, es verbindet sich nur, nachdem es aktiviert worden ist. Es gibt jedoch Befürchtungen, dass sich dies ändern könnte: ein Beispiel wäre das permanente Senden von weiteren Daten, etwa für Versicherungsgesellschaften. Sorgen bereitet auch ein möglicher unbefugter Zugang zu Datenbanken, in denen eCall-Daten gespeichert werden. Ab September 2009 werden alle neuen Autos in den teilnehmenden Ländern mit eCall-Geräten ausgerüstet sein.

Parkhaus fährt. Es ist dieselbe Technik, die in den Städten verwendet wird, um gestohlene Fahrzeuge zu identifizieren. Er dachte eigentlich, dass solche Systeme überflüssig werden, nachdem das eCall-System mit Galileo-Satellitennavigation eingeführt wurde. Offensichtlich wissen aber organisierte Banden genau, wie das System ausgeschaltet werden kann. Und er weiß, dass in einigen Ländern sogar gefordert wird, dass der Fahrer selbst in der Lage sein sollte, das eCall-System zu deaktivieren. Solche Forderungen bringen immer Schwierigkeiten für die Autoindustrie mit sich! Und warum ist es so, dass die Kriminellen der Technik immer einen Schritt voraus zu sein scheinen?

Zweckentfremdung

Datenbanksysteme sind gegenüber Zweckentfremdungen anfällig, darunter versteht man die Verwendung von Daten für andere Aufgaben als ursprünglich geplant. Ein Beispiel dafür ist die norwegische Datenbank über Asylantragsteller, die auch biometrische Informationen wie Fingerabdrücke enthält. Sie wurde der Polizei für Ermittlungen bei strafbaren Handlungen zur Verfügung gestellt. Der ursprüngliche Zweck der Datenbank war es, die Identität von Asylanten zu überprüfen.

Er parkt das Auto, steigt aus und steuert auf den Quick-Check-In für sein Terminal zu. Er hält seinen Finger auf den Sensor und schaut direkt in die Kamera. Ein grünes Licht leuchtet auf, und die Tür öffnet sich.

Obwohl die Sensoren für Fingerabdrücke viel besser sind, als sie es früher waren, haben einige Leute immer noch Schwierigkeiten, diese zu verwenden: Sein Großvater ist so ein Beispiel. Obwohl er eigentlicher ein sehr rüstiger achtzigjähriger Mann ist, wird er zunehmend isoliert. Heutzutage muss man sich bei allen möglichen Gelegenheiten mit Fingerabdrücken ausweisen. Er ist des ganzen Theaters und Ärgers überdrüssig, den man über sich ergehen lassen muss, wenn die eigenen Fingerabdrücke nicht von Sensoren gelesen werden können. Daher bleibt er oft lieber gleich zuhause.

Peter geht manchmal zur Bibliothek, um sich *echte* Bücher auszuleihen. Er schmunzelt, wenn er daran denkt, wie sein Bibliotheksprofil aussehen muss. Wenn Nachrichtendienste dieses jemals bei der Suche nach verdächtigen Personen analysiert haben, könnten sie sich gefragt haben, warum ein dreißigjähriger Mann sich Bücher wie "Dating für Senioren" oder "Unsere Freunde, die Vögel" ausborgt.

Vor einigen Jahren, direkt nachdem ein größerer Terrorangriff in den USA verhindert werden konnte, wurde tatsächlich vorgeschlagen, dass Sicherheitsbehörden alle möglichen Datenbanken durchsuchen dürfen sollten. Und das betraf nicht nur vermutliche Verbrecher oder Terroristen. Sie wollten alle Daten, von Bibliotheken, Elektrizitäts- und Gasverbrauchsmustern, Verkehrsdaten für das Telefon und das Internet, Reisen bis hin zu Einkaufsgewohnheiten, analysieren. Durch das Suchen nach verdächtigen Mustern wollten sie mögliche Terroristen identifizieren.

Sein Kollege Alex war damals sehr empört gewesen, und Peter hatte versucht, mit ihm zu diskutieren: Bestimmt würden sie diese Maßnahmen nicht ergreifen, wenn sie nicht gute Gründe dafür hätten? Und die Behörden sollten doch tun, was auch immer sie konnten, um Terroristen zu

fangen. Alex war davon nicht überzeugt, und meinte, dass zumindest anonymisierte Daten für diese Analysen verwendet werden sollten: „Wenn sie etwas verdächtig finden, können sie sich ja über einen Gerichtsbeschluss die wahre Identität zeigen lassen. Es gibt keinen wirklichen Grund, warum sie alles über jeden wissen sollten!“

Peter war nicht wirklich daran interessiert gewesen, das Thema weiter zu diskutieren, aber sein Kollege sprach ihn in jeder Mittagspause immer wieder darauf an, und schlussendlich hatte er eine Petition gegen den Vorschlag unterschrieben. „Aber eigentlich verstehe ich die Aufregung nicht wirklich“, sagte er zu sich. „Bestimmt ist dies nur ein Problem für jene, die etwas zu verbergen haben?“ Andererseits ertappte er sich dabei, sich selbst zu fragen, ob es irgendwo gespeichert worden ist, dass er diese Petition unterschrieben hat.

Total Information Awareness (TIA)

TIA war ein Programm der DARPA (Defence Advanced Research Projects Agency) der US-Regierung. Es lässt sich am ehesten mit dem Begriff "allumfassende Auswertung von Informationen" übersetzen. Das TIA-Programm umfasste drei Kategorien von Software-Werkzeugen: automatische Sprachübersetzung, Suchmaschinen und Mustererkennung sowie fortgeschrittene Systeme zur Entscheidungs-findung.

Das Ziel von TIA war es, terroristische Angriffe vorhersagen zu können, ehe sie eintreten. Es war beabsichtigt, dass das System private und öffentliche Datenbanken wie auch das Internet nach verdächtigen Daten durchsucht, die auf einen Terroristenangriff hinweisen könnten. Im September 2003 wurde die Finanzierung von TIA vom US-Kongress gestoppt, aber viele der Projekte innerhalb des Programms werden unter anderem Namen weitergeführt.

Carla bleibt eine Weile in der stillen Zone sitzen und liest ihr Buch. Dann macht sie sich auf den Weg zum Sicherheitscheck.

Eine Folge der zunehmenden Forderung nach Kontrollen war es, dass Sicherheits-gates nicht nur an Flughäfen, sondern auch im internationalen Zugverkehr und vielen anderen Orten, an denen viele Personen zusammenkommen, eingerichtet wurden. Sie weiß, dass es in einigen Ländern sogar bei den Eingängen von Einkaufszentren und in Sporthallen Sicherheitschecks gibt. Vor einigen Jahren konnte ein Selbstmordattentäter am Eingang eines Einkaufszentrums, nahe an dem Ort, wo ihr Sohn wohnt, festgenommen werden. Anscheinend hatten sie gerade begonnen, eine neue Technologie zum Durchleuchten einzusetzen, von der der Attentäter noch nichts wusste. Dennoch ist sie froh, dass man in ihrem Land nicht so weit gegangen ist. Bislang werden die Passagiere nur auf Flughäfen und auf Bahnhöfen durch-leuchtet.

Sie selbst macht sich keine Sorgen über die Sicherheit in Einkaufszentren; soweit sie weiß, hat es in ihrem Land bislang noch keine einzige Bedrohung in diesem Bereich gegeben. Aber sie hat Statistiken gesehen, die zeigen, dass mehr Leute dazu übergehen, in den kleineren Läden in den Stadtzentren einzukaufen; die Einkaufs-zentren behaupten, dass sie Einnahmeverluste erleiden müssen, weil es ihnen nicht erlaubt wird, neue Scanner-technologien wie die „Nackte Maschine" einzusetzen.

Carla nimmt ihren Reisepass heraus und geht zum Irisscanner. Sie weiß, dass einige Länder immer noch Fingerabdrücke in ihren Ausweisen und Reisepässen verwenden, aber sie meint, dass es sicherer ist, die Iris zu benutzen. Das Lesegerät vergleicht ihre Iris mit den in ihrem Reisepass gespeicherten Daten. Sie war beunruhigt darüber, aber ihr Sohn, der in der Informationstechnikindustrie arbeitet, hat ihr versichert, dass es jetzt völlig unbedenklich sei. "Die ursprüngliche Verschlüsselung im ersten Reisepass war ziemlich schwach", sagte er, "aber mit der jetzt verwendeten Verschlüsselung würde ein Supercomputer Tausende von Jahren brauchen, um die Verschlüsselung zu knacken! Dazu kommt noch, dass in den frühen Reisepässen die tatsächliche Abbildung des Gesichts, der Finger-abdrücke oder der Iris gespeichert wurden. Jetzt speichern sie diese Daten nur mehr in

Form von Templates - reduzierten digitalen Datensätzen, welche die wichtigsten Merkmale der Iris und des Gesichts enthalten. Selbst wenn es gelänge, die Verschlüsselung zu knacken, wäre es damit nicht möglich, das Gesicht oder die Iris nachzubilden, um den Passinhaber zu imitieren."

Ihr ist auch zugesichert worden, dass das Lesegeräte ihr Iris-Abbild nur verwendet, um es mit dem im Reisepass gespeicherten Template vergleichen zu können, und dass es nicht in einer zentralen Datenbank gespeichert wird. Sie ist sich nicht so sicher, was geschieht, wenn ihr Reisepass an ausländischen Grenzen kontrolliert wird. Werden dort die Daten auch nach dem Vergleich gelöscht?

Sie erinnert sich daran, dass es vor einigen Jahren einen Skandal mit einer zentralen Fingerabdruckdatenbank gab – war es in den USA? Viele Fingerabdrücke wurden von einem Angestellten gestohlen und an eine internationale Verbrecherorganisation verkauft. Tausenden von Menschen wurde dadurch ihre Identität gestohlen und sie erlebten viele Arten von Problemen - etwa dass sie bei Grenzkontrollen in den Fahndungslisten aufschienen, oder ihre Bankkonten geleert wurden. Besonders schwierig war es, weil es sehr lange dauerte, ehe die Regierung eingestand, dass Daten verloren gegangen waren. Und in der Zwischenzeit wollte ihnen niemand glauben, dass ihre Identitäten gestohlen worden waren - oder dass es überhaupt möglich war, die Fingerabdrücke von irgendjemand zu verwenden, um seine Identität zu stehlen!

Carla weiß das aber besser. Letzten Sommer wurde einem Freund ihres Sohnes

Funketiketten (RFID)

RFID (Radio Frequency Identification) ist eine Technologie zur automatischen Identifikation unter Verwendung von Radiowellen. Winzige integrierte Schaltungen (Chips), welche die zur Identifikation notwendigen Informationen enthalten, werden in Dokumenten eingebettet oder in Produkte integriert. Mittels eines *Lesegeräts* können die Informationen von allen Funketiketten innerhalb eines bestimmten Bereichs abgerufen werden.

RFID-Etiketten oder Tags, wie sie in Englisch bezeichnet werden, gibt es sowohl in *aktiver* als auch *passiver* Form. Aktive Tags werden zum Beispiel eingesetzt, um die Mautgebühren für LKWs automatisch abzubuchen. Sie enthalten eine Batterie und können daher mehr Informationen speichern und auch aus größeren Distanzen gelesen werden. Passive Tags enthalten keine Batterie, sie entnehmen die benötigte Energie direkt aus dem Radiosignal, das vom Lesegerät ausgesendet wird. Eine typische Anwendung von passiven Tags ist der neue europäische Reisepass.

Die meisten Tags stellen ihre Informationen jedem Lesegerät in der Nähe zur Verfügung; es gibt aber auch Tags, die ein Passwort verlangen oder andere Formen der Zugangskontrolle eingebaut haben.

Biometrischer Reisepass

Ein biometrischer Reisepass besteht aus dem normalen Dokument mit einem zusätzlich eingebetteten Chip.

Der Chip enthält obligatorische und optionale Daten. Außerdem gibt es eine Photographie des Besitzers als visuelle Verknüpfung zwischen dem Besitzer und dem Reisepass.

Die Internationale Zivilluftfahrtorganisation (International Civil Aviation Organization - ICAO) hat einen Chip für den Reisepass ausgewählt, der über Funk ausgelesen werden kann (RFID). Das *Gesicht* wurde von der ICAO bei Reisepässen als biometrisches Hauptmerkmal ausgewählt; *Fingerabdrücke* und *Iris* werden als weitere, sekundäre biometrische Merkmale empfohlen. Die Europäische Union hat nur Fingerabdrücke als sekundäres Merkmal ausgewählt.

Biometrische Reisepässe haben viele Debatten hervorgerufen, insbesondere im Zusammenhang mit der Sicherheit der biometrischen Informationen. Es wird befürchtet, dass die im Chip gespeicherten biometrischen Informationen ohne Wissen des Eigentümers gestohlen werden könnten, indem der Datenaustausch belauscht oder heimlich Lesegeräte in die Nähe gebracht werden.

Um diese Sorgen auszuräumen, ist ein System zum Schutz des Zugangs (Basic Access Control - BAC) entwickelt worden. Bei BAC benutzt das Kontrollsystem einen „Schlüssel“, der aus den frei zugänglichen Daten (dem Strichcode) abgeleitet wird, um den Chip entsperren und auslesen zu können. BAC ist als nicht sicher genug kritisiert worden; tatsächlich ist es Sicherheitsexperten innerhalb von kurzer Zeit gelungen, die Verschlüsselung aufzuheben.

die Identitätskarte gestohlen, kurz bevor er und seine Familie in Urlaub fahren wollten. Er fürchtete, dass sie alles abbrechen müssten, weil seine Identität als gestohlen aufgelistet sein würde. Offensichtlich kann aber das Schengen Informationssystem, das in vielen europäischen Ländern verwendet wird, Personen berücksichtigen, deren Identität gestohlen wurde. Daher konnten er und seine Familie wie geplant reisen, und er wurde nie für einen Verbrecher oder einen Terroristen gehalten, obwohl seine neue ausgestellte Identitätskarte wahrscheinlich gründlicher überprüft wurde als die eines durchschnittlichen Reisenden.

Nach der Identitätsüberprüfung wird Carlas Gepäck durchleuchtet, bevor sie selbst durch etwas gehen muss, dass als die *nackte Maschine* bezeichnet wird. Sie ist erleichtert, dass die wirkliche „nackte Maschine“ in ihrem Land niemals auf Flughäfen oder Bahnhöfen eingesetzt wurde.

Personenscanner („Nackte Maschine“)

Röntgen- oder Terahertzstrahlen können Materialien durchdringen. Sie können daher auch für die Entdeckung und Darstellung von unter der Kleidung verborgenen Gegenständen verwendet werden.

Ein Personenscanner nutzt diese Technik, um zu erkennen, ob eine Person Waffen oder Sprengstoffe an ihrem Körper versteckt hat. Es gibt sehr unterschiedliche Systeme; manche offenbaren alles unter der Kleidung - nicht nur Waffen oder Sprengstoffe - daher stammt auch der aus dem Englischen übernommene Name „**Nackte Maschine“** (naked machine). Diese Art der Sicherheitstechnologie ist am Londoner Flughafen Heathrow (Terminal 4) seit 2004 getestet worden. Andere Systeme nehmen Bilder von verborgenen Objekten auf und projizieren sie auf eine geschlechtslose Puppe.

Die Sicherheitsbehörden haben verschiedene Systeme bewertet, und entschieden, dass es genauso sicher war, ein Modell zu kaufen, bei dem unter der Kleidung versteckte Sachen auf einer geschlechtsneutralen Puppe abgebildet werden.

Carla ist wegen ihres Körpers befangen, und sie ist froh, dass die jungen Männer am Sicherheitsgate sie nicht nackt zu sehen bekommen. Sie muss ihre Schuhe ausziehen, aber davon abgesehen hat sie keine Probleme und sitzt bald bequem im Zug.

- o -

Peter eilt durch die Flughafenhalle zur Sicherheitskontrolle. Natürlich müssen sogar die Quick-Check-In-Kunden sich einer Form der Sicherheitsüberprüfung unterziehen, aber sie haben einen eigenen Zugang, und es sind nur Vielflieger darunter. Niemand vergisst hier einen Gürtel mit Metallschnalle abzulegen, oder ist dumm genug, Kleingeld in den Taschen zu lassen. Und es ist schon Jahre her, dass Businessschuhe noch Metallteile enthielten. Er schluckt kurz und geht durch die *nackte Maschine*. "Warum muss es hier immer so kalt sein?" denkt er sich, und errötet, als er bemerkt, dass eine der Wachen eine Frau in seinem Alter ist.

Vorratsdatenspeicherung

Eine Datenbank ist eine organisierte Sammlung von Daten. Es wird allgemein anerkannt, dass man wesentlich mehr über eine Person erfahren kann, wenn Daten aus verschiedenen Quellen zusammengefügt werden als wenn diese Daten jeweils einzelnen betrachtet werden. Es ist daher ein wichtiges Prinzip des Datenschutzes, dass in Datenbanken jeweils nur jene Informationen gesammelt werden dürfen, die für den Zweck dieser Datenbank notwendig sind, und dass die Daten gelöscht werden sollen, sobald sie nicht mehr benötigt werden.

In letzter Zeit ist ein Trend zu beobachten, nach dem Regierungen mehr Daten als für den ursprünglichen Zweck erforderlich sind, speichern wollen und unterschiedliche Datenbanksysteme für Sicherheitszwecke zusammenführen wollen. Zumeist sind Daten aus dem Bereich Informations- und Kommunikationstechnologien, wie Kommunikationsverkehrsdaten von Telefonen, Mobiltelefonen und Internetnutzung gemeint, wenn die Einführung von Vorratsdatenspeicherung diskutiert werden.

Die EU hat eine Richtlinie über die Vorratsdatenspeicherung erlassen. Daten darüber, wer mit wem, wann und wo kommuniziert hat, werden gespeichert, aber nicht der Inhalt der Kommunikation. Diese Daten können bis zu zwei Jahre lang aufbewahrt werden.

Verschiedene Behörden in den USA haben

berichtet, dass sie im Jahr 2005 persönliche Daten von kommerziellen Datensammlern im Wert von $ 30 Millionen gekauft haben. Diese Agenturen sammeln und verknüpfen Daten aus unterschiedlichen Quellen und verkaufen diese an ihre Kunden. Die Quellen können öffentliche Datenbanken sein, Informationen die über das Internet frei verfügbar sind oder Daten, die im privaten Eigentum sind, z.B. Kundendaten von Versandhäusern oder Internetdiensten.

Dennoch begrüßt er es, dass am Flughafen die *wirklich* nackte Maschine eingesetzt wird. Irgendwie fühlt er sich sicherer dabei.
Peter bemerkt eine zusätzliche Sicherheitseinrichtung, die er zuvor noch nie gesehen hat. Nach der nackten Maschine befindet sich ein zweites "Tor"; manche der Passagiere werden aufgefordert, durch dieses durchzugehen. Er erinnert sich vage daran, gehört zu haben, dass ein neues Sicherheitssystem in diesem Flughafen getestet werden soll. Dieses erfasst angeblich Daten wie die Körpertemperatur, Schweiß, Pulsfrequenz usw. Fakten, die ein Zeichen für Krankheiten wie SARS oder eine Vogelgrippe sein könnten oder anzeigen können, dass eine Person nervös ist. Manche der Testpersonen werden in ein Verhörzimmer in der Nähe geführt. Er ist froh, dass er nicht für den Test ausgewählt wurde, selbst wenn er gesund ist und ein reines Gewissen hat. "Ist es angebracht, diesen Test hier durchzuführen? Wissen sie nicht, dass die Leute, die das Quick-Check-In verwenden, es eilig haben?"
Er geht zum Gate und setzt sich hin. Vielleicht sollte er Yasmin anrufen und ihr sagen dass er kommt? Sie arbeitet für den Autohersteller, den sein Autohaus vertritt, er hat sie bei der letzten Autoausstellung, die er besuchte, kennengelernt. Sie verstanden sich vom ersten Moment an sehr gut, und er würde sie gerne wieder sehen. Andererseits zögert er, sie mit seinem Handy anzurufen. Er weiß, dass Yasmins Bruder in einer Jugendgruppe in seiner Moschee sehr aktiv ist und dass Yasmin wahrscheinlich auf irgendeine Art als Teil des Netzwerks ihres Bruders überwacht wird. Es tut ihm leid, dass er nicht, als er das letzte Mal in Asien war, einige anonyme Telefonwertkarten gekauft hatte. Es ist nicht mehr erlaubt, solche Karten in Europa zu verkaufen.

Abhören
Unterschiedliche Technologien können genutzt werden, um die Aktivitäten und Kommunikation von Bürgern im Internet, beim Telefonieren oder in bestimmten Gebieten zu belauschen. Eine bekannte Form ist das Abhören von Telefongesprächen. Dabei wird ein Abhörgerät in Telefonzentralen installiert, das Abhörgerät kann die Gespräche des Verdächtigen erfassen oder auch gegen Telefone von Personen gerichtet werden, von denen man annimmt, dass der Verdächtige sich an sie wenden wird.
Eine erweiterte Version des Abhörens erfasst unterschiedslos alle Kommunikationsmöglichkeiten (Telefon, Mobiltelefon, Internet), die auf verdächtige Aktivitäten untersucht werden. Ein Beispiel dafür ist das Echelon Netzwerk, das von einem Bündnis zwischen den USA, Großbritannien, Kanada, Australien und Neuseeland betrieben wird. Das System wurde ursprünglich zur Überwachung der Kommunikation in der Sowjetunion und in Osteuropa eingesetzt. Kommunikationsmuster können analysiert werden und der Inhalt kann nach bestimmten Stichwörtern durchsucht werden.

Er will auch nicht das Internet nutzen. Wer weiß, was hier am Flughafen alles protokolliert wird? Er ist sich nicht einmal sicher, welche Regeln heutzutage gelten. Hat die Polizei direkten Zugang zu diesen Arten von Daten oder brauchen sie eine richterliche Vollmacht? Er denkt sich plötzlich, dass er die Debatte über den Schutz der Privatsphäre besser verfolgen hätte sollen. Er wird bestimmt seinen Kollegen fragen, wenn dieser ins Flugzeug einsteigt.
Das letzte Mal, als er mit Yasmin ausging, erwähnte sie, dass sie sich sicher war, dass ihre E-Mails abgehört werden, und sie bat ihn darum, ein Verschlüsselungsprogramm zu verwenden, wenn er ihr schreiben wollte. "Eine unverschlüsselte E-Mail ist wie eine Postkarte", erklärte sie. "Jeder, der Zugang zu ihr bekommt, kann sie lesen - hast du das nicht gewusst?"
Eigentlich wollte er ihr schreiben. Aber er

musste feststellen, dass das E-Mail-Programm, das sie im Büro verwenden, keine Verschlüsselung integriert hat, und er war noch nicht dazu gekommen, ein anderes Programm zu installieren. Er hofft, dass sie ihm nicht böse ist, dass er sich die ganze Zeit nicht gemeldet hat. "Ich werde es ihr erklären, wenn wir uns treffen", denkt er sich.

Es ist Zeit, ins Flugzeug einzusteigen. Er geht ans Gate, drückt seinen Finger auf den Sensor und geht als einer der ersten Passagiere an Bord. Es gibt noch mehr als genug Platz für das Handgepäck. Er denkt an seinen Kollegen, der wahrscheinlich immer noch in der Schlange vor der Sicherheitskontrolle steht, bevor er sich zurücklehnt und seine Augen schließt.

- o -

"Mama ist schon auf dem Weg", sagt Carlas Sohn zu seiner Frau, nachdem er eine Nachricht auf seinem Mobiltelefon erhalten hat. "Sie sollte in drei Stunden hier sein." Seine Mutter weiß es nicht, aber das neue Mobiltelefon, das er ihr zu Weihnachten geschenkt hat, ist mit einem *Friend Finder* genannten Dienst verbunden. Diese Technik ist eine neue Version der Peilsender, wie man sie aus alten Kriminalfilmen kennt. Hier konnte man einen Verdächtigen als kleinen Punkt auf einer Landkarte verfolgen. Der Hauptunterschied ist, dass heute dazu das im Mobilgerät integrierte Galileo-System nutzt wird. Er kann dadurch die Bewegungen seiner Mama auf einer Landkarte verfolgen, sogar wenn er in seinem eigenen Wohnzimmer in einem anderen Land sitzt.

Er versucht, sie nicht zu oft zu beobachten - es meint, dass er schon ein wenig zu sehr in ihr Privatleben eindringt, aber er hat einige Vorgaben programmiert, die Alarme auslösen, etwa wenn sie sich lange Zeit in ihrem Haus nicht bewegt oder wenn sie nachts nicht nachhause kommt. Schließlich sie wird älter, und er kann sich ja nicht so um sie kümmern, wie es eigentlich sein sollte, weil er in einem anderen Land lebt.

Sein Telefon läutet: "Hallo, ich bin es, Mama! Ich bin jetzt auf dem Weg zu euch - ich sollte in etwa drei Stunden am Bahnhof ankommen".

Technologien zur Förderung der Privatsphäre

Technologien, die direkt dazu beitragen, die Privatsphäre zu schützen, werden als privatsphärenfördernde oder privatsphären-freundliche Technologien bezeichnet.

Anonymisierung ist ein Beispiel dafür. Es gibt Dienste, die eine anonyme elektronische Kommunikation für normale Benutzer ermöglichen. Dabei werden die Verbindungen zwischen Nutzern und die Spuren, die sie hinterlassen, versteckt. Damit kann eine unerwünschte Identifizierung verhindert werden. Bezahlung mit Bargeld oder die Nutzung von nicht registrierten Wertkarten sind traditionelle Mittel, die Anonymität zu bewahren.

Identitäts-Management ist auch eine Form privatsphärenfördernder Technologien: In einigen Fällen wollen Sie sich vielleicht nicht identifizieren, sondern ein Pseudonym (zum Beispiel bei Foren im Internet) verwenden. Um die Verknüpfung von Daten schwieriger zu machen, kann es nützlich sein, verschiedene Benutzernamen (die Ihre Identität nicht zeigen) und Passwörter für verschiedene Zwecke zu verwenden. Identitätsmanagementsysteme helfen Ihnen dabei, Ihre verschiedenen Benutzernamen und Passwörter zu verwalten. Für viele Dienstleistungen muss nur eine Eigenschaft überprüft werden - zum Beispiel das Alter oder der Überziehungsrahmen. In solchen Fällen kann etwa ihre Bank, ihr Telekommunikationsanbieter oder ihr Arbeitgeber als vertrauenswürdige Stelle fungieren, die dafür garantiert, dass die Eigenschaft zutrifft, ohne ihre Identität preiszugeben.

Verschlüsselung ist eine andere Möglichkeit, Inhalte für andere Personen unleserlich zu machen. Weil alle Formen elektronischer Kommunikation belauscht oder manipuliert werden können, ist es in vielen Fällen entscheidend, dass die Kommunikation in verschlüsselter Form stattfindet.

Annex 4 Questionnaire and interview guide

4.1 Questionnaire in German – Austrian Version

Fragebogen zu Sicherheitstechnologien und Privatsphäre

Herzlich willkommen zur Meinungsbefragung über Einstellungen zu Sicherheitstechnologien und Privatsphäre im Rahmen des PRISE-Projekts!

In diesem Fragebogen wird Ihnen eine Serie von Fragen gestellt. *Bitte ringeln Sie die Nummer neben der Antwort ein, die Sie geben wollen.* Sie dürfen nur *eine* Antwort auf jede Frage geben, außer es ist ausdrücklich erwähnt, dass "Sie mehr als eine Antwort auf diese Frage geben können". Falls Sie eine Antwort irrtümlich oder ungewollt einringeln, streichen Sie diese bitte durch und ringeln dann die richtige Antwort ein. Sie können jederzeit Fragen stellen, wenn Sie beim Ausfüllen nicht sicher sind, wie einzelne Fragen gemeint sind.

Zu Ihrer Person:

1. Geschlecht

1. männlich
2. weiblich

2. Alter

- Alter: ____

3. Wie viele Personen leben in Ihrem Haushalt?

1. 1 Person
2. 2 Personen
3. 3 Personen
4. 4 Personen oder mehr

4. Haben Sie Kinder?

1. Ja
2. Nein

5. Wohnen Kinder bei Ihnen zuhause? *(Mehr als eine Antwort möglich*)

1. Nein
2. Ja, 14 Jahre oder jünger
3. Ja, älter als 14 Jahre

6. Was ist Ihre höchste abgeschlossene Ausbildung?

1. Volks- oder Hauptschule
2. Lehre
3. Allgemeinbildende oder Berufsbildende Höhere Schule
4. Kolleg
5. Bakkalaureat
6. Fachhochschule oder Universität

7. Welchen Beruf haben sie?

- Beruf: _____

8. Leben Sie in einer Stadt oder auf dem Land?

1. Großstadt
2. Kleinstadt
3. Ländlicher Bezirk

9. Wie oft verwenden Sie ein Mobiltelefon?

1. Mindestens einmal am Tag
2. Mindestens einmal in der Woche
3. Mindestens einmal im Monat
4. Seltener als einmal im Monat
5. Ich verwende kein Mobiltelefon

10. Wie oft schreiben Sie E-Mails?

1. Mindestens einmal am Tag
2. Mindestens einmal in der Woche
3. Mindestens einmal im Monat
4. Seltener als einmal im Monat
5. Ich schreibe nie E-Mails

11. Wie oft verwenden Sie das Internet?

1. Mindestens einmal am Tag
2. Mindestens einmal in der Woche
3. Mindestens einmal im Monat
4. Seltener als einmal im Monat
5. Ich verwende das Internet nie

12. Wie oft reisen Sie mit öffentlichen Verkehrsmitteln?

1. Mindestens einmal am Tag
2. Mindestens einmal in der Woche
3. Mindestens einmal im Monat
4. Seltener als einmal im Monat
5. Ich reise nie mit öffentlichen Verkehrsmitteln

13. Wie oft reisen Sie mit dem Flugzeug (Hin- und Rückflug zählen als eine Reise)?

1. Mehr als 5mal pro Jahr
2. 3-5mal pro Jahr
3. 1-2mal pro Jahr
4. Seltener als 1 mal pro Jahr
5. Nie

14. Wie oft reisen Sie mit dem Auto?

1. Mindestens einmal am Tag
2. Mindestens einmal in der Woche
3. Mindestens einmal im Monat
4. Seltener als einmal im Monat
5. Ich reise nie mit dem Auto

Allgemeine Fragen zu Sicherheitstechnologien und Privatsphäre

Im Folgenden finden Sie eine Reihe von Ansichten oder Behauptungen über Sicherheitstechnologien und Privatsphäre, die in öffentlichen Debatten oft gebraucht werden. In welchem Ausmaß sind Sie mit diesen Aussagen einverstanden?

Geben Sie bitte für jede Aussage an, inwieweit Sie mit ihr einverstanden sind.

- Wenn Sie glauben, dass die Aussage völlig richtig ist, ringeln Sie bitte 1 "Ich bin völlig einverstanden" ein.
- Wenn Sie glauben, dass die Aussage richtig ist, aber einige Vorbehalte haben, ringeln Sie bitte 2 "Ich bin teilweise einverstanden" ein.
- Wenn Sie es unmöglich finden, zu beurteilen, ob die Aussage richtig oder falsch ist, wählen Sie bitte 3 "Ich bin weder einverstanden noch nicht einverstanden".
- Wenn Sie glauben, dass die Aussage falsch ist, aber einige Zweifel haben, wählen Sie bitte 4 "Ich bin teilweise nicht einverstanden".
- Wenn Sie glauben, dass die Aussage völlig falsch ist, ringeln Sie 5 "Ich bin überhaupt nicht einverstanden" ein.

15. Die Sicherheit der Gesellschaft hängt völlig von der Entwicklung und Nutzung neuer Sicherheitstechnologien ab.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

16. Viele Sicherheitstechnologien erhöhen nicht wirklich die Sicherheit, sondern werden nur eingesetzt, um zu zeigen, dass etwas gegen den Terrorismus getan wird.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden

5. Ich bin überhaupt nicht einverstanden

17. Wer nichts zu verbergen hat, muss sich auch nicht vor Sicherheitstechnologien fürchten, die die Privatsphäre verletzen.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

18. Wenn Sicherheitstechnologien verfügbar sind, könnten wir sie ohne weiteres auch benutzen.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

19. Die Privatsphäre sollte nicht ohne einen begründeten Verdacht auf kriminelle Absichten verletzt werden.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

20. Es ist unangenehm, überwacht zu werden, auch wenn man keine kriminellen Absichten hat.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

21. Neue Sicherheitstechnologien werden wahrscheinlich von staatlichen Behörden missbraucht werden.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

22. Neue Sicherheitstechnologien werden wahrscheinlich von Verbrechern missbraucht werden.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

Sicherheitstechnologien

In diesem Abschnitt möchten wir Sie zu Ihrer Einstellung zu bestimmten Sicherheitstechnologien und ihrer Verwendung befragen.
In den grauen Textboxen finden Sie sehr kurze Beschreibungen der Technologien, die in den anschließenden Fragen diskutiert werden. Mehr Informationen zu diesen Technologien finden Sie in den Szenarien, die an Sie ausgesandt wurden und auch hier aufliegen.

Ein Teil dieser Fragen bezieht sich auf akzeptable Anwendungen dieser Technologien; hier wird es zumeist möglich sein, mehr als eine Antwort zu geben.

Der andere Teil der Fragen betrifft bestimmte Aussagen. Für jede Aussage möchten wir Sie bitten, anzugeben in welchem Ausmaß Sie mit ihnen einverstanden sind.

Biometrische Verfahren

Biometrische Verfahren identifizieren Personen automatisch aufgrund ihrer biologischen Merkmale oder ihres Verhaltens. Biometrische Verfahren können verwendet werden, um Zugang zu Gebäuden oder zu Information (Computern, Daten) zu kontrollieren. Die am häufigsten gebrauchten Verfahren nutzen Fingerabdrücke oder Gesichtsmerkmale.

Biometrische Merkmale können in Form des Originals oder als so genannte „Templates“ gespeichert werden. Das Template ist ein reduzierter digitaler Datensatz, der aus dem Original abgeleitet wird. Aus Datenschutzgründen wird empfohlen, nur das Template zu speichern und das Original zu löschen. Bei Ausweisen und Strafverfolgungsbehörden werden jedoch oft auch die Originalabbildungen aufbewahrt, etwa bei biometrischen Reisepässen oder Gesichtserkennungssystemen.

Einer der wesentlichen Vorteile von biometrischen Verfahren ist, dass ein starker Bezug zur jeweiligen Person vorhanden ist. Biometrische Verfahren ermöglichen bessere Zugangskontrollen und Identitätsdiebstahl wird viel schwieriger, wenn persönliche Daten an die biometrischen Merkmale der Person gebunden sind. Dies ist auch der größte Nachteil biometrischer Systeme. Ist ein Satz von biometrischen Daten einmal geknackt, so ist er für immer verloren.

Biometrischer Reisepass

Ein biometrischer Reisepass besteht aus dem normalen Dokument mit einem zusätzlich

eingebetteten Chip, der die biometrischen Daten enthält. Der Chip kann von einem Lesegerät auch aus einem gewissen Abstand gelesen werden.

Biometrischer Reisepässe haben Debatten verursacht, weil befürchtet wird, dass die im Chip gespeicherten biometrischen Informationen ohne Wissen des Eigentümers gestohlen werden könnten, indem der Datenaustausch belauscht oder heimlich Lesegeräte in die Nähe gebracht werden.

Eine Herausforderung für biometrischer Systeme im Allgemeinen ist es, eine Balance zwischen der False Acceptance Rate (FAR) und False Rejection Rate (FRR) zu finden. Von *falscher Annahme* (oder *falsch positiv*) spricht man, wenn ein System eine Person fälschlicherweise identifiziert. Wenn das System hingegen eine registrierte Person nicht identifiziert, dann spricht man von, *falscher Ablehnung* (oder *falsch negativ*).

23. Welche biometrischen Verfahren würden Sie persönlich bei Zugangskontrollen nicht stören? *(Mehr als eine Antwort möglich*)

1. Gesichtserkennung
2. Fingerabdrücke
3. Iriserkennung
4. Es gibt kein biometrisches Verfahren, das mich bei Zugangskontrollen nicht stören würde
5. Ich weiß es nicht

24. In welchen Fällen ist die Anwendung biometrischer Verfahren für Zugangskontrollen akzeptabel? *(Mehr als eine Antwort möglich*)

1. Für Sicherheitskontrolle in Banken
2. Für Flughafensicherheit
3. Für Sicherheitskontrollen in Geschäften oder Einkaufszentren
4. Für Grenzkontrollen
5. Für Sicherheitskontrollen in zentralen Bus- und Zugbahnhöfen
6. Für Sicherheitskontrollen in Sportstadien und bei anderen Großereignissen
7. Für Sicherheitskontrollen bei anderen, nicht angeführten privaten Ereignissen oder Dienstleistungen
8. Sie sind nie akzeptabel
9. Ich weiß es nicht

Ausgewählte Aussagen zu biometrischen Verfahren

25. Biometrische Daten (z.B. Fingerabdrücke oder DNS-Proben) von allen Bürgern in einer zentralen Datenbank zu speichern, ist ein akzeptabler Schritt, um Verbrechen zu bekämpfen.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

26. Bei der Nutzung biometrischer Reisepässe fühle ich mich wegen des Risikos, dass meine biometrischen Daten gestohlen werden könnten, verunsichert.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

Videoüberwachung

Von Videoüberwachung mit *aktiven Kameras* spricht man, wenn die Person, die die Vorgänge am Monitor beobachtet, die Kamera durch Bewegen oder Zoomen steuern kann, um einer Person oder einer sich abzeichnenden problematischen Situation folgen zu können. Aktive Kameras können mit automatisierten visuellen Überwachungsprogrammen kombiniert werden, die komplizierte Verfahren verwenden, um verdächtiges Verhalten zu erkennen oder Personen anhand von in Datenbanken gespeicherten Fotos zu identifizieren.

Passive Kameras: Diese Kameras zeichnen auf, was in einer bestimmten Stelle (zum Beispiel in einem Kiosk) geschieht. Die Aufzeichnungen werden nur dann betrachtet, wenn es besondere Vorfälle gibt, etwa einen Raub, Kampf usw.

Automatische Gesichtserkennung

Bei automatischen Gesichtserkennungssystemen wird das Gesicht einer Person automatisch erfasst und mit in einer Datenbank gespeicherten Informationen zur Identifikation oder Zugangskontrolle verglichen. Solche Systeme werden normalerweise verwendet, um sicherzustellen, dass eine Person beispielsweise nicht auf einer Liste von bekannten Verbrechern oder Terroristen ist.

Automatische Kennzeichenerfassung

Diese Systeme werten die von Videokameras erfassten Nummerntafeln aus und vergleichenden sie mit einer Datenbank. Systeme zur Kennzeichenerkennung werden in mehreren Ländern eingesetzt. Hauptsächlich werden sie verwendet, um Mautvergehen oder Geschwindigkeitsübertretungen zu verfolgen, aber sie werden auch verwendet, um gestohlene Fahrzeuge zu identifizieren.

Personenscanner („Nackte Maschine“)

Röntgen- oder Terrahertzstrahlen können Materialien durchdringen. Sie können daher auch für die Entdeckung und Darstellung von unter der Kleidung verborgenen Gegenständen verwendet werden.

Ein Personenscanner nutzt diese Technik, um zu erkennen, ob eine Person Waffen oder Sprengstoffe an ihrem Körper versteckt hat. Es gibt sehr unterschiedliche Systeme; manche offenbaren alles unter der Kleidung - nicht nur Waffen oder Sprengstoffe - daher stammt auch aus dem Englischen übernommene Name „**Nackte Maschine“** (naked machine). Diese Art der Sicherheitstechnologie ist am Londoner Flughafen Heathrow (Terminal 4) seit 2004 getestet worden. Andere Systeme nehmen Bilder von verborgenen Objekten auf und projizieren sie auf eine geschlechtslose Puppe.

27. Wo können Sie Videoüberwachung akzeptieren? (Mehr als eine Antwort möglich)

1. In Geschäften
2. In Umkleidekabinen, um Ladendiebstahl zu verhindern
3. In zentralen Bus- und Zugbahnhöfen
4. In Banken
5. In Flughäfen
6. In Sportstadien und bei anderen Großereignissen
7. An allen öffentlichen Orten
8. Sie ist nirgendwo akzeptabel
9. Ich weiß es nicht

28. Was denken Sie über die Anzahl von Überwachungskameras auf öffentlichen Plätzen im Allgemeinen?

1. Es sollte mehr Überwachungskameras auf öffentlichen Plätzen geben
2. Die Anzahl von Überwachungskameras auf öffentlichen Plätzen ist angemessen
3. Es sollte weniger Überwachungskameras auf öffentlichen Plätzen geben
4. Es sollte überhaupt keine Überwachungskameras auf öffentlichen Plätzen geben
5. Ich weiß es nicht

29. In welchen Fällen ist das Scannen von Personen nach versteckten Gegenständen notwendig? *(Mehr als eine Antwort möglich*)

1. In Schulen
2. In zentralen Bus- und Zugbahnhöfen
3. In Flughäfen
4. In Einkaufszentren
5. Es ist nie notwendig
6. Ich weiß es nicht

30. Welche Art des Scannens würden Sie akzeptabel finden? *(Mehr als eine Antwort möglich*)

1. Ein Scannen, das alles unter der Kleidung zeigt
2. Eine Durchleuchtung, bei der versteckte Gegenstände auf eine Puppe projiziert werden
3. Die Messung von Körperhitze, Schweiß und Pulsfrequenz
4. Das Scannen nach metallischen Gegenständen
5. Eine Durchleuchtung des Gepäcks mittels Röntgenstrahlen

6. Das Scannen ist nie akzeptabel
7. Ich weiß es nicht

Ausgewählte Aussagen zu Videoüberwachung und dem Scannen von Personen

31. Durch Videoüberwachung fühle ich mich sicherer.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

32. Videoüberwachung verletzt meine Privatsphäre.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

33. Das Scannen von Personen nach versteckten Gegenständen ist ein akzeptables Mittel, um Terrorismus zu verhindern.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

Technologien zur Ortung

Es ist möglich, die ungefähre Position von Mobiltelefonen aus den Koordinaten der nächstgelegenen Funkstationen zu berechnen.

Für eine genauere Ortung werden satellitenbasierte Systeme genutzt:

GPS ist das derzeit vorhandene System, die Abkürzung steht für *Global Positioning System*. Das zukünftige System heißt *Galileo* und soll im Jahr 2010 betriebsbereit sein. Es wird genauer als das GPS-System sein, und soll auch innerhalb von Gebäuden funktionieren.

eCall

Das eCall-System soll in Autos eingesetzt werden. Das Gerät enthält Sensoren, die es nach einem Unfall aktivieren. Es löst einen automatischen Notruf aus und übermittelt Information über die Zeit, den genauen Standort und das betroffene Fahrzeug.

Das Gerät wird nicht permanent mit einem mobilen Datenübertragungsnetz verbunden sein, es verbindet sich nur, nachdem es aktiviert worden ist. Es gibt jedoch Befürchtungen, dass sich dies ändern könnte: ein Beispiel wäre das permanente Senden von weiteren Daten, etwa für Versicherungsgesellschaften. Sorgen bereitet auch ein möglicher unbefugter Zugang zu Datenbanken, in denen eCall-Daten gespeichert werden. Ab September 2009 werden alle neuen Autos in den teilnehmenden Ländern mit eCall-Geräten ausgerüstet sein.

34. Für welchen Zweck ist die Ortung von Mobiltelefonen akzeptabel? ***(Mehr als eine Antwort möglich***)

1. Polizeiliche Ortung der Mobiltelefone von vermuteten Terroristen oder Verbrechern aufgrund einer gerichtlichen Anordnung
2. Polizeiliche Ortung jedes Mobiltelefons ohne gerichtliche Anordnung
3. In Notfällen, z.B. bei einem Unfall, einem verlorenen Kind oder einer verwirrten Person
4. Sie ist nie akzeptabel
5. Ich weiß es nicht

35. Für welchen Zweck ist die Ortung von Autos akzeptabel? ***(Mehr als eine Antwort möglich***)

1. Polizeiliche Ortung der Autos von vermuteten Terroristen oder Verbrechern aufgrund einer gerichtlichen Anordnung
2. Polizeiliche Ortung jedes Autos ohne gerichtliche Anordnung
3. Ortung um gestohlene Fahrzeuge ausfindig zu machen
4. Um Geschwindigkeitskontrollen durchzuführen und Strafmandate auszustellen
5. Automatischer Notruf im Falle eines Autounfalls
6. Sie ist nie akzeptabel

7. Ich weiß es nicht

36. Sollte das eCall-System automatisch in allen neuen Autos installiert werden?

1. Ja
2. Ja, aber es sollte möglich sein, eCall auszuschalten
3. Nein, es sollte eine Wahlmöglichkeit geben
4. Nein, es sollte keinesfalls installiert werden
5. Ich weiß es nicht

Ausgewählte Aussagen zu Ortungstechnologien

37. Die Möglichkeit, alle Mobiltelefone zu orten, verletzt die Privatsphäre.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

38. Die Möglichkeit, die Mobiltelefone von Verdächtigen orten zu können, ist ein gutes Werkzeug für die Polizei bei der Untersuchung von und Vorbeugung gegen Terrorismus und Kriminalität.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

39. Die Möglichkeit, alle Autos orten zu können, verletzt die Privatsphäre.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

40. Die Möglichkeit, alle Autos orten zu können, ist ein gutes Werkzeug für die Polizei bei der Untersuchung von und Vorbeugung gegen Terrorismus und Kriminalität.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

Vorratsdatenspeicherung

Eine Datenbank ist eine organisierte Sammlung von Daten. Es wird allgemein anerkannt, dass man wesentlich mehr über eine Person erfahren kann, wenn Daten aus verschiedenen Quellen zusammengefügt werden als wenn diese Daten jeweils einzelnen betrachtet werden. Es ist daher ein wichtiges Prinzip des Datenschutzes, dass in Datenbanken jeweils nur jene Informationen gesammelt werden dürfen, die für den Zweck dieser Datenbank notwendig sind, und dass die Daten gelöscht werden sollen, sobald sie nicht mehr benötigt werden.

In letzter Zeit ist ein Trend zu beobachten, nach dem Regierungen mehr Daten als für den ursprünglichen Zweck erforderlich sind, speichern wollen und unterschiedliche Datenbanksysteme für Zwecke wie Sicherheit zusammenführen wollen. Zumeist sind Daten aus dem Bereich Informations- und Kommunikationstechnologien, wie Kommunikationsverkehrsdaten von Telefonen, Mobiltelefonen und Internetnutzung gemeint, wenn die Einführung von Vorratsdatenspeicherung diskutiert werden.

Total Information Awareness (TIA)

TIA war ein Programm der DARPA (Defence Advanced Research Projects Agency) der US-Regierung. Es lässt sich am ehesten mit dem Begriff "allumfassende Auswertung von Informationen" übersetzen. Das TIA-Programm umfasste drei Kategorien von Software-Werkzeugen: automatische Sprachübersetzung, Suchmaschinen und Mustererkennung sowie fortgeschrittene sowie fortgeschrittene Systeme zur Entscheidungsfindung.

Das Ziel von TIA war es, terroristische Angriffe vorhersagen zu können, ehe sie eintreten. Es war beabsichtigt, dass das System private und öffentliche Datenbanken wie auch das Internet nach verdächtigen Daten durchsucht, die auf einen Terroristenangriff hinweisen könnten. Im September 2003 wurde die Finanzierung von TIA vom US-Kongress gestoppt, aber viele der Projekte innerhalb des Programms werden unter anderem Namen weitergeführt.

Zweckentfremdung

Datenbanksysteme sind gegenüber Zweckentfremdungen anfällig, darunter versteht man die Verwendung von Daten für andere Aufgaben als ursprünglich geplant. Ein Beispiel dafür ist die

norwegische Datenbank über Asylantragsteller, die auch biometrische Informationen wie Fingerabdrücke enthält. Sie wurde der Polizei für Ermittlungen von strafbaren Handlungen zur Verfügung gestellt. Der ursprüngliche Zweck der Datenbank war es, die Identität von Asylanten zu überprüfen.

41. Für welche der folgenden Zwecke finden Sie Vorratsdatenspeicherung von Kommunikationsverkehrsdaten akzeptabel? *(Mehr als eine Antwort möglich*)

1. Zur Verhütung von terroristischen Angriffen im Allgemeinen
2. Für die Untersuchung von terroristischen Angriffen
3. Zur Verhütung von Verbrechen im Allgemeinen
4. Für die Untersuchung von Verbrechen
5. Für kommerzielle Zwecke
6. Sie ist nie akzeptabel
7. Ich weiß es nicht

42. Für welche der folgenden Zwecke finden Sie die Verknüpfung und Auswertung von persönlichen Daten aus verschiedenen Datenbanken akzeptabel? *(Mehr als eine Antwort möglich*)

1. Zur Verhütung von terroristischen Angriffen im Allgemeinen
2. Für die Untersuchung von terroristischen Angriffen
3. Zur Verhütung von Verbrechen im Allgemeinen
4. Für die Untersuchung von stattgefundenen Verbrechen
5. Für kommerzielle Zwecke
6. Es ist nie akzeptabel
7. Ich weiß es nicht

Ausgewählte Aussagen zur Vorratsdatenspeicherung

43. Öffentliche Stellen sollten alle Daten speichern, die sie aus Sicherheitsgründen als notwendig betrachten.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

44. Daten von Telefon, Mobiltelefon und Internetnutzung sollten nicht über das Ausmaß hinaus gespeichert werden, welches für Abrechnungszwecke erforderlich ist.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

45. Die Auswertung und Verknüpfung von Daten aus unterschiedlichen Datenbanken mit persönlichen Informationen verletzt die Privatsphäre.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

46. Die Auswertung und Verknüpfung von Daten aus unterschiedlichen Datenbanken, ist ein gutes Werkzeug für die Polizei, um Terrorismus zu verhindern.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

47. Dass Datenbanken für etwas anderes als den Originalzweck verwendet werden, ist ein ernstes Problem für die Privatsphäre.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

Abhören

Unterschiedliche Technologien können genutzt werden, um die Aktivitäten und Kommunikation von Bürgern im Internet, beim Telefonieren oder in bestimmten Gebieten zu belauschen. Eine bekannte Form ist das Abhören von Telefongesprächen. Dabei wird ein Abhörgerät in Telefonzentralen installiert, das Abhörgerät kann die Gespräche des Verdächtigen erfassen oder auch gegen Telefone von Personen gerichtet werden, von denen man annimmt, dass der Verdächtige sich an sie wenden wird.

Eine erweiterte Version des Abhörens erfasst unterschiedslos alle Kommunikationsmöglichkeiten (Telefon, Mobiltelefon, Internet), die auf verdächtige Aktivitäten untersucht werden.

48. Für welche der folgenden Zwecke ist das Abhören akzeptabel? ***(Mehr als eine Antwort möglich***)

1. Zur Verhütung und Untersuchung von terroristischen Angriffen aufgrund einer gerichtlichen Anordnung
2. Zur Verhütung und Untersuchung von terroristischen Angriffen ohne gerichtliche Anordnung
3. Zur Verhütung und Untersuchung von Verbrechen aufgrund einer gerichtlichen Anordnung
4. Zur Verhütung und Untersuchung von Verbrechen ohne gerichtliche Anordnung
5. Für kommerzielle Zwecke
6. Es ist nie akzeptabel
7. Ich weiß es nicht

49. Welche Methoden des Abhörens von Telefongesprächen durch die Polizei sind akzeptabel?

1. Das Abhören aller Gespräche auf mögliche Hinweise
2. Das Abhören von Verdächtigen und Personen, die diese möglicherweise kontaktieren werden
3. Das Abhören von Verdächtigen
4. Das Abhören ist völlig unannehmbar
5. Ich weiß es nicht

Ausgewählte Aussagen zum Abhören

50. Abhören ist ein gutes Werkzeug für polizeiliche Ermittlungen.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

51. Abhören ist eine ernste Verletzung der Privatsphäre.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

Technologien zur Förderung der Privatsphäre

Technologien, die direkt dazu beitragen, die Privatsphäre zu schützen, werden als privatsphärenfördernde oder privatsphärenfreundliche Technologien bezeichneten.

Anonymisierung ist ein Beispiel dafür. Es gibt Dienste, die eine anonyme elektronische Kommunikation für normale Benutzer ermöglichen. Dabei werden die Verbindungen zwischen Nutzen und die Spuren, die sie hinterlassen versteckt.

Identitäts-Management ist auch eine Form privatsphärenfördernder Technologien: In einigen Fällen wollen Sie sich vielleicht nicht identifizieren, sondern ein Pseudonym (zum Beispiel bei Foren im Internet) verwenden. Um die Verknüpfung von Daten schwieriger zu machen, kann es nützlich sein, verschiedene Benutzernamen (die Ihre Identität nicht zeigen) und Passwörter für verschiedene Zwecke zu verwenden. Identitätsmanagementsysteme helfen Ihnen dabei, Ihre verschiedenen Benutzernamen und Passwörter zu verwalten.

Verschlüsselung ist eine andere Möglichkeit, Inhalte für andere Personen unleserlich zu machen. Weil alle Formen elektronischer Kommunikation belauscht oder manipuliert werden können, ist es in vielen Fällen entscheidend, dass die Kommunikation in verschlüsselte Form stattfindet.

52. Welche Arten von privatsphärenfördernden Technologien sollten legaler Weise für alle Bürger verfügbar sein? *(Mehr als eine Antwort möglich*)

1. Anonyme Telefonwertkarten
2. Verschlüsselungssoftware
3. Identitätsmanagementsysteme
4. Keine privatsphärenfördernden Technologien sollten legal verfügbar sein
5. Ich weiß es nicht

Ausgewählte Aussagen zu privatsphärenfördernden Technologien

53. Privatsphärenfördernde Technologien sind in der Gesellschaft von heute eine Notwendigkeit, um die Privatsphäre zu erhalten.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

54. Privatsphärenfördernde Technologien sollten nicht legal sein, wenn sie polizeiliche Ermittlungen und die Verhütung von Terrorismus und Verbrechen schwieriger machen.

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

Konflikte bei der Verwendung der Sicherheitstechnik

Im Folgenden stellen wir Ihnen jetzt eine Reihe von Dilemmata vor, die bei der Nutzung von Sicherheitstechnologien für die Privatsphäre auftreten. Wir möchten Sie bitten, dass Sie für jede Frage sowohl über Vorteile als auch Nachteile nachdenken und dann Ihre Antwort geben. *Auf alle Fragen in diesem Abschnitt können Sie mehr als eine Antwort geben.*

55. Die Nutzung von Fingerabdrücken beim Ein- und Aussteigen in öffentliche Verkehrsmittel könnte eine automatische Abbuchung der Fahrtkosten von Ihrem Konto ermöglichen. Dies würde die Bezahlung um einiges leichter machen, würde aber bedeuten, dass Ihre Fahrten gespeichert werden und Sie Ihre Fingerabdrücke als Ausweis benutzen müssen. Wie würden Sie sich dabei fühlen? *(Mehr als eine Antwort möglich*)

1. Ich kann die Speicherung meiner Fahrten und die Nutzung von Fingerabdrücken akzeptieren, weil dadurch die Bezahlung einfacher wird.
2. Ich kann dies nur akzeptieren, wenn meine Fingerabdrücke nur als „Templates“ gespeichert sind und diese nicht rekonstruiert werden können.
3. Ich kann dies nur akzeptieren, wenn die Daten zu meinen gespeicherten Reisen nach der Bezahlung gelöscht werden.
4. Die Verwendung von Fingerabdrücken sollte eine Möglichkeit, aber nicht die einzig verfügbare Form der Bezahlung sein.
5. Ich würde meine Fingerabdrücke nie als Identifikation bei der Nutzung öffentlicher Verkehrsmittel verwenden.
6. Ich weiß es nicht.

56. Eine umfassende Registrierung in einer Flughafendatenbank und die Akzeptanz von bestimmten Sicherheitstechnologien, die alle als verletzend für die Privatsphäre angesehen werden können, würden eine schnelle Abfertigung in Flughäfen ermöglichen. Welche Sicherheitstechnologien und Verletzungen ihrer Privatsphäre würden Sie für eine schnellere Abfertigung im Flughafen akzeptieren? *(Mehr als eine Antwort möglich*)

1. Ich würde es akzeptieren, umfassend überprüft und in einer permanenten Flughafensicherheitsdatenbank gespeichert zu werden und dann bei allen weiteren Flügen biometrische Verfahren zur Identifizierung zu verwenden.

2. Ich würde es akzeptieren, durch "nackte Maschinen" zu gehen.
3. Ich würde es akzeptieren, dass Schweiß, Körpertemperatur und Pulsfrequenz gemessen werden.
4. Ich würde meine Privatsphäre nicht für ein schnelles und bequemes Check-In am Flughafen aufgeben.
5. Ich weiß es nicht.

57. Aktive Überwachungskameras und automatische Gesichtserkennung, bei der Gesichter von Menschen mit den in einer Datenbank gespeicherten Fotografien von bekanntem Terroristen abgeglichen werden, sind Sicherheitstechnologien, die verwendet werden können, um Terrorangriffe z.B. in Flughäfen oder Bahnhöfen zu verhindern. Diese Sicherheitstechnologien könnten möglicherweise einen Terrorangriff verhindern, aber ihre Wirksamkeit ist nicht bewiesen. Sie könnten auch dazu führen, dass unschuldige Personen mit Terroristen verwechselt und ausführlichen Befragungen unterzogen werden. Unter welchen Bedingungen sollen diese Technologien eingesetzt werden? *(Mehr als eine Antwort möglich*)

1. Aktive Kameras und automatische Gesichtserkennung sollten eingesetzt werden, ganz gleich wie viele unschuldige Personen mit Terroristen verwechselt werden.
2. Aktive Kameras und automatische Gesichtserkennung sollten eingesetzt werden, aber nur wenn wenige unschuldige Personen mit Terroristen verwechselt werden.
3. Aktive Kameras und automatische Gesichtserkennung sollten nur eingesetzt werden, wenn niemand mit Terroristen verwechselt wird.
4. Aktive Kameras und automatische Gesichtserkennung sollten nur an Orten eingesetzt werden, an denen viele Verbrechen aufgetreten sind oder die sehr verwundbar für Terrorangriffe sind.
5. Aktive Kameras und automatische Gesichtserkennung sollten nirgendwo benutzt werden.
6. Ich weiß es nicht.

58. Neue Technologien machen es möglich, Daten von verschiedenen Datenbanken, welche persönliche Informationen beinhalten, zu verknüpfen und zu durchsuchen, um verdächtige Muster in der persönlichen Kommunikation und Internetnutzung zu entdecken. Der Zweck ist, Angriffe vorauszusehen und zu verhindern, aber dies bedeutet auch, persönliche Daten von unschuldigen Personen zu analysieren. Welche Möglichkeiten für die Polizei zur Verknüpfung der Durchsuchung verschiedener Datenbanken finden Sie akzeptabel? *(Mehr als eine Antwort möglich*)

1. Die Polizei sollte Zugriff auf alle Datenbanken haben und sie kombinieren können, um verdächtige Muster zu finden, die mögliche Terroristen identifizieren können.
2. Die Polizei sollte nur Zugriff auf Datenbanken haben und sie kombinieren können, wenn die Daten anonym sind und nur durch einen Gerichtsbeschluss die Identität eines Verdächtigen offen gelegt werden darf.
3. Die Polizei sollte niemals Datenbanken kombinieren und nach verdächtigen Mustern durchsuchen dürfen.
4. Ich weiß es nicht.

59. Das eCall-System könnte in allen neuen Autos installiert werden, um im Falle eines Unfalls einen Notruf auszusenden. Dieses System könnte auch verwendet werden, um Autos für andere Zwecke zu orten, z.B. wenn sie gestohlen werden oder wenn sie für Verbrechen oder Terroranschläge verwendet werden. Dies erfordert aber, dass die Bewegungen von Autos mit eCall fortlaufend erfasst und gespeichert werden. Welche Nutzungen von eCall finden Sie akzeptabel? *(Mehr als eine Antwort möglich*)

1. Ich finde es akzeptabel, dass eCall von der Polizei aktiviert werden kann, um ein Auto ausfindig zu machen, falls es notwendig ist, um Verbrechen oder Terror zu verhindern.
2. Ich finde es akzeptabel, dass eCall jederzeit aktiv ist und benutzt werden kann, um Geschwindigkeitsübertretungen zu bestrafen.
3. Ich finde es akzeptabel, dass die Bewegungen meines Autos mit eCall fortlaufend erfasst und gespeichert werden.
4. eCall sollte nicht für andere Zwecke verwendet werden, als Unfälle zu melden.
5. Das Installieren von eCall in Autos sollte freiwillig sein.
6. Ich weiß es nicht.

60. Privatsphärenfördernde Technologien können dazu beitragen, die Privatsphäre zu schützen, wenn man per Telefon oder E-Mail kommuniziert und wenn man das Internet verwendet. Sie können aber auch für strafbare Aktivitäten oder von Terroristen benutzt werden. Wenn es darum geht, die Privatsphäre gewöhnlicher Bürger zu bewahren, welche Risiken sind Sie bereit, für einen legalen Zugang zu privatsphärenfördernden Technologien zu akzeptieren? *(Mehr als eine Antwort möglich*)

1. Ich kann legale anonyme Telefonwertkarten akzeptieren, obwohl sie polizeiliche Untersuchungen oder die Verhinderung von Terror und Verbrechen schwieriger machen könnten.
2. Ich kann die legale Verwendung von Verschlüsselungstechnologien akzeptieren, obwohl sie polizeiliche Untersuchungen oder die Verhinderung von Terror und Verbrechen schwieriger machen könnten.
3. Ich kann Anonymität im Internet akzeptieren, selbst wenn es bedeutet, dass Personen, die nach Bombenbauanleitungen suchen, nicht von der Polizei verfolgt werden können.
4. Ich kann akzeptieren, dass Internetanonymität bedeutet, dass Personen, die nach Kinderpornographie suchen, nicht von der Polizei verfolgt werden können.

5. Ich kann keine privatsphärenfördernden Technologien akzeptieren, die polizeiliche Untersuchungen oder die Verhinderung von Terror und Verbrechen schwieriger machen könnten.
6. Ich weiß es nicht.

61. Wenn eine Sicherheitstechnologie einen hohen Grad an Sicherheit bietet, welche Folgen können Sie für Personen akzeptieren, die diese Technologie nicht nutzen können, und welche für Personen, die sie aus Gründen der Privatsphäre nicht verwenden wollen? ***(Mehr als eine Antwort möglich***)

1. Ich kann es akzeptieren, dass Leute, die aus Gründen der Privatsphäre nicht bereit sind, diese Technologien zu verwenden, von der Nutzung einiger öffentlicher Dienste ausgeschlossen sind.
2. Ich kann akzeptieren, dass Leute, die außerstande sind, die Technik zu verwenden, davon ausgeschlossen sind, einige öffentliche Dienste zu nutzen.
3. Ich kann akzeptieren, dass Leute, die aus Gründen der Privatsphäre nicht bereit sind, diese Technologien zu verwenden, in gewisser Weise behindert werden, wenn sie mit öffentlichen Verkehrsmitteln reisen.
4. Ich kann akzeptieren, dass Leute, die außerstande sind, diese Technologien zu verwenden, in gewisser Weise behindert werden, wenn sie mit öffentlichen Verkehrsmitteln reisen.
5. Ich kann keinerlei Folgen für Personen akzeptieren, die aus Gründen der Privatsphäre nicht bereit sind, diese Technologien zu verwenden.
6. Ich kann keinerlei Folgen für Personen akzeptieren, die außerstande sind, diese Technologien zu verwenden.
7. Ich weiß es nicht.

Demokratiepolitische Aspekte

Im folgenden Abschnitt werden Sie mit einigen Aussagen über demokratische Aspekte neuer Sicherheitstechnologien konfrontiert. Wer sollte einen Einfluss bei Fragen von Sicherheitstechnologien und Privatsphäre ausüben dürfen und in welcher Weise?

In welchem Ausmaß sind Sie mit den folgenden Ansichten einverstanden oder stimmen Sie nicht überein? Bitte teilen Sie uns Ihre Meinung zu den einzelnen Ansichten mit. Bitte geben Sie nur eine Antwort auf jede Frage.

62. Politiker müssen wichtige Fragen immer in öffentlichen Debatten und öffentlichen Anhörungen diskutieren, bevor sie Entscheidungen über die Einführung neuer Sicherheitstechnologien treffen.

1. Ich bin völlig einverstanden
2. Ich bin teils einverstanden
3. Ich bin einverstanden oder bin nicht einverstanden auch nicht
4. Ich bin teils nicht einverstanden
5. Ich bin nicht einverstanden

63. Das Thema Sicherheit und Privatsphäre ist so kompliziert, dass es keinen Sinn macht, die Öffentlichkeit in Diskussionen dieser Angelegenheit einzubeziehen.

1. Ich bin völlig einverstanden
2. Ich bin teils einverstanden
3. Ich bin einverstanden oder bin nicht einverstanden auch nicht
4. Ich bin teils nicht einverstanden
5. Ich bin nicht einverstanden

64. Menschenrechtsorganisationen sind immer berechtigt, gehört zu werden, wenn wichtige Entscheidungen über Sicherheit und Privatsphäre getroffen werden.

1. Ich bin völlig einverstanden
2. Ich bin teils einverstanden
3. Ich bin einverstanden oder bin nicht einverstanden auch nicht
4. Ich bin teils nicht einverstanden
5. Ich bin nicht einverstanden

65. Es ist wichtig, dass private Unternehmen, die an der Herstellung von Sicherheitstechnologien beteiligt sind, auch berechtigt sind, gehört zu werden, wenn wichtige Entscheidungen über Sicherheit und Privatsphäre getroffen werden.

1. Ich bin völlig einverstanden
2. Ich bin teils einverstanden
3. Ich bin einverstanden oder bin nicht einverstanden auch nicht
4. Ich bin teils nicht einverstanden
5. Ich bin nicht einverstanden

66. Bei bedeutsamen Entscheidungen über die Verwendung von Sicherheitstechnologien ist es unbedingt notwendig, dass alternative Lösungen untersucht und in die Debatte einbezogen werden.

1. Ich bin völlig einverstanden
2. Ich bin teils einverstanden
3. Ich bin einverstanden oder bin nicht einverstanden auch nicht
4. Ich bin teils nicht einverstanden
5. Ich bin nicht einverstanden

Vorschläge zu einer privatsphärenfördernden Verwendung von Sicherheitstechnologien

Im folgenden Abschnitt möchten wir Ihnen einige Vorschläge vorstellen, wie man Sicherheitstechnologien einführen, nutzen und entwickeln kann, ohne die Privatsphäre zu verletzen. Für jeden Vorschlag bitten wir Sie darum, anzugeben, wie wichtig es wäre, den Vorschlag durchzuführen.

Wenn Sie es sehr wichtig finden, dass dem Vorschlag gefolgt wird, ringeln Sie bitte 1 "sehr wichtig" ein.
Wenn Sie den Vorschlag wichtig finden, ihm aber keine hohe Priorität beimessen, wählen Sie 2 "wichtig".
Wenn Sie finden, dass es nicht sehr wichtig ist, wählen Sie 3 "wenig wichtig".
Wenn Sie finden, dass es überhaupt nicht wichtig ist oder dem Vorschlag nicht gefolgt werden sollte, ringeln Sie 4 " überhaupt nicht wichtig" ein.
Wenn Sie nicht sicher sind, was Sie antworten sollen, wählen Sie bitte 5 "Ich weiß es nicht".

Vorschläge

67. Die Sammlung von persönlichen Daten von unverdächtigen Personen muss anonym sein, bis eine Identifikation durch einen Gerichtsbeschluss gestattet wird.

1. Sehr wichtig
2. Wichtig
3. Wenig wichtig
4. Überhaupt nicht wichtig
5. Ich weiß es nicht

68. Nur bevollmächtigtes Personal darf Zugang zu gesammelten persönlichen Daten haben.

1. Sehr wichtig
2. Wichtig
3. Wenig wichtig

4. Überhaupt nicht wichtig
5. Ich weiß es nicht

69. Vor der Einführung müssen neue Sicherheitstechniken auf ihre Wirkungen auf die Privatsphäre hin untersucht werden.

1. Sehr wichtig
2. Wichtig
3. Wenig wichtig
4. Überhaupt nicht wichtig
5. Ich weiß es nicht

70. Die Finanzierung von Forschungsprojekten über neue Sicherheitstechnologien sollte von einer gründlichen Analyse von den Wirkungen auf die Privatsphäre abhängig sein.

1. Sehr wichtig
2. Wichtig
3. Wenig wichtig
4. Überhaupt nicht wichtig
5. Ich weiß es nicht

Abschließende Fragen

Sie haben viele unterschiedliche und detaillierte Fragen über Sicherheitstechniken und Privatsphäre beantwortet. Abschließend möchten wir Ihnen noch zwei Fragen stellen.

72. Haben Sie Ihre Einstellung zu Sicherheitstechnologien im Allgemeinen geändert, während Sie diesen Fragebogen ausgefüllt haben?

1. Ja, meine Einstellung zu Sicherheitstechnologien im Allgemeinen ist positiver geworden
2. Ja, meine Einstellung zu Sicherheitstechnologien im Allgemeinen ist negativer geworden
3. Nein, ich habe meine Einstellung nicht geändert
4. Ich weiß es nicht

73. Wenn Sie weitere Anmerkungen zu Sicherheitstechnologien hinzufügen möchten, oder wenn Sie Kommentare geben möchten, für die in diesem Fragebogen keine Gelegenheit vorgesehen war, so können Sie diese hier hinzufügen:

1. Ich habe nichts hinzuzufügen
2. Ihre Bemerkungen:

_____
_____
_____
_____
_____
_____
_____
_____

4.2 Interview guide in German

Interviewleitfaden

die fett gedruckten Fragen müssen diskutiert werden. Unter jeder Frage steht eine kurze Notiz über den Zweck dieser Frage.
Für die meisten dieser Fragen gibt es untergeordnete Fragen. Diese Fragen sind als Anregung gedacht, und sie können benutzt werden, um die Diskussion anzuregen, wenn es notwendig ist. Diese untergeordneten Fragen müssen nicht gestellt werden, wenn es nicht notwendig ist, um die Diskussion anzuregen.

Interviewfragen

Erstens: was sind Ihre unmittelbaren Gedanken über Sicherheitstechnologien und Privatsphäre?
Zweck der Frage: dies ist eine offene Frage um die Debatte anzuregen und den Teilnehmern die Chance geben, ihre unmittelbare Haltung zu präsentieren.

Zweitens: was halten Sie von der Szenarien?
Zweck der Frage: die Teilnehmer zu veranlassen darüber zu reden, was sie in den Szenarien gelesen haben, um eine Idee davon zu bekommen, welche Gefühle sie bei der präsentierten möglichen Zukunft haben.

Untergeordnete Fragen, um die Diskussion anzuregen - nur falls notwendig:

- wie ist das Gleichgewicht zwischen Sicherheit und Privatsphäre in den Szenarien?
- Denken Sie, das es wichtig ist die Vorteile in den Szenarien zu erreichen?
- Stellen die Szenarien ein Bild einer attraktiven Zukunft war?

Drittens: was denken Sie, sind die wichtigen positiven Potenziale von Sicherheitstechnologien?
Zweck der Frage: die Teilnahme dazu zu bringen, an die positiven Potenziale zu denken und einen Eindruck davon zu bekommen, was sie für den wichtigsten Gewinn von Sicherheitstechnologien halten.

Untergeordnete Fragen, um die Diskussion anzuregen - nur falls notwendig:

- was können Sie mit Sicherheitstechnologien gewinnen - können Sie sein Beispiel geben?
- Was ist die wichtigste positive Möglichkeit?
- Warum ist dies wichtig?

Viertens: über welche negativen Effekte von Sicherheitstechnologien sind besorgt?
Zweck der Frage: die Teilnehmer dazu zu veranlassen, an die negativen Seiten von Sicherheitstechnologien zu denken, die Bedrohungen, und einen Eindruck davon zu bekommen, was sie als die größte Bedrohung ansehen.

Untergeordnete Fragen, um die Diskussion anzuregen - nur falls notwendig:

- was sind negative Effekte von Sicherheitstechnologien - können Sie ein Beispiel geben?

- Welches ist der wichtigste negative Effekt von Sicherheitstechnologien?
- Warum ist es wichtig?

Fünftens: wann denken Sie, dass Sicherheit wichtiger ist als die Privatsphäre - und wann umgekehrt?
Zweck der Frage: die Teilnehmer dazu anzuregen, die Konflikte und Dilemmata von Sicherheit und Privatsphäre zu diskutieren (trade offs) um einen Eindruck davon zu bekommen, in welchen Situationen und wie viel von Privatsphäre sie für Sicherheit aufzugeben bereit sind.

Untergeordnete Fragen, um die Diskussion anzuregen - nur falls notwendig:
- in welchen Bereichen oder Situationen finden sie es in Ordnung, das Sicherheitstechnologien in die Privatsphäre eindringen?
- In welchen Bereichen oder Situationen finden Sie, dass Privatsphäre wichtiger ist als Sicherheit?

Sechstens: wer sollte beteiligt sein, wenn entschieden wird, welche neuen Sicherheitstechnologien eingesetzt werden?
Zweck der Frage: den demokratiepolitischen Standpunkt der Teilnehmer zu erfahren und einen Eindruck von der Wichtigkeit verschiedene Interesses Gruppen einzubinden, wenn über die Einführung neuer sichert Technologien entschieden wird

Untergeordnete Fragen, um die Diskussion anzuregen - nur falls notwendig:
- welche Interessensgruppen sollten gehört werden? (Bürger im Allgemeinen, Menschenrechtsorganisationen, Entwickler von Sicherheitstechnologien, Politiker, usw.)

Siebtens: haben Sie irgendwelche Vorschläge für die Regulierung der Entwicklung und Einführung von neuen sichert Technologien?
Zweck der Frage: um Anregungen von den Teilnehmern zu bekommen, wie die Entwicklung und Einführung von neuen Sicherheitstechnologien in geregelt werden soll

Untergeordnete Fragen, um die Diskussion anzuregen - nur falls notwendig:
- sollte es irgendwelche Beschränkungen für die Entwicklung von Sicherheitstechnologien geben oder sollten Sicherheitstechnologiefirmen alles entwickeln dürfen, was sie möchten?
- Sollten Regierungen jede neue Sicherheitstechnologien einführen, die sie für wichtig halten oder soll das Beschränkungen beziehungsweise Regelungen geben - und welche Regelungen?

Achtens: hat ihre Teilnahme in der heutigen Veranstaltung ihre Haltung zu Sicherheitstechnologien und Privatsphäre verändert? Wenn Ja, warum?
Zweck der Frage: Oma raus zu finden, ob Information und Diskussion über das Sicherheitstechnologien und Privatsphäre der Haltung der Teilnehmer geändert hat

Neuntens: gibt es abschließende Anmerkungen, Punkte oder Botschaften, die sie anfügen möchten? (Frage an alle Teilnehmer; der Runde)

Zweck der Frage: um den Teilnehmern die Chance geben, eine letzte Aussage zu treffen, bevor das Interviewmeetings endet.

Untergeordnete Fragen, um die Diskussion anzuregen - nur falls notwendig:

- hat Sie etwas während der Diskussion besonders beeindruckt?

Daumenregeln
Daumenregeln und Tipps, wie man die Gruppeninterviews auf eine gute Art durchführt.

Einführung
Beginnen Sie mit einer selbst Vorstellung "der Name ist, ich bin von, und ich werde diese Gruppendiskussion moderieren

Annex 5 Transcripts of group interviews

In the following subchapters contain the anonymized transcripts of the three group interviews; both the text and the codes[1] used by the transcriber are in German. The titles correspond to the rooms in which these interviews were conducted.

5.1 Clubraum

Meine erste Frage wäre jetzt einmal ganz allgemein, was sind so Ihre unmittelbaren ersten Gedanken, wenn es um Sicherheitstechnologien geht. Also das Thema Sicherheitstechnologie und Privatsphäre, das Spannungsfeld, das da aufgemacht ist.

Na ja, dass wir dauernd überwacht sind, zum Beispiel in der U-Bahn, das ist schon irgendwie ... weiß ich nicht, da bin ich mir nicht gut vorgekommen. (??) [0.37] wohl gefühlt, aber mit der Kamera ehrlich gesagt nein. Und ich habe eigentlich noch nie Angst gehabt und die angefangen jetzt zu überwachen. (??) Also ich finde das genügte vollauf. Der Karlsplatz, sehe ich ein, aber alles andere finde ich nicht. Also da fühle ich mich wirklich nicht wohl.

Die Kameras machen es für Sie eher unsicher?

Unsicher nicht, aber es ist ... ich finde es nicht in Ordnung. Auf der Straße nicht. Ich finde, wenn wir mehr Polizei haben. Ich weiß das als Kind vorm Krieg. Da war viel mehr Polizei auf der Straße. Wir haben uns als Kinder wohl gefühlt. Wenn wir was gewollt haben, sind wir zu dem Polizisten hingegangen. Erstens hat er einem jede Auskunft gegeben, dann hat er Ihnen geholfen. Also ich finde, wir haben uns nie bedrängt gefühlt, das hat für uns dazu gehört und wir haben uns sicher gefühlt. Da waren mehr Polizisten und (??) [1.46] durch diese Kamera, weil da muss ich mich dann (??), und ich (??), also ich finde diese ganze Technik von ein paar da oben und von der Industrie, die das Geschäft machen will, und wir sind die (Descheks).

Sie fühlen sich nicht unbedingt sicherer dadurch, dass es Kameras gibt?

Nein, überhaupt nicht. Überhaupt nicht. Wie gesagt, am Karlsplatz oder am Flughafen sehe ich das noch ein, wo das so extrem ist, dass die dann da die

---

[1] ... Satzabbruch
(Wort) phonetische Erfassung / Namen immer phonetisch
(?) unverständliches Wort
(??) unverständlicher Satzteil
(???) längere unverständliche Passage
[Wort] Anmerkungen in eckigen Klammern
Zeilenwechsel = Sprecherwechsel

Bomben ... was ja auch nicht so oft vorgekommen ist. Diese ganze Überwachung, die nackte Maschinen da, also ich finde, das ist ein Horror. Ich kann mich da nicht wohl fühlen. Und ich finde, die schrecken da garantiert keinen ab, wenn sich der das mitnehmen will. Sie sehen ja, sie machen so viel Stichproben auf unserem Flughafen überhaupt, und die kommen mit allem ... sind sie durchgekommen, also ... Aber wie gesagt, ein paar von der Regierung und die Industrie, die wollen das haben.

Wie sehen das die anderen?

Ich bin nicht aus Wien, ich komme aus einer größeren Stadt südlich Wiens, wo es schon seit längerer Zeit sicherheitspolitische Debatten gibt und Debatten über den Einsatz von zum Beispiel Überwachungskameras, vor allem dort, wo ... es gibt in dieser Stadt eben (eine Meile) [3.25] vergleichbar in Wien wie ...

Karlsplatz, oder?

... Karlsplatz [Personen sprechen gleichzeitig] wie, ja, wo halt viele Lokale hintereinander sind und dort viele Jugendliche sind, und da wo es keine Woche gibt, wo nicht mindestens einer niedergeknüppelt wird. Und wie die Dame im Vorfeld gesagt hat, es gibt dort kaum Polizei, die ordnend einschreitet. Nur dann, wenn jemand, das ist mir selbst passiert, die Polizei ruft, dann kommen sie schon. Aber sonst ist das mehr oder weniger, sage ich jetzt, anonym. Dass es Verbrechen gibt und da fände ich es sehr gut, wenn dort eben zum Beispiel solche Kameras aufgebaut werden, weil es glaube ich schon abschreckt, dass man sagt, jetzt machen wir nichts, weil man nicht genau weiß, ich werde gefilmt dabei. Das ist meine Meinung. Das zweite ist, ich bin ... in dieser Stadt gibt es eine große Schule, eine technische Schule, ich bin dort Lehrer, und vor 14 Tagen ist es passiert, dass vom Weg von der Schule zum Bahnhof, wir haben sehr viele Extremisten, ist es einem Mädchen passiert, nach Schulschluss um 16 Uhr, dort aufgelauert zu werden und dem Mädchen sind dann am Arm und Oberkörper Stichwunden zugefügt worden. Die ist am nächsten Tag in die Schule gekommen vom Krankenhaus, war komplett vermummt natürlich. Psychisch total darnieder, und auch dort würde ich es gut finden, dass die Wege – und diese Stadt ist eine Schulstadt – gesichert sind. Wie auch immer gesichert. Dort gibt es Großschulen. Und in meiner Schule zum Beispiel sind 1.500 Schüler, und da gibt's ... das weiß man ganz genau, dass es da strategische Verkehrsknoten gibt. Und dort könnte ich mir durchaus vorstellen, um solche Handlungen zu unterbinden, eben verstärkt Sicherheitsmaßnahmen zu treffen. Wie gesagt, wie auch immer.

Anstelle der Polizei. Sie haben eher dafür plädiert, mehr Polizei.

Ja, aber wenn das so extrem ist, sehe ich das ohne Weiteres, aber ich finde, wenn die Polizei präsent ist, immer wieder durchfährt oder wenn man dort beim Schulschluss ist, kann das auch nicht so eskalieren, wie es da ist.

Ich habe das Problem, ich weiß, weil ich da ein bisschen involviert auch bin, wir haben das Problem, dass sozusagen der Pingpongball hin und her gespielt wird. Wer ist kompetent?

Ja, ja, genau, das ist ja das.

Dass die Polizei dann sagt, ich kann dort mit Hunden zum Beispiel nicht durchgehen, weil es den Hunden zu laut ist. [Personen sprechen gleichzeitig] Aber solche Äußerungen werden dann gemacht. Und Fakt ist, dass zu wenig überwacht wird, zu wenig kontrolliert wird. Ich möchte dort überhaupt keine einzelnen ...

Schuld zuweisen?

Nein, nein, keine Einzelne ... ich möchte nicht sagen, dass dort nur die Polizei sein muss, es sollte nur kontrolliert werden und nicht einfach gesagt werden, nein, das geht nicht, und wenn dann was passiert ist, dann wird man tätig, dann ist es aber meistens schon zu spät. Und das Mädchen, sage ich jetzt noch mal, also das ist glimpflich davon gekommen. Wenn man das zum Beispiel mein Kind ist, dann würde ich wahrscheinlich verrückt, wenn das passiert, weil wenn das nicht so ein couragiertes Mädchen ist und sie die noch mehr einschüchtern, wer weiß, was da passiert. Am hellichten Tag. Und das finde ich nicht in Ordnung. Und deshalb glaube ich, es sollten Maßnahmen, Überwachungsmaßnahmen gerechtfertigt sind.

Das wäre nicht schlecht, aber wer zahlt das wieder? Die Schule sagt, wir haben kein Geld. Sie kriegt ja nur einen gewissen ... Vielleicht kommt die Polizei ...

Zur Finanzierung später. Wir können die Runde fertig machen mit dieser ersten Frage, was Ihnen einfällt als das Wichtigste.

Auf der anderen Seite finde ich eine Überwachungskamera wäre nicht schlecht, aber was hat man eigentlich davon, wenn das Kind schon erstochen ist und dann erkennt, wer der Täter ist? Also ich glaube, es wäre doch dann irgendwie besser, wenn eine Polizei vorhanden wäre, die das von vorn herein verhindern kann.

Na ja, das ist das Problem, dass ich nicht weiß, wo brauche ich den Polizisten oder die zwei Polizisten. Weil ich kann ja nicht den Weg von der Schule bis zum Bahnhof jetzt zum Beispiel kann ich ja nicht alle 50 Meter oder 100 Meter einen Polizisten einstellen.

Na ja, aber wenn mehrere dort wären.

Aber wenn die immer auf und ab gingen, also ich weiß nicht, ob das nicht besser ist.

Ich glaube, dass die Präsenz von einem Menschen da eigentlich mehr verhindert als eine Überwachungskamera. Obwohl die auch nicht schlecht ist.

Wie ich den Vorfall bei der Polizei gemeldet habe, waren die wirklich innerhalb ... eineinhalb Minuten hat das gedauert.

Ja, aber das ist zu spät. Ich denke mir, wenn man etwas nicht im Vorfeld ...

Aber bis der Polizist ins Rennen kommt ...

Na, ich denke immer, wenn man solche Sachen nicht im Vorfeld bekämpfen kann, dann wird die Überwachungskamera letztendlich nicht wirklich viel helfen. Weil sie wird zwar aufzeichnen, aber was habe ich davon, von einem Täter, der sowieso sich nicht als Täter sieht? Der das sowieso morgen wieder macht. Also den kann man ja nicht einmal bestrafen, weil er ja vielleicht nicht einmal strafmündig ist. Was macht man dann mit so was? Mit der Überwachungskamera oder mit irgendeiner Überwachung? Also wenn das nicht passiert, dass man es verhindert, indem dass man selber Initiative ergreift oder irgendwelche Menschen, weiß ich nicht, die das verhindern, wird das wahrscheinlich auch nichts nützen.

Und Polizei (??) [10.09] was das früher mal, und heute, wo sie eine Funkstreife haben, aber dann ist schon Sense. Also ein Witz, nicht? Da muss wirklich ... aber das ist momentan, wenn da was passiert, sind sie da, und alles andere, was kleinere Sachen sind, fällt unter den Tisch. Aber wenn, wie gesagt, bei uns habe ich noch nie einen Wachmann gesehen, außer in der Funkstreife, die an uns vorbeifährt, aber sonst?

Ja, ich glaube auch, dass die Polizei nicht wirklich Kompetenz hat, irgendwas zu verändern. Ich habe heute zum Beispiel gehört im Radio irgendwo, da war ein Mädchen, also die hat man in der Schule bedroht, dass sie wirklich psychische Probleme hatte und sich umbringen wollte. Also weiß ich nicht, wie da eine Überwachungskamera oder irgend so ein technisches Gerät irgendwo Abhilfe schaffen sollte, wenn die Menschen nicht selber drauf kommen, dass die irgendwas anderes verändern müssen im Zusammenleben, denke ich.

Ich würde da noch mal gern fragen, diese ...

Dass man mit Überwachung, sei es jetzt abgesehen davon, dass also im Schulgebäude Polizei von vorn herein drin auch eine Frage ist, ne? Die Polizei kann nicht ohne, dass es dringend ist, automatisch im Schulgebäude stationiert sein.

Nicht Schulgebäude, aber ... [Personen sprechen gleichzeitig]

Und ich meine, denn sicher kann auch eine Videoüberwachung nicht alle Gefährdungen minimieren. Ich selber bin sehr ambivalent gegenüber diesen Geschichten, denn einerseits habe ich schon den Eindruck, dass der Trend dazu ist, dass man in manchem der Versuch ist, das über Gebühr einzusetzen, andererseits sicher an ganz speziellen ... Mir wäre es allerdings sozusagen eine wirkliche, und zwar im Detail und sozusagen für jeden eine echte Verhältnismäßigkeit zur

Prüfung einer Prognose, und sicher, hundertprozentig ist gar nichts, aber es ist zum Beispiel, wie es im privaten Bereich bei Banken ist, finde ich auch, ist es schon ein wichtiges Hilfsmittel, da die Banküberfälle so zugenommen haben, finde ich es dort für gerechtfertigt.

Mit der Videokamera haben sie aber noch keinen gefangen.

Ich meine, wenn die Banküberfälle in einer Frequenz der sechziger Jahre wären, würde ich es als nicht gerechtfertigt empfinden. Aber jetzt, wo wirklich praktisch kein Tag vergeht, wo im Großraum Wien nicht mehrere Banküberfälle sind, da halte ich das für gerechtfertigt. Und ein anderes Beispiel eben, südlich von Wien, das ist, dass man bei der (SCS) die Parkplätze videoüberwacht hat, und das scheint schon eine gewisse Abschreckung zu sein, denn diese Autoeinbrüche und Diebstähle sind ganz markant zurückgegangen.

Wobei die ersten Untersuchungsergebnisse haben gezeigt, dass dort, wo die Überwachungskameras eingesetzt werden, die Kriminalitätsrate zurückgeht, das Problem ist nur, dass sich das Ganze dann irgendwo anders hin verlagert.

Einerseits verlagert und zweitens längerfristig dann wahrscheinlich auch wieder etwas einpendelt. Aber dass in so jetzt ... Karlsplatz, oder ... in so wirklich neuralgischen Stellen, und wenn eben so ... man kann sicher nicht den Schulweg überwachen, aber wenn eben ... und sei es, es muss ja auch nicht einzementiert sein, dass das für die nächsten 20 Jahre so sein muss, aber dass sagen wir dann, wenn vor der Schule gehäuft Beschwerden stattfinden, dass man das dann neu einschätzt.

Ja, ich sehe das so wie zum Beispiel die Polizei stellt ja Geschwindigkeitsmessgeräte auch an neuralgische Punkte, und ganz bewusst an bestimmte Punkte, weil sie von vorn herein annimmt, dass dort zum Beispiel Geschwindigkeitsübertretungen massiv passieren. Die stellen das nicht xy-mäßig auf, sondern man weiß das. Und genauso stelle ich mir das eben vor. Wo halt keine Laterne steht, wo es halt dunkel ist, wo es eng ist, wo besonders man sich gut verstecken kann, so stelle ich mir das vor.

Jetzt haben wir nur über Videoüberwachung gesprochen. Ich würde gern jetzt noch mal ein bisschen aufmachen und noch mal Sie einladen, an diese Szenarien zu denken, die im Vorfeld ausgeschickt worden sind. Was halten Sie davon? Was halten Sie von diesen Zukunftsbildern, die da beschrieben sind?

Also ich finde das einen Horror. Ob das im Internet ist, ich habe zwar keins, aber ich sehe es bei meinem Enkel, und das Telefon, ich finde das einen Horror, und ich finde, man erwischt trotzdem keine ... diese ganzen Terroristen und so, weil sie sind so clever, dass sie immer wieder die Technik gleich heraus haben und dann nützt das Ganze nichts.

Gab es da auch was, was Ihnen gefallen hat in diesen Beschreibungen? Wo Sie sagen, das ist eigentlich eine gute Idee? Gibt es so was?

Ach Gott, ja, was sie ... zum Beispiel, gut ist, dass sie eine Straßenbahn oder den Bahnfahrschein mit Fingerabdruck. Ich habe eine Jahreskarte, mit der kann ich in ganz Wien herumfahren und ich kann mir eine Bahnkarte, eine Jahreskarte kaufen, da brauche ich auch nichts, [Tonstörungen / 16.43]

Na ja, ich glaube also die Sache mit den biometrischen Methoden, da sind wir schon so eindeutig (konvertiert), ich würde sagen, also so der Fingerabdruck, wo man sich da als Verbrecher fühlt, also man gibt irgendwas von sich, weil der Fingerabdruck ist doch einmalig, den hat man nur.

[Personen sprechen gleichzeitig]

Es ist auf jeden Fall ein Vorurteil damit verbunden.

Wenn das eine (patschige) Firma ist, wo da viel passieren kann. Sicher, das ...

Interne Sicherheitstechniken in einem Unternehmen, aber für Fahrscheine, das ist ...

[Personen sprechen gleichzeitig]

Das ist ja da ... steckt ja da drinnen.

[Personen sprechen gleichzeitig]

Das sind ja fiktive Szenarien, das ist ja noch nicht jetzt wirklich ...

Ja, na ja. [Personen sprechen gleichzeitig] Na ja, aber Sie sehen eben, mit was für einem Argument sie das schon geschrieben haben, dass du dann Zeit hast und was passiert. Der Super Check da am Flughafen ja auch, also ...

Ja, man kann die Dinge immer von zwei Seiten sehen. Es hat alles zwei Seiten, Vorteile und Nachteile.

Sehen Sie da Vorteile?

Der Vorteil?

Da bin ich skeptisch, weil es ganz einfach der einmalige Identitätsnachweis ist. Und ich meine, ja, das kann man vielleicht ... Verbrecher können das vielleicht verfälschen, die haben das ja auch schon probiert, also wo es ... habe ich gelesen.

Ja, sowieso.

Dass man das transplantiert dann eben die Fingerabdrücke oder sich die so verfälschen lässt, dass die nicht mehr erkennbar sind. Aber ja, wie weit das wirklich geht, kann ich nichts dazu sagen. Ja, da bin ich dafür ...

Ja, vor allem ist da wirklich die Gefahr des Datenmissbrauchs. Man muss sozusagen wirklich schon an jedem Eck und Ende mit so einem persönlichen Identifikationssignal kommen, dann hat man wirklich mehr oder minder das, was ja ... Und das habe ich den Eindruck, dass es durchaus eine gewollte Entwicklung ist von also öffentlicher Hand oder politisch gewollt ist.

Dass was gewollt ist?

Eben eine möglichst durchgehende Identifikation. Sozusagen der gläserne Bürger möglichst. Und dass es scheibchenweise ja geradezu systematisch betrieben wird. Den Eindruck habe ich schon.

Und wie fühlen Sie sich dabei?

Ich meine, dass das in die Richtung geht, wo in 10 Jahren man sagen muss, Metternich würde vor Neid erblassen. Diese Entwicklung sehe ich. Darum bin ich bei eben so einer anonymen, wo noch nichts passiert ist, dass es innerhalb von 48 Stunden gelöscht wird, halte ich für so eine Videoüberwachung an einer Haltestelle noch für relativ ... ich meine sicher, aber noch relativ eher vertretbar als dass man für jede Kleinigkeit da einen ... sozusagen seine persönliche ... sich persönlich identifizieren muss.

Wenn Sie noch mal an die Szenarien denken, gibt’s da noch irgendetwas, was Ihnen noch in Erinnerung ist, und wie geht es Ihnen damit?

Es sind so viele unterschiedliche Dinge. Wenn ich dann zum Beispiel dieses System in Autos hernehme, wo ich sage, wenn ich einen Unfall habe und es wird sofort ein Signal losgeschickt, man kann mich orten und ich bin irgendwo in Hintertupfing, sage ich jetzt einmal, dann wird es mir wahrscheinlich, wenn ich der Betroffene, sehr angenehm sein, dass dann möglichst schnell jemand da ist. Wenn mein Auto gestohlen worden ist, mir ist schon eins gestohlen worden, wäre ich sehr froh, wenn man jetzt zur Polizei gehen könnte und sagen könnte, bitte einschalten und schaut, wo die sind mit meinem Auto. Das ist immer der Fall, wenn ich ein Betroffener bin. Wenn ich eine betroffene Mutter bin, deren Kind niedergeknüppelt worden ist, bin ich sehr froh, wenn ich sofort eine Information habe, wer war das, wie haben die ausgeschaut und jetzt fange ich an zu suchen. Ich gebe der Dame total Recht und Ihnen auch Recht, das ist ... man ist ... wegen einer Fahrkarte muss ich nicht unbedingt den Abdruck meines Daumens hergeben müssen oder vielleicht in nächster Zeit, bevor ich (??) [21.29] Das ist ...

Bevor Sie einsteigen dürfen. [lacht]

Das ist ...

Wir haben gelacht. Vor 50 Jahren haben wir über so manches gelacht. Und heute ist das ...

[Personen sprechen gleichzeitig]

Das ist ja eben die Diskussion. Es kommen sehr viele Punkte und Aspekte. Wenn sie mir meine Bankomatkarte stehlen und ich meine Bankomatkarte dann ...

Das finde ich für ...

Also dann bin ich auch froh, wenn ...

Ja, genau.

... wenn ich eine Identifikation habe.

Aber ich muss die Wahl haben. Außerdem muss ich die Wahl haben.

Ja, ich glaube, die Freiwilligkeit muss da sein. Ich bin nicht verpflichtet dazu, dass ich das System nutzen muss so wie bei dem Auto.

Ja, das hat ... das ist auch bestimmt richtig.

Dass ich sagen kann, ja, ich schalte das ein oder ich installiere mir das, ich möchte das benutzen, das System. Aber die Freiwilligkeit muss mir als Bürgerin zugestanden werden.

Aber das will der Staat eben nicht. Der will das in jedem Auto haben.

Na ja, ... [Personen sprechen gleichzeitig]

... ein Terrorist ist.

Nein, das ist ... also das mit dem Terrorismus ...

Na, aber Sie haben es ja ...

... das ...

Nein, aber Sie haben ... also das ist aber die Ausrede.

Ja, das ist eine Ausrede.

Das ist ... ja eben. Na ja, für einen normal denkenden Menschen ist ...

Es ist ganz logisch, wenn ich so einen Druck erzeuge, dann kommt der Gegendruck. Sie werden Terrorismus nicht abschaffen können.

Ja, eben.

Mit den ganzen Methoden.

Ja, aber Sie sehen doch ...

Und da darf man nicht vergessen, da steht eine Wirtschaftslobby auch hinter dem Ganzen.

Das wird sich nicht ändern.

Es geht ja jetzt glaube ich auch nicht darum, dass irgendwas abgeschafft ...
one
Oder aufgehalten wird.

Jetzt hat die Geschichte gezeigt, dass weder die Todesstrafe ...

Ja, eben.

[Personen sprechen gleichzeitig]

Es wird so was auch nicht abschrecken.

Nein.

Ich denke mir, was dahinter ist, und das Ganze ist, nehme ich einmal an, darum ist ja das Beispiel auch gekommen, dass das jetzt sehr stark forciert wird seit eben den Vorfällen da in Amerika und dass das von Amerika unheimlich gepuscht wird.

Sowieso.

Und die brauchen das, um ihre Datenbanken zu kommen mit Hilfe von der ... was weiß der Teufel, und darum sitzen wir wahrscheinlich auch da, dass man einmal so vorfühlt, was ...

Na sowieso.

... was halten Sie davon.

Das sehen Sie schon an der Grenze, was da anläuft.

Sie haben es eben angesprochen, nämlich mit diesem Auto, wenn man einen Unfall hat. Welche Vorteile würden Sie noch sehen? Also Vorteile aus Ihrer Sicht

von Sicherheitstechnologien, die da jetzt diskutiert wurden? Jetzt sind wir nur bei den Vorteilen.

[Personen sprechen gleichzeitig]

Na ja, das hat einen Vorteil und Nachteil. Na ja.

Das ist subjektiv.

Wenn das nur für das gebraucht wird. Aber sie suchen ja Menschen auch, die machen ja dann aus dem ... wer da drinnen sitzt, die wollen ja auch wissen, wer da fährt und wer da drinnen sitzt und wenn dann was passiert, sondern auch wollen sie es ja gespeichert haben. Das ist dasselbe bei den Einkaufszentren, wo sie die Karten haben. Das ist dasselbe. Die wollen wissen, was wer wann ...

Ja, im Prinzip können sie alles kontrollieren damit.

Das sind jetzt Nachteile, die Sie nennen. Ich wollte noch mal kurz bei den Vorteilen bleiben. Bei der Überwachung.

Ja, ich denke, beim Handy haben wir gesagt ... da sind in einigen Ausnahmesituationen, wenn ich das ... wenn ich zum Beispiel weiß, ich habe eine Tante oder die Großmutter, die halt nicht mehr heim findet, und oft ...

Gibt’s ja. Das ist ja ...

[Personen sprechen gleichzeitig]

Ich möchte es nicht haben, dass mein Kind weiß, was weiß ich, wenn ich am Klo sitze und was ... ich finde das nicht gut. Aber wenn einer das haben will, schon. Aber die wollen ja dann jedes Handy so machen.

Das ist ... das sind eben diese Grenzfälle. Also sicher, wenn die Frage ist, muss ich die jetzt in eine Pflegeanstalt geben, weil sie sonst nicht mehr ...

Aber ich meine, das kann auch ...

Wenn die nicht mehr nach Hause findet, können Sie sie sowieso nicht mehr daheim allein lassen, weil dann ist jeden Tag ...

Das kommt darauf an, wo.

Na ja.

Und also ich finde, dass einige ... es gibt ... aber das sind immer nur Grenzsituationen, und dass das der Aufhänger ist, dass man sozusagen generell nur deswegen, weil eben manche Notfälle zum Beispiel auch, wenn man einen

Ausflug macht, eine Gebirgstour, ist natürlich, dass man das Glück haben muss, dass dann auch wirklich noch der Empfang da ist. Aber das in so Situationen gibt, wo man also nicht wie bei uns üblich, darum dieses Verkehrsunfallsbeispiel ist sagen wir im normalen Straßenverkehr die Deckungsrate ziemlich groß. Während wenn man halt irgendwo im Gebirge verunglückt unter Umständen ist es ...

Im Wasser, im Gebirge.

Und da kann es ...

Ja, es muss ...

... kann es von Vorteil sein, kann es auch gezielt von dem Träger eingesetzt werden. Aber erstens muss er wissen von der Möglichkeit im Positiven wie im Negativen, und das, was ich schon sehe, dass solche Sachen wie Grenzsituationen als Aufhänger benutzt werden, dass man generell jetzt, wie da das Beispiel, dass offensichtlich ... das weiß die Mutter oder Großmutter gar nicht, was das Handy alles kann, da sagen wir aber haha, denn wir wissen es. Sie ist dort und dort. Aber es gibt die Großmutter die Möglichkeit mit dem Telefon, da hören die auch mit, die sehen es ein, und der ist ja in ein paar Minuten dort und wenn irgendwas ist, wenn der Sohn im Ausland ist und wie es da geschrieben ist, kann der sowieso nicht viel machen. Aber da hat man ein Telefon in einer Pflegezentrale. Und das sind auch Dinge, oder man braucht nur einen Knopf drücken. Also ich finde solche Sachen sind viel besser, weil der ist wirklich gleich da und hilft. Im Gegenteil, eine Person, wenn der irgendwo ist ... Ich finde, solche kosten ein bisschen mehr, das kostet was, aber für so was wäre ich auch.

Wenn man dann eine kompetente Pflegeperson hat.

Ja. Das sind die Pflegefälle, so mit den Heimhilfen und so, die haben so Stationen, und da kriegt er das auf die Uhr so was, und wenn da was passiert und die melden sich nicht, kommt wer in der nächsten Viertelstunde.

Das ist wieder etwas, diese Systeme, die da derzeit sind, sind alle praktisch festnetzgebunden.

Diese Armbänder sind aber mit Funk.

[Personen sprechen gleichzeitig]

Ich meine aber, dass sozusagen ...

[Personen sprechen gleichzeitig]

Ich habe geglaubt, dass das anders ist. Weil die ganzen Systeme sind, wenn man sich in den eigenen vier Wänden aufhält.

Da muss man einen Telefonanschluss haben, dass das funktioniert.

Also es ist zum Teil jetzt schon angesprochen worden. Meine nächste Frage wäre, in welchem der ...

Darf ich noch ganz kurz etwas hinzufügen?

Ja, bitte.

Das, was man heraushört aus der ganzen Geschichte ist, dass sich manche in ihrem demokratischen Denken halt beeinflusst fühlen und irritiert fühlen.

Irritiert, ja.

Auf der anderen Seite denke ich mir, sollte man sich auch nicht so, sage ich jetzt einmal, so wichtig nehmen, zu glauben, dass der Staat den Herrn Meier und den Herrn Müller überwacht. Ich nehme mal an, dass der Staat dort überwacht, wo es notwendig erscheint. Und das ist – und darum ist es ja da auch angeführt – zur Verbrechensbekämpfung. Der will den Herrn Müller nicht überwachen, ob der jetzt zum Billa oder zum Lidl oder zu Merkur geht. Das wird völlig wurscht sein. Und wenn er dann überwacht und sagt, ha, der Herr Meier war beim Lidl, ja, dann war der halt beim Lidl.

Dass mehr oder weniger von staatlicher Seite Daten missbraucht werden.

Das glaube ich nicht.

Also die Verbrechensbekämpfung wäre so ein Bereich, wo Sie sagen, da verzichte ich auf meine Privatheit ein Stück, wenn dafür Verbrechen bekämpft werden.

Ja, und der Verbrecher wird dann im Vorfeld sagen, nein, das mag ich nicht. Ich mag jetzt nicht, dass ich überwacht werde wie der Herr Müller. Und deshalb ist es ja dann auch nicht möglich zu unterscheiden zwischen einem Verbrecher und dem Herrn Müller, sondern es muss dann, wenn ich das selbst von einem gerichtlichen Bescheid habe, muss das möglich sein, dass ich dann hinein komme in das Telefon. Das sind ja die Sicherheitssachen. Der wird sich nicht vorher deklarieren und sagen, hallo, ich bin ein Verbrecher und mich dürft jetzt überwachen.

Aber Verbrechensbekämpfung ist ein Bereich, wo Sie sagen, da nehme ich auch in Kauf, dass meine Privatsphäre ...

Ja, aber ohne dass ich sie jetzt antaste. Wer sagt denn jetzt mir, die es einführen, dass Sie keine – Entschuldigung – jetzt keine Verbrecherin sind.

Ja, genau. Das sehe ich genauso.

Oder Sie oder Sie.

Ja, aber ich bin 76 Jahre alt geworden, aber ohne das ist das ... [Personen sprechen gleichzeitig]

Dass die Technologie eine andere geworden ist.

Aber jetzt kommen ...

[Personen sprechen gleichzeitig]

... kommen die anderen auch so viel dazu, werden in Mitleidenschaft gezogen. Nicht nur die Verbrecher.

In der Schule, wo es früher auch nicht der Fall war.

[Personen sprechen gleichzeitig]

Wo sie die Möglichkeit haben, mit einer Schrotflinte reinzukommen und in die Menge zu schießen, was tue ich dann?

Das ist ja ...

Vielleicht gibt’s auch irgendwann einmal Technologien, die heute jetzt noch nicht eingeführt sind. Aber abzuwarten, bis etwas passiert ist und dann zu sagen, na, das hat sich eh gezeigt, dann sind alle unheimlich gescheit und haben gesagt, ja, das Täterprofil hat ... Das sieht man ja oft, und in Wirklichkeit sind fünf oder sechs Leute niedergeschossen worden. Einen Schmarrn hat es da gegeben. Also noch einmal, mir ist das ein bisschen zur Haut gegangen, wie das Mädchen gekommen ist und mir gesagt hat, ich bin dort allein gegangen und keiner war dort, der geholfen hätte.

Es hilft Ihnen niemand.

Die beiden Burschen mit dem Messer, da schaue ich mir an ...

[Personen sprechen gleichzeitig]

Keiner. Nicht einmal auf der Hauptstraße.

[Personen sprechen gleichzeitig]

Aber was nützt die eingeschaltete Kamera? Wenn es soweit ist? Also das ist ...

[Personen sprechen gleichzeitig]

Zumindest habe ich ... weiß ich, ich werde, wenn ich jetzt dort Täter wäre, habe ich ... muss ich zumindest schon eine Hemmschwelle, eine große Hemmschwelle überwinden, weil ich weiß, ich werde da gefilmt.

[Personen sprechen gleichzeitig]

Ja, schon.

[Personen sprechen gleichzeitig]

Nein, ich glaube das nicht, dass diese Täter eine Hemmschwelle haben. Aber ich bin so generell auch nicht gegen die Überwachung, weil ich mir denke, vielleicht schreckt es den einen oder anderen ab, das ist vielleicht nicht das Schlechteste. Ich denke mir nur ...

Wenn ich nur zwei oder drei von denen ...

Ja, ist es ein Erfolg. Ja, also ich habe prinzipiell nichts gegen Überwachung. Ich finde es auch in der U-Bahn ganz gut, weil wenn man am Abend fährt und wirklich alleine in einem Waggon drin ist und es sitzt hinter mir en Herr, vielleicht nicht so ein Herr, sondern vielleicht ein bisschen ein heruntergekommener Herr, dann habe ich vielleicht auch ganz ein gutes Gefühl, wenn das überwacht wird. Also prinzipiell habe ich nichts gegen überwachen. Nur ich denke mir, gewisse Sachen, die so in die Technologie hineingehen, die sollten vielleicht auch ein bisschen gerichtlich überprüft werden, ob es wirklich so krass ausarten muss oder ob man das alles so haben muss.

Ich möchte noch mal gern umgekehrt fragen.

Die Polizei ist machtlos.

Ich möchte gern umgekehrt noch mal fragen, und zwar, gibt es auch Bereiche Ihrer Privatsphäre, wo Sie sagen, da verzichte ich auf keinen Fall. Da würde ich auf keinen Fall Informationen hergeben. Da war schon das Beispiel vom Fingerabdruck. Vielleicht gibt’s noch andere Bereiche, wo Sie sagen, da ist mir die Privatsphäre viel wichtiger wie meine oder die öffentliche Sicherheit.

Ja, vor allem dieser ganze Bereich, der ja bereits jetzt ausufert, die zum Teil auch Datenverknüpfung und Datentransfer im privaten und im kommerziellen Bereich.

Genau.

Dass da zumindest jeder sich deklarieren muss, wenn er (??) [35.10] anruft und wann er sagt, ich habe Ihre Daten, wenn man nicht selber also die gegeben hat oder was, Sie haben ja uns Ihre Daten geschickt oder ich habe Ihre Daten dort und dort erhalten.

[Personen sprechen gleichzeitig]

Da kann man am lebenden Beispiel hier sehen, wie hier die Daten – außer Ihnen – wie die ...

[Personen sprechen gleichzeitig]

Das läuft aber so.

Das ist so verkauft worden, da gibt’s welche, die kaufen das auf und dann verkaufen sie es wieder.

Über Internet wird dann ...

Es wird immer unübersichtlicher, aber es ist auch so, eben wenn man irgendwann einmal bei irgendeinem Spielchen mitgemacht hat, und dann steht irgendwo ganz klein gedruckt, nicht nur Daten für die eigene Firma und den angeschlossenen Firmen oder des Konzerns oder konzernerweitert, und da ist auch eine PR-Agentur drin und eine Werbeagentur drin, die dann die lustig weiter verkauft. Also in dem Bereich finde ich, wird viel zu wenig gemacht, die Daten zu schützen. Ich habe gar nichts dagegen, dass die Firmen abfragen und sozusagen ein Grundprofil erstellen wollen.

Sie haben nichts dagegen?`

Aber ... Nein. Den Wunsch kann ich durchaus nachvollziehen. Und ich meine, es ist auch sicher bei einigen, wenn man also da Kunde sein will, wird man auch gern sein Wunschprofil hergeben, was man gern hat und was einen ... also wenn irgendwelche Angebote, besondere Neuigkeiten sind, dann auch schicken dürfen. Aber dass da wirklich eine ausufernde Grauzone ist, wo man dann eben ständig vom ... adressiert jetzt wurscht, ob postalisch oder Internet oder was, adressiert wird, benachrichtigt wird und kommen. Ich meine, das übersteigt oft das Gewollte bei weitem um das Zigfache, ohne dass man nachvollziehen kann, wo man das einstellen kann.

Also das waren jetzt so Informationen über Ihre Person. Vielleicht gibt’s andere Meinungen jetzt dazu, ob die Privatsphäre geschützt gehört oder wichtiger ist wie Sicherheitsaspekte?

Im Internet zum Beispiel. Also wenn man Internetbenutzer ist.

Ja, genau, ist auch öffentlich.

Also für mich ist es zum Beispiel undenkbar, ohne das Internet zu arbeiten oder arbeiten zu können. Dass man dort also wesentlich mehr Sicherheit einbaut. Das simpelste Beispiel, obwohl ich alle möglichen Filter installiert habe, sind die täglichen Spams, die reinkommen, obwohl ich nirgends und absolut immer ändere

meinen Code, dass ich das trotzdem kriege. Also dort bewegen wir uns noch, sage ich jetzt einmal, im Neandertal. Dort gehört auf jeden Fall was gemacht. Genauso am Gebiet, wenn ich sage, ich mag es nicht mehr, aber das E-Banking, was da für Kriminalität passiert. Wo noch? Wo kann man das noch ... Es sind so viele Sachen möglich.

[Personen sprechen gleichzeitig]

Mit der Sozialversicherung und jetzt mit der neuen E-Card und so, also da würde ich schon auch eventuelle missbräuchliche Verwendungen vermuten. Das ist mit der E-Card genauso. Sie können genau feststellen, wie oft ist der im Krankenstand oder die, oder was hat die für Leiden, warum geht die zum Arzt, wie oft? Das kann also alles gehen bis ... ja, wenn man das ... Das ist aber auf einer legalen staatlichen Ebene, was sich da abspielt. Also das kann man immer benutzen für irgendwas.

Diese Verknüpfung von personenbezogenen Daten.

Das sind personenbezogene Daten, weil Sie haben ... mit Ihrer Sozialversicherungsnummer sind nur Sie. Das ist sonst niemand. Und das sind genau personenbezogene Daten. Und also da würde ich also eher zurückschrecken als vor einer Kamera, die irgendeine finstere Ecke überwacht. Bei diesen Daten. Weil die wissen dann alles. Es geht bis zum Finanzamt und so. Und da ist es mir persönlich ...

[Personen sprechen gleichzeitig]

Da ist ja schon immer eine, die fragt immer, wenn das Finanzamt oder die Polizei was gesucht hat, haben sie es erst ... obwohl sie es abgestritten hat. Ich weiß es hundertprozentig, immer die Daten hergeben für so manche Sachen. Da würde ich sagen nein. Und die gibt sie heute noch her.

Aber interessanterweise mit diesen ganzen persönlichen Daten, trotzdem funktioniert offenbar irgendwie verschiedene Bereiche des Staats, die er gern kontrollieren möchte, doch nicht so, wie sie es gerne hätten, so wie mit Arbeitslosen, die dazu verdienen und über die Grenzen kommen oder so. Das gelingt ihnen nicht. Oder mit irgendwelchen illegal eingeheimsten Unterstützungen oder Förderung.

Da können sie nicht ...

Na ja, aber auch so, sie könne auch verschiedene Sachen nicht so wirklich kontrollieren. Also das ist irgendwie ...

Nicht alle Daten sind verknüpft.

Ja, offenbar nicht. Aber ... oder man kann es noch nicht wirklich nutzen. Aber das kann ja noch kommen. Ich meine, solange eine Demokratie funktioniert und wir in so einer Demokratie leben, ich meine, das ist alles ...

Das ist keine Frage der Demokratie, sondern dass dabei sehr verschiedene Systeme benutzt werden und daher die Verknüpfung nicht so einfach ist.

Ich würde schon annehmen, dass in einer Demokratie ...

Demokratie war jetzt das Stichwort. Ich habe folgendes Problem. Wir haben noch 10 Minuten und noch vier Fragen, wobei man die wahrscheinlich etwas schneller beantworten kann. Vielleicht können wir eine Runde machen. Die erste ist eine demokratiepolitische Frage, nämlich wer sollte beteiligt sein, wenn solche Technologien eingeführt werden und es darum geht, was dürfen sie, was dürfen sie nicht. Also die Frage, die halt auch diskutiert wird, wenn es um die Beteiligung geht. Vielleicht können wir eine Runde machen, dass jeder kurz sagt, wie er sich das vorstellt.

Darf ich anfangen?

Ja, bitte fangen Sie an.

Dass es anders läuft, wie Sie jetzt gefragt haben, habe ich beim Herfahren gehört. Also ich habe vorhin das Autoradio an gehabt und da ist heute beschlossen worden, dass zum Beispiel so dieses E-Controlling und das Abhören ... das war um 17.30 Uhr in Ö3, dass da eben heute eine große Entscheidung gefallen ist. Also ...

Meine Frage war, wer sollte aus Ihrer Sicht gefragt werden, wer soll beteiligt sein bei solchen Entscheidungen.

Na ja, da kann man nur die Regierung sagen, aber die Regierung ist heute so selbstherrlich, dass die aufs Volk nicht mehr eingeht. Was ihnen zusagt und was ihnen die Industrie vorgibt, das wird gemacht. Und ob das ein Volksbegehren ist, interessiert die gar nicht.

Sie sagen, die Regierung soll entscheiden, aber Sie sind nicht zufrieden?

Ja, darum wähle ich sie ja. Die sollen dann halt fragen das Volk, soll man das einführen? Kann ja fragen, so wie es in der Schweiz ist. Nichts Unnötiges, aber das sind unsere ... aber die sind so selbstherrlich, dass sie sagen ... Also was ... Die Herren oben und sonst nichts.

Können wir die Runde vielleicht fertig machen?

Na ja, primär kann ich mir vorstellen, geht es nur über die Regierung. Aber ich habe auch Bedenken dabei, weil ich wähle zwar eine Partei, aber ich wähle nicht solche Entschlüsse. Das ist ein kleines Mosaiksteinchen in einer bestimmten

Legislaturperiode. So was. Und das kann durchaus sein, dass ich jetzt die oder jene Partei wähle, aber mit dem Beschluss nicht einverstanden bin.

Ja, genau.

Also da gehören viel mehr Ebenen dazu, basisdemokratische Maßnahmen, Gesetzt, also bei solchen Sachen, wo es in meine Privatsphäre reingehen kann, da muss auf jeden Fall ich auch gefragt werden, egal mit welchen Maßnahmen. Und es kann nicht so sein, dass über meinen Kopf hinweg entschieden wird. Und das wird glaube ich, da gebe ich Ihnen Recht, das wird schon sehr wohl gemacht. Und ich glaube auch, dass das bereits sehr stark gemacht wird. Aber das ist eben die Meinung, nicht der Herr Meier oder sonst was, sondern bei so genannten verdächtigen Personen, wird das sicher schon sehr lange und sehr intensiv gemacht. Und wenn jemand verdächtig ist, dann hat derjenige, der was wissen will über den Verdächtigen, alle Daten, die er haben will.

Ja, sowieso.

Danke. Ich würde gern die Runde fertig machen mit der Frage. Wer soll beteiligt werden, wenn das entschieden wird.

[Eine Person verlässt den Raum]

Ich glaube, es sollten verschiedene Gremien ausgewählt werden, wo man sich ein bisschen verlassen kann, dass diese Menschen auch, wie soll ich sagen? Ein bisschen ein Nachdenken beschäftigt. Also die nicht nur dafür sind und sagen, ja, alles klar, machen wir es. Sondern die hergehen und das Für und Wider sehr gut abwägen. Also ich würde das nicht so unbedingt gleich freigeben. Ich würde auf jeden Fall zuerst einmal Widerstand bieten, damit man einmal auslotet, was ist jetzt wie effizient oder was kommt überhaupt richtig hin, dass man es auch brauchen kann. Und dann ... ja, kann man sich ja dafür entscheiden. Aber man sollte Widerstand leisten.

Welche Gremien würden Sie sagen?

Na ja, zum Beispiel, was weiß ich, bei der Überwachung immer richterliche Beschlüsse einholen. Also dass nicht einfach irgendjemand jetzt frei Haus überwacht werden kann.

Und aufklären.

Sondern dass man wirklich ...

Wie so was funktioniert und warum das gemacht wird, richtig aufklären, nicht nur so ...

Und auch, es ist immer so ein zweischneidiges Schwert. Weil es wird immer welche geben, denen man genug Angst gemacht hat, dass sie dann einfach dafür sind. Aber ich glaube, wenn es eine gewisse, weiß ich nicht, gewisse Menschen, die ein bisschen was davon verstehen, ein bisschen nachdenken und dann eben einen Widerstand spüren, dann müssen sie irgendwie das Ganze verbessern und ...

Und die ...

Wir haben noch 10 Minuten.

Ja, in 10 Minuten soll es dann dem Ende zugehen. Danke.

Ja, also ich würde sagen, im Rahmen einer Rechtsstaatlichkeit muss das Ganze abgehandelt werden, natürlich steht es den Bürgern immer frei, in einer Demokratie ihren Protest kundzutun bzw. dass man eben auch basisdemokratische oder direktdemokratische Dinge anspricht, sie Volksbegehren etc., und eben politische Parteien dazu auch benutzt jetzt unter Anführungszeichen, das eben durchzubringen. Da wäre vielleicht auch zu überlegen, einen verfassungsrechtlichen Schutz da einzubauen, dass das in der Verfassung drin ist, in der österreichischen, und ansonsten würde ich also schon, auch wenn viele Lücken und Schwachstellen in unserer Demokratie sind, schon dafür plädieren, dass man auf die Demokratie oder die demokratische Ordnung vertrauen kann und ... ja, und die Instrumente nutzt, die es in der Demokratie gibt.

Ich bin nur einerseits dafür, dass da wirklich verbindliche basisdemokratische mit einer entsprechenden öffentlichen Diskussion ... Es kommt natürlich jetzt auch immer darauf an, welche Bereiche und was. Sagen wir so, auf jeden Fall die den ... die Teile der Bevölkerung, die hauptbetroffen sind. Das heißt Videokamera, ich finde, es muss nicht in ganz Österreich eine Volksabstimmung erfolgen, wenn an irgendeiner Stelle so was montiert wird. Aber unter welchen Bedingungen so was montiert werden kann im Prinzip. Was sozusagen, wenn man so will, die Verfahrensweise ist, nach der man da die Kriterien setzt, das fände ich wäre wichtig. Und es wäre wichtig, eine lokal basisdemokratische Dings für ... die in dem Fall Anrainer oder wenn es um spezielle Internetnutzungsfragen geht, um das betroffene Hauptklientel. Mit dem Für und Wider. Und da sollten natürlich schon auch ... es ist nur halt die Gefahr, dass die, die es einführen wollen, und vor allem, wenn es um technische Konstruktionen geht, sitzen dort natürlich auch die Fachleute. Die aber nicht unabhängig argumentieren können dürfen.

Ja, es gibt aber schon ... Wieso, es gibt genug Professoren, die unabhängig sind, die nicht für die Firmen ...

Ja, nein, es ist ...

Aufzeigen, das und das kann passieren oder das und das wird passieren.

Gerade in diesen Technologien habe ich den Eindruck, dass da oft die also konstruierten ... die Firmen, die also wirklich mit Innovationen und in dem Fall habe ich jetzt nicht das Recht zu sagen, die Technologien, auch die schon alteingefahrenen und alteingesessenen und Alttechnologien. Und da ist es in der Durchführung dann doch sehr oft, dass man sozusagen unabhängige echte Fachkräfte gar nicht so leicht kriegt, weil das eben in erster Linie innerhalb von Firmen weiter entwickelt wird und selbst wenn dann ein unabhängiger Professor mal die Basis geliefert hat von diesem Wissen, hat er sozusagen ... Darum finde ich, ist das immer ein kritischer Punkt, wie kann man das auf sachlicher Ebene überhaupt ... das Für und Wider, noch dazu dann Laien klar machen.

Ich würde gern einmal bei den Sicherheitstechnologien bleiben. Haben Sie jetzt im Zuge der Auseinandersetzung konkrete Vorschläge für die Regulierung solcher Technologien? Ist Ihnen was eingefallen? Hat sich was aufgetan?

Wie meinen Sie das?

Wie wir jetzt auch diskutiert haben, was müsste sein, unter welchen Bedingungen würden Sie dem zustimmen? Also relativ konkrete Vorschläge. Sie haben ein Beispiel genannt mit der Videokamera irgendwo in einem Park, dass man da ...

Na ja, das haben wir eigentlich eh, für das sind wir ja. Das ist, finde ich, für alle da. Aber für so manche Sachen eben nicht. Aber das ist Ansichtssache halt auch.

Ich meine, es ist zum Beispiel so, wo es um sicherheitsfördernde Technologien gegangen ist, weil schon das nicht unter dem Vorwand, dass ... weil das auch von Verbrechern missbraucht werden kann, sondern der Allgemeinheit diese Technologien zur Verfügung stellt. Dass umgekehrt dann in speziellen Fällen, und das ist eben noch immer, gewisse Entschlüsselungscodes ... aber das wird ja sowieso ...

Na ja, das ist ...

... gemacht. Es ist sicher etwas komplizierter, weil man genau das gleiche da hat, aber es gibt ja Wege, trotzdem an Informationen heranzukommen.

Die Frage noch einmal, diese Regulierungsfrage. Gibt es irgendeinen Bereich, wo Sie sagen, das sollte verboten sein? Das sollte man nicht entwickeln dürfen oder da sollte man gar nicht weiter auch Geld in die Entwicklung stecken. In all diese Bereiche, die wir da diskutiert haben.

Also diese Durchleuchtungsmaschinen finde ich sehr bedenklich auch vom gesundheitlichen Aspekt her. Mit welchen Strahlen man da arbeitet, also alle Durchleuchtungstechniken sind mit Röntgenstrahlen oder sonstigen nicht gerade gesunden Dingen. Also das würde ich gesundheitsbedenklich ... also gesundheitlich äußerst bedenklich finden und das lehne ich also rigoros ab. Ich

persönlich. Außerdem durchleuchten, durch den Körper durchzugehen, das ist ethisch auch schon sehr bedenklich.

Dass der mit dem Detektor ...

Detektor ist okay. Dass man ...

[Personen sprechen gleichzeitig]

Aber wie wir es jetzt derzeit haben, dass man ganz einfach am Flughafen ... ja, das sehe ich alles ein. Wir wollen auch entsprechende Abstriche machen. Aber ...

Also das Problematische sind die Strahlen?

Also dieser gesundheitliche Aspekt.

Ja, wenn das jetzt kein Problem wäre, wenn das ganz ungefährlich ist, wäre es dann auch ...

Das kann ich mir nicht vorstellen. Die Strahlen ...

[Personen sprechen gleichzeitig]

Das kann ich mir physikalisch nicht vorstellen, ich bitte um Entschuldigung, aber ... [lacht]

Ich finde, das ist ein ganz wichtiger Aspekt. Nämlich es geht ja nicht darum, dass der gesundheitliche Aspekt viel zu wenig berücksichtigt wird, und zwar die Langzeit und die Intensität. Es sind natürlich irgendwelche elektromagnetische Felder, die da aufgebaut werden.

[Personen sprechen gleichzeitig]

Aber dass die zunehmen und weil man da ständig jetzt, wie es schon ist, ständig sozusagen durch solche Strahlen und Polungen durchgeht, und die ständig am Körper hat ...

Also Sicherheitstechnologien dürfen nicht die persönliche Gesundheit beeinträchtigen.

Ja, also denke ich schon. Zumindest ist es ... viel zu wenig wird das derzeit eindeutig heruntergespielt.

Ja, muss ich Ihnen beipflichten.

Nämlich vor allem mit der Intensität, in der sich der Gebrauch entwickelt hat. Ich glaube nicht, dass das jetzt akut hoch gefährliche Dinge sind. Aber dieses ständige ...

Gibt es sonst noch etwas, wo Sie sagen, das dürfte eigentlich nicht sein? Das gehört eingeschränkt, verboten? Gibt es noch andere Bereiche? Das war die Gesundheit.

Also gesundheitliche Aspekte sicher.

Die wollen ja das auch (vom Schweiß) [55.40] und was sie alles noch machen, also ich finde das ist auch ... das gehört auch nicht.

Was will man damit erreichen? Angst oder Nervosität zu messen. Oder wie?

[Personen sprechen gleichzeitig]

Also das ist auch etwas.

Das auch.

Geht auch in die persönliche Sache hinein.

Ja, genau.

Und das würde ich auch ...

[Personen sprechen gleichzeitig]

Und nicht zuletzt, weil ich da ziemlich überzeugt bin, die ganzen Nervositätsmessungen und so weiter, dass da die Fehlinformationen weitaus größer sind.

Eben, bei Flugangst.

Das obendrein.

Also auf jeden Fall, wenn überhaupt sozusagen diskutabel, dann eine genau Ab-... schon eine sehr ernsthafte Abwägung in der Verhältnismäßigkeit, welcher Eingriff ist das und was kann ich mir erwarten.

Ist gar nicht notwendig. Die haben eh so viel Daten, dass sie das auch noch brauchen. Gar so ...

Ja, eben, zum Beispiel das. Und dass man also auf konventionellen ... jetzt habe ich schon den Eindruck, dass in vielen ... dass halt immer so eine neue Welle das fast eine Modewelle geworden ist und dass man da neu entwickelt und sich gar

nicht besinnt, was bringt das wirklich gegenüber weniger invasiven, gegenüber weniger kritischen Methoden für Vorteile, ganz abgesehen von den Kosten, aber auch direkt in der Wirksamkeit für Vorteile und natürlich auch ... also eine sehr sorgfältige Abwägung der verschiedenen Aspekte, wo ich den Eindruck habe, dass momentan man halt etwas auf der Modewelle reitet und daher ... und natürlich auch große Interessen dahinter sind, die ich meine naturgemäß alles, was ihnen im Weg steht, herunterspielen. Und ...

Ich muss ein bisschen auf unsere Zeit schauen. Ich würde gern mit ihnen weiter diskutieren, das ist ganz spannend. Wir haben noch zwei Fragen und wir sind schon über der Zeit. Die eine Frage kann man vielleicht in einer Runde machen. Das ist nämlich jetzt ganz was anderes. Nämlich ob die Teilnahme, Ihre Teilnahme an der Veranstaltung heute Ihre Haltung zur Sicherheit, zu diesem Thema Sicherheitstechnologie / Privatsphäre in irgendeiner Weise beeinflusst hat und wenn ja, dann würde ich kurz ... würde es mich interessieren, inwiefern.

Also mich hat das schon beeinflusst, weil ich vorher eigentlich nicht wirklich darüber nachgedacht habe, ich habe mich eigentlich nicht beeinträchtigt gefühlt durch diese Überwachung. Aber wenn man das so ganz im Detail betrachtet, dann denkt man sich doch ein bisschen was dabei. Und also so ganz egal ist es mir nicht.

Wie ist es bei Ihnen?

Ja, also bei mir ist mein Standpunkt klar. Ich habe den schon vorher gehabt. Also ich habe jetzt keine neuen Erkenntnisse bezogen oder so. Ja, vielleicht bisschen was daraus gelesen jetzt mit dem AutoCall, das wusste ich nicht alles. Aber ich meine jetzt so rein vom Technischen habe ich ein paar Erkenntnisse bezogen aus den Unterlagen. Aber meinen Standpunkt hatte ich vorher schon.

Wie ist es bei Ihnen?

Ich glaube nicht, dass sich mein Standpunkt verändert hat. Aber sicher ist etwas, also ich habe mich glaube ich bisher nie über so einen Zeitraum gedanklich damit beschäftigt. Ich habe immer nur ... das ist immer sozusagen quasi nebenher gelaufen, so blitzlichtartmäßig, aber dass ich sozusagen darüber ein paar Stunden mich ausschließlich damit beschäftigt habe, das nicht.

Und bei Ihnen?

Ja, mich hat das schon immer interessiert und ich habe da immer diskutiert mit Jungen und so, wisst ihr das? Es ist gut, aber ich habe da meinen Standpunkt. Und wie gesagt, das ist variabel. Karlsplatz oder so, wie der Herr gesagt hat, bei dem Schulweg, ohne Weiteres da, wenn es keine Polizei gibt, wo ich immer glaube, die Polizei wäre besser als das, aber wenn es die nicht gibt, ist die Videokamera ... Nur wissen Sie, der Widersinn. Die Kamera, es muss ja einer beim Fernsehen sitzen,

sonst bringt ja das nichts, wenn da keiner da sitzt, keiner beim Bildschirm, bringt ja das nicht viel.

Aber da gibt's ja schon Systeme, die das kontrollieren.

Wieso können sie dann nicht einen richtigen Menschen da nehmen?

Ja, wir werden das aufnehmen und es ...

Verstehen Sie das? Wie gesagt, wenn die präsent sind, ist das ganz ein anderes Gefühl.

Na ja, man wollte ja die Polizei reduzieren auf der Straße. Wir haben in unserer Geschichte da viele Negativbeispiele, was Polizei bedeutet auf der Straße.

Ja, ist klar. Aber ...

In der österreichischen Geschichte.

... Sie kennen, wir haben in der Polizei sowieso so viele (Blaue) [1.01.03] drinnen, dass das sowieso nicht länger diskutieren können, wir haben den, wir haben es gemacht, wir haben und wir werden es weiter haben. Aber das hat mir der Straße im Verhältnis, wenn die gut ausgebildet sind, nichts zu tun. Weil der ist dann eben nur für die Straße und für die Menschen, der muss aber ausgebildet dafür sein. Ich weiß nicht, aber wie gesagt, wir haben ein Sicherheitsgefühl gehabt und das war so für unsere Eltern auch, weil wir gewusst haben, der geht mit und tut und dann und dann, der ist immer präsent.

Ich glaube, das Argument ist jetzt sehr klar. Sie haben es vorher gut ausgeführt, dass Sie das besser finden würden.

Ja.

Noch eben diese eine Frage, und das ist eine offene Frage, ob es noch etwas gibt, was Ihnen wichtig ist, was nicht angesprochen worden ist.

Das eine finde ich noch, da ist ein Beispiel drin, in Amerika, wie sie ihm die Identität gestohlen haben. Dass der erst nach Monaten zugegeben haben, dass es das gibt, was die Menschen in der Zeit ... was die mitgemacht haben. Bis das die angenommen worden sind, dass das der, der und der Mensch ist. Das finde ich einen Horror. Dass man da sofort, wenn man das angibt, zur Polizei geht oder sagt, mir ist das und das passiert, dass das sofort kontrolliert wird, ob das stimmt und ob das wahr ist. Aber dass der dann die Bestätigung kriegt, der ist es. Und nicht, dass er monatelang kein Geld nicht kriegt und so ...

[Personen sprechen gleichzeitig]

Das ist die Trägheit der Systeme, der Verwaltungsapparat.

Und das ist aber das Wichtigste für den Menschen.

Haben Sie noch was? Weil wir werden rausgeworfen um halb zehn. Haben Sie noch was, was Ihnen ganz wichtig ist? Wo Sie sagen, das haben wir nicht diskutiert oder das wollen Sie noch sagen am Schluss.

Ja, eigentlich nur, was zur Sprache kommt bei all den Systemen, eben auch die Definition, sozusagen was ist ein Terrorist? Um damit schon auch, wer bestimmt, wann und gegen wen das eingesetzt werden kann. Denn ich meine, es sind immer wieder oder auch in der Nachbarschaft, und auch in unserer, es passiert sehr leicht, dass das eine politische Motivation kriegt und sozusagen dass jeder, der also nicht konform mit der Machthaberschaft ist, dann geoutet wird und das, ich glaube, das ist – wie der Herr auch sagt – der Herr Meier und der Herr Müller nicht, aber wodurch wird er auffällig? Ja.

In Amerika, USA, hat es ja gereicht, arabischer Herkunft zu sein.

Genau.

Nach 9-11, ne? Oder?

Zum Beispiel.

Und wie war das in London mit der U-Bahn, mit der Underground, wie da der Anschlag war, da hat man doch einen Mann erschossen, weil die dachten, von den Kameraufnahmen, das ist ein Verdächtiger und ... ja, also das sind Mutmaßungen, irgendwelche Vorurteile. Es sind Zuschreibungen, die passieren, aber ich meine, die Dinge ...

Aber Entschuldigung, heute oder gestern, was habe ich wieder gelesen? Weil der gesagt hat, der Wagen, den der oder ... da sind sie gleich in zwei Wohnungen und weil die dritte nicht aufgegangen ist, haben sie die eingebrochen, haben aufgebrochen, haben gar nicht gewusst warum. Nur weil da einer gesagt hat, das ... Na ja, aber wenn das wirklich ein Terrorist ist, der sowieso überwacht wird in der Wohnung, ein Nachbar dort, der seine Wohnung hin hat.

[Personen sprechen gleichzeitig]

Ich glaube, wir könnten sicher noch eine Stunde diskutieren.

[Personen sprechen gleichzeitig]

15 Minuten haben wir noch. Es gibt auch noch was zu Essen.

Ja, dann müssen wir ...

Sie müssen ganz schnell ...

[Personen sprechen gleichzeitig]

Es ist zwar über Regelmaßnahmen ... und dass geredet werden muss, wann so was eingesetzt wird und welche ... aber wie wird das kontrolliert? Wer kontrolliert das?

[Personen sprechen gleichzeitig]

Darf ich Sie einladen weiter zu diskutieren am Buffet? Wir müssen jetzt da raus. Vielen Dank für die Teilnahme, vielen Dank für die Beträge. Kommen Sie gut nach Hause. Wir sehen uns noch beim Buffet. Vielen Dank.

[Ende]

5.2 Johannessaal[2]

Was sind Ihre spontanen Gedanken über Sicherheitstechnologie und Privatsphäre? Das ist unsere Einstiegsfrage.

Spontan, wo ich diese negative Erfahrung aus dem Bekanntenkreis kenne, weil ich meinen Mann, der Computerfachmann ist und sich damit auskennt, einiges genauer weiß und daher also prinzipiell auch weiß, wie leicht diese Technologien unterlaufen werden können. Also mein spontaner Gedanke ist, fangen werden sie mit solchen Technologien diejenigen, die nichts gemacht haben und diejenigen, die man sucht, Terroristen, die immer an erster Stelle bei den Fragen gestanden sind, Verbrecher, die haben genügend Möglichkeiten, das zu unterlaufen. Also die würde man genau damit nicht fangen. Also es ist so spontan und generell mein erster Gedanke.

Also ich sehr unbelastet, auch durchaus interessiert, aber doch mit einer gewissen Grenze, also dass doch nicht alles immer beachtet wird. Ich würde schon sagen, bei Großveranstaltungen und verschiedenen Plätzen durchaus, aber sich nicht für Bahnkarten oder Straßenbahn und so weiter, also das sollte doch eher im Privaten bleiben. Das würde ich nicht wollen. Also das nicht.

[Mann, in beiden Aufnahmen nicht zu verstehen] Videoüberwachung und so weiter einsetzt. (??)

Also grundsätzlich finde ich das gut, wenn man in U-Bahn-Stationen zum Beispiel einen Vertreter hätte, (??), aber da hört es dann auch irgendwo auf. Also wenn es darum geht, die Sicherheitstechnologie, die Sicherheit von Menschen unterstützt, ist es zu keinen Unfällen oder Tötungen oder wie auch immer kommt, finde ich das in Ordnung für mich auch. Es geht niemanden was an, wann ich wo bin etc. Das geht niemanden was an.

Gut. Da haben wir sozusagen den Rahmen einmal abgesteckt. Jetzt haben Sie alle diese Szenarien im Vorfeld gelesen. Sind die für Sie ausgewogen gewesen? Was sagen Sie zu den Szenarien? Hat das sozusagen Ihre Gedanken zu dem beeinflusst? Angeregt?

Durchaus schon angeregt oder darüber nachgedacht im weitesten Sinn, weil ich nicht sehr viel reise. Also mit diesen ganzen Überprüfungen weniger zu tun, aber doch zum Beispiel mehr darüber nachgedacht, was es geben könnte, was mich schon irgendwie auch ... diese vielen Untersuchungen, ob die nicht auch gesundheitsschädlich sind. Also wenn jemand fliegt, der ununterbrochen

[2] [Die meisten ?? treten auf, wenn ein Mann spricht, alle anderen sind gut zu verstehen, er leider fast gar nicht]

möglicherweise mit Röntgen oder was auch immer in Verbindung kommt, also würde ich dann schon irgendwo das ein bisschen hinterfragen.

Ich glaube, die Schwierigkeit besteht darin, dass hier durch den internationalen Terrorismus (??) irgendwann einmal etwas passieren wird. Also werden Probleme entstehen, wo immer auch hier, intensiver oder auch weniger intensiver. (??) ohne konkrete Hinweise (??).

Wir müssen nicht immer die Runde durchmachen, sondern ...

Ich würde auch prinzipiell sagen, eine absolute Sicherheit gibt es nicht. Also dieses, dass wir uns völlig absichern und alles verhindern im Vorfeld schon, das gibt es nicht. Oder dann stellen wir jeden unter einen Betonsturz, jeden einzelnen Menschen, oder am besten, man bringt gleich alle Leute um, das ist am allersichersten. Ich bin da ein bisschen zynisch.

Ja, dass es sehr schwierig ist, das jetzt im Vorhinein irgendwie (??).

Eben, ganz genau.

Nein, da ist keine Lösung.

Da geben wir wirklich unsere Freiheit auf.

Es wird immer Situationen geben, wo dann die Polizei oder CIA oder was immer helfen kann. Mit den Videoaufzeichnungen und so weiter, dass die dann möglicherweise (??) Aber es werden wahrscheinlich mehr gute Menschen unter Anführungszeichen auf dem Videoband sein als Terroristen. Deswegen bin ich da (nicht dafür).

Obwohl ich nicht besonders ... obwohl es mich nicht besonders stört, wenn ich da irgendwo drauf bin. Ich habe damit kein Problem, sagen wir mal so.

Die Videoüberwachung ist ja vielleicht noch das Harmloseste, weil in dem Moment finde ich, wo ich mich in der Öffentlichkeit bewege, bin ich eigentlich nicht mehr privat. Also insofern ist das weniger Verletzung der Privatsphäre wie wenn vor allem also verschiedenste Daten verknüpft werden miteinander. Weil dann wird es gefährlich, wenn man dann überlegt, na ja, dann kommt die nächste Krankenversicherung und sagt: Sie haben dort und dort Zigaretten gekauft und Sie haben das und das eingekauft und Ähnliches, und Sie waren da und Sie haben ... Und plötzlich ... Und Sie kriegen eine höhere Prämie, die Sie bezahlen müssen, oder wir nehmen Sie nicht mehr. Und Ähnliches. Also da finde ich, da geht es wirklich ... da besteht die Möglichkeit so stark, dass die persönliche Freiheit eingeschränkt wird, das ist eigentlich es für mich ein Horrorszenarium, dieses Verbinden.

Ich finde, dass man ohne konkrete Hinweise solche (?) oder solche Videobänder (??). [längere Passage unverständlich] ... dienlich ist, das solle man auswerten. (??)

Das heißt, es überwiegt bei Ihnen in der Gruppe eher so die Angst vor den negativen Effekten der Überwachung, wenn ich mir die Statements so anhöre. Gibt es was, wo Sie sozusagen die positiven Potenziale irgendwie finden, wo Sie sagen, okay, dafür schon oder dafür zahlt es sich auf, dafür darauf zu verzichten? Oder was wäre eine Anwendung, wo Sie sagen okay, das geht schon? Oder das geht schon. Also sehen Sie irgendwo ...

Na ja, ich denke mal schon, wenn es wirklich um Verbrechen geht oder zum Beispiel gerade bei Kindern oder wo man dann schon mit dem genetischen Abdruck so die Täter doch relativ schnell findet unter Umständen, und das ist doch sehr oft der Fall, und ich denke mir, da gibt's schon große Erfolge, was man nicht unterschätzen soll, was trotzdem auch wichtig ist.

Das ist aber Fahndung im Nachhinein.

Na ja, im Nachhinein. Ja.

Das ist nicht ...

Nicht vorher.

... präventiv. Ja, also das glaube ich muss man auseinander halten. Aber natürlich, Fahndungserfolge gibt's.

Aber ich könnte ja da anknüpfen und eine provokante Frage stellen. Wie ist es bei einem verurteilten Straftäter, also Sexualstraftäter, der seine Strafe abgesessen hat, wieder freigelassen wird, und dessen Adresse jetzt im Internet bekannt gegeben wird oder dessen Adresse im Bezirk, wo er dann wohnt, bekannt gegeben wird. Sozusagen um zu verhindern, dass er wieder Straftaten begehen kann. Ja oder nein?

Na ja, das ist natürlich schon ein Punkt, gerade bei den Sexualstraftätern, da sieht man schon, dass das einfach ein Problem ist, das durchaus strenger behandelt werden sollte. Bin ich schon der Meinung.

Wo soll der dann wohnen?

Ja, das weiß ich nicht, das ist dann nach dem Dings ...

In Amerika läuft das so. In Amerika läuft das schon so. Und es gibt bei uns auch Stimmen, die das gerne hätten.

Aber wenn Sie jetzt eine Tochter hätten, dass die ... und man ... es gibt ja sehr, sehr viele Wiederholungstäter. Das muss man schon sagen.

Das ist völlig richtig. Ich habe ja auch mehr provokant gefragt. Aber man muss sich dann die Frage stellen. Tut man das oder ...

Aber vielleicht würde das schon verhindern, dass sich der wirklich irgendwo ... ich meine, ob das jetzt wirklich jetzt so weit geht, dass es [Tonstörung] aber er sollte zumindest nachweislich kontrolliert werden. Also da wäre ich schon dafür.

Also diese anonymen Telefon (??), wie will man das überprüfen? (??) wenn der telefoniert, wie soll man das überprüfen?

Kann man nicht.

Also es gibt Länder, wo man sich jetzt beim Kauf der Karte registrieren muss.

[Personen sprechen gleichzeitig]

(??) Bankgeheimnis und jetzt muss man (??) Aber wie wollen Sie das (??). Und kein Mensch weiß, wer das gekauft hat.

Und wer es verwendet natürlich.

(??) kein Mensch weiß, wer es ist.

[Personen sprechen gleichzeitig]

(??)

Je dichter das Netz ist, umso teurer wird die Wertkarte. Gut. Wann glauben Sie, dass Sicherheit wichtiger ist als Privatsphäre und wann umgekehrt? Kann man das überhaupt so sagen?

Gar nicht.

Ich glaube nicht, dass man das wirklich sagen kann. Ich hoffe nicht, dass sich die Welt so schnell entwickelt.

Ich glaube, es geht uns auch teilweise viel zu gut, um das wirklich beurteilen zu können. Also ich wohne im (??) wo das Auto meines Mannes (??) du fährst jetzt in die Straße (??) einsteigen. Also ich finde es einfach idiotisch. Aber da müsste man die ganze Zeit (??). Ich glaube, wir leben auf einer Insel der Seligen und haben daher wahrscheinlich noch gar nicht so die Übung. Wir wurden Gott sei Dank schon (??) Großereignisse. Wir waren Zuschauer, okay, aber (??) oder in Österreich.

Eine Idee ist, haben Sie Angst vor der Europameisterschaft? Das ist ein Großereignis. Das wäre so was, wo man sagen kann ...

Nein, Angst nicht, aber ich hoffe, dass es halbwegs in Bahnen verläuft.

Ja, das wird schon bisschen chaotisch werden, aber ...

Aber wäre das für Sie ein Grund, sozusagen an der Sicherheitsschraube zu drehen?

Nein.

Weil dann halt viele Menschen kommen.

Nein, es ist für mich prinzipiell nicht, weil das ist keine Alternative, weil Privatsphäre hat mit meinem freien Willen, mit meiner freien Entscheidung zu tun. Und in dem Moment, wo ich einen Teil Privatsphäre aufgebe, gebe ich einen Teil Entscheidungen auf, meinen Willen auf, und das bin ich nicht bereit, da nehme ich lieber mehr Risiko in Kauf. Wie ich am Anfang gesagt habe, das Leben ist nun mal lebensgefährlich. Man kann nicht alles absichern. Da will ich lieber meine freie Entscheidung.

(??) durchsetzen sollte mit der Überprüfung (??) ziemlich stark, dass die jederzeit wissen, wo ich fahre und wann ich fahre.

Kommt überhaupt nicht in Frage.

Und automatisch (??). Also das finde ich ganz (??).

Aber ...

(??) nach Deutschland fahren, 250, dann muss man (??), ohne diese (??).

Aber wie stehen Sie genau dazu, genau das System im Auto bietet jetzt zum Beispiel eine Versicherung an, dass man das freiwillig machen kann. Unter der sozusagen Überschrift, wer wenig fährt, soll wenig zahlen, weil er wenig Risiko generiert. Und dazu braucht man diese Technologie im Auto. Und das machen manche Menschen freiwillig.

Und dann werden sie merken, wofür das noch benützt wird. [lacht]

(??) Man sollte sich dieses System (??) mindestens, weiß ich nicht, 20, 30 Stunden (??) Wenn ich Hilfe brauche, bewusstlos bin und dann (??). Aber das wäre schon die einzige Ausnahme.

[Personen sprechen gleichzeitig]

Okay, genau.

Oder man fährt einfach zu langsam, das gibt’s genauso.

Die sind vielleicht nicht unbedingt ein Sicherheitsrisiko, die sind dafür unroutiniert beim Fahren. Also was soll das?

Gut. Wer sollte aus Ihrer Sicht beteiligt sein, wenn darüber entschieden wird, wann Sicherheitstechnologien eingesetzt werden? Also ist das sozusagen eine Frage, die einfach in der Wirtschaft entschieden wird? Ist das eine politische Frage? Ist das eine Frage für die Öffentlichkeit? Weil es gibt unterschiedliche Interessengruppen. Es gibt sozusagen ein wirtschaftliches Herstellen, es gibt die Politik, die Sicherheit verkauft, oder auch die Grundrechte verkauft. Es gibt NGOs, die sich um die Grundrechte bemühen. Es gibt Bürgerinnen und Bürger wie Sie, also wer sollte das sozusagen bei einer großen Änderung oder bei Einführung solcher Systeme beteiligt sein?

Möglichst viele.

Nicht einzelne Interessengruppen.

Nein. Also ganz sicherlich nicht, weil die eben nur speziell ihre Interessen durchzubringen.

Haben Sie irgendwelche Vorschläge für die Regulierung der Entwicklung und der Einführung solcher Technologien? Das heißt, sollte man irgendwelche Beschränkungen sich überlegen? Also was Sie meinen aus Ihrer Sicht, ist absolut ein No-No, oder sollten wir irgendwelche bestehenden Regelungen verschärfen oder geht das sozusagen seinen demokratischen Gang in unserer parlamentarischen Demokratie?

Also ich denke mir, es müsste grundsätzlich gefragt werden, welche (??), informiert werden darüber, was da passiert, wenn ich die Wahl habe zu sagen, okay, Sie dürfen die und die Daten an die und die Unternehmen weiterleiten. Ich will aber dezidiert gefragt werden. Und das gilt für Internet, das gilt für alle Bereiche. Bis auf irgendwelche Plätze. Aber solange ich dafür zahle, für diese Dienstleistung, will ich explizit gefragt werden.

Ja.

Aber sozusagen spezielle neue Regulierungen sind jetzt nicht irgendwie für Sie wesentlich? Weil im Prinzip sozusagen gibt’s demokratische Kontrolle im Parlament. Die Frage ist also, wer involviert werden soll, ab wann könnte man ... man könnte sozusagen fantasieren, ob man mehr als parlamentarische Kontrolle und Öffentlichkeitsbeteiligung haben will.

Ja, mehr.

Das würde ich schon sagen.

Es gibt ganz seltene Dinge. Aber an sich wählen wir in der repräsentativen Demokratie unsere Parlamentarier.

Ja, ja, aber ...

Das ist mir aber zu wenig.

... man sollte trotzdem noch einmal, also ...

Ich glaube, es sind die wenigsten darüber informiert, wenn sie am Bankomat Bargeld ziehen, wird automatisch ein Foto gemacht. Dazu sind Banken berechtigt. Ich glaube einfach, dass jeder laufend informiert werden muss darüber, was machbar ist und ob er damit einverstanden ist. Das kann ich über große Tageszeitungen machen. (??).

Das muss ja nicht (??).

Das heißt, aus Ihrer Sicht sind die Betreiber aufgerufen zu informieren, was sie tun?

Genau.

Das wäre so ein Ansatz.

Auf jeden Fall, ja.

(??)

Also ich ...

Ich weiß nicht, ob es (??).

(??) Weiß ich nicht, 15 Jahre, und (??). Und darum würde ich mich wirklich dagegen stellen, unter anderem auch eben andere anhalten und (??) obwohl es nur 3- oder 4.000 Schilling waren zu dieser Zeit, und dann abgehoben 30.000 Schilling. (??) Und geendet hat das Ganze damit, dass sie dort nur die Diebstahlsanzeige gemacht haben an einem Sonntag, und am Montag (??) bei der Bank und bei der Polizei. Und die 10.000 Schilling, die der gute Mann (??) und dann (??) limitiert auf 5.000 Schilling. Und dann hat er noch ein paar Mal abgehoben und (??), dass er diese 10.000 Schilling wurden nicht rückvergütet. (??) Und das war damals ein Fall für den (??), und der hat gesagt, (??) weil jeder Schilling, (??) obwohl ihm das gestohlen wurde und man das gemeldet hat und er hat keinen Anspruch auf Rückvergütung. (??) 20.000 Schilling bekommen und 10.000 Schilling habe ich nie zurück bekommen und das ist ja nicht von heute auf morgen da. Das ist ja (??) Es hat gedauert ein halbes Jahr. Und für dieses halbe Jahr wurden mir für die gesamten 30.000 Schilling die Zinsen (ge....). Das ist ja die Kluft. Das muss man sich einmal vorstellen. (??). Da war kein Punkt dabei,

nichts aufgeschrieben. Ich habe ein einziges Mal (??) und er stand dort an. Also das war nicht so wie jetzt mit einem Pensionist (??). Aber dann muss man das hinnehmen. Und da habe ich einmal Geld abgehoben in Wien, das war das einzige Mal, (??). Sonst habe ich nur immer eingezahlt. (??).

Das ist ungewöhnlich.

So was gibt's auch. (??) Da habe ich ganz schön draufgezahlt.

Spannend für uns wäre noch zu wissen, ob die Teilnahme an der heutigen Veranstaltung irgendwie Ihre Haltung zu dem Themenkomplex beeinflusst hat. Oder ob Sie in Ihrer Haltung bestärkt werden.

Eigentlich nicht. Eher das Interesse ein bisschen mehr dafür, das würde ich sagen.

Gleich geblieben? Weil Sie vorher schon für das Thema sozusagen sensibilisiert waren, sonst hätten Sie nicht zugesagt oder so? Ja?

Ja, eher. Ich hatte schon dezidierte Ansichten dazu.

Ja, ich war ein bisschen hellhöriger, einfach ein bisschen ... sich vielleicht ein bisschen mehr damit zu befassen. Das war eigentlich bei mir jetzt vielleicht. Aber nicht so, dass ich meine Meinung geändert hätte.

(??) Das ist genau 14 Tage / drei Wochen. Und da wollte ich nachschauen, wie schaut das da aus, (??). Und dann hat sich das herausgestellt, dass der gute Mann 30.000 Schilling abgebucht hat von meinem Konto und das (??) Und dadurch habe ich auch schon gesagt, (??) Geld abgehoben. Und ich habe am Montag bei Ihnen um 9 Uhr den (??) gezählt in der Bank. (??) Und ich habe dann gesagt, dass (??). Man muss sich das einmal vorstellen, dann hat der gute Mann gesagt: Lösen Sie das Konto auf am Montag. Dann wäre es nie so weit gekommen. Das muss man sich vorstellen. Er kann das nur in Österreich sperren.

Konnte man vor 15 Jahren (??) das europaweit machen.

[Personen sprechen gleichzeitig]

Aber vielleicht ... Ich glaube, dass viele nicht wissen, dass diese Rahmen, diese großen Rahmen vorhanden sind. Also ich habe meinen Rahmen mit Absicht auf null, weil ich will das sowieso nicht. Wenn irgendwas ist, dass eben ... nicht drüber. Aber das muss man wissen.

Ja, aber die informieren nicht.

[Personen sprechen gleichzeitig]

Wir bieten Ihnen statt Ihrer Bankkarte eine Kreditkarte. Ich sage, ich will das nicht. Ich will das nicht. Bin hingegangen, Sie, ich will nicht automatisch eine Bankomatkarte. Ja, die kann ja viel mehr. Ich will das nicht. Gibt es nicht nach wie vor die Bankkarte, wo ich ... Ja, die können Sie auch haben. Man muss nachfragen. Das ist nämlich auch das Ärgerliche. Unter allen möglichen Vorwänden wird einem irgendwas Tolles angeboten, ohne dass man genau informiert wird. Darum dieses Informieren ist ja schon ein Punkt, das ist schon sehr wichtig. Und das sollten sie eigentlich freiwillig machen, diese Institutionen, und nicht immer erst auf Nachfrage, weil man misstrauisch geworden ist.

(??).

Gut. Das waren im Prinzip die Fragen. Wichtig wäre noch, welche abschließenden Bemerkungen, Punkte, welche Botschaften haben Sie sozusagen uns mitzugeben jenseits der ausgefüllten Fragebögen? Also was ist Ihnen wichtig?

Mir ist wichtig, dass eben die persönliche Sicherheit (??). Und auch, dass man selbst bestimmen kann, wie weit jemand (??) Gedanken macht. Und da wäre es halt wichtig auch, dass es vielleicht einzelne (??) gibt, welche Daten werden irgendwo erhoben, oder wie (??). Offen zu legen, welche Merkmale wurden (??) Firmen ihre (??) veröffentlichen müssen auch, ob Unternehmen regelmäßig (??) melden müssen, welche Daten sie erhoben haben und was mit den Daten passiert, wie lange die aufbewahrt werden und wann es vernichtet wird.

Ja, (??) also die ganze Geschichte mit Datenschutz (??) absolut nicht (??) Beispiel erwähnen. Es geht um Geld, oder? Und da (??) und man hat sich um den Mann oder die Frau überhaupt nicht gekümmert. Und dann ist der Tag X gekommen und (??) wann kommt er dann? Und dann ist ein Prospekt gekommen von 7-Sterne-Hotels, von der ganzen Welt. 7-Sterne-Hotel, ich weiß nicht (??) alles okay, nur frage ich mich (??). Hundert Jahre hat man sich nicht um die (?) gekümmert. Und erst nach Darlegung der Bankkonten (??) das (??). Das ist meine Meinung. Und es wird auch nicht so kommen, dass man wirklich (??) eine Frage der Zeit. Das wäre jetzt so (??).

Naked Mashine. Die Nackte Maschine.

(??)

Sie kennen die Naked Mashine schon?

Bitte?

Sie kennen die Naked Mashine schon?

[lacht] Ja. Ich habe sie (??).

Mich auch.

Ja. [lacht] Man muss sich vorstellen, (??). [lacht] (??)

Scherze sind überhaupt nicht (?).

(??).

Ja, ich würde sagen, also auf jeden Fall mehr Information und doch gewisse Grenzen. Irgendwo ist es zu Ende. Also gewisse Überwachung sehr wohl, aber nicht um jeden Preis und nicht alles und jeden. Und nicht für irgendwelche konventionellen Sachen. Also Überwachung überprüfen, was man falsch macht.

Ich würde was ganz Prinzipielles sagen. Jeder soll weniger Angst haben. Bei der Angst packt man nämlich die Leute, dass sie für solche Sachen zusagen. Wenn die Amerikaner nicht auf das 9-11 alle derartig geschockt reagiert hätten, dann wären die massiven Gesetze, die in Amerika durchgegangen sind, nicht so stillschweigend durchgegangen. Und dass jetzt erst eigentlich viele Leute in der Bevölkerung in Amerika aufhorchen und merken, was sie da an Freiheit aufgegeben haben. Also das sollte man vielleicht selber einfach bei sich überlegen, ein bisschen weniger Angst, dann ist man vielleicht weniger anfällig für die Zusage zu solchen Überwachungen und solchen Einschränkungen.

Ja.

Ja, im Prinzip ...

Sind wir uns ziemlich einig.

Es scheint eine recht homogene Gruppe zu sein. [alle lachen]

Ja, vielleicht auch noch, was wird aus unseren Fragebögen? Können Sie die Leute (??)

Also wir hoffen ja schon stark mit dem Projekt tatsächlich sozusagen in die Ausschreibungsbedingungen des Rahmenprogramms reinzukommen, mit den Ergebnissen, und ja, also das wäre sozusagen Politikberatung at it’s best. Weil dann würden wir wirklich gestaltend mitarbeiten können. Wir machen jetzt einmal die Auswertung in den sechs Ländern. Schauen dann sozusagen, was kommt. Den nationalen Report kriegen sie, wo Sie mitgearbeitet haben. Und wie dann unsere Ergebnisse sind, dann weiter verarbeitet werden, weiß ich nicht, aber es ist ein Versuch zumindest einen kleinen Beitrag der Bürgerinnen und Bürger sozusagen zu machen. Wobei man sagen muss, die Kommission verstärkt auf solche Instrumente hört und sie veranstaltet und auch finanziert. Also da kann man sagen, okay, es wird Geld dafür ausgegeben. Also das nicht völlig egal, das ist schon einmal aus meiner Sicht die erste wichtige Botschaft. Ja, wir sind ein bisschen früher fertig, das hängt damit zusammen, dass die Gruppe einfach kleiner war, dass die Gruppe homogen war. Ich danke Ihnen für die Beteiligung. Jetzt gibt’s

noch den Rest vom Buffet, es gibt aber jetzt auch Wein und Bier dazu. Und dann gibt’s noch ein kleines Abschiedsgeschenk. Jedenfalls herzlichen Dank für die Beteiligung. Danke.

[Ende]

5.3 Museumszimmer

In diesem Sinne möchte ich jetzt gleich die erste Frage in die Runde werfen. Was sind jetzt Ihre ersten Eindrücke, die bei Ihnen entstanden sind in Bezug auf Sicherheitstechnologien und in Bezug auf Privatsphäre oder Privatheit?

Also das erste Erfreuliche für mich war, dass sich anscheinend die EU auch interessiert, was sich die Bürger denken. Weil diese ganze Diskussion, oder was man so im Fernsehen mitkriegt oder so, ist eigentlich nie hier rübergekommen. Also man weiß ja nie, was das jetzt wirklich bewirkt, diese Auswertungen. Ob dann irgendwer dann irgendwelche Gesetze entwirft, ob man sich daran hält auch oder ob das irgendwie Einfluss nimmt auf die Gesetze, die beschlossen werden, aber ich finde es einmal gut, dass man überhaupt einmal so etwas macht und man mal die Bürger befragt, was sie davon halten. Und nicht immer über die Bürger hinweg zu beschließen, was gemacht wird.

Sonst noch erste Eindrücke?

Also ich habe das Konvolut, das wir zugeschickt bekommen haben, sehr intensiv gelesen und habe mir gedacht, also vieles weiß ich nicht, wusste ich nicht, einiges habe ich jetzt schon mitgekriegt und ich finde es sehr interessant und hoffe, ich höre noch mehr jetzt.

Ja, ich finde es wichtig, dass man uns sensibilisiert auch. Die Bevölkerung. Und weil wir das letztlich auch tragen müssen, die Auswirkungen im täglichen Leben, im Privatleben, letztlich entscheiden glaube ich werden dann die Politiker.

Ich frage mich, wieso die Studie in Österreich, Deutschland, skandinavischen Ländern durchgeführt wird und wieso ... und Spanien. Und wieso nicht in Ländern wie England, Frankreich, Italien, die vielleicht in einigen Bereichen ganz anders sind als die skandinavischen oder deutschsprachigen Länder. Zum Beispiel die Engländer ein ganz anderes Bedrohungsszenario vor Terrorismus vielleicht haben und dadurch vielleicht anders auf Sicherheitstechnologie ansprechen. Und auch Franzosen, die immer ein bisschen eine eigenwillige Meinung zu diversen ... zu allen Themen haben. Oder alternativ die Italiener.

Also ich möchte in dem Fall nicht inhaltlich Stellung nehmen, weil es nicht darum geht, dass ich Ihre Frage beantworte, sondern es geht eher darum, dass Sie vielleicht ... ob Sie dazu eine Meinung haben. Das ist auch jetzt nicht so gedacht, dass man wirklich reihum die Frage stellt, sondern dass Sie wirklich untereinander aufeinander eingehen sollen und das wäre also das, was gewünscht ist.

Das (??) durch diese Frage.

Aber vielleicht, was glauben Sie dazu?

(??)

Sonst irgendwelche ersten Eindrücke noch in Bezug auf die Sicherheitstechnologie?

Also ich glaube, man geht relativ locker damit um ohne nachzuforschen, wohin werden die Daten gegeben. Ich nehme ein Beispiel. Also ich bin Nichtraucher. Es gibt bei den Zigarettenautomaten die Möglichkeit, sich auszuweisen über die Bankomatkarte. Für mich ist die nächste Folge, dass alle, die Zigaretten kaufen, bei der nächsten Krankenkassenabrechnung 20 Prozent mehr zahlen könnten, weil eben die Raucher ein größeres Krebsrisiko haben.

Das ist schlecht. Beim letzten Mal hat mich einer gefragt, ob ich ihm die Bankomatkarte borgen kann, damit er sich Zigaretten ziehen kann.

Und Sie haben das gemacht?

Na ja, er war definitiv über 16, für mich kein Problem.

Ja, aber ...

Na ja, Sie müssen ...

Ich nehme nicht an, dass die Daten jetzt schon gespeichert werden. Aber es ist durchaus möglich, dass diese Form von Daten gespeichert wird. Und wir geben unsere Daten in jedem Billa weiter. Wenn ich eine Karte habe bei Billa oder eine Vorteilskarte bei der ÖBB, dann weiß ich über die Connection, zu welchen Leuten ich dann über die ÖBB-Adresse Zusendungen bekommen habe, mit denen ich vielleicht gar nichts zu tun haben möchte. Das war meine Frage als erstes, woher ist meine Adresse? Und die Antwort war sehr schön. Sie haben das outgesourct, wie das jetzt so schön heißt. Der andere macht die Arbeit.

Das ist immer so. Wie ich angerufen worden bin, habe ich auch gefragt, warum gerade ich? Woher meine Nummer ist? Und der hat auch gesagt, na ja, die steht da im Computer. Und ich rufe einfach an.

Es gibt Datenbanken mit unserem Namen und Telefonnummern und unserem Beruf und unserem Alter, mit allem. Das gibt es jetzt schon.

Und wenn mir jemand ...

Es ist nur die Frage, was noch dazu kommt.

Ich bin mir auch sicher, dass da schon drin steht, diese Person macht gern bei Meinungsumfragen mit. Also mich ruft einmal im Monat jemand an wegen einer

Meinungsumfrage und alle in meinem Freundeskreis werden nie angerufen. Und wenn man da einmal mitmacht, hat man schon den Stecken ...

Ist das etwas, was Sie als problematischen Aspekt von Sicherheitstechnologie oder eben von Technologie, von Datenverwaltung ansehen?

Nicht als problematisch, weil in dem Moment ... Also ich merke jetzt, dass ich irgendwo ... also dass viele Meinungs-... oder einfach so, es gibt ja viele Firmen, die Adressen sammeln und einfach Daten. Und die wissen, aha, Zielgruppe so und so, Ausbildung und der hat vielleicht ein gutes Verdienst, den kann man bessere Prospekte schicken über neue teure Autos. Und ist mir klar, dass ich dann darunter falle. Es gibt halt die Möglichkeit, man macht solche Meinungsumfragen nicht mit, dann sagt man okay, Meinung ... wird nie wieder angerufen. Oder vielleicht noch zwei, drei Mal, und dann hört es auf und dann weiß man, man hat jetzt seine Ruhe davor. Und wird vielleicht jetzt von diesen Meinungsumfragen nicht mehr verfolgt. Es gibt noch andere, die auch genug Daten sammeln werden. Andererseits sage ich aber auch, denke ich mir, wenn mich jemand befragt, dann habe ich wenigstens die Möglichkeit, dass ich irgendwie etwas beeinflussen kann. Also das ist immer dieses Hin und Her, will ich meine Meinung preisgeben. Aber ... also natürlich möchte ich nicht alle meine Wünsche oder irgendetwas verraten, aber andererseits, wenn man sich denkt, dass man vielleicht irgendwie die Zukunft beeinflussen kann, vielleicht strengere Regeln für Datenspeicherung und so weiter, dann ...

Auf der anderen Seite verdienen viele Studenten ihr Geld damit, dass sie sich auf die Straße stellen und diese Meinungsforschungsinstitute unterstützen. Das ist ja auch ein positiver Aspekt.

Also wir unterstützen damit die Studenten?

Ich unterstütze die Studenten. Sie müssen was tun, sie müssen auf Leute zugehen, sie lernen damit ...

Das wäre ein Potenzial für Sicherheitstechnologie, oder ... ich meine, ich werfe das nur in die Runde. Ich frage, wenn wir jetzt diskutieren über Probleme oder problematische Aspekte von Sicherheitstechnologien und von Potenzialen, wie würden Sie das einordnen?

Also in einer Großstadt kann ich mich nicht abschotten.

Auf dem Land noch weniger, denke ich.

(??) in der Großstadt. Ich bin persönlich der Meinung, dass in vielen Datenbanken mehr Daten von uns erfasst und gespeichert sind, als wir es glauben. Und in dem Moment, wo Sie mit der Bankomatkarte bei Billa oder sonst wo zahlen, können die irgendwas erhalten. Ob die Ihren Namen mit abspeichern oder nicht, sei dahin gestellt. Das wissen wir nicht so genau. Wir wissen aber dann genau, dass es

abgespeichert wird, wenn Sie beim (??) die Einkaufskarte hat, dann muss man den Namen noch dazu wissen. Sie wissen es aber, wenn Sie mit E-Mail die ganzen Werbegeschichten zugeschickt bekommen. Also ich bin persönlich der Meinung, dass Sicherheit und ein zusätzliches Datensammeln und Anlegen von Datenbanken dazu führt, dass wir zum gläsernen Menschen werden. Also davon gehe ich absolut aus. Ich habe selbst ein Unternehmen. Ich gebe selber Geld für (?) aus. Wir wissen alle zusammen, dass der größte Datendiebstahl innerhalb des Betriebes stattfindet, dadurch, dass wir vernetzt werden. Und die Diebstähle in dem Fall kann man verhindern. Sie haben das Geldbeispiel gebracht, beim Zigarettenautomaten die Bankomatkarte und zum Schluss war es die Krankenversicherung und erhöhte Prämien dazu. Und da könnte man inzwischen dann ein Beispiel sehen. Zu Ihren Fallbeispielen, die Sie da gebracht haben, habe ich auch eine Meinung. Wenn ich heute von einem Fingerabdruck rede, dann bin ich zwar nicht der Meinung, dass ich als Verbrecher abgestempelt bin, sondern dass ich eine eindeutige Identität zu mir selbst habe. Wenn von einer Datensicherungskarte die Rede ist, wenn ein Familienvater seine Karte verliert und jetzt bangen muss, dass man da viel erfahren kann, dann verstehe ich das schon überhaupt nicht. In der heutigen Zeit habe ich eine Bankomatkarte mit einem Chip drauf, und wenn ich die Bankomatkarte verliere, gebe ich die Nummer an, sperre die Karte und ich bin in kürzester Zeit Inhaber einer neuen Bankomatkarte. Jetzt stelle ich mir die Frage, warum soll das nicht genauso funktionieren können? Warum ist beim Identitätsdiebstahl – so sehe ich es – es nicht möglich ist, ein Duplikat herzustellen und diese Karte zu sperren, damit sie niemand benutzen kann. Ja, das sind so meine Vorstellungen dazu.

Also wenn ich Sie richtig verstehe, finden Sie diesen Aspekt der Szenarien nicht schlüssig.

Ich finde, dass man es ganz verschwitzt hat, (??) [10.44] ich merke nur so oft bei den Betriebssystemen, Software, ich finde so, man wird dem Terrorismus auf der Welt nicht Herr und versucht jetzt mit mehr Gewalt alles an Datenmaterial zu finden, zu suchen, zu verknüpfen, zu scannen, ohne genau zu wissen, wie hoch die Fehlerquote darin überhaupt ist. Mitte der neunziger Jahre hat es die Diskussion zwischen General Motors und Microsoft gegeben, weil Microsoft General Motors vorgeworfen hat, ihr baut Autos mit einer Technologie des vergangenen Jahrtausends. Wo Microsoft darauf so reagiert hat und so gesagt hat ... General Motors so reagiert hat, wenn wir die Autos so produzieren würden wie Microsoft die Betriebssysteme, müsste man, wenn man Autobahn fährt, alle 25 Minuten das Auto neu gestartet werden. Ich springe mal in die Gegenwart. Mein letztes Auto, das ich gehabt habe, ist 21 mal wegen der Elektronik in der Werkstatt gestanden, dreimal wegen einem Software-Absturz. (Wissen Sie, das ist für mich nicht so sehr lustig, weil ich habe dann sicherlich ein Problem in meinem Unternehmen. Wenn es dann um die Person geht und dann permanent die falschen Personen ausgewählt werden, dann ist keine Technik so perfekt, dass man halt wirklich die Personen miteinander ... eine Grenzwahrscheinlich von 99 Prozent haben kann, dann wird das ganze System meines Erachtens ziemlich unlustig werden.)

Zu dem, dass man ... eben zu der Genauigkeit, da denke ich mir immer, es ist auch gefährlich, wenn es einmal zu genau ist. Irgendwann gibt es einmal ... okay, wir haben 99,99 Prozent Genauigkeit mit Fingerabdrücken. Und jetzt schafft es trotzdem irgendwer, der irgendwo einbricht, und es kommt heraus beim Fingerabdruck, das war ich. Dann komme ich ins Gefängnis, weil es heißt, wir haben 99,99 Prozent Genauigkeit. Das muss der gewesen sein. Also diese ...

Man muss überlegen, man hat eine Technik eingeführt. Und wer ist quasi der Erste, der weiß, wie man die Sicherheitstechniken knackt, nämlich genau die wir erwischen wollen.

Ja. Das war ja ... [Personen sprechen gleichzeitig]

So ist es ja wirklich in der Realität. Mercedes oder BMW haben sich Sicherheitssysteme ausgedacht, dass diese Autos nicht mehr ... ja, stehlen haben sie sie schon noch können, aber starten haben sie nicht mehr können. Die Autos fahren aber alle. Und ein jeder wundert sich und sie geben viel Geld aus dafür und das funktioniert trotzdem nicht, weil diejenigen, die die Autos stehlen, sind die Allerersten, die diese Techniken zu überlisten wissen.

Das ist ja irgendwo der Punkt, der mich ein bisschen zu der Überlegung bringt, nämlich dass wir auf der einen Seite Sicherheitstechnologie sagen und auf der anderen Seite Worte wie Datenbank und Datenspeicherung verwenden. Und jeder, der mit Datenbanken und überhaupt Daten zu tun hat, weiß, dass es keinen Schlüssel gibt, der nicht knackbar ist. Das ist einfach so. Also das ist Tür und Tor geöffnet für jeden Missbrauch. Wer es missbrauchen will, der findet einen Weg dazu.

[Personen sprechen gleichzeitig]

Und in dem Konvolut steht auch drinnen, wenn man sicher sein will, dann soll man persönliche Gespräche führen und nicht telefonieren. Zum Beispiel. Steht drinnen. Und man soll auch bar zahlen. Nur das ist sicher. Steht in diesem Konvolut drinnen. Also das ist ja erschreckend. Jetzt ist man soweit, dass man mit Netbanking zahlen will.

Jetzt haben wir 's endlich soweit.

Jetzt bin ich soweit, und jetzt soll ich das wieder rückgängig machen?

Ich meine, es ist klar, wenn Sie bei Billa einkaufen und mit der Karte zahlen, es gibt – weiß der Teufel welche Institute, die würden ein Vermögen bezahlen, um genau diese Daten zu kriegen.

Aber der Fall (Lukona) [14.40] ist ja in einem Caféhaus aufgeflogen. Das war ein persönliches Gespräch. Wo ein anderer zugehört hat.

Vielleicht darf ich Sie diesbezüglich gleich fragen, wie schätzen Sie in dem Fall die Szenarien, die Sie bekommen haben, ein? Haben Sie das als positiv oder als eher schwierig empfunden?

Na ja, ich bin hellhörig geworden. Noch dazu habe ich in letzter Zeit gerade bei meinen E-Mails verschiedenes gefunden, was man mir anbietet. Irgendwelche Aktien und solche Dinge. Jetzt habe ich mir gedacht, da hat wirklich jemand schon ... Wer hat das geknackt? Und wie ich das gelesen habe, bin ich hellhörig geworden. Da habe ich mir gedacht, schrecklich. Ich werde das auch melden und werde ...

Sie werden sich noch wundern. Je älter die E-Mail-Adresse wird, je voller wird der (??). [15.30]

Vielleicht darf ich zu dem was vorher gefallen ist, noch kurz eine Frage stellen. Und zwar im Zusammenhang mit Sicherheitstechnologie und ob sie den Namen verdient, wie Sie das gesagt haben. Worin oder wann sind Ihrer Meinung nach – es sind alle natürlich angesprochen – wann sind Sicherheitstechnologien wichtiger als die Privatsphäre? Oder umgekehrt, wann ist die Privatsphäre wichtiger? Also fallen Ihnen da Beispiele ein?

Ich denke nicht, dass man es über einen Kamm scheren darf. Man geht immer von der Allgemeinheit aus und das geht einfach nicht. Und ich muss wirklich differenzieren zwischen allgemeinen Bürgern, unbescholten und wirklich jemand, der unter Verdacht steht. Also ich wehre mich dagegen, dass man sagt, jeder muss seine Privatsphäre preisgeben. Das ist ja ... ein Gerichtsbeschluss muss da sein. Wir sind in einer Gesellschaft, also noch gilt die Unschuldsvermutung bei uns ja. Und dass man eine Beweislast umkehrt, gibt es noch nicht. Aber das wäre schon in die Richtung, und das würde ich schrecklich finden.

Ja, man kann es vielleicht ein bisschen differenzieren und sich die Frage stellen, ob vielleicht bei Grenzkontrollen oder neuralgischen Punkten wie Flughäfen oder ... man kann das dann auch noch weitergehen und sagt vielleicht Bahnhöfe, öffentliche Plätze und so weiter, ob nicht da vielleicht zum Zweck der Sicherheit der Allgemeinheit eine stärkere Kontrolle gerechtfertigt ist als anders herum. So. Vielleicht einmal die Grenze und den Flughafen genauer kontrollieren sozusagen. Und ist es da vielleicht eher gerechtfertigt, dass jeder, der dort ist, in einer gewissen Weise kontrolliert wird und in einer gewissen Weise dadurch ja auch seine Privatsphäre eingeschränkt ist.

Aber wenn doch die Allgemeinheit weiß, dass dort kontrolliert wird, kann ich es mir wieder aussuchen.

Ob du dorthin gehst?

Ganz genau.

Das heißt, man müsste praktisch wissen, wo wird man wie kontrolliert.

Am Schwedenplatz kann ich es mir nicht mehr aussuchen.

Aber da weiß man es.

Aber am Schwedenplatz kann es auch für einen persönlich zum Vorteil werden, dass dort kontrolliert wird.

Natürlich kann es immer irgendwie zu einem Vorteil werden.

Das muss man ja auch werten, also dass zum Beispiel ein Überfall am Schwedenplatz relativ rasch geregelt werden kann.

Ich meine, es geht natürlich immer noch Zeit von dem Moment an, wo die Tat passiert und dass jemand vielleicht auf dem Video sieht, bis dann auch jemand zu Hilfe kommt. Das kann ja schon zu spät sein. Also es ...

Das ist richtig. Aber wenn jemand verletzt wird, sehen die den Tathergang.

Ja. Aber ...

Ja, das ...

Das heißt, das könnte man vielleicht unter positive Aspekte in der Sicherheitstechnologie verbuchen?

Ich glaube, das Problem ist nicht an sich, dass videoüberwacht wird, sondern man kann nur so streng sagen, es wird ... die Daten werden am nächsten Tag gelöscht und so weiter, und es wird immer versprochen, es hat nie wer Einsicht. Warum kann man sich auf YouTube täglich irgendwelche Videos von Überwachungskameras ansehen, die alle am nächsten Tag gelöscht werden?

Weil sie öffentlich sind. Wenn Sie wissen, dass Sie überwacht werden, dass Sie in eine Überwachungskamera reingelaufen sind, können Sie den Betreiber anschreiben und der muss einen Auszug schicken. Das ist EU-Recht. Und genau mit dem Ausschnitt können Sie machen, was Sie wollen. [Personen sprechen gleichzeitig] Also das ist ...

Wenn ich jetzt irgendwie einbreche im Supermarkt durch die Glasscheibe und verletzt am Boden liegen bleibe, dann hat das der Einbrecher selbst bei dem angefordert und dann ins Internet gestellt?

Vielleicht der Einbrecher, der durch die Scheibe geflogen ist, oder jedenfalls einer, der irgendwo im Bild zu sehen war. Diese Leute haben einen ... [Personen sprechen gleichzeitig]

Es gibt auch Fälle, wo das nicht angefordert worden ist, und trotzdem hat man sie gesehen.

Ja, dann haben wir ein Problem in der ...

Also die Schwachstelle für Sicherheitstechnologien ist wieder der Mensch.

Ein anderer unterschätzter Bereich ist ja eigentlich die Übertragung von Daten ohne Kabel. Kabellose Übertragung von Daten, wie zum Beispiel den Chip in den neuen Reisepässen, den man ja auch lesen kann und dafür muss man nicht mit dem Scanner drüberfahren, sondern es geht über weitere Entfernungen auch. Oder ansonsten in einem Internetcafé oder irgendwo anders, wo ein kabelloses Internet angeboten wird, wenn man dort mit seinem Computer im Internet ist, ist es sehr leicht für andere, Zugangsdaten herauszufinden, wie Passwörter, E-Mail-Accounts und so weiter. Das kann man ja ... könnte im Grunde jeder von uns machen und muss nur die Software dafür gratis aus dem Internet runterladen. Das ist nichts, was kompliziert wäre.

Also die biometrischen Pässe, da ärgert mich auch extrem, dass einfach die Regierung Bürger für dumm verkauft. Da wird gesagt, es kommt ein biometrischer Pass und die Daten sind gespeichert, aber die sind sicher. Die kann niemand auslesen. Und zwei Tage später kann man schon auf irgendwelchen Technikforen lesen, ja, in Deutschland hat man es geschafft, Chaos Computerclub hat präsentiert, aus 10 Meter Entfernung kann jeder Pass ausgelesen werden, ohne dass man irgendwelche spezielle Technologie braucht. Und? Drei Jahre später kommt dann der Pass mit der veralteten Technologie raus. Also da glaubt man wirklich, die verkaufen uns für die dumm, die Regierung.

Wir sammeln Informationen, es ist sicher, und dann, um ein anderes Beispiel zu nennen, auf der Bank Austria hat man ja schon diese Bankomaten mit irgendeinem Werbefolder auch hängen, was nichts anderes ist als ein Lesegerät, wo man den Code rauslesen kann. Dann wurde gesagt, Finger weg. Das Witzige war, ein paar Tage später dann im Foyer drinnen hing wirklich so ein Folder dort. Dann frage ich die, da haben sie gesagt, nein, das ist unser eigener, da kann nichts passieren. Aber das sind genau die Themen. Die Datensicherheit ist ein absolutes Thema. Und ich wollte noch zwei Beispiele bringen. Das eine Beispiel ist jetzt über 10 Jahre zurück, da kann man es eh schon öffentlich publik tun. Eine Sicherheitsbeauftragte Firma hat 1995 die Sicherheit der Flugsicherung Wien Schwechat untersucht. Und sie haben gebraucht 7 Sekunden, bis sie im System waren und die Flugzeuge umleiten konnten. Das sollte man aber schon glauben, dass die ein bisschen sich in der Sicherheit auch auskennen. Und das zweite, um bestehende Sicherheiten einmal zu untersuchen über den gläsernen Menschen, das war am Mittwoch in der (? [22.40] bin um 6 Uhr 55 weggeflogen, habe mich eingeparkt ungefähr um 6 Uhr 15 am Parkplatz. Was glauben Sie, was ich sehe auf dem Parkplatz? Zwei Flughafenpolizisten, die Pickerln an den Autos kontrolliert haben. Ja. Sie schauen so.

Was bedeutet das?

Ja bitte, die sind doch sicherlich nicht dort, um die Prüfung der Plaketten zu überprüfen.

Ach so, okay. Sondern ...

[Personen sprechen gleichzeitig]

Okay.

Also das sind so Dinge ...

Also in dem Fall, Sie ... wenn ich Sie richtig verstehe, dann deuten Sie das jetzt einfach, als dass die da praktisch nicht der Sicherheit dienen, sondern einfach irgendwelche läppischen ... um es mal salopp zu formulieren.

[Personen sprechen gleichzeitig]

Ich hatte das nicht wertend gemeint. Darf ich Sie auch noch fragen, nur so vielleicht?

Ich finde, dass man unterscheiden muss die Bereiche, wo es wirklich unangenehm ist, also wo man sozusagen in seiner Privatsphäre echt eingeschränkt ist und Orte, wo ... Mir persönlich ist es zum Beispiel wurscht, wann ich gefilmt werde, dass ich am Sonntag in der Früh um 6 Uhr am Bahnhof mich auf den Weg nach München mache. Also das ist mir wirklich ziemlich egal. Also kann ich eigentlich sagen. Wenn zu gleichen Zeit ein Verbrechen passiert auf dem Bahnhof, das dann doch aufgeklärt wird, eben weil mitgefilmt wird, dann freue ich mich sogar.

Ja, aber wenn Sie jetzt rund um die Uhr ein Handy mit sich tragen müssten, wo ständig aufgezeichnet wird, wo Sie sind.

Ja, das ist was anderes. Ich sage ja, da muss man unterscheiden.

Ja, aber genau um die Themen geht es heute.

Von der ständigen Überwachung war eigentlich nicht die Rede. Und der Fragebogen hat ja auch dazu gedient, das ein bisschen zu differenzieren. Und man wurde ja persönlich gefragt, mit richterlichem Beschluss, wären Sie einverstanden, dass das und das abgehört wird oder so. Und das ist schon ein Unterschied. Ich meine, sicher, wir müssen uns, ganz gleich, was wir für eine Einstellung haben, dann müssen wir uns à la longue gesehen für die Zukunft daran gewöhnen, dass der Mensch immer mehr und mehr überwacht wird. Also ich glaube, das ist nicht jetzt nur in dem terroristischen Vorfeld, wo es das gegeben hat, es verlangt einfach die Entwicklung der Zeit, die Entwicklung der Länder, die Entwicklung der Grenzen, EU etc., also ich glaube, dass wir da nicht drum herum kommen. Aber

ich finde es trotzdem toll, dass es solche Diskussionen gibt und dass ein jeder seine Meinung und seine Befürchtungen natürlich auch loswerden kann.

(??) [25.18]

Die Frage wollte ich auch gleich stellen. Was hat das mit dem zu tun? Warum müssen wir mehr überwacht werden?

[Personen sprechen gleichzeitig]

Das müssen Sie die Politiker fragen. Weil die setzen ja die Initiative.

Sie haben das jetzt so klar für Sie definiert. Sie haben das so klar gesagt, das ist für Sie klar, dass wir mehr überwacht werden.

Es ist die Entwicklung so. Es ist die Entwicklung so.

Ja, aber warum? Haben Sie eine Erklärung dafür?

Das müssen Sie die terroristischen Bereiche der Bevölkerung fragen.

Terroristische Bereiche der Bevölkerung? Ist das relevant für uns hier?

Ja, selbstverständlich. Weil Sie ja potenziell an einem öffentlichen Platz ... es weiß ja niemand, dass Sie unbescholten sind. Sie werden ja irgendwann einmal zufällig vielleicht einmal zu sehen sein auf einem Bild und Sie sind natürlich auch zwangsläufig betroffen.

Ich frage mich in dem Zusammenhang ganz einfach, weil Terrorismus, wovor fürchten wir uns eigentlich? Vor welchem Terrorismus fürchten wir uns? Woher kommt die Paranoia, die wir haben?

Vor Terrorismus muss man sich nicht vielleicht ... Man sagt so, die Freiheit des Einzelnen hört dort auf, wo sie den anderen einschränkt. Und ich glaube, das ist das grundlegende Problem. Wenn ich nicht Geld genug habe für meinen Bedarf und mir denke, der Nachbar hat da eine Brieftasche und ein Handy und da schaue ich, dass ich da dran komme, und ist das ein Übergriff.

Ja.

Und das ist aber ein Übergriff im Begrenztem. Und die Übergriffe gehen aber weiter hinaus, weil mit einem Handy gibt sich ein hochgradiger Verbrecher nicht ab. Wir wissen genau, erst mit den Millionen wird es interessant.

Also das haben wir ...

[Personen sprechen gleichzeitig]

Ich glaube ...

Der Terrorismus haben wir aber doch ...

Wir sind die Drehscheibe, was ich so rausgelesen habe. Aber was jetzt war mit den Georgiern und mit den Asylanten mit der Stradivari. Das weiß man seit Jahren, dass die das Diebesgut per Postpaket nach Georgien schicken. Das weiß die Polizei, das wissen alle. Wir haben ein Recht, in Österreich ein Grundrecht, dass das Post-... es gibt ein Postgeheimnis. Und das gilt auch auf Pakete. Das darf ... ohne den richterlichen Befehl dürfen wir uns die Pakete mit den Disketten oder sonst was ... was aber bei jedem Flugzeug sein darf. Ich weiß das aus einer ... von einem Richter, der mit den Asylanten zu tun hat und die sagen das auch.

Das heißt in dem Fall, wenn ich Sie richtig verstehe, nur um es zu klarifizieren, wäre das jetzt ein Kontext, wo Sie sagen, dass da die Sicherheitstechnologie über der Privatsphäre sehen soll?

Richtig. Hundertprozentig. Wenn man weiß, dass das Diebesgut ins Ausland geschafft wird, und das war so klar mit der Stradivari, ich meine, das ist ja ein Beispiel aus der letzten Zeit, dass da sehr wohl ausgewertet werden kann. Und die (Salera) [28.38] ist auch über Kamera ... auch illegal über Kamera gefunden worden.

Ja, schon, aber ...

Das ist halt ...

[Personen sprechen gleichzeitig]

Diese Stradivari, obwohl dieses Instrument viel Geld wert ist, nicht (??) [29.00] sicher verwahrt, lasse ich nicht (??)

Das unterschreibe ich völlig.

Das sind Werte, die haben nicht einmal ... Es ist eine Öffentlichkeitswirksamkeit da, weil das Zeug so teuer ist. Und weil einer aus dem Museum das heraus geklaut hat, wo er sich einen Gag nur daraus machen wollte.

Weil wir zurzeit noch nicht der gläserne Mensch sind. Ja? Deshalb wissen wir das Recht oder dieses Privileg noch nicht zu schätzen.

Natürlich.

[Personen sprechen gleichzeitig]

Das Erbstück von der Oma, der letzte Ring nach Georgien oder ...

Das ist aber ein bisschen politisch jetzt.

Na ja.

Na ja schon, Entschuldigung.

[Personen sprechen gleichzeitig]

Das ist genauso wie die Stradivari ist nicht gesichert genug.

Das würde ich noch eher einsehen, wenn ins Leben gerufen werden könnte, dass die Tageseinbrüche in Wohnungen (??) [30.00] in ganz normale Wohnung, also wenn man da eine Lösung finden würde.

Das ist sehr aktuell jetzt.

Da muss ich dann sagen, da ist jeder Bürger nicht gefeit davor, dass die halt ins Haus kommen und die Wohnungstür aufgebrochen ist. Aber ...

Das heißt, wenn ich Sie richtig verstehe, dann wäre das ein Kontext, wo Sie sagen, für den Schutz der persönlichen Wohnung wäre eine Sicherheitstechnologie, die wäre da angebracht.

Ja, die wäre ...

Das heißt, da würden Sie auch eine Einbuße von der Privatsphäre in Kauf nehmen?

An sich ja.

Stimmen Sie dem auch zu?

Schauen Sie, es gibt immer Beispiele und Möglichkeiten, wo Sicherheitstechnologie jedweder Art sinnvoll ist. Für jede Art von Technologie. Es gibt Beispiele, wo es wunderbar klar ist. Das wesentliche Problem, das ich bei all diesen Technologien sehe, ist der Missbrauch, der möglich ist. Und solange man das nicht ausschließen kann, ist die Diskussion einfach nicht sinnvoll.

Dann habe ich gleich eine Frage anschließend. Wer sollte in dem Fall bei der Entscheidung über die Implementierung, also die Einführung oder die Genehmigung von neuen Sicherheitstechnologien mitreden, wer soll da ... welche Bevölkerungsgruppen sollten da mit entscheiden Ihrer Meinung nach?

Es kann ja eine Zusammensetzung sein, wo nicht nur die Techniker drinnen sitzen, sondern (Kontivisionäre) [31.26] der Technik drin sitzen, Politiker drinnen sitzen. Ich glaube, da muss eine Anzahl von Menschen drinnen sitzen, die ausreichend – wie soll ich mich ausdrücken – Erfahrungsschatz in seinem Leben gesammelt hat.

Und das sind glaube ich dann auch die Enscheidungsträger, weil der Techniker will es verkaufen und der Politiker will sich hervortun, dass er wieder gewählt wird. Die meinen sowieso, man muss alles mit der großen Kappe über uns drüber stülpen, zahlen will es dann auch wieder niemand. Also das ist glaube ich gar nicht so einfach zu beantworten.

Das ist ganz schwer zu beantworten.

Ich finde, das ist ganz einfach. Das ist eine Entscheidung, die der Gesetzgeber zu treffen hat, das wird im Nationalrat entschieden und rundherum, das ist ... [Personen sprechen gleichzeitig]

Bitte, wer bereitet es nach?

Die Entscheidung ...

[Personen sprechen gleichzeitig]

Der Nationalrat.

Moment.

Meiner Meinung nach ist das eine Sache, die der Gesetzgeber zu entscheiden hat und rundherum ist die Interessenvertretung von beiden Seiten. Auf der einen Seite die Technik und Industrie, die das Zeug verkaufen will und auf der anderen Seite Menschenrechtsorganisationen, oder andere Organisationen, die besorgt sind um die Privatsphäre der Bürger.

Wen würden die anderen noch hineinsetzen in so ein Konsortium? Oder wer sollte Ihrer Meinung nach entscheiden?

Zivilingenieure sollten da drin sein, Techniker, die nicht davon leben, dass ihre Produkte gekauft werden. Und dann unabhängige Techniker, die zum Beispiel sagen, dass das Speichern von E-Mails nichts bringt bei der Fahndung von Terroristen, weil die verwenden eh schon längst Verschlüsselungen.

Darf ich ganz kurz was sagen? Was mein Nachbar zuerst gesagt hat, also intern wird am meisten gestohlen. Datendiebstahl betriebsintern. Ich bin in der Textilbranche und meine Schüler sind also ganz frustriert immer, wenn ich sage, also das Meiste stiehlt das Personal. Sie wollen doch nicht sagen, wir stehlen? Natürlich. Weil sie sich am besten auskennen. Und bei der Sicherheitstechnologie stiehlt der oder der knackt das System, der sich am besten auskennt. Die Polizei weiß auch, auf welche Leute sie zurückgreifen können, wenn sie was knacken müssen.

Was bedeutet ...

Die wissen, welcher Schlosser die Technologie überlisten kann. Man holt sich teilweise aus den (?) [34.14] raus, um die Türen zu öffnen.

Und was bedeutet das jetzt im konkreten Sinn?

Also viele Leute müssen dabei sein.

Also sozusagen auch die, die das System überlisten können?

Natürlich. Weil die können das auch bauen. Die jungen Leute, die zum Beispiel Computerprogramme aus Fadheit knacken, die sind einbezogen worden und nicht zu Strafen verdonnert, zum Mitarbeiten. Auf die andere Seite, um das System zu sichern.

Und wenn wir jetzt von der Entscheidung über das Einführen von neuen Sicherheitstechnologien reden, dann sind das also praktisch die verschiedenen Gruppen, die Ihnen dazu einfallen?

Die gehören alle zusammen.

Fällt Ihnen da auch noch was ein vielleicht?

Na ja, ich finde dann die Moral, wo bleibt da die Moral?

Genau. Sie sagen es.

Das ist erschreckend. Ist denn da jeder Anständige ist dann soweit, dass er sich dazu hergibt? Oder womöglich unter Druck dann hergeht, ist das auch arg.

Das heißt, wir nehmen Menschenrechtsorganisationen auch noch mit rein, und dann haben wir so viele beieinander, dass sowieso nie ein Ergebnis rauskommt.

Das wäre ein sehr vernünftiger Schritt zum Beispiel. Oder es kommen ein paar kleine Ergebnisse heraus, die wirklich zielführend sind.

Das ist erschreckend. Dann ist ja wirklich ...

[Personen sprechen gleichzeitig]

Tür und Tor jeden Missbrauchs öffnen.

Ja, genau das ist es.

Was hätten Sie für Empfehlungen für diese Problematik? Also was hätten Sie für Empfehlungen in Bezug auf die Regulierung? Wenn es um die Entwicklung und Einführung neuer Sicherheitstechnologie geht.

Also ich bin der Meinung, wenn die EU hier solche Richtlinien einführt, so hat die EU mal in erster Linie ihre Außengrenzen dementsprechend zu sichern. Dann haben wir natürlich an Länder ausgeliefert, die bei weitem nicht die finanziellen Mittel haben, vielleicht auch nicht den ... keine Ahnung, moralisch Einsicht hätten, so wie man es sich vorstellt zum einen. Und zum anderen kann sich jedes Land wohl über selbst an der Nase nehmen und sagen, wir schauen auf unser Land selbst. Wir passen auf unsere Flugplätze, auf unsere Bahnhöfe auf, auf unsere eigenen Grenzen.

Nur mit welchen Mitteln?

Na ja, welche Mittel, das sei mal dahingestellt. Ich kann das nicht beantworten. Also ich kann immer nur sagen, man muss das subtil angehen, denn man kann nicht einfach jetzt sagen, die Technologie hat eine Geschwindigkeit, dass ich sage, neue Technologie ist für mich sowieso ein Reizwort. Eine neue Technologie heißt für mich, funktioniert eh nicht am Anfang. Und die stülpen wir jetzt drüber, ohne darüber nachzudenken. Ich meine, man denkt schon nach darüber. Aber die Fehlerquoten haben wir dann hinten auch. Und bei meinem Beispiel zu bleiben, es werden die großen Automarken dieser Welt nicht zum Spaß Autos verkaufen, die nicht funktionieren. Das hätte es bei Mercedes vor fünf Jahren nicht gegeben und bei BMW vor fünf Jahren nicht gegeben.

Verstehe ich Sie richtig, dass Sie sagen wollen, es muss also langsam ... diese Technologien müssen getestet werden?

Die müssen wirklich ausgereift sein. Das muss wirklich ausgetestet sein.

Sie schütteln so mit dem Kopf?

Na ja, weil nicht jeder Programmierer weiß, dass ausgereifte Software schon wieder veraltet ist.

Ja.

Das ist ein ungeschriebenes Gesetz in der Softwareentwicklung.

Also das heißt, immer dran bleiben. Immer dran bleiben. Immer vorwärts.

Das ist allesamt nicht sicher. Das kann alles ausgehen.

Ja, wie Sie vorhin gesagt haben mit dem Homebanking. Jetzt können Sie es endlich und jetzt sollen Sie es nicht mehr machen.

Ja. [lacht]

Entschuldigen Sie, das geht uns allen so.

Ja, natürlich.

Sie lesen auf jeder Homepage: Achtung, tun Sie keinen Mails mit irgendwelchen (?) [38.10] oder sonst was. Jetzt kann ich mir lebhaft vorstellen, wenn man das nicht tagtäglich macht, hat man sofort die Skepsis und am liebsten wieder zur Bank hinein marschiert, seine Scheine abgibt, dann sagt der Banker zu Ihnen: Aber wenn Sie das da machen, kommt das viermal so früh als wenn Sie das da machen.

Genau das habe ich mir gedacht, werde ich wieder machen.

Ja, das macht man so lange, bis der Banker sagt, dass die Überweisung viermal soviel kostet, wenn Sie es bei der Bank abgeben. Das ist ja heute so.

(??) [38.41] zum Beispiel erspart man sich einen Teil der Kosten über die Versicherungsprämie. Weil zuerst gesprochen wurde, wer trägt die Kosten.

Wenn Sie ...

Also wenn man eine Versicherung auch bei Autos hat, wenn man einer Versicherung nachweisen kann, dass das Auto diebstahlgesichert ist, ein zweites Mal gegenüber dem Normalen, dann ist die Versicherungsprämie gering geringer.

Das heißt also, das wäre ein Vorteil der Sicherheitstechnologie?

Ja. Ich habe so einen Fall bei einer Bekannten, die hat das Auto von einer Botschafterin aus dem Ostblock gekauft und das hat eine zusätzliche Diebstahlsicherung. Und zwar keine elektronische. Sie hat zwei elektronische Sicherungen und die dritte Sicherung ist ein Pflock, der durch die Kupplung, durchs Getriebe durchgeht oder irgendwo. So eine Stange. Damit ist die Versicherungsprämie gegen Diebstahl ...

Wenn wir jetzt bei diesem Beispiel bleiben. Jetzt nehmen wir an, es wäre eine Technologie, die auch den Standort bekannt gibt, damit das eine Sicherheitstechnologie ist, wie wir sie heute gehört haben. Was würden Sie dazu sagen? Würden Sie in Kauf nehmen, dass die Versicherungsprämie ein bisschen geringer ist und dafür diesen Standortmesser als Sicherheitsmechanik mitführt oder wären Sie eher dagegen?

Unter der Voraussetzung, dass ich selber wählen kann, wann diese Sicherung aktiv ist, bin ich dafür.

Also in diesem Fall kann man das.

Das heißt also, Ihnen wäre wichtig, dass Sie selber entscheiden können, wann diese Daten an wen gehen.

Ich muss entscheiden können, wann ich überwacht werde und wie.

Aha.

Ich habe zum Beispiel (??) [40.24] dass es jedes Auto haben sollte. Aber es ist von uns allen die Meinung, wann das aktiviert ist oder wann ich es selbst aktiviere, dass (??). Weil das ist unmöglich, stellen Sie sich vor, Sie fahren mit dem Auto 180 Stundenkilometer und es ist 70 und so wie es da drin steht mit dem Bankeinzug sind Sie um 50 Euro leichter. Ich meine, wissen Sie, da sage ich jetzt wirklich, das ist dann die modernste Form in einen neuartigen Kommunismus zurückzukommen.

Ja, aber es ist doch so, dass wir uns alle einig sind, dass die Geschwindigkeitslimits eigentlich sinnvoll sind, und dass man sie eigentlich einhalten soll. Wieso wollen wir uns dann nicht kontrollieren lassen? Fahren wir alle zu schnell? Was wir ja tun, aber ... Warum sind wir dann eigentlich dafür, dass die Geschwindigkeitslimits so wie sie sind gut sind? Es macht manchmal sogar Sinn, wenn man das Limit überschreitet, weil wir zum Beispiel einen Flug erwischen müssen am Flughafen und dann sage ich okay ...

Ja, aber das kommt einmal im Jahr vor. Wir fahren aber doch wesentlich öfter zu schnell.

Aber Sie wissen schon, dass die Gewolltheit der Geschwindigkeit in Wien zwischen 10 und 15 Stundenkilometer auf den Tafeln übertrieben ist, um nämlich in Wien nicht über 60 zu kommen.

Wobei das jetzt ein Thema ist, das ein bisschen abgleitet. Und ich möchte gern schon bei den Sicherheitstechnologien bleiben. Es ist richtig. Also Sie haben gesagt, es gibt ja manchmal auch einen Sinn hinter bestimmten Regulierungen, aber um noch mal beim Thema zu bleiben. Wir haben vorher lebhaft diskutiert, es gab eine Dilemmasituation. Fallen Ihnen vielleicht noch einerseits Leute ein oder Gruppen ein, die bei solchen Entscheidungen mitreden sollten, damit es gute Entscheidungen sind? Oder ...

Datenschutzkommission zum Beispiel.

Warum kann man nicht unseren Vorfahren ein bisschen Gehör schenken, weil die haben das glaube ich (??) [42.30]. Das waren ...

[Personen sprechen gleichzeitig]

Ja, das waren einfach die erfahrenen Menschen. Die sind schon 60, 70 Jahre auf der Welt und haben auch die entsprechende Erfahrung. Und warum kann man dann nicht ein Konsortium von erfahrenen Menschen zusammenstellen, die mit ihrem Verstand ans Werk gehen und sagen dann, weiß ich nicht, keine Ahnung, sagt mir mal, wie das funktioniert und so, wenn wir einen Verbrecher haben, wenn

Sie den scannen, filmen und vergleichen und sonst was, wenn der mit der Perücke herumrennt, wie erkennt man den? Oder was auch immer.

Ich glaube, das geht genau aus dem Grund nicht, weil ständig dieses Wort neue Technologien da im Raum herum schwebt.

Na ja ...

Der Ältestenrat, ich weiß nicht, ob sich wirklich wer im fortgeschrittenen Alter mit solchen Dingen auskennt.

Ob die mitkommen in den neuen Technologien.

Richtig, ja.

Das heißt, wir hätten das Problem von Sicherheitstechnologien, dass sie vielleicht nicht für alle Gruppen zugänglich sind?

Definitiv, ja.

Ja.

Das ist definitiv richtig.

Wie stehen Sie zu dem? – Um in dem Fall die Frage noch einmal zurück, also in dem Fall auf die Regulierungen, kreative Empfehlungen. Also Empfehlungen von Ihnen hier, die Sie hier sitzen, fällt Ihnen noch etwas ein? Wie Regulierungen bezüglich neuer Sicherheitstechnologien gestaltet werden sollen. Regulierungen für die Implementierung neuer Technologien, aber auch in dem Fall für die Entwicklung neuer Technologien. Haben Sie da irgendwelche Vorschläge?

Also ich finde die Entwicklung ist ja jedenfalls wichtig. Man sollte die nicht einfach abblocken, weil man sagt, das könnte eine Gefahr sein, das zu entwickeln. Das wird ja sowieso entwickelt. Außerdem bin ich der Meinung, dass so etwas aus Kostengründen und aus Gründen der Effizienz im europäischen Rahmen geforscht gehört, also was ja auch gemacht wird. In einem nationalen Rahmen bringt so was nichts. Und dann beim Einsatz finde ich, dass man schon sehr aufpassen muss, was setzt man ein und wie setzt man es ein. Aber wenn es eingesetzt wird, wie jetzt zum Beispiel beim Auto eine Box, dann würde das nichts bringen, wenn es freiwillig wäre, wenn man es abschalten könnte, weil dann braucht man es eigentlich überhaupt nicht. Weil jeder, der nicht erkannt werden will, schaltet es schon ab.

Entschuldigen Sie, (??) [45.00] wenn Sie auf der B 303 einen Unfall haben und zufälligerweise Ihr Handy nicht funktioniert, ist das ein Vorteil, wenn Sie auf den Knopf draufdrücken können, dass man Sie findet. Also das Individuum ist

vollkommen uninteressant, sondern die Öffentlichkeit ist interessant, dass man weiß, wo Sie gerade fahren.

Es geht ja um die Nachverfolgbarkeit, wo ... wenn man jemanden ... also wenn die Polizei, sagen wir mal, regelt, wie das genau abläuft, das ist ja eine andere Sache mit einem gerichtlichen Beschluss, sagen wir mal, aber wenn die mit Hilfe der Box jemanden finden wollen, dann wäre das halt dumm, wenn derjenige, der nicht gefunden werden möchte, das abschalten kann.

[Personen sprechen gleichzeitig]

Und das soll der Grund dafür sein, dass ich jetzt jahrein, jahraus mit dem Signal durch die Gegend fahren muss, meine Daten aufgezeichnet werden und ich eigentlich jederzeit zum Verbrecher werden kann.

Also ist die Frage, dass man es überhaupt nicht einführen sollte. Aber Freiwilligkeit ist sinnlos.

Entweder so oder überhaupt nicht.

Wissen Sie, (??) [46.16] keine Technologie dazu gehabt, sondern (??).

Ich verstehe schon den Vergleich. Ich glaube, das ist ja ... kommt oft vor, dass eine neue Sicherheitstechnologie mit Überwachungsstaat so ein bisschen gleichgesetzt wird. Es ist auch ein echtes Problem. Und deswegen muss man irgendwie sicherstellen, dass diese Technologie nicht einfach von jedem unbegrenzt eingesetzt werden kann, sondern dass so was stark reguliert wird. Dass nicht einfach vielleicht ... ja.

Das geht nicht nur um die Regulierung, sondern um den illegalen Zugriff. Und sobald das Ding irgendwo gespeichert ist und sobald auch nur irgendeine Netzwerkleitung darauf ist auf dem Rechner ... Bababababa.

Vielleicht darf ich das ein bisschen konkreter machen. Sie haben die Szenarios alle gelesen, die beiden ...

[Handy klingelt] Entschuldigung.

Die beiden, von Carla und dem Herrn, der zum Flughafen muss. Wie denken Sie, wenn Sie sich die Zukunft vorstellen in so einer Art, wie sie dort beschrieben worden ist, ist das etwas, was Sie positiv finden oder eher nicht so positiv?

Ja, positiv ist (??) [37.40]

So global kann man das sicher nicht sagen. Also wenn man eine gewisse Sicherung auf dem Flughafen (??) [47.51] fortführen kann und das in einem sage ich jetzt einmal vernünftigen Ausmaß passiert, ohne dass man meine Iris dort

scannt, obwohl ich am Flughafen wahrscheinlich gar nichts dagegen hätte, dann ist das okay.

Das ist interessant.

Aber wenn ... ich weiß nicht, die Carla und die Kindern oder Enkel überwacht wird oder gerade mit dem Zug fährt oder ob sie jetzt aus dem Haus geht oder nicht, dann finde ich das bedenklich.

Na ja, das ist bedenklich.

Zum anderen muss ich sagen, wenn ich meine Eltern sehe, die 75 oder 80 Jahre alt sind, und ich hätte so ein System, wäre ich beruhigter, wenn ich weiß, wo sie jetzt gerade sind.

Aber dieses System gibt’s offenbar schon. Dieses Telefon.

Das Notfallsystem, das man umhängt?

Nein, nein, das meine ich nicht. Ich meine, er erklärt doch da, dass er seiner Mama ein Telefon gekauft hat, ein Handy gekauft hat, und da kann er sie anrufen. Sie weiß aber noch nichts davon, er kann sie beobachten.

Na ja gut, das ... solche Sachen gibt es. Das ist ... [Personen sprechen gleichzeitig]

Aber trotzdem, was bedeutet das für Sie? Ist das etwas, was Ihnen Behagen bereitet?

Nein, das behagt mit nicht.

[Personen sprechen gleichzeitig]

Entschuldigung. Wir verstehen uns sonst nicht. Ist das etwas, was Ihnen als Vorstellung behagen würde?

Nein, das behagt mir nicht. Das ist Unbehagen. Überhaupt, wenn meine Kinder sagen, du, jetzt schenke ich dir so ein Telefon und wenn du erlaubst, wir werden schauen, ob du zu Hause bist und ob es in der Wohnung sich was bewegt, ja, dann finde ich es in Ordnung. Aber wenn sie das also mir kaufen oder anschaffen ungefragt und ich weiß davon nicht, das ist entsetzlich.

Aber von der Idee her ...

Dann entmündigen sie doch.

Aber was halten Sie jetzt von dem? Die Kinder kaufen es, Sie freuen sich darüber und dann denken Sie darüber nach, wer kann jetzt noch alles nachschauen? Auf die Idee müssen Sie einmal kommen.

Ja, da kann niemand nachschauen. Wieso?

[Personen sprechen gleichzeitig]

Das geht ja nur Telefon gegen Telefon.

Nein. Na ja ...

Also von dem habe ich das ja gelesen, da habe ich gefragt meine Kinder, gibt's so was? Haben sie gesagt, oh ja, ich glaube schon. Haben sie gesagt, das gibt's schon.

Aber das wird vielleicht nur jemand machen können, der Ihre Telefonnummer hat.

Auf jeden Fall jeder, der bei Ihrem Netzbetreiber arbeitet. Also jeder nicht, aber ...

Na ja, aber jetzt kommt der Missbrauch dazu. Da sehen Sie aber immer ...

Also das finde ich nicht in Ordnung. Das finde ich nicht okay für mich.

Oder wenn Sie nehmen biometrische Daten, also da muss ich ein bisschen ausholen. Das haben wir ja ... immer wieder kommt man in diese Diskussionen von wegen, dass Risikosportler oder Extremsportler höhere Versicherungsbeiträge zahlen müssen, dass vielleicht Raucher höhere Versicherungsbeiträge zahlen müssen. In unserem netten Nachbarland gibt es die Diskussion wegen der Fettsteuer und so weiter, ja? Na ja, und jetzt zeichnen wir Gencodes und lauter so was halt auf, ne, und dann sieht man halt, der hat vielleicht ein Herzinfarktrisiko aufgrund seines Gentests. Was passiert damit? Werden diese Daten dann wirklich nicht weitergegeben? Werden die Versicherungen ... müssen die Leute dann wieder mehr zahlen? (??) [50.58] im Beruf, und so weiter, und so fort. Also ich finde diese Diskussion zieht einen ganzen Rattenschwanz nach sich.

Wenn Sie das genau nehmen, wären wahrscheinlich solche Daten heute bereits auswertbar, nämlich durch das Bezahlen mit Kreditkarten oder Bankomatkarten bei Lebensmitteln.

Für Fahrscheine.

Nein, für die Fahrscheine kann ich auf die Person nicht rückschließen, aber einfach aufgrund des Einkaufs im Lebensmittelgeschäft kann natürlich ein Grundverhalten der gesunden oder ungesunden Ernährung zum Beispiel ...

Das persönliche Profil spiegelt sich da wider in meinem Einkaufsverhalten und so. Darum sind die ja so teuer, diese Daten.

[Personen sprechen / lachen gleichzeitig]

Ihnen beiden entnehme ich daher explizit auch, dass das eher ein Nachteil von solchen Technologien ist. Ist das ...

Definitiv. Der Missbrauch steht groß drüber. Über jedem Vorteil.

Es muss nicht immer ein Nachteil sein.

Missbrauch ist nicht immer Nachteil?

Nein.

Nein, sie spricht gerade von der Technologie.

Entschuldigung.

Von den neuen Technologien. Wenn diese Diskussionen über (Transfette) [52.08] zum Beispiel gesteuert wurden und siehe da, vorher war überall das drin und ...

Gut, wobei diese Diskussion jetzt glaube ich nicht unbedingt nicht an Sicherheitstechnologie gekoppelt ist.

Nein, das war nur so ein Beispiel.

Das ist nur ein Beispiel.

Ach so.

Wie jemand darauf reagieren kann, wenn man Daten sammelt.

Ja, das ist ja ...

[Personen sprechen gleichzeitig]

Da haben Sie vollkommen Recht. Da haben Sie vollkommen Recht.

Ja.

Aber ...

Wir wissen zum Beispiel, dass Medikamente, und das ist der nächste Punkt, welche Leute nehmen wie viele Medikamente? Nehmen wir jetzt die Abrechnung für die Gebietskrankenkasse und so weiter, was wird das die Krankenkassen kosten? Das ist ja die Zukunft, wie viel darf man die überhaupt dann einmal

kosten? Das ist ja das nächste. Sie haben ja Ihre Mittel überschritten. Das ist die Folge.

Und was bewirkt es? Eine Oma, die einmal im Jahr zum Doktor geht, hat ein schlechtes Gewissen.

Sammelt für drei andere Leute.

Das ist richtig.

Und die, die sowieso jeden Tag zum Doktor gehen, die gehen weiterhin jeden Tag zum Doktor.

Also aufgrund der Zeit möchte ich gerne, damit wir noch ausreichend Raum haben für eine abschließende Reflexion in irgendeiner Form, möchte ich Sie gerne einzeln fragen, was Sie von dem heutigen Tag, von den Diskussionen jetzt, mit dem Vortrag, von den Szenarien vom heutigen Tag mitnehmen, ob Sie quasi gleich nach Hause gehen, wie Sie gekommen sind, oder ob Sie was mitnehmen. Vielleicht machen wir es noch mal der Reihe nach.

Ich werde sicher mitnehmen durch das, was alles besprochen worden ist ...

Entschuldigung, es so zu präzisieren auch ob sich Ihre Haltung geändert hat. Das ist etwas, was vielleicht auch wichtig ist noch mal.

Also die Haltung hat sich nicht geändert. Wie es bei Diskussionen üblich ist, es wird ans Bewusstsein ... also man hat im Bewusstsein, was alles passieren kann, gerade alle möglichen Szenarien, wenn man denkt, okay, vielleicht ist es doch nicht überall die Videokamera so nett und hin und wieder, wenn ich eine sehe, lächele ich nicht rein, sondern dann gehe ich vielleicht auf die Seite, wenn ich schlecht drauf bin. Und dass es keine allgemeine Lösung gibt, es gibt Sicherheitstechnologien, die gut sind und welche, die schlecht sind. Es ist immer irgendwo ein Kompromiss und es wird nie eine Sicherheitstechnologie geben, die immer ... die voll was Positives hat oder voll was Negatives hat, das wird es nicht geben. Und darum ist eigentlich ein Gedanke von mir während der Diskussion, es sollen sich die ganzen Regierungen nicht darauf versteifen, dass man neue Sicherheitstechnologie braucht, weil wir müssen das Verbrechen und den Terrorismus bekämpfen. Also man sollte vielleicht wieder einen Schritt zurückgehen und nicht nur die Ursache bekämpfen, sondern, was überhaupt das Problem ist. Vielleicht einmal, Terrorismus kann man nicht nur mit Röntgen und Scannen lösen.

Also nicht die Folge, sondern die Ursache.

Auf diplomatischer Ebene kann man auch viel Terrorismus lösen zum Beispiel. Dass man halt da mal wieder zurück denkt und schaut, warum gibt es Einbrecher,

warum gibt es Überfälle, dass man über das Ganze vielleicht auf einer menschlichen Ebene löst und nicht mit der Technik löst.

Ich hoffe auf die Jüngeren, dass die immer neue Technologien entwickeln und dass davon alle profitieren. Das hoffe ich sehr. Und es war sehr interessant für mich und ich werde auch darüber nachdenken, über Verschiedenes. Und für mich persönlich, ich möchte weder, dass man mich bevormundet telefonisch oder dass man kontrolliert meine Bevorratung oder meine Einkaufs-... was ich halt einkaufe, meine ganzen Gewohnheiten.

Geht niemanden was an.

Ja.

Wäre das nicht schön bei Billa an der Kasse, wenn man sagt: Sie haben heute keine Milch gekauft. [alle lachen / Personen sprechen gleichzeitig]

Es steht ja drin in dem ...

Darüber können wir uns auch nachher noch unterhalten. Aber vielleicht ...

Es steht in den Skripten drinnen.

Das heißt, Ihre Haltung hat sich schon ein bisschen in Richtung kritischer ...

Hat sich geändert, finde ich schon, ja weil es steht drinnen, dass man sogar das Einkaufsverhalten kontrolliert unter Umständen.

Danke.

Ja, es wird einem immer mehr und mehr bewusst, dass die Errungenschaft, die wir sozusagen erreicht haben, im Hinblick auf ein bequemeres Leben, Abwicklung des Tagesablaufs, Bezahlung mit Karten etc., auch nachteilig sein kann eben weil Adressen verkauft werden, weitergegeben werden. Darüber ist nicht gesprochen worden, ob das überhaupt gesetzlich erlaubt ist oder ob das halt irgendwie durchgeht, ohne dass das ein Tatbestand wäre. Aber letztendlich glaube ich doch, dass ein jeder eine gewisse Freiheit auch hat, sich sein Leben auch so in Bahnen zu lenke, wo man sagt, wo es nicht unbedingt sein muss, zahle ich jetzt bar oder bei der Firma auf gar keinen Fall übers Konto, dass man sich selbst in seinem Bereich sicher auch ein bisschen kanalisieren kann, was macht man mit meinen Daten, ist das jetzt notwendig in dem Fall, und nicht blind einfach jedem die Karte in die Hand drücken. Ich glaube, das ist auch ... hat sicher auch zum Denken angeregt heute für mich.

Ich möchte schon hinuntergehen, ich habe nämlich noch drei Seiten auszufüllen.

[Personen sprechen gleichzeitig]

Haben Sie noch irgendwelche Anmerkungen, bevor Sie gehen? Weil das wird dann noch eine nächste Runde sein, oder ist das für Sie mittlerweile okay?

Das ist okay.

Danke. Vielleicht Sie noch.

(??) [57.57] Sicherheit ist sicher (??) Technologie kann unterstützend einwirken und man sollte sich glaube ich distanzieren, immer wieder auf die neuesten Technologien zu hoffen und darauf zu setzen. Und ich kann mich nur anschließen. Sicherheit ist nicht nur Technologie, sondern Sicherheit ist viel, viel mehr.

Ich glaube, die Leute sollten ein bisschen am Unrechtsbewusstsein gepackt werden. Wir müssten uns nicht einmauern, wenn nicht gestohlen wird. Man braucht keine Sicherheit, wenn der andere mein Eigentum akzeptiert. Beim Autofahren mit der Technologie vom Bremsweg, da ist das ein bisschen anders, aber bei Verbrechen, bei Terrorismus, glaube ich, dass man da auf die Menschen direkt einwirken sollte.

Ist das eine Folge der heutigen Diskussionen?

Nein.

Inwiefern hat sich Ihre Haltung eventuell verändert oder auch nicht durch den heutigen Tag?

Ich habe ein paar Sachen gelesen, was technisch bereits möglich wäre und noch nicht ist. Die Entwicklung geht permanent weiter, das lässt sich nicht aufhalten. Und die Jungen, die nachkommen, wenn ein Ältestenrat gefragt wird und ich bin jung, denke ich mir, was macht der alte Dackel dort? Und das zu Recht. Und wenn ich jetzt alt bin und der Kollege sitzt da neben mir und meint ... er hat vollkommen Recht, er muss einfach gegen den Wind, es muss sein. Warum soll er es sich sagen lassen? Er versucht es auch, und Recht hat er.

Also wenn ich heute etwas mitgenommen habe, dann sicher, dass Sicherheit Kontrolle braucht und zwar auf der einen Seite, wo ich ganz besonders finde, dass mehr Kontrolle sein müsste, ist der Einsatz von Sicherheitstechnologie und Datenbanken durch private, um andere oder um uns alle ... um unser Kaufverhalten zum Beispiel auszuspionieren und so weiter. Und von staatlicher Seite her finde ich, ist der Einsatz von Sicherheitstechnologie ... sollte vielleicht relativ stark an gerichtliche Beschlüsse gebunden sein und Datenbanken prinzipiell anonymisiert sein. Und auf gerichtlichen Beschluss erst die Identität einzelner Verdächtiger freigegeben werden. Was mir auch nicht bewusst war vor dieser Diskussion heute insgesamt, war was es für einzelne technische Möglichkeiten gibt. Da war doch einiges Neues dabei. Und es ist sehr erstaunlich, wie schnell sich das entwickelt

und ich bin mir absolut sicher, dass in fünf bis zehn Jahren schon ganz andere Möglichkeiten da sind, über die wir heute uns noch nicht einmal träumen lassen.

Ja, ich glaube nicht, dass sich meine Grundhaltung zu dem Thema wesentlich verändert hat im Laufe des Gesprächs heute. Für mich ist ganz einfach die persönliche Freiheit ein so großes Gut, als dass man es einfach leichtfertig aufgibt oder irgendwie daran wackelt, weil es geht immer noch ein Stückchen weiter und immer ein Stückchen weiter. Ich halte die Aussage von dem ersten Redner für sehr vernünftig, dass man vielleicht endlich einmal beginnt, sich mit der Frage nach dem Warum auseinander zu setzen, das heißt warum gibt es Terrorismus, warum gibt es Verbrechen? Und nicht immer nur die Folgen bekämpft. Das ist mir auch schon damals im Zusammenhang mit dem 11. September aufgefallen. Es hat niemand jemals die Frage gestellt, warum ist es überhaupt gemacht worden. Sofort Barrikaden und Wegfall der persönlichen Grundrechte und so weiter, und so fort. Das wäre mir schon ein Anliegen, dass man den Ursachen ein bisschen mehr auf den Grund geht.

Also ich habe damit gerechnet, dass wenn der Kollege kommt und dass wir noch 10 Minuten Zeit haben. Ich möchte Ihnen aber trotzdem noch die Gelegenheit geben, finale Kommentare oder irgendetwas was Ihnen auch am Herzen liegt, was Sie nicht mit nach Hause nehmen wollen, hier zu lassen und irgendwie Ihre Meinung abzugeben. Ich meine, wenn es noch irgendwas gibt, was bisher noch keinen Raum gefunden hat. Wenn es nichts gibt, können wir das durchaus auch natürlich unten noch weiterführen. Wobei es da natürlich nicht mehr auf dem Band sein wird, was schade wäre. Also falls noch was da ist, können wir das noch machen, aber ansonsten, wenn nichts Grobes mehr da ist, dann danke ich Ihnen ganz, ganz herzlich und wünsche Ihnen noch einen wunderschönen Ausklang und hoffe auch, dass Sie mit den zugestellten Unterlagen dann weiter etwas anfangen können, dass Sie sich weiter mit dem Thema in dieser Form beschäftigen können. Danke.

[Ende]

Annex 6 - Frequency Tables Austria

q1sex

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	male	7	41,2	41,2	41,2
	female	10	58,8	58,8	100,0
	Total	17	100,0	100,0	

q2age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	25	1	5,9	6,3	6,3
	32	1	5,9	6,3	12,5
	38	1	5,9	6,3	18,8
	39	1	5,9	6,3	25,0
	42	1	5,9	6,3	31,3
	48	1	5,9	6,3	37,5
	49	1	5,9	6,3	43,8
	55	2	11,8	12,5	56,3
	56	1	5,9	6,3	62,5
	58	1	5,9	6,3	68,8
	60	1	5,9	6,3	75,0
	62	1	5,9	6,3	81,3
	69	1	5,9	6,3	87,5
	75	2	11,8	12,5	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q3household Persons in houshold ink self

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	9	52,9	52,9	52,9
	2	6	35,3	35,3	88,2
	4 or more	2	11,8	11,8	100,0
	Total	17	100,0	100,0	

q4children

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	9	52,9	52,9	52,9
	no	8	47,1	47,1	100,0
	Total	17	100,0	100,0	

q5childhome1 No children

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	1	5,9	5,9	5,9
	yes	16	94,1	94,1	100,0
	Total	17	100,0	100,0	

q5childhome2 14 or younger

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q5childhome3 15 or older

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	94,1	94,1
	yes	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q6edu

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	5,9	5,9	5,9
	2	1	5,9	5,9	11,8
	3	6	35,3	35,3	47,1
	5	1	5,9	5,9	52,9
	6	8	47,1	47,1	100,0
	Total	17	100,0	100,0	

q7occupstring

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Certificated nurse	2	11,8	11,8	11,8
	Commercial clerk	1	5,9	5,9	17,6
	Dental assistant and real-estate agent	1	5,9	5,9	23,5
	General practitioner, medical officer	1	5,9	5,9	29,4
	Management consultant	1	5,9	5,9	35,3
	Missing	1	5,9	5,9	41,2
	Projekt management / commercials - self-employed	1	5,9	5,9	47,1
	retired	2	11,8	11,8	58,8
	Consultant	1	5,9	5,9	64,7
	Student	1	5,9	5,9	70,6
	Teacher	1	5,9	5,9	76,5
	Toolmaker	1	5,9	5,9	82,4
	University teacher	1	5,9	5,9	88,2
	Vocational school teacher	1	5,9	5,9	94,1
	White-collar worker - software development	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q8district

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Metro	14	82,4	82,4	82,4
	Provincial town	2	11,8	11,8	94,1
	Rural	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q9phone

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	14	82,4	82,4	82,4
	at least once a week	2	11,8	11,8	94,1
	never	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q10email

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	9	52,9	52,9	52,9
	at least once a week	5	29,4	29,4	82,4
	at least once a month	2	11,8	11,8	94,1
	never	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q11internet

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	10	58,8	58,8	58,8
	at least once a week	4	23,5	23,5	82,4
	at least once a month	1	5,9	5,9	88,2
	never	2	11,8	11,8	100,0
	Total	17	100,0	100,0	

q12publictransport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	7	41,2	41,2	41,2
	at least once a week	6	35,3	35,3	76,5
	at least once a month	3	17,6	17,6	94,1
	less than once a month	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q13plane

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	more than 5 times a year	1	5,9	5,9	5,9
	3-5 times a year	3	17,6	17,6	23,5
	1-2 times a year	5	29,4	29,4	52,9
	less than 1 time a year	5	29,4	29,4	82,4
	never	3	17,6	17,6	100,0
	Total	17	100,0	100,0	

q14car

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	4	23,5	23,5	23,5
	at least once a week	11	64,7	64,7	88,2
	at least once a month	1	5,9	5,9	94,1
	less than once a month	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q15general The security of society is absolutely dependent on the development and use of new security technologies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	1	5,9	5,9	5,9
	partly agree	5	29,4	29,4	35,3
	partly disagree	7	41,2	41,2	76,5
	completely disagree	4	23,5	23,5	100,0
	Total	17	100,0	100,0	

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	4	23,5	23,5	23,5
	partly agree	8	47,1	47,1	70,6
	neither agree nor disagree	1	5,9	5,9	76,5
	partly disagree	3	17,6	17,6	94,1
	completely disagree	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	partly agree	5	29,4	29,4	29,4
	partly disagree	7	41,2	41,2	70,6
	completely disagree	5	29,4	29,4	100,0
	Total	17	100,0	100,0	

q18general When security technology is available, we might just as well make use o it

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	1	5,9	5,9	5,9
	partly agree	4	23,5	23,5	29,4
	neither agree nor disagree	2	11,8	11,8	41,2
	partly disagree	5	29,4	29,4	70,6
	completely disagree	5	29,4	29,4	100,0
	Total	17	100,0	100,0	

q19general Privacy should not be violated without reasonable suspicion of criminal intent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	15	88,2	88,2	88,2
	partly agree	1	5,9	5,9	94,1
	partly disagree	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q20general It is uncomfortable to be under surveillance, even though you have n criminal intent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	7	41,2	41,2	41,2
	partly agree	7	41,2	41,2	82,4
	neither agree nor disagree	1	5,9	5,9	88,2
	partly disagree	2	11,8	11,8	100,0
	Total	17	100,0	100,0	

q21general New security technologies are likely to be abused by governmental agencies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	3	17,6	17,6	17,6
	partly agree	9	52,9	52,9	70,6
	neither agree nor disagree	2	11,8	11,8	82,4
	partly disagree	2	11,8	11,8	94,1
	completely disagree	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q22general New security technologies are likely to be abused by criminals

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	9	52,9	52,9	52,9
	partly agree	4	23,5	23,5	76,5
	partly disagree	2	11,8	11,8	88,2
	completely disagree	2	11,8	11,8	100,0
	Total	17	100,0	100,0	

q23biom1 Facial characteristics

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	70,6	70,6	70,6
	yes	5	29,4	29,4	100,0
	Total	17	100,0	100,0	

q23biom2 Fingerprints

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	8	47,1	47,1	47,1
	yes	9	52,9	52,9	100,0
	Total	17	100,0	100,0	

q23biom3 Iris recognition

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	76,5	76,5	76,5
	yes	4	23,5	23,5	100,0
	Total	17	100,0	100,0	

q23biom4 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	64,7	64,7	64,7
	yes	6	35,3	35,3	100,0
	Total	17	100,0	100,0	

q23biom5 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q24biom1 Bank

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	10	58,8	58,8	58,8
	yes	7	41,2	41,2	100,0
	Total	17	100,0	100,0	

q24biom2 Airport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	5	29,4	29,4	29,4
	yes	12	70,6	70,6	100,0
	Total	17	100,0	100,0	

q24biom3 Store

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	94,1	94,1
	yes	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q24biom4 Border

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	64,7	64,7	64,7
	yes	6	35,3	35,3	100,0
	Total	17	100,0	100,0	

q24biom5 Central bus and train station

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	14	82,4	82,4	82,4
	yes	3	17,6	17,6	100,0
	Total	17	100,0	100,0	

q24biom6 Stadium and crowded

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	10	58,8	58,8	58,8
	yes	7	41,2	41,2	100,0
	Total	17	100,0	100,0	

q24biom7 Other private service

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	88,2	88,2	88,2
	yes	2	11,8	11,8	100,0
	Total	17	100,0	100,0	

q24biom8 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	14	82,4	82,4	82,4
	yes	3	17,6	17,6	100,0
	Total	17	100,0	100,0	

q24biom9 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q25biom Storing biometric data (e.g. fingerprints or DNA samples) of all citizens in a central database is an acceptable step to fight crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	partly agree	7	41,2	43,8	43,8
	neither agree nor disagree	2	11,8	12,5	56,3
	completely disagree	7	41,2	43,8	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q26biom The use of the biometric passport makes me feel insecure because of the risk of my biometric data being stolen

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	6	35,3	40,0	40,0
	partly agree	6	35,3	40,0	80,0
	neither agree nor disagree	1	5,9	6,7	86,7
	completely disagree	2	11,8	13,3	100,0
	Total	15	88,2	100,0	
Missing	99	2	11,8		
Total		17	100,0		

q27visual1 Store

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	9	52,9	56,3	56,3
	yes	7	41,2	43,8	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q27visual2 Dressing room

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	88,2	93,8	93,8
	yes	1	5,9	6,3	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q27visual3 Central bus and train station

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	8	47,1	50,0	50,0
	yes	8	47,1	50,0	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q27visual4 Bank

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	1	5,9	6,3	6,3
	yes	15	88,2	93,8	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q27visual5 Airport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	2	11,8	12,5	12,5
	yes	14	82,4	87,5	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q27visual6 Stadium and crowded

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	7	41,2	43,8	43,8
	yes	9	52,9	56,3	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q27visual7 All public

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	70,6	75,0	75,0
	yes	4	23,5	25,0	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q27visual8 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	100,0	100,0
Missing	99	1	5,9		
Total		17	100,0		

q27visual9 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	100,0	100,0
Missing	99	1	5,9		
Total		17	100,0		

q28visual How do you feel about the number of CCTV cameras in public spaces in general?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	there should be more	1	5,9	6,3	6,3
	the number is appropriate	11	64,7	68,8	75,0
	there should be less	2	11,8	12,5	87,5
	there should be no	2	11,8	12,5	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q29visual1 School

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	76,5	81,3	81,3
	yes	3	17,6	18,8	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q29visual2 Central bus and train station

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	76,5	81,3	81,3
	yes	3	17,6	18,8	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q29visual3 Airport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	3	17,6	18,8	18,8
	yes	13	76,5	81,3	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q29visual4 Shopping mall

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	100,0	100,0
Missing	99	1	5,9		
Total		17	100,0		

q29visual5 Public buildings

		Frequency	Percent
Missing	99	17	100,0

q29visual6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	70,6	75,0	75,0
	yes	4	23,5	25,0	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q29visual7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	100,0	100,0
Missing	99	1	5,9		
Total		17	100,0		

q30visual1 Reveal everything

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q30visual2 Mannequin projection

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	64,7	64,7	64,7
	yes	6	35,3	35,3	100,0
	Total	17	100,0	100,0	

q30visual3 Body heat, sweat & heart rate

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q30visual4 Metal

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	7	41,2	41,2	41,2
	yes	10	58,8	58,8	100,0
	Total	17	100,0	100,0	

q30visual5 Luggage x-ray

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	9	52,9	52,9	52,9
	yes	8	47,1	47,1	100,0
	Total	17	100,0	100,0	

q30visual6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	76,5	76,5	76,5
	yes	4	23,5	23,5	100,0
	Total	17	100,0	100,0	

q30visual7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q31visual CCTV surveillance makes me feel more secure

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	3	17,6	17,6	17,6
	partly agree	6	35,3	35,3	52,9
	neither agree nor disagree	3	17,6	17,6	70,6
	partly disagree	1	5,9	5,9	76,5
	completely disagree	4	23,5	23,5	100,0
	Total	17	100,0	100,0	

q32visual CCTV surveillance infringes my privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	3	17,6	17,6	17,6
	partly agree	7	41,2	41,2	58,8
	neither agree nor disagree	2	11,8	11,8	70,6
	partly disagree	4	23,5	23,5	94,1
	completely disagree	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q33visual Scanning of persons for detection of hidden items is an acceptable tool for preventing terror

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	2	11,8	11,8	11,8
	partly agree	5	29,4	29,4	41,2
	partly disagree	5	29,4	29,4	70,6
	completely disagree	5	29,4	29,4	100,0
	Total	17	100,0	100,0	

q34local1 Terrorists and criminals w court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	4	23,5	23,5	23,5
	yes	13	76,5	76,5	100,0
	Total	17	100,0	100,0	

q34local2 Any w/o court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q34local3 Emergency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	3	17,6	17,6	17,6
	yes	14	82,4	82,4	100,0
	Total	17	100,0	100,0	

q34local4 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	94,1	94,1
	yes	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q34local5 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q35local1 Terrorists and criminals w court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	4	23,5	25,0	25,0
	yes	12	70,6	75,0	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q35local2 Any w/o court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	100,0	100,0
Missing	99	1	5,9		
Total		17	100,0		

q35local3 Stolen vehicles

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	4	23,5	25,0	25,0
	yes	12	70,6	75,0	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q35local4 Speeding

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	88,2	93,8	93,8
	yes	1	5,9	6,3	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q35local5 Automatic accident reporting

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	4	23,5	25,0	25,0
	yes	12	70,6	75,0	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q35local6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	100,0	100,0
Missing	99	1	5,9		
Total		17	100,0		

q35local7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	100,0	100,0
Missing	99	1	5,9		
Total		17	100,0		

q36local Should eCall automatically be installed in all new cars?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	1	5,9	6,3	6,3
	yes but possible to deactivate	6	35,3	37,5	43,8
	no, optional	9	52,9	56,3	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q37local The possibility of locating all mobile phones is privacy infringing

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	11	64,7	68,8	68,8
	partly agree	3	17,6	18,8	87,5
	neither agree nor disagree	1	5,9	6,3	93,8
	partly disagree	1	5,9	6,3	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q38local The possibility of locating a suspect's mobile phones is a good tool for the police in investigating and preventing terror and crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	5	29,4	31,3	31,3
	partly agree	7	41,2	43,8	75,0
	partly disagree	3	17,6	18,8	93,8
	completely disagree	1	5,9	6,3	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q39local The possibility of locating all cars is privacy infringing

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	12	70,6	75,0	75,0
	partly agree	1	5,9	6,3	81,3
	neither agree nor disagree	2	11,8	12,5	93,8
	partly disagree	1	5,9	6,3	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q40local The possibility of locating all cars is a good tool for the police in investigating and preventing terror and crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	1	5,9	6,3	6,3
	partly agree	5	29,4	31,3	37,5
	neither agree nor disagree	2	11,8	12,5	50,0
	partly disagree	2	11,8	12,5	62,5
	completely disagree	6	35,3	37,5	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q41data1 Prevention of terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	64,7	64,7	64,7
	yes	6	35,3	35,3	100,0
	Total	17	100,0	100,0	

q41data2 Investigation of terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	7	41,2	41,2	41,2
	yes	10	58,8	58,8	100,0
	Total	17	100,0	100,0	

q41data3 Prevention of crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	70,6	70,6	70,6
	yes	5	29,4	29,4	100,0
	Total	17	100,0	100,0	

q41data4 Investigation of crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	8	47,1	47,1	47,1
	yes	9	52,9	52,9	100,0
	Total	17	100,0	100,0	

q41data5 Commercial

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q41data6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	76,5	76,5	76,5
	yes	4	23,5	23,5	100,0
	Total	17	100,0	100,0	

q41data7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q42data1 Prevention of terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	10	58,8	58,8	58,8
	yes	7	41,2	41,2	100,0
	Total	17	100,0	100,0	

q42data2 Investigation of terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	6	35,3	35,3	35,3
	yes	11	64,7	64,7	100,0
	Total	17	100,0	100,0	

q42data3 Prevention of crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	76,5	76,5	76,5
	yes	4	23,5	23,5	100,0
	Total	17	100,0	100,0	

q42data4 Investigation of crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	4	23,5	23,5	23,5
	yes	13	76,5	76,5	100,0
	Total	17	100,0	100,0	

q42data5 Commercial

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q42data6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	88,2	88,2	88,2
	yes	2	11,8	11,8	100,0
	Total	17	100,0	100,0	

q42data7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q43data Government institutions should store all data they find necessary for securi reasons for as long as they consider it necessary

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	2	11,8	11,8	11,8
	partly agree	3	17,6	17,6	29,4
	neither agree nor disagree	1	5,9	5,9	35,3
	partly disagree	4	23,5	23,5	58,8
	completely disagree	7	41,2	41,2	100,0
	Total	17	100,0	100,0	

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	11	64,7	64,7	64,7
	partly agree	4	23,5	23,5	88,2
	partly disagree	1	5,9	5,9	94,1
	completely disagree	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q45data Scanning of and combining data from different databases containing personal information is privacy infringing

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	8	47,1	47,1	47,1
	partly agree	6	35,3	35,3	82,4
	partly disagree	2	11,8	11,8	94,1
	completely disagree	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q46data Scanning of and combining data from different databases is a good tool fo police to prevent terror

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	3	17,6	17,6	17,6
	partly agree	6	35,3	35,3	52,9
	neither agree nor disagree	1	5,9	5,9	58,8
	partly disagree	2	11,8	11,8	70,6
	completely disagree	5	29,4	29,4	100,0
	Total	17	100,0	100,0	

q47data Databases being used for something else than the original purpose is a serious privacy problem

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	16	94,1	94,1	94,1
	completely disagree	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q48wire1 Prevention and investigation of terrorism w court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	4	23,5	23,5	23,5
	yes	13	76,5	76,5	100,0
	Total	17	100,0	100,0	

q48wire2 Prevention and investigation of terrorism w/o court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	94,1	94,1
	yes	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q48wire3 Prevention and investigation of crime w court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	2	11,8	11,8	11,8
	yes	15	88,2	88,2	100,0
	Total	17	100,0	100,0	

q48wire4 Prevention and investigation of crime w/o court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	94,1	94,1
	yes	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q48wire5 Commercial

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q48wire6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	88,2	88,2	88,2
	yes	2	11,8	11,8	100,0
	Total	17	100,0	100,0	

q48wire7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q49wire What methods of eavesdropping is acceptable?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	persons that suspect is expected to contact	6	35,3	37,5	37,5
	suspects	8	47,1	50,0	87,5
	totally unacceptable	2	11,8	12,5	100,0
	Total	16	94,1	100,0	
Missing	d.k.	1	5,9		
Total		17	100,0		

q50wire Eavesdropping is a good tool for police investigation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	4	23,5	23,5	23,5
	partly agree	4	23,5	23,5	47,1
	neither agree nor disagree	1	5,9	5,9	52,9
	partly disagree	5	29,4	29,4	82,4
	completely disagree	3	17,6	17,6	100,0
	Total	17	100,0	100,0	

q51wire Eavesdropping is a serious violation of privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	9	52,9	52,9	52,9
	partly agree	3	17,6	17,6	70,6
	neither agree nor disagree	1	5,9	5,9	76,5
	partly disagree	3	17,6	17,6	94,1
	completely disagree	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q52protect1 Anonymous calling cards

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	5	29,4	33,3	33,3
	yes	10	58,8	66,7	100,0
	Total	15	88,2	100,0	
Missing	99	2	11,8		
Total		17	100,0		

q52protect2 Encryption programmes

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	4	23,5	26,7	26,7
	yes	11	64,7	73,3	100,0
	Total	15	88,2	100,0	
Missing	99	2	11,8		
Total		17	100,0		

q52protect3 Identity management

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	7	41,2	46,7	46,7
	yes	8	47,1	53,3	100,0
	Total	15	88,2	100,0	
Missing	99	2	11,8		
Total		17	100,0		

q52protect4 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	88,2	100,0	100,0
Missing	99	2	11,8		
Total		17	100,0		

q52protect5 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	76,5	86,7	86,7
	yes	2	11,8	13,3	100,0
	Total	15	88,2	100,0	
Missing	99	2	11,8		
Total		17	100,0		

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	7	41,2	46,7	46,7
	partly agree	6	35,3	40,0	86,7
	neither agree nor disagree	2	11,8	13,3	100,0
	Total	15	88,2	100,0	
Missing	99	2	11,8		
Total		17	100,0		

q54protect Privacy enhancing technologies should not be legal if they make police investigation and prevention of terror and crime more difficult

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	1	5,9	6,3	6,3
	partly agree	4	23,5	25,0	31,3
	neither agree nor disagree	1	5,9	6,3	37,5
	partly disagree	3	17,6	18,8	56,3
	completely disagree	7	41,2	43,8	100,0
	Total	16	94,1	100,0	
Missing	99	1	5,9		
Total		17	100,0		

q55dilem1 Accept registration of travel and fingerprints

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	94,1	94,1
	yes	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q55dilem2 Accept only if template

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	14	82,4	82,4	82,4
	yes	3	17,6	17,6	100,0
	Total	17	100,0	100,0	

q55dilem3 Accept only if deleted

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	14	82,4	82,4	82,4
	yes	3	17,6	17,6	100,0
	Total	17	100,0	100,0	

q55dilem4 Accept only if not exclusive

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	76,5	76,5	76,5
	yes	4	23,5	23,5	100,0
	Total	17	100,0	100,0	

q55dilem5 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	6	35,3	35,3	35,3
	yes	11	64,7	64,7	100,0
	Total	17	100,0	100,0	

q55dilem6 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q56dilem1 Accept database and biometrics

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	70,6	70,6	70,6
	yes	5	29,4	29,4	100,0
	Total	17	100,0	100,0	

q56dilem2 Accept naked machine

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	70,6	70,6	70,6
	yes	5	29,4	29,4	100,0
	Total	17	100,0	100,0	

q56dilem3 Accept sweat, body heat and heart rate scanning

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q56dilem4 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	6	35,3	35,3	35,3
	yes	11	64,7	64,7	100,0
	Total	17	100,0	100,0	

q56dilem5 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q57dilem1 Accept all consequences

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q57dilem2 Accept only low rate of false positives

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	70,6	70,6	70,6
	yes	5	29,4	29,4	100,0
	Total	17	100,0	100,0	

q57dilem3 Accept only no false positives

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	64,7	64,7	64,7
	yes	6	35,3	35,3	100,0
	Total	17	100,0	100,0	

q57dilem4 Accept only in exposed places

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	8	47,1	47,1	47,1
	yes	9	52,9	52,9	100,0
	Total	17	100,0	100,0	

q57dilem5 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	76,5	76,5	76,5
	yes	4	23,5	23,5	100,0
	Total	17	100,0	100,0	

q57dilem6 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q58dilem1 Accept all access for counter terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	94,1	94,1
	yes	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q58dilem2 Accept only if anonymous and w court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	4	23,5	23,5	23,5
	yes	13	76,5	76,5	100,0
	Total	17	100,0	100,0	

q58dilem3 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	76,5	76,5	76,5
	yes	4	23,5	23,5	100,0
	Total	17	100,0	100,0	

q58dilem4 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q59dilem1 Accept locate car to prevent crime or terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	10	58,8	58,8	58,8
	yes	7	41,2	41,2	100,0
	Total	17	100,0	100,0	

q59dilem2 Accept speeding tickets

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	94,1	94,1
	yes	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q59dilem3 Accept register all movements

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q59dilem4 Accept only accidents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	70,6	70,6	70,6
	yes	5	29,4	29,4	100,0
	Total	17	100,0	100,0	

q59dilem5 Accept only if voluntary

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	5	29,4	29,4	29,4
	yes	12	70,6	70,6	100,0
	Total	17	100,0	100,0	

q59dilem6 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q60dilem1 Accept calling cards

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	4	23,5	23,5	23,5
	yes	13	76,5	76,5	100,0
	Total	17	100,0	100,0	

q60dilem2 Accept encryption

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	8	47,1	47,1	47,1
	yes	9	52,9	52,9	100,0
	Total	17	100,0	100,0	

q60dilem3 Accept Internet anonymity - bomb

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	9	52,9	52,9	52,9
	yes	8	47,1	47,1	100,0
	Total	17	100,0	100,0	

q60dilem4 Accept Internet anonymity - child pornography

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	70,6	70,6	70,6
	yes	5	29,4	29,4	100,0
	Total	17	100,0	100,0	

q60dilem5 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	76,5	76,5	76,5
	yes	4	23,5	23,5	100,0
	Total	17	100,0	100,0	

q60dilem6 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	94,1	94,1
	yes	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q61dilem1 Accept exclusion of refusers from public service

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	14	82,4	82,4	82,4
	yes	3	17,6	17,6	100,0
	Total	17	100,0	100,0	

q61dilem2 Accept exclusion of unabled from public service

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	88,2	88,2	88,2
	yes	2	11,8	11,8	100,0
	Total	17	100,0	100,0	

q61dilem3 Accept refusers are impended when public transport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	88,2	88,2	88,2
	yes	2	11,8	11,8	100,0
	Total	17	100,0	100,0	

q61dilem4 Accept unabled are impended when public transport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	94,1	94,1	94,1
	yes	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q61dilem5 Accept no consequences for refusers

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	6	35,3	35,3	35,3
	yes	11	64,7	64,7	100,0
	Total	17	100,0	100,0	

q61dilem6 Accept no consequences for unabled

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	6	35,3	35,3	35,3
	yes	11	64,7	64,7	100,0
	Total	17	100,0	100,0	

q61dilem7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	100,0	100,0	100,0

q62demo Politicians must always submit important questions to public debate and public hearings before making decisions on implementing new security technologies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	12	70,6	70,6	70,6
	partly agree	5	29,4	29,4	100,0
	Total	17	100,0	100,0	

q63demo The subject of security and privacy is so complicated that it makes no sense to include the general public in discussions of this issue

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	1	5,9	5,9	5,9
	partly agree	3	17,6	17,6	23,5
	partly disagree	2	11,8	11,8	35,3
	completely disagree	11	64,7	64,7	100,0
	Total	17	100,0	100,0	

q64demo Human rights organisations are always entitled to be heard when important decisions on security and privacy are made

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	13	76,5	76,5	76,5
	partly agree	4	23,5	23,5	100,0
	Total	17	100,0	100,0	

q65demo It is important that private companies involved in producing security technologies are also entitled to be heard when important decisions on security and privacy are made

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	11	64,7	64,7	64,7
	partly agree	3	17,6	17,6	82,4
	neither agree nor disagree	2	11,8	11,8	94,1
	completely disagree	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q66demo In relation to significant decisions on the use of security technologies, is imperative that alternative solutions are elucidated and included in the debate

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	16	94,1	94,1	94,1
	partly agree	1	5,9	5,9	100,0
	Total	17	100,0	100,0	

q67suggest Collection of personal data from unsuspicious individuals must be anonymous until identification is authorized by court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	17	100,0	100,0	100,0

q68suggest Only authorized personnel can have access to collected personal data

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	17	100,0	100,0	100,0

q69suggest Prior to implementing, new security technologies must be checked for privacy impact

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	15	88,2	93,8	93,8
	some importance	1	5,9	6,3	100,0
	Total	16	94,1	100,0	
Missing	d.k.	1	5,9		
Total		17	100,0		

q70suggest Funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	14	82,4	82,4	82,4
	some importance	1	5,9	5,9	88,2
	little importance	2	11,8	11,8	100,0
	Total	17	100,0	100,0	

q71end Have you changed your attitude towards security technologies in general the course of completing this questionnaire?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes, more positive	3	17,6	17,6	17,6
	no	14	82,4	82,4	100,0
	Total	17	100,0	100,0	

eduISCED97

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	lower secondary level of education	1	5,9	5,9	5,9
	upper secondary level of education	7	41,2	41,2	47,1
	first stage of tertiary education	9	52,9	52,9	100,0
	Total	17	100,0	100,0	

Annex 7 Comments from the questionnaire

- Health related issues (x-ray load etc.) should also be taken into consideration (e.g. many checks for frequent travelers)

- Research on security technologies should be supported. Deployment should however take into account privacy and assess the costs and benefits.

- or any decision on the implementation of security technologies the proportionality should be checked whether is strictly - by politically and hierarchically/organisationally independent evaluators

- All my answers must be seen in context of accordance with the rule of law - for states not conforming the Western understanding of democracy the so-called security technologies need to be disapproved because of suspicion of abuse; this is specifically valid for political changes within a country. Corresponding guidelines need to be obligatory for all EU states - otherwise the risks are too high.

- it was not a question whether one regards these technologies as an effective weapon against terrorism etc. This is not the case. All of them can be circumvented, if sufficient criminal potential is present.

- This questionnaire is not serious. The four questions from 37 to 40, suggest the assumption that in question of 40 yes well in question 38 suspicious persons are the basis. Question 70 mostly serves in your own interests, doesn't it?

- I think, that in borderline cases the right of privacy does not prevail. John Doe simply does not notice when eavesdropping etc. is applied.