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

Illustrated Scenarios – German Version

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

Author(s): Christine Hafskjold, The Norwegian Board of Technology
Translation: Johann Čas, Institute of Technology Assessment
Maren Raguse, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Illustrations: Åsne Flyen

Classification: Public

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**

Preface

The **PRISE**-project aims at contributing to a secure future for the European Union consistent with European citizens' civil rights - in particular privacy – and their preferences.

The project will:

- Develop criteria and guidelines for privacy compliant security research and technology development.
- Transform the results into scenarios that present applications of security technologies and measures that comply with civil rights and privacy to a varying degree.
- Test these scenarios in a set of participatory technology assessment procedures in different European states, allowing for a substantiated indication of public perception and citizens' preferences.
- Elaborate the sets of criteria and guidelines with direct involvement of providers of security technologies, private and public users and implementers, institutions and bodies shaping policies and regulation as well as organisations representing potentially and actually conflicting interests.
- Disseminate the results to actors relevant for the shaping of technologies and policies.

This document is a presentation of the scenarios developed in Work Package 4. Before being presented to the groups of lay people in different European states, the scenarios will be translated into their native language. The scenarios aim at giving the lay people insight into different security technologies and how they can be applied in everyday life in a near future. We try to address different approaches to the technologies, both from a user point of view, and in the society.

The technical descriptions in this document are adapted from *D 2.2 Overview of Security Technologies*.

The PRISE project would like to thank the group of experts that have helped us in developing the scenarios:

Asle Fossberg, The National Police Computing and Material Service

Marit Gjerde, The Norwegian Police University College

Nina Græger, Norwegian Institute of International Affairs

Ove Skåra, The Norwegian Data Inspectorate

Thomas Olsen, Norwegian Research Center for Computers and Law

We would also like to thank Jordi Mas, Deputy Director of the Catalan Foundation for Research and Innovation, who has been kind enough to provide feedback on the scenarios during the process.

Introduction

This document will present you with some scenarios showing how security technologies and surveillance may be used in everyday situations – in the near future.

1.1 What is security technology?

Security can be defined as the absence of danger – that is a state where the desired status quo is not threatened or disrupted in any way. In the context of the **PRISE** project, security is understood as the security of the society – or more precisely – of the citizens that constitute the society.

The term *security technology* can cover everything from private alarm systems and virus protection systems for PCs to border control systems and international police co-operation. In our scenarios we mainly focus on technologies or means (systems, legislation etc.) that are meant to enhance the security of the society against threats from individuals, or groups of individuals (not from states). This covers crime-fighting, anti-terror activities, border control activities etc.

In the scenario text we introduce some facts about the different technologies, to help you understand how they work today and their potential for the future.

1.2 What is privacy?

Privacy is generally associated with the protection of the integrity, autonomy and private life of the individual. Basically, it's about people's right to choose how they want to live their life, and what things they want to keep private. Privacy is considered a basic human right, and the first regulation of privacy is article 12 in the Universal Declaration of Human Rights.

What makes the protection of privacy difficult is the fact that privacy is almost always competing against other goods in society, such as mobility, efficiency, security or convenience. For example; even if we know that carrying a mobile phone that is turned on makes it possible to trace where we are, most of us would not dream of leaving the phone at home! And most people prefer having an RFID token in their car, rather than waiting in line to pay with (anonymous) cash when driving onto a toll-road.

Research suggests that many people are not concerned about technologies that infringe their privacy because they feel they have nothing to hide. Experts fear that this will result in a loss in privacy for the society that can be difficult to regain once it is gone. And even the most law-abiding citizen may find himself in a situation where he wouldn't want to be watched or traced.

When it comes to security technologies and surveillance, critics claim that a lot of the measures that are implemented are not suited to combat terror, but only to reassure the public that "something is being done". This is because the measures can be circumvented or because the threat they address is too unlikely to justify the action taken against it. A much used example of this is the banning of anonymous calling cards in many countries. Critics of this ban claim that it only stops ordinary people who would like to be anonymous; the criminals have ways of circumventing it by registering with a fake identity or using stolen mobile phones.

Some of the anti-terror initiatives, in particular in the United States, are very privacy infringing, such as eavesdropping telephone calls, screening electronic communication without a warrant or analysing someone based on data collected from different sources without informing the person in question.

An important privacy principle is that a person should be informed when his or her personal data is stored and processed, and that it is possible to get access to the data and check that it is correct. Personal data should only be collected and stored if it is really necessary and it should be deleted when it is no longer needed for the original purpose.

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 Gesichtserkennungssystemen. 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, 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

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 Videoüberwachungssysteme 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 Autokennzeichen 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.

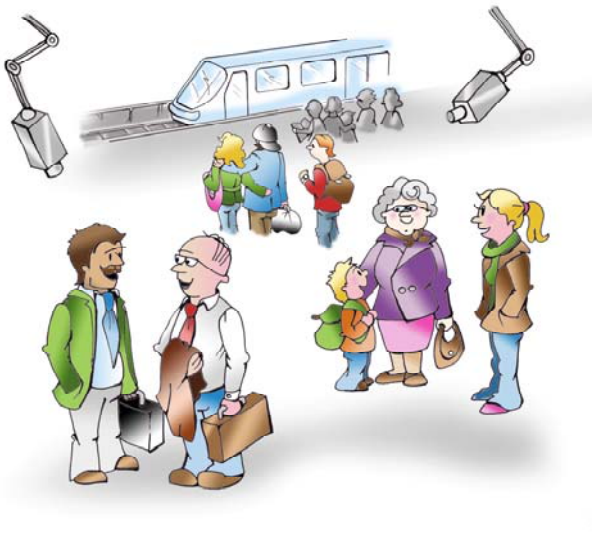
neuen Autos standardmäßig eingebaut, und es soll automatisch einen Notruf absetzen, wenn das Auto in einen Unfall verwickelt ist. Weil es das Galileo-System nutzt, kennt es die genaue Position des Autos.

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 satelliten-basierte 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."

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.

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 sein Personalausweis 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 sein neu ausgestellter Personalausweis wahrscheinlich gründlicher überprüft wurde als der 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.

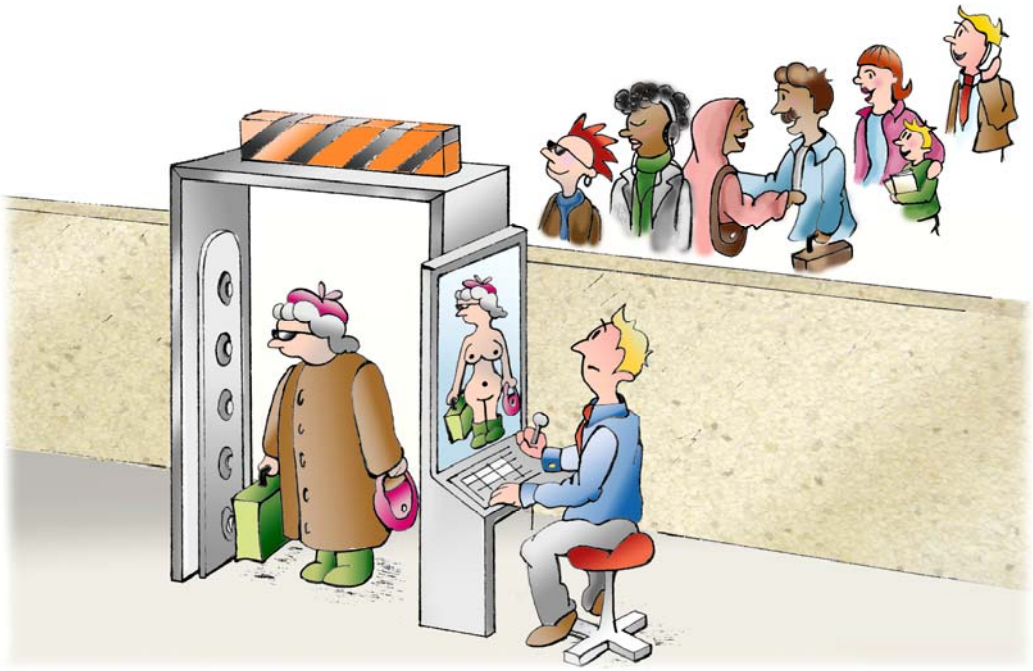
Personenscanner („Nackte Maschine“)

Röntgen- oder 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 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.

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.



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

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.

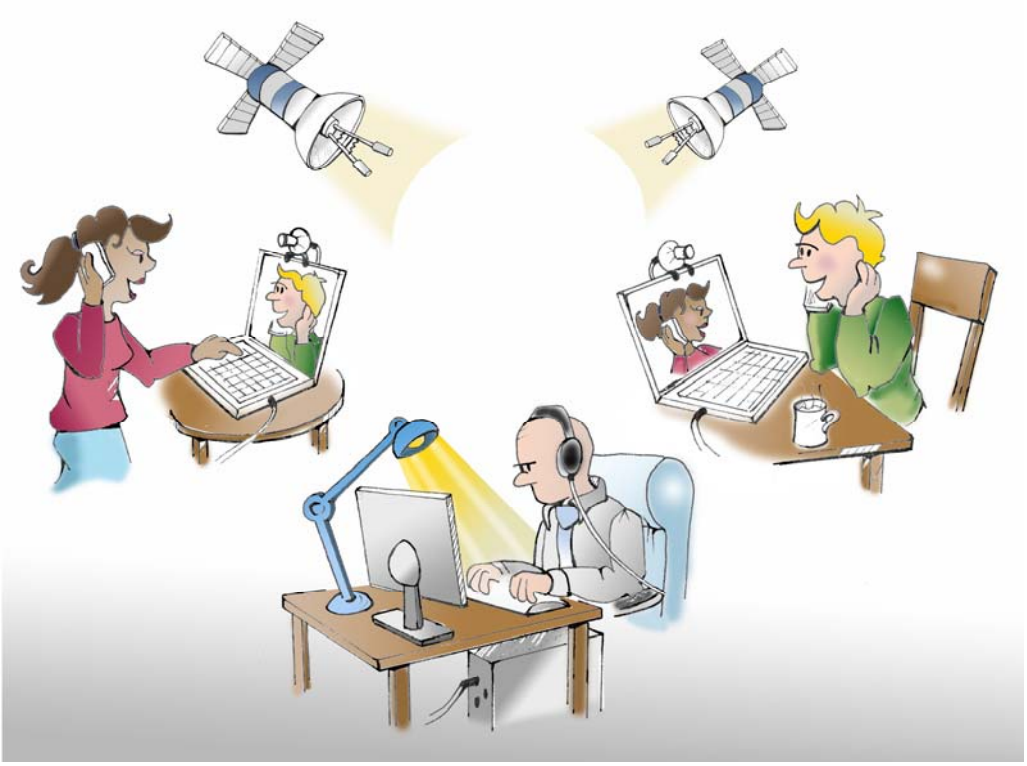
Das letzte Mal, als er mit Yasmin ausging, erwähnte sie, dass sie sich sicher war, dass ihre E-Mails abgehört werden, und sie bat ihn darum, ein Verschlüsselungsprogramm zu verwenden, wenn er ihr schreiben wollte. "Eine unverschlüsselte E-Mail ist wie eine Postkarte", erklärte sie. "Jeder, der Zugang 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 Arbeit-geber 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.