Wenn der Computer verschwindet

Was Datenschutz und Sicherheit in einer Welt intelligenter Alltagsdinge bedeuten

Marc Langheinrich, Friedemann Mattern
Departement Informatik, ETH Zürich

Kurz und bündig

Mit der weiter zunehmenden Miniaturisierung der Computertechnologie werden in absehbarer Zukunft Prozessoren und kleinste Sensoren in immer mehr Alltagsgegenstände integriert, wobei die traditionellen Ein- und Ausgabemedien von PCs, wie etwa Tastatur, Maus und Bildschirm, verschwinden und wir stattdessen „direkt" mit unseren Kleidern, Armbanduhren, Schreibstiften oder Möbeln kommunizieren (und diese wiederum untereinander und mit den Gegenständen anderer Personen). Solch eine Entwicklung hat weit reichende Konsequenzen für die Bereiche Sicherheit und Datenschutz, da wir ohne intensive Anstrengungen auf technischer, rechtlicher, wie auch sozialer Ebene schnell in Gefahr laufen, diese schöne neue Welt voller „smarter" und kommunikationsfreudiger Dinge in einen orwellschen Überwachungsstaat zu verwandeln.

Der verschwindende Computer

Der Fortschritt in der Informationstechnik und Mikroelektronik scheint weiterhin ungebrochen dem mooreschen Gesetz zu folgen, welches bereits seit mehreren Jahrzehnten recht präzise voraussagt, dass sich die Leistungsfähigkeit von Prozessoren etwa alle 18 Monate verdoppelt [Mo65]. Speicherkapazität und Kommunikationsbandbreite weisen derzeit sogar eine noch höhere Steigerungsrate auf. Zusammen mit Fortschritten in den Materialwissenschaften (z.B. „leuchtendes Plastik" oder „smart paper" mit elektronischer Tinte) lassen diese Entwicklungen die Annahme zu, dass unsere nahe Zukunft voll sein wird von kleinsten, spontan miteinander kommunizierenden Prozessoren, welche aufgrund ihrer flexiblen Formgestaltung und ihres vernachlässigbaren Preises leicht in Alltagsgegenstände integriert und dadurch kaum mehr als Computer im heutigen Sinne wahrgenommen werden.

Immer kleiner werdende Sensoren, vom einfachen Temperaturfühler und Lichtsensor hin zu Miniaturkameras, zusammen mit immer leistungsstärkeren Prozessoren und drahtlosen Kommunikationstechniken ermöglichen aber eine immer umfangreichere Erfassung und automatische Wahrnehmung der Umwelt. Sei es durch stationäre Installation von Funksensoren an Fassaden, Türen oder Einrichtungsgegenständen, sei es durch Integration von Informationstechnik in verschiedenste Alltagsgegenstände wie Möbel, Kleidung oder Accessoires – die Dinge in unserer Umgebung werden „smart" werden und über ihre ursprüngliche Funktionalität hinaus eine breite Palette zusätzlicher wünschenswerter (oder auch überflüssiger) „Services" anbieten können, wie z.B. Brillen, die uns beim zufälligen Treffen eines Bekannten durch das Einblenden dessen Namens auf die Sprünge helfen, oder Schreibstifte, die alle unsere Notizen digitalisieren und in einer Datenbank ablegen. Prinzipiell jedenfalls werden viele Gegenstände der Zukunft mittels spontaner Vernetzung und intelligenter Kooperation Zugriff auf jegliche in Datenbanken oder im Internet gespeicherte Information besitzen bzw. jeden passenden internetbasierten Service nutzen können. Die Grenzen solch eines „Internet der Dinge" liegen vermutlich weniger in der Technik, sondern sind allenfalls ökonomischer (was darf der Zugriff auf eine bestimmte Information kosten?) oder rechtlicher Art (was darf ein Gegenstand wem verraten?) [Mat01].

Weitere Fortschritte in den Materialwissenschaften beginnen nun, auch das äussere Erscheinungsbild des Computers drastisch zu verändern: Neuartige Werkstoffe in Form hochflexibler oder gar faltbarer Displays und Laserprojektionen aus einer Brille direkt auf die Netzhaut des Auges könnten in Zukunft traditionelle Ausgabemedien ersetzen. Im Bereich der Eingabemedien macht die Erkennung gesprochener Sprache langsame, aber stetige Fortschritte; schnellere Prozessoren werden die Erkennungsraten bald deutlich steigern. Flach in der Tapete, zusammengefaltet in der Tasche oder integriert in die Umgebung – mit miniaturisierter Informationstechnik und Sensorik können Informationen in naher Zukunft überall und jederzeit gewonnen und zugänglich gemacht werden. Der Computer als wahrnehmbares

Gerät ist dann verschwunden – er ist eine Symbiose mit den Dingen der Umwelt eingegangen und wird höchstens noch als eine unsichtbare Hintergrundassistenz wahrgenommen [Mat02].

Lückenlose Überwachung?

Während die Vision des „verschwindenden Computers" Designern und Ergonomen eine Vielzahl neuer Möglichkeiten zur Schaffung produktiver und benutzerfreundlicher Geräte bietet, sind es gerade die Aspekte der Unaufdringlichkeit und Nichtwahrnehmung, welche Datenschützern Kopfzerbrechen bereiten.

Schon beim Surfen im Internet sind sich die Wenigsten darüber im Klaren, dass nicht nur jeder Einkauf, sondern i.A. auch alle Mausklicks protokolliert werden und potentiell über ihre Vorlieben Auskunft geben können. Sollten sich „smarte" Alltagsgegenstände durchsetzen, wäre mit dem Ausschalten des PCs keineswegs auch die elektronische Datensammlung beendet: Ein mit Sensoren versehenes Haus würde seine Bewohner auf Schritt und Tritt verfolgen, um z.B. rechtzeitig Lichter ein- und auszuschalten; eine smarte Armbanduhr würde ständig die aktuelle Position des Benutzers ermitteln und weitermelden, um so ortsbezogene Dienste (z.B. die lokale Wettervorhersage oder die Anzeige des Rückwegs zum Hotel) nutzen zu können. So entstehen, durchaus ungewollt, quasi als Nebenprodukt der Verwendung solcher bequemer oder qualitätssteigender Dienste, leicht individuelle Aktivitätsprotokolle, welche beinahe lückenlos Auskunft über das Leben einer Person geben.

Erschwerend kommt hinzu, dass die unauffällige Einbettung von Computertechnik in Alltagsgegenstände oft im direkten Widerspruch zum Grundsatz der Offenlegung von Datensammlungen steht: die wenigsten Alltagsgegenstände verfügen etwa über akustische oder visuelle Signalgeber, mit denen sie die Aufmerksamkeit des Benutzers auf sich ziehen könnten, um diesen auf eine stattfindende Überwachung hinzuweisen. Auch würde die grosse Zahl elektronischer Transaktionen und Sensormessungen, die dann jeder Einzelne tagtäglich unbemerkt anstiesse, eine solche individuelle Benachrichtigung schnell ad absurdum führen. Elektronische Transaktionen und detaillierte Sensormessungen bilden jedoch die Grundlage der Vision vom verschwindenden Computer: Nach den eher ernüchternden Ergebnissen der Künstlichen Intelligenz in den vergangenen Jahren setzt man in der Informatikforschung nun auf das Prinzip der „Smartness", bei der eine Vielzahl von eher banalen Messgrössen auf eine kleine Anzahl vordefinierter Situationen abgebildet wird, um so eine gewisse Art von Kontextverständnis zu erreichen. Diese Konzentration auf den Kontext als Basis für „smartes" Verhalten führt jedoch unweigerlich zu einem „Sammeln auf Vorrat", denn erst in der nachträglichen Analyse der Daten offenbaren sich oft unerwartete Zusammenhänge, die eine Situation charakterisieren. Auch wenn viele der Messgrössen auf den ersten Blick nicht sonderlich vertraulich wirken sollten (z.B. die Schrittfrequenz einer Person oder deren Anzahl Lidschläge pro Minute), könnten anspruchsvolle Data-Mining-Systeme aus den zusammengeführten Einzeldaten weitaus sensitivere Informationen (z.B. den Nervositäts- oder Alkoholisierungsgrad einer Person) extrahieren.

Vertraulichkeit und Authentizität

Eine wichtige Voraussetzung zum Schutz persönlicher Daten in einem „Internet der Dinge" ist die Datensicherheit, worunter klassischerweise Vertraulichkeit, Zugriffsschutz und Authentizität fallen, aber im allgemeineren Sinne auch Eigenschaften wie Vertrauenswürdigkeit, Verfügbarkeit, Verlässlichkeit und Funktionssicherheit verstanden werden [ISTAG02].

In einer Welt smarter Dinge dürfte ein Hauptproblem des Risikomanagements – wie sich in diesem Umfeld der Begriff „Sicherheit" vielleicht auch charakterisieren lässt – in der Heterogenität und der grossen Zahl der beteiligten Komponenten liegen, die in einer offenen Umgebung sicher zusammenspielen sollen, wobei erschwerenderweise die Komponenten typischerweise mobil sind und untereinander spontane Kooperations- und Kommunikationsbeziehungen eingehen können. Klassische Sicherheitsprinzipien (z.B. Firewalls, Zertifikate, kryptographische Schlüssel), die i.A. eine eher statische Struktur und zentrale Autoritäten voraussetzen, genügen dann nicht mehr und lassen sich kaum geeignet auf die zu erwartenden Grössenordnungen hochskalieren.

Hinsichtlich der Vertraulichkeit ist zunächst offensichtlich, dass durch die notwendigerweise drahtlose Kommunikation mobiler Gegenstände eine im Prinzip einfache Mithörmöglichkeit durch benachbarte Empfänger gegeben ist – in der Regel erscheint also eine Verschlüsselung der Kommunikation unab-

dingbar. Dem stehen in manchen Fällen jedoch mangelnde Ressourcen entgegen: Kleinste Sensoren etwa haben nur sehr wenig Energie zur Verfügung, eine Verschlüsselung der weiterzumeldenden Sensordaten kann den Energiebedarf vervielfachen, was einige Anwendungen unmöglich macht.

Weiterhin ergeben sich durch die Mobilität von IT-Komponenten und dadurch, dass viele kleinere Alltagsgegenstände Sensoren und ein „Gedächtnis" bekommen, neue Sicherheitsanforderungen aufgrund des möglichen Verlusts oder Dienstahls solcher Dinge: Diese könnten dann einem Fremden Aufschluss über die sehr private Lebensgeschichte des eigentlichen Besitzers geben. Ein smartes Ding darf also nur einem autorisierten Kommunikationspartner etwas mitteilen – womit sich die Frage stellt, wer in welcher Weise Autorisierungen vornehmen kann und ob sich dies weitgehend automatisieren lässt.

Offensichtlich wird man nur einer vertrauenswürdigen Instanz Zugriff auf private Daten gestatten bzw. Handlungen im eigenen Interesse ermöglichen wollen. So sollte etwa eine ortsbewusste Spielzeugpuppe für Kinder nur den Eltern (bzw. deren elektronischen Helfern) ihren Aufenthaltsort verraten, oder die Dienstwaffe eines Polizisten sollte sich nur entsichern lassen, wenn der richtige smarte Fingerring in unmittelbarer Nähe ist. Das Problem der Autorisierung ist deshalb eng verbunden mit dem Problem, die Authentizität einer (vertrauenswürdigen) Instanz zweifelsfrei festzustellen sowie eine Art „Urvertrauen" zu anderen Instanzen zu bekommen.

Stajano schlägt vor, zur Herstellung dieses Urvertrauens das Prinzip der Prägung zu verwenden [Staj00]: Analog zu den Graugänsen des Verhaltensforschers Konrad Lorenz [Lor35] soll der erste physische Kontakt zweier smarter Dinge eine Vertrauensbasis aufbauen. Lorenz beschreibt zusammen mit seinem Schüler Paul Leyhausen das Prägungsprinzip so: „Die junge Graugans betrachtet jeden grossen, dunklen und bewegten Körper, den sie nach dem Schlüpfen aus dem Ei erstmalig erblickt, als „Mutter" und folgt ihm bedingungslos überall hin... Der Prägungsvorgang dauert nur wenige Augenblicke, und die Prägbarkeit hält nur kurze Zeit nach dem Schlüpfen an... Danach ist eine Änderung nicht mehr möglich, der Vorgang ist irreversibel" [Ley68].

Der Vorteil der Prägung liegt darin, dass diese in dezentraler Weise, ohne eine zusätzliche Autorität, erfolgen kann. In der Praxis wird man den physischen Kontakt je nach Situation verschieden realisieren. Es kann beispielsweise der spezifische Kontext zweier zusammen bewegter bzw. beschleunigter Objekte zur Einrichtung einer Vertrauensbeziehung genutzt werden [Holo0]. So liesse sich z.B. eine Kreditkarte durch kurzes Schütteln zusammen mit einem Handy so prägen, dass diese nur noch funktioniert, wenn sie sich in unmittelbarer Nähe des Handys befindet.

So einfach das Prinzip der Prägung scheint – viele Details bleiben offen, z.B.: lassen sich Prägungen einfach ändern, wenn ein Gegenstand rechtmässig einen anderen Besitzer erhält? Auch darüber hinaus wirft der Aspekt Sicherheit in einer Welt intelligenter Alltagsdinge noch viele ungelöste Fragen auf. Vertraut man mobilen Programmen, die als Update automatisch und unbemerkt in einen smarten Gegenstand geladen werden? Oder: kann ein zumindest eingeschränkter Funktionsumfang gewährleistet werden, wenn Sicherheitsmassnahmen parziell kompromittiert sein sollten? Technische Sicherheitslösungen, wie immer sie auch aussehen, müssen schlussendlich nutzergerecht realisiert, sozial akzeptiert und in vertrauenswürdige organisatorische und rechtliche Strukturen eingebunden werden. Die wichtige Frage, was eigentlich in welchem Umfang geschützt wird und wer in verschiedenen Situationen die Kontrolle, aber auch die Verantwortung über Sicherheitsmassnahmen hat, ist allerdings eher in gesellschaftlicher und politischer Hinsicht zu beantworten.

Grosser Bruder und kleine Geschwister

Technische Aspekte wie Sicherheitsprotokolle, Energieeffizienz und Benutzungsschnittstellen stellen derzeit die meistdiskutiertesten Herausforderungen für eine Zukunft mit allegenwärtigen Computern dar. Doch auch in Bereichen von Soziologie, Rechts- und Wirtschaftswissenschaften wirft eine solche Entwicklung eine Reihe von Fragen auf.

Während Datenschützer anfangs zunächst den allwissenden Staat, inzwischen aber mehr und mehr informationshungrige Marketingabteilungen grosser Firmen im Blickfeld haben, wird mit Miniaturkamera und in die Kleidung integriertem Computer jeder Einzelne zum ständigen Datensammler. Zwar ist Soziologen die gegenseitige Beobachtung in einer Gemeinschaft nicht neu, doch birgt der gleichzeitige Fort-

schritt in der Speichertechnologie die Gefahr, mittels lückenlosem digitalen Video- und Audioarchiv einem jeden von uns ein nahezu perfektes Gedächtnis zu ermöglichen. Dass dieses nicht nur an die mündlich vereinbarten Termine letzter Woche, sondern auch jede noch so kleine Notlüge oder ein gebrochenes Versprechen erinnern kann, könnte persönliche Gespräche, auch intimer Natur, nachhaltig verändern: An die Stelle des allwissenden „grossen Bruders" treten zahllose „kleine Geschwister" in Form neugieriger Nachbarn und eifersüchtiger Bekannter, deren Hemmschwelle für ein gelegentliches Bespitzeln mit dem technischen Aufwand für solch eine Überwachung sinken dürfte.

Auch im Zusammenhang mit dem erhöhten Sicherheitsbedürfnis der jüngsten Zeit erscheint solch eine Entwicklung brisant: An Stelle eines öffentlichen Aufrufs an potenzielle Zeugen nach einem Verbrechen könnte schon bald die freiwillige Freigabe der persönlichen sensorischen Datenbanken einer ganzen Bevölkerungsgruppe stehen, welche zusammen mit hoch entwickelten Suchalgorithmen eine Rasterfahndung ungeahnten Ausmasses erlauben würde. Ähnlich den immer populärer werdenden freiwilligen DNA-Analysen würden sich bei solchen Massnahmen all jene verdächtig machen, die den Sicherheitsorganen den uneingeschränkten Zugriff auf ihr „digitales Gedächtnis" verweigerten.

Selbst wenn die technische Realisierbarkeit solcher Szenarien noch in ausreichender Ferne liegen sollte, so birgt deren grundlegendes Prinzip – dh. die sekundäre Nutzung von Daten jenseits ihres ursprünglichen Zwecks – schon in näherer Zukunft Konfliktpotenzial. Nachdem Leihwagenfirmen bereits die Vorteile von GPS-Empfängern und Mobilfunk für das Lokalisieren gestohlener Wagen zu schätzen gelernt haben, gibt es inzwischen erste Verleiher, die mit der gleichen Technologie auch den pfleglichen Umgang des Mieters mit dem Fahrzeug sicherstellen: so erhebt z.B. eine Mietwagenfirma in den USA ihren Kunden eine Gebühr für „gefährliches Fahren", sobald sich der Wagen mit mehr als 79 Meilen pro Stunde bewegt [CNET01]. Einige Versicherer erwägen auch bereits den Einsatz von flugzeugähnlichen „Black Boxes" am Fahrzeug, um Kunden auf den individuellen Fahrstil optimierte Prämien berechnen zu können bzw. im Schadensfall die Schuldfrage zu klären. Schleichend entsteht so ein feinmaschiges Überwachungsnetz, welches schon bald die klassische Unschuldsvermutung in der Rechtssprechung in eine grundsätzliche Schuldvermutung umkehren könnte: Wer keine eigene Aufzeichnungen des fraglichen Zeitpunktes vorweisen kann, da er bewusst auf die damit verbundenen Vorteile wie z.B. geringere Prämien verzichtet, macht sich verdächtig.

Auf wirtschaftlicher Seite wird die weitere Durchdringung der Alltagswelt mit Informationstechnik zunächst die Versorgungskette optimieren helfen, bei der durch eine lückenlose Verzahnung der Erfassungssysteme sowohl Hersteller als auch Detail- und Zwischenhändler zu jedem Zeitpunkt exakte Zahlen zur Planung ihrer Produktion bzw. Bestellmengen zur Verfügung stehen, um damit kapitalintensive Lagerbestände zu minimieren. Es bleibt abzuwarten, wie derart eng vernetzte und hoch optimierte Versorgungssysteme im Falle unvorhergesehener Ereignisse reagieren. Einen Vorgeschmack bot bereits die kurzzeitige Sperrung der US-kanadischen Grenze nach dem 11. September 2001, als die amerikanische Automobilproduktion durch das Ausbleiben kanadischer Zulieferer aufgrund der minimal kalkulierten Lagerbestände innert weniger Stunden grösstenteils zum Erliegen kam.

Letztlich werden durch eine Welt voller intelligenter Alltagsdinge auch komplett neue Geschäftsmodelle möglich. Leasingverträge werden nicht nur die tatsächliche Nutzung eines Autos dank einer Black Box genauestens erfassen können, sondern vielleicht auch auf andere Alltagsgegenstände wie beispielsweise Möbel oder Kleidung ausgedehnt werden: So könnten Sensoren den genauen Gebrauch einer Waschmaschine oder TV-Gerätes exakt protokollieren, um bei Überschreitung der vertraglich vereinbarten Nutzung automatisch einen Aufschlag zu berechnen. Ähnlich wie beim Auto-Leasing könnte solch eine Entwicklung ihren Anfang in gewerblichen Umgebungen (z.B. Hotels) nehmen, aber aufgrund veränderter Preisstrategien der Hersteller letztendlich auch für Privatpersonen finanziell attraktiver als Eigenbesitz werden. Dass wir dann nicht mehr nur von unseren Nachbarn und Bekannten, sondern sogar von unseren eigenen Haushaltsgeräten überwacht werden (die ja als Leasinggeräte loyal gegenüber dem Händler bleiben), verschärft nicht zuletzt auch die Datenschutzproblematik weiter.

Ausblick

Datenschutz und Sicherheit waren noch nie sonderlich attraktiv, da sie sowohl Anbietern als auch Nutzern von Diensten eine erhöhte Aufmerksamkeit abverlangen und gleichzeitig deren Handlungsmög-

lichkeiten oft signifikant einschränken [Roso1a]. Im Zeitalter intelligenter Alltagsdinge wird ihnen jedoch eine noch weitaus grössere Rolle zuteil werden als bisher, sofern wir nicht einige unserer demokratischen und menschlichen Grundrechte in Frage stellen wollen.

Hier ist zunächst der Gesetzgeber gefordert, wenn er überholte Sicherheits- und Datenschutzbestimmungen der technischen und marktwirtschaftlichen Realität anpassen muss, die durch die Vereinfachung von Datensammlung und dem Verschwimmen von Grenzen zwischen Datensubjekt und Datensammler gekennzeichnet ist [Roso1b]. Klare Richtlinien, wie etwa eine elektronische Kennzeichnungspflicht für Sensoren, könnten einer ungewollten Proliferation von versteckter Überwachungstechnik zuvorkommen. Ebenso muss bei aller Dringlichkeit der Verbrechensbekämpfung eine schleichende Totalüberwachung durch zukünftige Gebrauchgegenstände des Alltags verhindert werden.

Ferner sollten sich Forschung und Entwicklung in der Informationstechnik stärker als bisher um die ethischen Konsequenzen kümmern, ähnlich wie dies zumindest teilweise schon in den Naturwissenschaften der Fall ist. „Code is Law" behauptet etwa der US-Rechtsprofessor Laurence Lessig [Les99] und bezieht sich dabei auf die von Softwareingenieuren geschaffenen Möglichkeiten einer Technologieplattform, welche oft „de-facto" in erheblicher Weise gesetzlichen Regelungen vorgreifen (als Beispiel seien hier digitale Kopierschutzmechanismen genannt, welche die oftmals bestehenden nationalen Rechte zum Besitz geistigen Eigentums ignorieren).

Interdisziplinarität dürfte also in Zukunft mehr denn je die Arbeit von Informatikern, Elektroingenieuren, Rechts- und Sozialwissenschaftern bestimmen. Dies lässt hoffen, dass – bei der Brisanz der hier andiskutierten Aspekte einer Welt intelligenter Alltagsdinge – eine fruchtbare und fächerübergreifende Diskussion doch noch zu der oftmals als Quadratur des Kreises angesehene Balance zwischen Bequemlichkeit, Sicherheit, und Freiheit führen wird.

Literaturverzeichnis

[CNET01] Robert Lemos: Rental-car firm exceeding the privacy limit? CNET News, June 2001. http://news.com.com/2100-1040-268747.html?legacy=cnet&tag=tp_pr

[Holoo] Lars Erik Holmquist, Friedemann Mattern, Bernt Schiele, Petteri Alahuhta, Michael Beigl, Hans-W. Gellersen: Smart-Its Friends – A Technique for Users to Easily Establish Connections between Smart Artefacts. Proc. Ubicomp 2001, Springer-Verlag LNCS 2201, pp. 116-122, 2001

[ISTAG02] IST Advisory Group: Trust, Dependability, Security & Privacy for IST in FP6. ftp://ftp.cordis.lu/pub/ist/docs/istag-security-wg61final0702.pdf

[Les99] Lawrence Lessig: Code and Other Laws of Cyberspace. Basic Books, 1999

[Ley68] Paul Leyhausen, Konrad Lorenz: Über die Wahl des Sexualpartners bei Tieren. In: Antriebe tierischen und menschlichen Verhaltens (gesammelte Abhandlungen), 131-141, Piper, 1968

[Lor35] Konrad Lorenz: Der Kumpan in der Umwelt des Vogels. Journal für Ornithologie 83: 137-215; 289-413, 1935

[Mato1] Friedemann Mattern, Marc Langheinrich: Allgegenwärtigkeit des Computers – Datenschutz in einer Welt intelligenter Alltagsdinge. In: G. Müller, M. Reichenbach (Hrsg.): Sicherheitskonzepte für das Internet, 7-26, Springer-Verlag, 2001

[Mato2] Friedemann Mattern: Ubiquitous Computing – Szenarien einer informatisierten Welt. In: A. Zerdick, A. Picot, K. Schrape, J.-C. Burgelman, R. Silverstone (Hrsg.): E-Merging Media – Digitalisierung der Medienwirtschaft, Springer-Verlag, 2002

[Mo65] Gordon E. Moore: Cramming More Components onto Integrated Circuits. Electronics 38, 8, pp. 114-117, 1965

[Roso1a] Alexander Roßnagel: Datenschutz in Zeiten der Terrorismusbekämpfung. FiFF-Kommunikation 4/2001, pp. 10-11, 2001

[Roso1b] Alexander Roßnagel, Andreas Pfitzmann, Hansjürgen Garstka: Modernisierung des Datenschutzrechts, Bundesministerium des Inneren, Berlin 2001. http://www.bmi.bund.de/downloadde/11659/Download.pdf

[Stajoo] Frank Stajano, Ross Anderson: The Resurrecting Duckling – What Next? In: Bruce Christianson et al. (eds.): Security Protocols, 8th Int. Workshop, Springer-Verlag LNCS 2133, pp. 204-214, 2000