Privacy in einer Zukunft mit allgegenwärtigen Informationstechnologien – Ein Widerspruch in sich?

Johann Čas

Innerhalb einer nicht allzu fernen Zukunft wird es der rasante technische Fortschritt in der Elektronik erlauben, die heutigen Visionen von allgegenwärtigen Informationstechnologien in realistische Optionen zu transformieren. Diese Aussicht erweckt tiefe Besorgnis über den Fortbestand der Privatsphäre, da zentrale Elemente des Pervasive Computing in direktem Widerspruch zu den Fundamenten des Datenschutzes stehen. Beträchtliche Anstrengungen wurden unternommen, um diesen Bedenken Rechnung zu tragen, jedoch mit bescheidenen Ergebnissen. Während die Bemühungen zwar Lösungen für einzelne Aspekte anboten, erwiesen sie sich als ungenügend, die Ängste zu zerstreuen. Sie machten im Gegenteil die prinzipiellen Unvereinbarkeiten zwischen dem Schutz der Privatsphäre und allgegenwärtigen Informationssystemen deutlich. Technische Maßnahmen können auf sich alleine gestellt nicht genügen, gleichgültig wie komplex und ausgefeilt sie auch sein mögen. Um nennenswerte Reste von Privatheit aufrechterhalten zu können, wird ein Mix von Privacy Enhancing Technologies, Beschränkungen bei der Nutzung von Pervasive Computing und neue Regulierungen notwendig sein.

1 Allgegenwärtige Informationstechnologien und Privacy

Die kommenden Jahre versprechen, eine neue Ära der Informationstechnologien einzuläuten, in der revolutionäre technische Systeme aus den Gedanken und Phantasien von Wissenschaftern, Technikern und Managern von IT-Konzernen in reale Anwendungen transferiert werden können. Das neue Paradigma der Informationstechnologie – bekannt unter Begriffen wie Pervasive, Calm oder Ubiquitous Computing und Ambient Intelligence – eröffnet einerseits völlig neue Möglichkeiten, Unzulänglichkeiten bestehender Informationssysteme zu überwinden; andererseits birgt es auch enorme Risken für Individuen und die Ge-

sellschaft in sich.[1] Ubiquitous Computing (UC) verspricht, ehemals unvorstellbare Möglichkeiten der Unterstützung menschlicher Aktivitäten durch eine Technologie, die unbemerkt und unbemerkbar im Hintergrund arbeitet.

Offensichtlich bedeuten und bedingen allgegenwärtige Dienste auch allgegenwärtige Beobachtung des Verhaltens, von Gewohnheiten, persönlichen Vorlieben und Abneigungen, politischer Zugehörigkeiten und des emotionalen Befindens. Während derzeit die Generierung von Daten überwiegend an Aktivitäten geknüpft ist, denen sich die Beobachteten bewusst sind und welche daher zumindest vom Prinzip her unter individueller Kontrolle stehen, entzieht das neue Paradigma den Individuen die Freiheit, diese Entscheidung treffen zu können. Obschon diese Freiheit auch heute in der Realität vielfach nur mehr eingeschränkt gegeben ist oder oft mit einem nicht akzeptierbaren Verzicht auf die volle Teilnahme am beruflichen oder privaten Leben verbunden ist – zum Beispiel auf Mobiltelefone oder die Nutzung des Internets (Acquisti 2004) zu verzichten –, schafft die Unmöglichkeit einer Beobachtung zu entgehen, dennoch völlig neue Voraussetzungen.

Es ist jedoch nicht die Menge an Daten allein, die Personen und Institutionen, welche sich mit der Privatsphäre beschäftigen, in einen Alarmzustand versetzen. Wenn Tastaturen und Mäuse durch Eingaben in natürlicher Sprache ersetzt werden, Identifikation oder Autorisierung über Passwörter durch biometrische Verfahren, bewusste und aktive Eingaben durch eine permanente Beobachtung des emotionalen Status mittels Emotiometrie[2], dann sind auch die verbliebenen Reste von Privacy massiv bedroht. Diese Gefahren werden von Entwicklern und Wissenschaftern im Bereich Pervasive Computering weitgehend gesehen und anerkannt. Beträchtliche Forschungsanstrengungen wurden unternommen, um allgegenwärtige Informationstechnologien zu entwickeln, welche die Privatsphäre respektieren.

Was aber fehlt, ist ein überzeugendes Konzept für die Gestaltung von „Pervasive-Computing"-Systemen, welches ein akzeptables Niveau an Privatsphäre in der Zukunft garantieren könnte. Die meisten der heute diskutierten Ansätze können die zukünftigen Technologien – in einem beschränkten Ausmaß – weni-

[1] Der Vielfalt von Begriffen steht eine noch größere Vielzahl von technischen Konzepten zur Realisierung von allgegenwärtigen Informationstechnologien gegenüber. Diese reichen von eher personenzentrierten Konzepten wie „Wearable Computing" und „intelligenten" Kaffeetassen über „intelligente" Räume bis hin zu „intelligentem Staub", eine Bezeichnung für winzigste, sich untereinander selbst vernetzende, mit sensorischen Fähigkeiten ausgestattete elektronische Komponenten. Für die hier geführte Diskussionen von Widersprüchen dieser Technologie mit dem Grundrecht auf Privatsphäre ist die technische Gestaltung der UC-Infrastrukturen ohne Belang. Diese resultieren im wesentlichen aus dem allen Konzepten gemeinsamen Ziel, aktive Interaktionen der Nutzer mit dem System durch deren permanente Beobachtung zu ersetzen.

[2] In Analogie zum Begriff Biometrie bezeichnet dieser Ausdruck die Messung von emotionalen Zuständen und deren Anwendung in der Informationstechnologie.

ger privacy-invasiv ausformen. Sie sind jedoch unzureichend, um das inhärente, privatsphärenzerstörende Potenzial zu überwinden. Andere Ansätze bergen wieder neue Bedrohungen für die Privatsphäre in sich, indem sie etwa auf einer verpflichtenden Identifikation der betroffenen Personen aufbauen.

Ein wesentlicher Grund für die beschränkten Möglichkeiten, privacy-freundliche „Pervasive-Computing"-Systeme zu gestalten oder sich auch nur vorstellen zu können, ist in dem Faktum zu sehen, dass dieses Technologiefeld in fundamentalen Widerspruch zu den wichtigsten Prinzipien des gegenwärtigen Datenschutzes steht. Diese Widersprüche zwischen Visionen über Pervasive Computing und den Fundamenten, auf denen ein zentrales Menschenrecht in demokratischen Gesellschaften aufbaut, implizieren, dass die Aufrechterhaltung von Privacy in einer zukünftigen Welt mit ubiquitären Informationstechnologien eine komplexe Aufgabe sein wird, welche Aktivitäten und Maßnahmen auf mehreren Ebenen erfordern wird. Eine dieser Maßnahmen wird es natürlich sein, das Recht auf Privatsphäre bereits beim Design dieser Technologien zu berücksichtigen und so weit als möglich „Privacy Enhancing Technologies" (PETs) zu integrieren. Bei einer zweite Kategorie von Maßnahmen wird es darum gehen, wenn notwendig, die Anwendung dieser Technologien selbst zu beschränken; eine dritte, dort wo die alten Regelungen nicht mehr greifen, neue regulative Fundamente für den Schutz der Privatsphäre zu schaffen. Nicht zuletzt wird es aber notwendig sein, breite öffentliche Debatten zu initiieren, damit die technische Entwicklung den Menschen dient anstatt die Menschen zu Sklaven der Technik zu machen.

Im nächsten Abschnitt werden einige Bedrohungen allgegenwärtiger Informationstechnologien für die Privatsphäre diskutiert. Im darauf folgenden Abschnitt werden Widersprüche zwischen den Prinzipien des Schutzes der Privatsphäre und dem Pervasive Computing analysiert. In zwei weiteren Abschnitten werden vorgeschlagene Maßnahmen diskutiert, mit denen allgegenwärtige Informationstechnologien privacy-verträglich gemacht werden sollen, und die Konsequenzen dieses Technologiefeld ist für die gesellschaftliche Nachhaltigkeit thematisiert.

2 Privacy-Risken des Pervasive Computing

Die UC-Visionen rufen Szenen aus Filmen über antike Zeiten in Erinnerung, in denen zahllose Sklaven versuchen, die Wünsche ihrer mächtigen Herren zu erahnen, um nicht in deren Ungnade zu fallen. In der Zukunft sollen unzählige elektronische Komponenten, welche unsichtbar in die alltägliche Umgebung integriert sind, die menschlichen Sklaven ersetzen. Natürlich konnten auch die antiken Herren Privatheit nicht in jener Form genießen, zu der sich dieses Kon-

zept bis zum heutigen Tage hin entwickelt hat. Sie konnten aber sehr wohl absolute Kontrolle und Herrschaft über ihre Untergebenen und damit auch über die „persönlichen Daten", die sie ihren Dienern preisgaben, ausüben.

In den Zeiten, die uns bevorstehen, werden mehr und mehr persönliche Daten offen gelegt werden – sowohl in quantitativer als auch in qualitativer Hinsicht – , allerdings ohne jegliche Kontrolle über Generierung, Austausch Weitergabe und Nutzung. Der quantitative Zuwachs resultiert aus der zunehmenden Durchdringung der Umwelt mit IT und dem perfekten Gedächtnis von Computern. Diese quantitative Steigerung impliziert auch eine neue Qualität der gesammelten Daten, da die Entstehung dieser Daten nicht mehr an Online-Aktivitäten oder die Nutzung von Telekommunikationsdienste geknüpft sein wird, sondern das gesamte Online- und Offline-Verhalten umfassen wird.

Eine Veränderung der Qualität der erfassten Daten wird durch den Übergang von textbasierten Informationen zu multimedialen Daten resultieren (Adams/ Sasse 2001). Außer dem Inhalt einer Nachricht enthüllen Texte zum Beispiel auch Informationen über die Lese- und Schreibfähigkeiten oder die Allgemeinbildung des Verfassers. Tonaufnahmen stellen darüber hinaus zusätzliche Informationen zur Verfügung, etwa einen möglichen Akzent oder rhetorische Fähigkeiten, während Videoaufzeichnungen visuelle Merkmale enthüllen, etwa die Bekleidung, die körperliche Verfassung oder die Körpersprache. Völlig neue Qualitäten an Informationen werden durch Sensoren möglich werden, welche die Fähigkeiten menschlicher Sinne übertreffen: Ein Beispiel wären Infrarot-Kameras, welche kleinste Veränderungen in der Blutzirkulation erfassen können, die noch weit davon entfernt sind, ein sichtbares Erröten zu erzeugen. Solche Veränderungen in der Durchblutung oder auch ein unmerkliches Zittern in der Stimme könnten einer Nervosität zugeschrieben werden, und diese Sensoren könnten so als ausgeklügelte und unsichtbare Lügendetektoren dienen. Da diese Daten zwischen unzähligen Sensoren, Prozessoren, Datenbanken und Ausgabegeräten ausgetauscht werden müssen, geht auch die Kontrolle über diese Daten zwangsläufig verloren.

Diese bekannten Bedrohungen für die Privatsphäre rufen zwei Hauptlinien von Reaktionen hervor: einerseits wird das „Ende der Privatsphäre" proklamiert (Whitaker 1999), andererseits wurde und wird versucht, Wege zur privatsphärenschonenden Gestaltung dieser Systeme zu finden. Einige diese Versuche werden in Abschnitt 4 diskutiert; hier zunächst zu den Folgen für die Privatsphäre.

2.1 Allgegenwärtige Überwachung und langfristige Datenspeicherung

Umgebungen mit allgegenwärtigen Informationstechnologien ähneln in großem Ausmaß perfekten Überwachungsinfrastrukturen. Die Durchdringung mit Informationstechnologien bleibt aber nicht auf die Umgebung beschränkt, in der wir leben oder arbeiten, sie macht auch vor den Menschen selbst nicht halt. Zum einen tragen sie RFID-Chips mit sich, welche in ihre Kleidung, persönlichen Gegenstände oder in ihre Körper integriert sind; zum anderen werden sie zu mit Audio- oder Videoaufnahmegeräten ausgestatteten Beobachtern. Elektronische Accessoires, die lebenslange Audioaufnahmen erlauben, sollen im Jahr 2008 zu Preisen von etwa $ 200 erhältlich sein; im Jahr 2010 sollen zum selben Preis lebenslange komprimierte Videoaufnahmen möglich werden (Halderman 2003). Dabei stellt aber die Möglichkeit, dass praktisch jede Person permanent Aufzeichnungen durchführen kann, nur einen kleinen Ausschnitt jener Bedrohungen für die Privatsphäre dar, die von vollständig implementierten UC-Systemen zu erwarten sind. Diesen Anwendungen fehlt immer noch die umfassende Überwachungskapazität, welche durch unzählige Sensoren und Prozessoren verkörpert wird. Sie verfügen nicht über Fähigkeiten zur spontanen Vernetzung und zum Zugriff auf beliebige Daten, die an beliebigen Orten gespeichert sind, und es mangelt ihnen an all den analytischen Fähigkeiten, mit denen Systeme allgegenwärtiger Informationstechnologien ausgestattet sein sollen. Trotzdem können bereits diese einfachen Aufnahmegeräte die Gefahren in perfekter Weise veranschaulichen: Jede Kommunikation, jeder persönliche Kontakt, jeder Austausch von Informationen, der vermeintlich im Privaten stattfindet, könnte mitgeschnitten und jederzeit wiedergegeben werden.

Viele Anwendungen von UC-Systemen erfordern, dass die erfassten Daten für extrem lange Zeiträume gespeichert werden. So ist es etwa das Ziel von künstlichen Gedächtnissen den lebenslangen Zugriff auf Aufzeichnungen von vergangenen Ereignissen zu ermöglichen. Die Lern- und Anpassungsfähigkeiten von UC-Systemen werden in der Regel von mehr Daten, welche längere Zeiträume umfassen, profitieren. Mit zunehmenden Rechenkapazitäten und sinkenden Speicherkosten werden wirtschaftliche Grenzen für Datensammlungen jegliche Bedeutung verlieren. Die Existenz dieser Daten bringt offensichtlich das Risiko ihres Missbrauchs mit sich. Peinliche Ereignisse, die normalerweise schnell wieder vergessen werden würden, könnten immer wieder in in das Gedächtnis zahlreicher Personen gerufen werden. Mögliche Fehlinterpretationen aufgrund mangelnder Informationen zum Kontext von bestimmten Handlungen bergen zusätzliche Risken für die Privatsphäre in sich.

2.2 Re-Personalisierung von Daten

Daten, die von pervasiven Informationssystemen gesammelt werden, sind prinzipiell persönliche Daten, oder es kann zumindest ein Personenbezug wiederhergestellt werden. Derzeit stellt in der Regel ein einzelner PC oder ein bestimmtes Gerät den Zugang zu Informationssystemen oder Telekommunikationsdiensten für individuelle Nutzer her. Der Begriff Personal Computer weist bereits darauf hin, dass die weit verbreitete Annahme, bei der Nutzung des Internets anonym zu sein, normalerweise nicht zulässig ist. Die Artefakte, welche zwischen den Nutzern und dem Informationssystem vermitteln, können aber auch genutzt werden, einen anonymen oder pseudonymen Zugang zu ermöglichen. Bei Pervasive Computing und dessen unzähligen Komponenten ist es hingegen der Nutzer selbst, der die Sammlung und Auswertung von Daten oder die Bereitstellung von Diensten initiiert und auslöst. Eine Art der Identifizierung der Person, die aktiv eine Leistung nachfragt oder unbewusst einen Prozess auslöst, ist daher unvermeidbar.

Die Möglichkeit, dabei Pseudo-Identitäten zu nutzen, ist in mehrfacher Hinsicht begrenzt. Bevor ein Sprachkommando interpretiert werden kann, muss die Präsenz einer Person erkannt werden; bevor die Mimik beobachtet werden kann, muss ein Gesicht erkannt werden; diese Personen und Gesichter müssen voneinander unterschieden werden, um sinnvolle Ergebnisse zu erzielen. Spracherkennung oder die Interpretation von Gesten erfordern die Erfassung von Audio- oder Videodaten; diese können auf einfache Weise zur biometrischen Identifizierung (wieder-) verwendet werden. Die Grundlage für kontextbasierte Dienste ist natürlich der Kontext selbst; mit der Erfassung des Aufenthaltsortes als einen wichtigen Teilaspekt des Kontextes werden in den meisten Fällen schon hinreichend Daten für eine persönliche Identifikation vorhanden sein. Nicht zuletzt macht UC nur Sinn, wenn die Systeme aus der Vergangenheit lernen und die Dienste entsprechend anpassen können. Dies erfordert wiederum, dass es diesen Systemen erlaubt sein muss, sich „zu erinnern“, das heißt persönliche Daten zu speichern und miteinander zu verknüpfen. Der normale Status von Pervasive Computing wird es daher immer sein, dass die persönliche Identität von erfassten Individuen (wieder-)hergestellt werden kann. Selbst wenn es gelänge, alle der genannten Wege zur Identifikation auszuschließen, könnte ein einzelner unbemerkter oder vergessener RFID-Chip in einem der mitgeführten Gegenstände die persönliche Identität preisgeben. Anstatt durch fehlende Glieder in Beweisketten wird der Normalzustand jedoch eher dadurch gekennzeichnet sein, dass genügend Daten vorhanden sind, um die Anonymität oder Pseudonymität zu durchbrechen.

2.3 Zunehmende Informationsasymmetrie

UC vergrößert notwendigerweise die bereits bestehenden Asymmetrien zwischen den beobachteten Individuen und den Datensammlern. Es war bereits in der Vergangenheit fast unmöglich, genau zu wissen, wer welche Daten sammelt, zu welchen Organisationen diese transferiert werden oder für welche Zwecke sie Verwendung finden. Dennoch waren die Datensammlungen zu einem großen Teil auf Bereiche konzentriert, bei denen die Nutzer Informationen freiwillig bereitstellten, etwa beim Ausfüllen von Formularen, oder bei denen die Nutzer sich zumindest prinzipiell bewusst sein konnten, dass Daten generiert werden, etwa bei der Nutzung von IKT. Weiters hatten die Bürger von Staaten mit modernen Datenschutzregelungen – zumindest theoretisch – das Recht, darüber informiert zu werden, welche Daten über sie zu welchem Zweck gesammelt wurden. UC-Umgebungen werden diese Situation auf den Kopf stellen. Der Wunsch, Dienste des „Pervasive Computing" in unaufdringlicher Weise zur Verfügung zu stellen, macht den Aufbau von Infrastrukturen notwendig, in denen die Nutzer permanent beobachtet und ihr Verhalten und ihre Aktionen unter Einbeziehung kontextueller Informationen autonom interpretiert werden. Die Ergebnisse werden in einen andauernden Lernprozess eingespeist, der die Grundlage für autonome Entscheidungen des Systems bildet, wie und wann die gesammelten Informationen genutzt oder weitergeleitet werden sollen.

2.4 Panoptische Gesellschaft

Die einzige realistische Annahme von Menschen, die in solchen Umgebungen leben, ist es, davon auszugehen, dass jegliche Aktivität oder Nichtaktivität überwacht, analysiert, weitergeleitet und gespeichert wird und in jedem beliebigen Zusammenhang in der Zukunft genutzt werden kann. Natürlich wird noch einige Zeit vergehen, ehe UC weit verbreitet sein wird, und natürlich wird es auch in Zukunft überwachungsfreie Zonen geben. Es wird sich aber niemand irgendwo sicher sein können, dass seine Handlungen wirklich nicht beobachtet werden und seine Gespräche nicht aufgezeichnet werden, oder dass sein gegenwärtiger Aufenthalt nicht in irgendwelchen Registern gespeichert wird. Auf diese Art und Weise wird das „Panoptikum" oder „Inspection-House" – ein von Jeremy Bentham (1791) primär für Gefängnisse und Irrenhäuser, aber auch für Schulen oder Fabriken entwickeltes Konzept – für öffentliche und private Räume im Allgemeinen zur Realität. Wie von Bentham beabsichtigt und von Foucault (1997) weiter thematisiert, ist allein die Möglichkeit der andauernden Beobachtung ausreichend, um strikte Disziplin und Gleichförmigkeit in Gesellschaften zu erzeugen.

Nichtsdestoweniger ist das Panoptikum immer noch eine unvollkommene Beschreibung der disziplinierenden Macht von „Pervasive Computing Systemen". Menschen, die in zukünftigen UC-Umgebungen leben, können mit fast hundertprozentiger Sicherheit davon ausgehen, dass sie beobachtet werden – im Gegensatz zum klassischen Panoptikum, in dem sich niemand sicher sein konnte, ob er oder sie zu einem bestimmten Zeitpunkt tatsächlich überwacht wird. Darüber hinaus waren klassische Überwachungsaktivitäten auf bestimmte Orte oder Zeiten beschränkt, während die Datensammlung durch UC diese zeitlichen und räumlichen Schranken überwindet.[3]

3 Widersprüche zu den Fundamenten von Privacy

Grundrechte sind zugleich eine der Voraussetzung und ein Ergebnis demokratischer Gesellschaften. Der Schutz der Privatsphäre ist eine zentrale Komponente der Menschenrechte, dementsprechend ist er sowohl in der Allgemeinen Erklärung der Menschenrechte der Vereinten Nationen (Artikel 12) und in der Grundrechtscharta der Europäischen Union (Artikel 7 und 8) festgeschrieben. Menschenrechte genießen besonderen Schutz in den Verfassungen demokratischer Staaten, in denen sie als unveränderliche Prinzipien verankert sind oder zumindest dadurch abgesichert sind, dass besonders hohe Anforderungen an ihre Veränderung und Anpassung geknüpft sind, um sie vor politischer Willkür zu bewahren.

Die erwähnten Artikel beschreiben das Recht auf Privatsphäre in allgemeiner Weise, welche keine detaillierten Untersuchungen von möglichen Inkompatibilitäten und Widersprüchen zwischen UC und diesen Grundrechten erlauben. Für diesen Zweck muss man auf konkrete Empfehlungen oder rechtlichen Normen zurückgreifen, die in Zusammenhang mit der Anwendung von Informationstechnologien entwickelt wurden. In diesem Bereich wurden Widersprüche zwischen der technischen Entwicklung und diesem Grundrecht schon früh offenbar. In den nächsten Abschnitten werden die wichtigsten Bedingungen und Vorschriften aus den OECD-Privacy-Guidelines (OECD 1980) und der EU-Datenschutzrichtlinie 95/46/EC (Europäisches Parlament und Rat 1995) mit inhärenten Eigenschaften von Pervasive Computing Systemen verglichen. Obwohl rechtlich nicht verbindlich, haben die OECD-Richtlinien – die seit einem Vierteljahrhundert unverändert gültig sind – in viele freiwillige Vereinbarungen und gesetzlich abgesicherte

[3] Zum Begriff der „Überwachung" siehe auch den Beitrag von Peissl i.d.B.

Regulierungen Eingang gefunden, darunter auch in die erwähnte Datenschutzrichtlinie der EU. Die OECD-Richtlinien legen acht Grundsätze für den Schutz der Privatsphäre fest: begrenzte Datenerhebung, Datenqualität, Zweckbestimmung, Nutzungsbegrenzung, Sicherung, Offenheit, Mitspracherecht und Rechenschaftspflicht (OECD 2003). Auf sie wird auch unter dem Begriff „Fair Information Principles" Bezug genommen, eine Bezeichnung, die für eine Reihe von ähnlichen Sammlungen von Regelungen zum Schutz der Privatsphäre verwendet wird. Ursprünglich stammt dieser Begriff von einer weniger umfangreichen Reihe von Regeln, die in den frühen siebziger Jahren in den USA entwickelt wurde. Die EU-Richtlinie hat wiederum die reale Welt in sehr signifikanter Weise beeinflusst. Einerseits musste sie in die nationalen Gesetze der Mitgliedstaaten der EU integriert werden, andererseits verbietet sie den Transfer von persönlichen Daten in Länder außerhalb der EU, welche über keinen vergleichbaren und angemessenen Schutz von persönlichen Daten verfügen. Dies veranlasste viele dieser Länder dazu, „freiwillig" ähnliche Schutzbestimmungen einzuführen.

Konflikte zwischen den Visionen von allgegenwärtigen Informationstechnologien und den OECD-Richtlinie können für alle acht Grundsätze, aus denen diese Richtlinie besteht, identifiziert werden (Čas 2002). Die nachfolgende Diskussion konzentriert sich aber auf die ersten vier dieser acht Prinzipien. Sie sind die unverzichtbaren Säulen, auf denen alle gegenwärtigen Bestimmungen zum Schutz der Privatsphäre ruhen. Ihre zentrale Rolle wird auch dadurch deutlich, dass sie sich sowohl in europäischen als auch kanadischen oder US-amerikanischen Regulierungen zum Schutz der Privatsphäre wieder finden (Iachello 2003).

3.1 Grundsatz der begrenzten Datenerhebung

Der erste Teil dieses Prinzips besagt, dass bei der Erhebung personenbezogener Daten Grenzen zu setzen sind, freilich ohne diese Grenzen näher zu bestimmen. Bereits die Grundidee von „Pervasive-Computing"-Infrastrukturen widerspricht diesem Grundsatz vollständig. Daten über Personen oder Objekte innerhalb der Reichweite von UC-Systemen werden aktiv, umfassend und andauernd gesammelt. Selbst wenn nur ein kleiner Teil dieser riesigen Mengen an Informationen tatsächlich gespeichert oder analysiert wird, werden die Prinzipien der Beschränktheit und Zweckbindung von Datensammlungen in ihr Gegenteil verkehrt. Der zweite Teil dieses Prinzips bezieht sich auf ein bewusstes und informiertes Einverständnis derjenigen Personen, deren Daten gesammelt werden. Während es grundsätzlich möglich scheint, dafür Bewusstsein zu schaffen, z. B. durch klar sichtbare Warnhinweise, welche anzeigen das UC-Systeme in Verwendung sind, werden detaillierte Informationen darüber, welche Objekte welche Daten zu wel-

cher Zeit erfassen, nicht mehr möglich sein. Diese sind sowohl aus praktischen Gründen als auch wegen der Inkompatibilität mit dem Ziel der Unaufdringlichkeit ausgeschlossen.

Eine der Anforderungen des Artikels 7 der EU-Datenschutzrichtlinie wird völlig unerreichbar, nämlich die Verpflichtung, jede Bearbeitung persönlicher Daten an das ausdrückliche Einverständnis der betroffenen Person zu knüpfen. Auch heute ist die Bedingung, dass die „… betroffene Person … ohne jeden Zweifel ihre Einwilligung gegeben" (Europäisches Parlament und Rat 1995), nicht in allen Fällen und jederzeit erfüllbar und durch eine Reihe von Ausnahmen abgeschwächt. Beispiele hierfür sind Datenverarbeitungen, um vertragliche Vereinbarungen zu erfüllen oder um vitale Interessen der betroffenen Person zu schützen. Für die Kategorie „öffentliches Interesse", welche auch Fragen der öffentlichen Sicherheit oder der Effizienz von Ermittlungsverfahren umfasst, bleiben die bekannten Probleme der gegenseitigen Abwägung von Grundrechten und der konfliktträchtigen Beziehung zwischen Freiheit und Sicherheit ein wichtiges Thema. Diese Konflikte werden aber durch allgegenwärtige Informationstechnologien dramatisch an Bedeutung gewinnen, da diese die Möglichkeiten der Überwachung in quantitativer und qualitativer dramatisch erhöhen und auf Bereiche ausdehnen werden, die sich heute einer permanenten und unbemerkten Beobachtung entziehen. Erfahrungen aus der Vergangenheit lehren uns, dass damit zu rechnen ist, dass die rechtlichen Befugnisse von Ermittlungsbehörden an die wachsenden technischen Möglichkeiten der Überwachung immer wieder angepasst werden.

Das Verhältnis zwischen der Möglichkeit einerseits, ein explizites Einverständnis der betroffenen Personen herzustellen, und den Überwachungskapazitäten von UC-Systemen andererseits verspricht in noch viel dramatischerer Weise aus dem Gleichgewicht zu geraten. Natürlich wird es immer Teile der Bevölkerung geben, die nichts gegen eine totale Überwachung in einer Welt mit allgegenwärtigen Informationstechnologien einzuwenden haben werden, insbesondere, wenn ihnen dafür eine höhere Sicherheit oder auch nur mehr Bequemlichkeit versprochen wird. Und wahrscheinlich wird es viele Personen geben, die entsprechende Vertragsklauseln unterschreiben, wenn dies von Anbietern von UC-Services vorausgesetzt wird, um in den Genuss ihrer Dienstleistungen kommen zu können. Man könnte natürlich auch diskutieren, ob solche Verträge noch gültigen gesellschaftlichen Normen entsprechen oder ob sie als unmoralisch oder sittenwidrig angesehen werden sollten, ähnlich dem Verkauf der eigenen Seele. Viel größere Sorgen muss aber der Umstand bereiten, dass keinerlei Möglichkeit besteht, der Überwachungsinfrastruktur zu entfliehen. Jene Teile der Bevölkerung, die nicht permanent überwacht werden möchten, können natürlich die Unterschrift unter solche Verträge verweigern. Wenn eine Person diese Entscheidung trifft, wird sie von den entsprechenden Dienstleistungen ausgeschlossen werden, jedoch be-

steht in einer perfekten UC-Welt kein Weg, der allgegenwärtigen Überwachung selbst zu entkommen. Allgegenwärtige Informationstechnologien werfen daher schwierige rechtliche Fragen auf, etwa die, ob ein „zweifelsfreies Einverständnis" zu etwas Unvermeidbaren überhaupt ein gültiger Teil von individuellen oder kollektiven Übereinkünften sein kann.

3.2 Grundsatz der Datenqualität

Dieser Grundsatz umfasst ebenfalls zwei Dimensionen: Erstens müssen die Daten korrekt, vollständig und aktuell sein, zweitens müssen personenbezogene Daten ihrer Zweckbestimmung entsprechen – dies wird bei den beiden nachfolgenden Prinzipien noch näher ausgeführt. Im Allgemeinen könnte erwartet werden, dass allgegenwärtige Informationstechnologien bei der ersten hier angesprochenen Dimension zu besseren Resultaten führen werden. Es wird aber erst nach genauer Kenntnis der eingesetzten Systeme und der Auswertung empirischer Daten tatsächlicher Anwendungen möglich sein, begründete Aussagen über Aspekte der Datenqualität zu treffen. Wenn zum Beispiel die betroffenen Personen mittels biometrische Methoden identifiziert werden, so ist ein bestimmter Anteil an Fehlzuordnungen von Daten zu Personen unvermeidbar. Eine Abnahme der fälschlicherweise identifizierten Personen (FAR – False Acceptance Rate) impliziert immer einen Anstieg der fälschlicherweise abgewiesenen Personen (FRR – False Rejection Rate) und umgekehrt. Darüber hinaus bedeutet ein Mehr an Daten nicht notwendigerweise bessere Daten. Um zu genaueren Daten zu gelangen, müssen regelmäßige Überprüfungen und Korrekturen vorgesehen werden. Dies ist aber ohne zentrale oder zumindest koordinierte Speicherung der Daten kaum vorstellbar; zentralisierte Formen der Datenspeicherung sind aber mit einem entsprechenden Missbrauchsrisiko behaftet.

3.3 Grundsatz der Zweckbestimmung

Im Zentrum dieses Prinzips steht die Anforderung, dass spätestens zum Zeitpunkt der Datenerhebung deren Zweck bekannt und identifizierbar sein muss. Nachfolgende Veränderungen dieses Zweckes sind nur erlaubt, wenn sie mit den ursprünglichen Intentionen vereinbar sind; darüber hinaus müssen diese Veränderungen entsprechend bekannt gegeben werden.

Das Ziel von pervasiven Informationstechnologien ist es aber nicht, einem einzelnen Zweck zu dienen, sondern den Nutzer in einer Vielzahl von mehr oder weniger vorhersehbaren Situationen zu unterstützen. Die Abwesenheit von präzisen Definitionen über mögliche Nutzungen impliziert auch, dass zahllose Szenarien über mögliche Anwendungen von UC-Systemen entwickelt werden können, jedoch kein Wissen darüber besteht, welche Dienste auf genügend große Nachfrage stoßen werden oder über akzeptable Relationen zwischen Kosten und Nutzen verfügen werden. Diese Kritik betrifft aber eine Vielzahl neuer Technologien und wäre allein noch kein ausreichender Grund für prinzipielle Bedenken gegenüber Pervasive Computing.

Das grundsätzliche Problem von UC ist somit die Tatsache, dass der Grundsatz der Zweckbestimmung auf den Kopf gestellt und damit ein zentrales Fundament des gegenwärtigen Datenschutzes beseitigt wird. Der Zweck der Datensammlung liegt hier ausschließlich in der Anhäufung von so viel Informationen über individuelle Verhaltensmuster und Präferenzen als möglich, der Kontext und der Zweck, in dem bzw. für den dieses Wissen angewendet werden wird, bleiben zum Zeitpunkt der Datenerfassung notwendigerweise unbekannt. Diese Unmöglichkeit, einen Zweck zu nennen, macht es auch unmöglich, dies zu fordern, und stellte so eine grundsätzliche Verletzung dieses Prinzips dar. Jeder Versuch, diesen Grundsatz dennoch aufrechtzuerhalten, würde aus praktischen Gründen scheitern und dem Ziel widersprechen, unaufdringliche UC-Systeme zu schaffen.

3.4 Grundsatz der Nutzungsbegrenzung

In Ergänzung zum Prinzip der Zweckbestimmung besagt dieser Grundsatz, dass Daten nicht offen gelegt, bereitgestellt oder genutzt werden dürfen, wenn dies nicht den Zwecken entspricht, die zum Zeitpunkt der Datenerhebung festgelegt worden sind. Ausnahmen von diesem Grundsatz sind möglich, wenn die betroffene Person einwilligt oder wenn die Bearbeitung im Rahmen gesetzlicher Bestimmungen erfolgt.

Das Fehlen einer anfänglichen Zweckbestimmung macht es auch unmöglich, irgendwelche Grenzen für sekundäre Nutzungen zu ziehen. Fundamentale und unvermeidbare Widersprüche zwischen den Prinzipien der Nutzungsbegrenzung und Zweckbestimmung einerseits und den Visionen von UC andererseits sind darüber hinaus in der technischen Gestaltung dieses System begründet. Die spontane Vernetzung von zahllosen und unsichtbaren Chips und der Austausch von Daten zwischen ihnen sind zentrale und unverzichtbare Komponenten von UC-Infrastrukturen. Abgesehen von technischen Problemen, welche eine Begrenzung des Transfers und der Nutzung von Daten mit sich bringen würde, wäre jeder

Versuch, den Grundsatz der Nutzungsbegrenzung zumindest teilweise durchzusetzen mit entsprechenden Einschränkungen beim Nutzen und der Benutzbarkeit von UC-Infrastrukturen verbunden. Der Nutzen wäre beschränkt, weil vorgegebene Zuordnungen von Daten zu Anwendungen auch die Anpassungs- und Lernfähigkeit diese Systeme beschränken würde; die Benutzbarkeit, weil ständige Nachfragen zum Einverständnis oder zu Ablehnung von Datentransfers wohl innerhalb kürzester Zeit die Grenze der Zumutbarkeit überschreiten würden.

4 Versuche zur Überwindung der Widersprüche

Die inhärenten und offensichtlichen Bedrohungen für die Privatsphäre durch allgegenwärtige Informationstechnologien haben nicht nur Ankündigungen über das Ende der Privatsphäre provoziert, sie stellen auch eine intellektuelle Herausforderung für Forscher und Entwickler dar. Als Antwort auf diese Herausforderung haben besorgte Wissenschafter zahlreiche Konzepte entwickelt, um zu versöhnen, was unversöhnlich scheint. Im Folgenden werden einige dieser Ansätze kurz skizziert und auf ihre Eignung hin diskutiert, die Bedrohungen für die Privatsphäre durch UC zu beseitigen oder zumindest zu mildern.

4.1 Identitätsmanagement

Die Prinzipien, die zum Schutz persönlicher Daten entwickelten wurden betreffen natürlich nur solche Daten, für die ein direkter oder indirekter Bezug zu einer Person besteht oder hergestellt werden kann. Es ist daher ein nahe liegender Ansatz, diese Daten zu anonymisieren oder zu pseudonymisieren, um mögliche Probleme mit der Privatsphäre zu vermeiden. Für traditionelle Informationssysteme und das Internet wurden eine Reihe von technischen und organisatorischen Methoden mit diesem Ziel entwickelt. Diese PETs (Privacy Enhancing Technologies) können grundsätzlich auch in UC-Umgebungen angewendet werden. Allerdings impliziert der Einsatz dieser Technologien zahlreiche und weit reichende Einschränkungen bei der Gestaltung von UC-Systemen. Beim ubiquitären Zugang zu Informationen ist zum Beispiel Anonymität nur möglich, wenn die Nutzer aktiv Anfragen initiieren. Eine der grundlegenden Eigenschaften von UC-Systemen – personalisierte, an individuelle Bedürfnisse im jeweiligen Kontext angepasste Dienstleistungen – erfordern zumindest Pseudo-Identitäten, an welche Benutzerprofile geknüpft werden können. Mithilfe von Identitätsmanage-

mentsystemen können Pseudo-Identitäten in einer benutzerfreundlichen Art und Weise erzeugt und administriert werden. Dieser Ansatz bietet viele Vorteile, wenn er innerhalb traditioneller Informationssysteme angewendet wird. Die berufliche Sphäre kann durch die Nutzung unterschiedlicher Identitäten, die vom privaten Leben getrennt werden oder die Verknüpfung von Daten über längere Perioden kann durch die regelmäßige Generierung von neuen Pseudo-Identitäten erschwert werden.

Bereits in gegenwärtigen Informationssystemen machen es zunehmend mächtige und effiziente Werkzeuge zur Analyse großer Datenmengen immer leichter, Pseudonyme offen zu legen und den Schutz zu limitieren, den diese eröffnen. Um in UC-Umgebungen überhaupt irgendeinen Schutz bieten zu können, müssen diese Pseudo-Identitäten der einzige Anknüpfungspunkt für Interaktionen bleiben. Konkret bedeutet dies, dass es etwa nicht erlaubt sein dürfte, zusätzlich Methoden biometrischer Identifikation anzuwenden und dass keine Audio- oder Videoinformationen gespeichert werden dürfen, da diese Daten eine nachträgliche biometrische Identifikation erlauben würden. Zusätzlich dürfen auch keine Lokalisierungsdaten erfasst werden. Erstens würden diese eine Verkettung von wechselnden Pseudo-Identitäten erlauben, zweitens würden Lokalisierungsdaten bei hinreichend großer Präzision oder andauernder Beobachtung jeden Versuch einer Anonymisierung oder Pseudonymisierung obsolet machen. Anonymität oder Pseudonymität können innerhalb von UC-Systemen nur erreicht werden, wenn diese derart radikal in ihren sensorischen Fähigkeiten wie auch in den Nutzungsmöglichkeiten beschränkt werden, dass sie wohl kaum noch den gegenwärtigen Visionen entsprechen würden.

Obwohl die Technologien des Identitätsmanagements keinen hinreichenden Schutz gegen die Personalisierung von Daten in UC-Welten bieten können, sind sie – zumindest theoretisch – in der Lage, das Problem des individuellen Einverständnisses zu jedem einzelnen Akt der Datenerfassung zu mildern. In UC-Umgebungen wird dies aus praktischen Gründen unmöglich sein; stattdessen könnten aber Profile, die in persönlichen digitalen Assistenten (PDAs) gespeichert und an auswählbare Identitäten geknüpft sind, situationsspezifisch Zustimmung oder Ablehnung signalisieren. In Anlehnung an die Spezifikationen der „Platform for Privacy Preferences“ (P3P) des World Wide Web Consortium (W3C) könnte eine mögliche Erlaubnis von der Übereinstimmung der „Privacy Policy“ des jeweiligen UC-Subsystems mit den gewählten Präferenzen des Nutzers abhängig gemacht werden. Unverzichtbare Voraussetzungen wären, dass die Nutzer die vollständige Kontrolle über die Profile behalten und dass eine Nulloption vorgesehen ist, das heißt, es muss möglich sein, jegliche Interaktion mit UC-Systemen zu unterbinden. In einer privacy-kompatiblen UC-Umgebung muss ein ausgeschalteter oder fehlender digitaler Assistent als Ablehnung jeglicher Beobachtung und

Datensammlungsaktivitäten interpretiert werden. Wenn sich mehrere Personen an einem Ort aufhalten, müssten die Vorgaben des am meisten restriktiven Teilnehmers zur Anwendung kommen. Dies würde auch implizieren, dass etwa Aufnahmen zur Unterstützung des eigenen Gedächtnisses nur möglich sind, wenn alle anwesenden Personen ihr Einverständnis dazu geben. Dies sind freilich nur notwendige, aber noch nicht hinreichende Bedingungen (siehe im nächsten Abschnitt). Weiters müssen auch in diesem Fall alle Beschränkungen hinsichtlich biometrischer Identifikation oder der Aufbewahrung von Daten, die nachträglich mittels biometrischer Methoden analysiert werden könnten, erfüllt sein.

4.2 Privacy-respektierende ubiquitäre Aufzeichnungen

Die Unterstützung des Gedächtnisses durch ubiquitäre Audio- oder Videoaufnahmen ist eine relativ einfache Anwendung. Der Mangel an Komplexität im Vergleich zu vollständigen UC-Systemen resultiert einerseits aus der einzigen Aufgabe, Audio- oder Videoaufnahmen ohne jegliche Interpretation oder Auswertung durchzuführen, andererseits aus dem Umstand, dass die dazu vorgesehenen Geräte von den beteiligten Personen kontrolliert werden.

Halderman et al. (2003) haben ein Lösungskonzept für die Bedrohungen der Privatsphäre durch ubiquitäre Aufnahmen entwickelt. Dieses kryptographische Konzept basiert auf den beiden Prinzipien Einverständnis und Vertraulichkeit. Das erste Prinzip legt fest, dass ohne das Einverständnis aller anwesenden Personen keine Aufnahmen durchgeführt und dass auch keine Aufnahmen freigegeben werden dürfen, sofern nicht alle Beteiligten damit einverstanden sind. Das zweite Prinzip besagt, dass die Entscheidung einer bestimmten Person, einer Wiedergabe zuzustimmen oder zu widersprechen, niemanden offen gelegt werden soll. In theoretischer Hinsicht erfüllen die entwickelten Protokolle der Mechanismen diese Anforderungen in perfekter Weise. Für praktische Anwendungen dürften sie aber kaum von Relevanz sein, zudem beinhalten sie neue Bedrohungen für die Privatsphäre.

Sogar in jenem Anwendungsgebiet, für welches dieses Konzept entwickelt wurde – „privacy enhanced Instant Messaging" – kann ein Einverständnis, privacyfördernde Systeme zu nutzen, einerseits Mogeleien nicht verhindern und birgt andererseits neue Risken in sich, wie die Autoren des Konzepts selbst anerkennen. Die Notwendigkeit, das Einverständnis aller beteiligten Personen einzuholen, um auf gespeicherte Daten zugreifen zu können, verbietet z. B. die anonyme Nutzung von solchen Instant-Messaging-Diensten. Zusätzliche Probleme treten auf, wenn dieses Modell auf allgegenwärtige Aufnahmen in alltäglichen Situationen ausgedehnt wird. Um überhaupt sinnvollerweise Überlegungen zur Zustim-

mung oder Ablehnung von Aufnahmen machen zu können, müsste zuallererst Vertrauen in das System hergestellt werden. Ohne eine vollständige und totale Kontrolle aller entwickelten und verkauften Technologien wäre ein solches Vertrauen kaum zu rechtfertigen, da ansonsten jeder x-beliebige Gegenstand über nicht konforme Aufnahmemöglichkeiten verfügen könnte. Ein Einverständnis zu einer Aufnahme würde gleichzeitig einem Einverständnis zur permanenten Verfolgung und Aufspürbarkeit gleichkommen, um gegebenenfalls Anfragen zur Freigabe von Aufnahmen beantworten zu können. Rationale Entscheidungen über die Gewährung oder Ablehnung der Freigabe bestimmter Daten werden in vielen Fällen ohne Zugriff auf die Inhalte nicht möglich sein. In anderen Worten bedeutet dies, dass der beabsichtigte Dienst – ein perfektes Gedächtnis – selbst eine Voraussetzung ist, um dieses System in einer die Privatsphäre schonenden Art und Weise nutzen zu können; etwa um entscheiden zu können, ob ein Gespräch, welches am Dienstag, den 3. März 2005, zwischen 3:15 und 3:20 Uhr nachmittags stattgefunden hat, freizugeben oder zu blockieren.

Die mangelnde Eignung dieses Ansatzes, „Ubiquitäres Recording" weniger privatsphärengefährdend gestalten zu können, wird noch offensichtlicher, wenn diese Dienste in geschäftlichen Bereichen angeboten werden sollen. Jeder Teilnehmer, der befürchtet, durch eine Freigabe benachteiligt werden zu können, könnte diese blockieren; der Tod einer beteiligten Person oder die Kündigung eines beteiligten Arbeitnehmers würde die aufgenommenen Daten in unzugängliche Bits verwandeln und das ganze System nutzlos machen. Ohne Hintertüren oder hinterlegte Generalschlüssel, mit denen Blockaden in bestimmten Situationen überwunden werden können, würden solche Systeme wohl kaum Käufer finden. Der Einbau von Hintertüren würde aber einem weit gehenden Verzicht auf die die Privatsphäre schützenden Eigenschaften dieses Ansatzes gleichkommen.

Da es keinen hundertprozentigen Schutz gegen nicht konforme Aufnahmegeräte geben kann, eignet sich dieses Modell auch nicht, die Privatsphäre wirklich zu schützen. Es kann im Gegenteil zu einem ungerechtfertigten Gefühl der Sicherheit verleiten. Darüber hinaus zerstört es wichtige Bereiche der Privatsphäre, indem es etwa Möglichkeiten der anonymen Teilnahme an Diskussionen oder Gesprächen einschränkt. Und trotz der zweifelhaften Beiträge zum Schutz der Privatsphäre erhöht der vorgeschlagene Ansatz die Systemkomplexität erheblich und macht ubiquitären Aufnahmetechnologien für die meisten der vorgesehenen Anwendungen nutzlos.

4.3 Digital Rights Management

Weitere Ansätze zur Schaffung von Privatsphären respektierenden pervasive Computingssystemen zielen darauf ab, Prinzipien und Technologien des „Digital Rights Managements“ (DRM) auf von UC-Systemen erfasste persönliche Daten anzuwenden. Die grundlegende Idee dieser Ansätze ist es, die Daten zu verschlüsseln und die Entschlüsselung beziehungsweise den Zugang zu diesen Daten nur zuzulassen, wenn bestimmte (vordefinierte) Bedingungen gegeben sind. Der Hauptunterschied dieser Ansätze zum vorherigen Beispiel des ubiquitären Aufnehmens besteht darin, dass diese Lösungen auch in komplexen Systemen allgegenwärtiger Informationstechnologien anwendbar sein sollen.

Der Charme der Anwendung von DRM-Technologien bei UC-Systemen bestehen darin, dass sie zumindest in der Theorie neue Wege eines privatsphärenschonenden Privatsphären schonenden Designs eröffnen, etwa durch die Integration neuer Dimensionen wie „Nähe“ oder „Lokalität“. Die Integration von Nähe könnte beispielsweise bedeuten, dass Geräte zur Unterstützung des Gedächtnisses nur funktionieren, wenn ihr Besitzer anwesend ist; Lokalität könnte sich zum Beispiel darin ausdrücken, dass ein Konferenztisch Informationen über vergangene Diskussionen an Personen freigibt, welche sich im Konferenzraum aufhalten, Anfragen von außen aber abweist. Weitere vorgeschlagene Wege, die Verletzung der Privatsphäre durch UC-Systeme zu begrenzen, bestehen darin, Datenbanken an einen Ort zu knüpfen (Shell 2002) oder den Zugang zu generierten Daten vom Vertrauen in die anfragende Person und von deren Reputation abhängig zu machen (Goecks/Mynatt 2002). „Privacy Tagging“, bei dem Metadaten genutzt werden, um die erlaubten Arten des Zugriffs auf diese Daten zu definieren, würde eine unbeschränkte Weitergabe der verschlüsselten Daten erlauben und dennoch sicherstellen, dass die Daten nicht die zugehörigen Informationsräume verlassen und außerhalb der zugewiesenen Nutzungen verwendet werden. DRM-Technologien könnten vorschreiben, dass eine bestimmte „Privacy Policy“ den Daten anhaftet, mit ihnen mittransferiert wird und entscheidet, wer in welcher Weise diese Daten nutzen darf (Jiang 2002).

In einer strikten Auslegung demonstrieren diese Beispiele jedoch eher fehlende Durchführbarkeit denn Möglichkeiten zum Schutz der Privatsphäre in einer Welt mit UC-Systemen. Das Problem ist die andauernde und unbemerkte Aufzeichnung von Daten selbst. Jeder Versuch, die Nutzung dieser Daten zu beschränken, ist zum Scheitern verurteilt oder birgt neue inakzeptable Risken auf gesellschaftlicher Ebene in sich.

Ein Grund für diese pessimistische Einschätzung steht in Zusammenhang mit dem Problem der Verschlüsselung. Eine prinzipielle Frage ist es, warum man in einer Welt, die durch die allgegenwärtige Erfassung, den spontanen Transfer und

einen universellen Zugang zu Daten definiert ist, überhaupt beabsichtigen sollte, Daten zu verschlüsseln. Abgesehen von dieser grundlegenden Frage der Systemgestaltung wird die Stärke der angewendeten Verschlüsselung durch Beschränkungen in der Rechenkapazität und beim Energieverbrauch der super-miniaturisierten Komponenten limitiert sein. Selbst wenn die erreichten Niveaus „Brute-Force-Attacken" zum Zeitpunkt der Erfassung verhindern können, so werden doch die zu erwartenden Zuwächse an Rechenkapazität den Schutz innerhalb der antizipierten Speicherfristen wirkungslos werden lassen. Zudem ist die Verschlüsselung ein zweischneidiges Schwert: Sie erleichtert sowohl das Verstecken von Daten als auch die Verifizierung von Identitäten (Lessig 1998). Eine weite Verbreitung von Verschlüsselungstechnologien und Infrastrukturen als Begleiterscheinung von Versuchen, UC-Systeme datenschutzfreundlich zu gestalten, würde auch Anreize schaffen, eine Identifikation auch für Dienste zu erzwingen, die früher anonym zugänglich waren.

Ein zweiter Grund für die pessimistische Beurteilung dieser Versuche, allgegenwärtige Informationstechnologien datenschutzfreundlich zu gestalten, betrifft die neuen Risiken, mit denen die Anwendung von DRM-Technologien behaftet sind. Um einen effektiven Schutz bieten zu können, müssen alle Geräte und Komponenten mit hardwaremäßig implementierten DRM-Fähigkeiten ausgestattet sein. Ansonsten könnte jeder Schutz leicht umgangen werden, indem einfach DRM-freie Geräte für die unsichtbare Erfassung oder erneute Aufzeichnung und anschließende freie Verbreitung von persönlichen Daten verwendet werden. Bei diesen Auswahlmöglichkeiten scheint eine mögliche Verletzung der Privatsphäre als Folge von DRM-freien Geräten im Vergleich zum vollständigen Schutz durch DRM die sicherlich zu bevorzugende Option zu sein. Das zweite Szenario würde nämlich eine perfekte Infrastruktur für Zensurmaßnahmen[4] darstellen, die weit effektiver wären als alle Versuche in der Vergangenheit, die öffentliche Meinung zu kontrollieren oder zu beeinflussen. Hier wäre noch anzumerken, dass der Versuch, UC-Systeme datenschutzfreundlich zu gestalten das Eintreten dieses Szenarios wohl nur marginal beeinflussen wird und der bestimmende Faktor die Implementierung von DRM-Systemen im Allgemeinen sein wird.

[4] Mittels DRM lassen sich nicht nur private Informationen vor unberechtigtem Zugriff schützen, sondern der Umgang mit jeder Art von Inhalten regeln: Hersteller von Betriebssystemen können etwa bestimmen, welche Software ausgeführt werden kann, Produzenten von Filmen können verhindern, dass nicht bezahlte Kopien abgespielt werden, und nicht demokratische Regime könnten die Verbreitung von missliebigen Informationen unterbinden.

5 Gesellschaftliche Nachhaltigkeit

Nachhaltigkeit ist ein Begriff, der leicht verständlich scheint, schon weniger leicht zu definieren und sehr schwer zu messen oder in operative Konzepte umzusetzen ist. Anfangs konzentrierten sich Nachhaltigkeitskonzepte hauptsächlich auf ökologische Aspekte. Eine allgemein akzeptierte Definition von nachhaltiger Entwicklung hat die World Commission on Environment and Development im Brundtland Commission Report im Jahre 1987 gegeben; sie definiert Nachhaltigkeit als eine Entwicklung, welche „die Bedürfnisse der heutigen Generation befriedigt, ohne die Möglichkeiten künftiger Generationen aufs Spiel zu setzen, ihre eigenen Bedürfnisse zu befriedigen". Pervasive Computing wird ohne Zweifel die Nachhaltigkeit auch in ökologischer Sicht stark betreffen – diese Effekte werden etwa durch die Produktion von zahllosen Komponenten, den Energiekonsum für den Betrieb von UC-Umgebungen oder durch das Recycling beziehungsweise die Entsorgung von Materialien und Gegenständen mit integrierter Elektronik bedingt sein.

Darüber hinaus beinhaltet Pervasive Computing sowohl neue Dimensionen als auch Bedrohungen für die soziale und gesellschaftliche Nachhaltigkeit. Es gibt noch keine allgemein anerkannte Definition von gesellschaftlicher Nachhaltigkeit, die meisten Konzepte konzentrieren sich auf ökonomische Parameter wie die Verfügbarkeit von Einkommenschancen oder die Einkommensverteilung. Die Bedrohungen von UC für Grundrechte verlangen nach einer Erweiterung bestehender Nachhaltigkeitskonzepte und nach einer Integration des Schutzes der Privatsphäre in die Definition gesellschaftlicher Nachhaltigkeit. Die Verwirklichung dieses Anspruchs verspricht den Grad der Komplexität von Nachhaltigkeitskonzepten auf eine neue Stufe zu heben. Im Gegensatz zur ökologischen Dimensionen, bei der die Erhaltung der natürlichen Ressourcen und der Umwelt ein klares und offensichtliches Ziel darstellt, stellen Möglichkeiten zur Veränderung und tatsächliche Veränderungen unverzichtbare Voraussetzungen für gesellschaftliche Nachhaltigkeit dar. Gesellschaften, die nicht gewillt oder fähig sind, sich an interne oder externe Veränderungen anzupassen und innovative Wege zu beschreiten, um mit neuen Herausforderungen fertig zu werden, sind längerfristig dem Untergang geweiht.

Grundsätzlich umfasst die Fähigkeit sich anzupassen auch die Option, Grundrechte aufzugeben; auf die Privatsphäre könnte dementsprechend verzichtet werden, wenn tatsächliche oder vermeintliche Zugewinne an Sicherheit oder Bequemlichkeit bevorzugt werden. Allerdings sind im Fall des Schutzes der Privatsphäre wesentlich komplexere Zusammenhänge zu berücksichtigen. Eine allgegenwärtige Überwachung erzeugt einen enormen Druck, sich „normal" zu benehmen

und nicht die ausgetretenen Pfade allgemein akzeptierten sozialen Verhaltens zu verlassen. Soziale Innovationen bedürfen aber Abweichungen durch einzelne Mitglieder der Gesellschaft, sowohl um neue Formen sozialer Interaktion zu erfinden, als auch um innovative Mechanismen in die Gesellschaft zu verbreiten. Pervasive Computing und die notwendigerweise daraus resultierende Überwachungsgesellschaft ist nicht eine bloß temporäre Innovationsbremse; die Grundlagen für gesellschaftliche Erneuerung werden dauerhaft zerstört. Ein uneingeschränkter Einsatz von UC-Geräten und von Systemen allgegenwärtige Informationstechnologien läuft daher einer nachhaltige gesellschaftliche Entwicklung zuwider. Darüber hinaus sind die sozialen und wirtschaftlichen Subsysteme einer Gesellschaft nicht unabhängig voneinander. Einschränkungen in Bezug auf abweichendes soziales Verhalten implizieren auch Einschränkungen bei innovativen Dienstleistungen und Produkten und damit auch einen Verlust an Wettbewerbsfähigkeit.

6 Schlussfolgerungen

Pervasive Computing beginnt die Fundamente und die Säulen, auf denen der gegenwärtige Schutz der Privatsphäre beruht, auszuhöhlen und zu zerstören. Wir müssen uns bewusst sein, dass „… the world we are entering is about to change these architectures of privacy more completely and more extensively than any such change that we have seen to date" (Lessig 1998). Diese Architekturen werden sowohl in einem übertragenen als auch in einem tatsächlichen Sinn verändert; es werden sowohl die rechtlichen und theoretischen Prinzipien des Schutzes der Privatsphäre aufgehoben als auch Artefakte, die gegenwärtig für Abschirmung und Verborgenheit stehen – wie Wände oder Bekleidung – dieser Funktionen beraubt, indem sie mit sensorischen Fähigkeiten ausgestattet werden.

Technische Lösungen, die einen effektiven Schutz der Privatsphäre bewirken können, sind grundsätzlich verfügbar. Ihre Integration in UC-Systeme erfordert jedoch weit gehende Einschränkungen der Funktionalität von solchen Systemen und den Verzicht auf Ideen, die den Kern des Paradigmas von allgegenwärtigen Informationstechnologien darstellen. Privatsphärenfreundliches Design, welches die Grundzüge von allgegenwärtigen Informationstechnologien nicht verletzt, kann hingegen nicht viel mehr als marginale Verbesserungen beim Schutz der Privatsphäre bewirken.

Regulative Beschränkungen der Verarbeitung und Nutzung von Daten, die durch UC-Infrastrukturen generiert werden, sind grundsätzlich notwendig und

sinnvoll, aufgrund der unsichtbaren Natur dieser Technologie wird es sich aber als sehr schwer erweisen, solche Regelungen auch zu kontrollieren und durchzusetzen. Es müssen daher neue Regeln sowohl für den Einsatz von Pervasive Computing als auch für die Nutzung von persönlichen Daten entwickelt werden.

Der Verzicht auf die Privatsphäre opfert ein Menschenrecht und ein Fundament demokratischer Gesellschaften. Es bedarf daher großer wissenschaftlicher Anstrengungen zur Erforschung der Funktionen von Privacy, zum Design von effektiven und benutzerfreundlichen privacy-fördernden Technologien und zur Entwicklung von innovativen Regulierungskonzepten, welche den Gefahren durch den technischen Fortschritt gerecht werden. Andernfalls könnte die Allgegenwart von „Pervasive-Computing"-Systemen in ihrer Allmacht münden.

Literatur

Acquisti, A., 2004, *Privacy and Security of Personal Information. Economic Incentives and Technological Solutions* (Preliminary draft. Final version forthcoming in: J. Camp and R. Lewis (Hrsg.), The Economics of Information Security, Kluwer, 2004); <http://www.heinz.cmu.edu/~acquisti/papers/acquisti_eis_refs.pdf>.

Adams, A. und Sasse, M. A., 2001, Privacy in multimedia communications: Protecting users, not just data, in: Blandford, A. und Vanderdonkt, J. (Hg.): *People and Computers XV – Interaction without frontiers. Joint Proceedings of HCI2001* <http://www.cs.ucl.ac.uk/staff/A.Sasse/adamshci2001.pdf>.

Bentham, J., 1791, Panopticon: or, the Inspection-House: Containing the idea of a new principle of construction applicable to penitentiary-houses, prisons, houses of industry, work-houses, poor-houses, manufactories, mad-houses, hospitals, and schools. With a plan of management adapted to the principle, *a series of letters, written 1787, from Crecheff to a friend in England*, Dublin: Thomas Byrne.

Čas, J., 2002, UC – Ubiquitous Computing oder Ubiquitous Control? in: Britzelmaier, B., Geberl, S. und Weinmann, S. (Hg.): *Der Mensch im Netz – Ubiquitous Computing*, Stuttgart: Teubner, 39-52.

Europäisches Parlament und Rat, 1995, *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* (24. Oktober 1995). Amtsblatt Nr. L 281 S. 31-50 (23.11.1995) <http://europa.eu.int/eur-lex/de/lif/dat/1995/de_395L0046.html>.

Foucault, M., 1977, *Discipline and Punish: The Birth of the Prison*, London: Penguin.

Goecks, J. und Mynatt, E., 2002, Enabling Privacy Management in Ubiquitous Computing Environments through Trust and Reputation Systems, *CSCW 2002 workshop Privacy in Digital Environments: Empowering Users*, 16.11., New Orleans <http://smg.media.mit.edu/cscw2002-privacy/submissions/jeremy.pdf>.

Halderman, J. A., 2003, *Digital Privacy-Rights Management for Ubiquitous Recording*, Dept. of Computer Science, Princeton University <http://www.cs.princeton.edu/~felten/privman.pdf>.

Halderman, J. A., Waters, B. und Felten, E. W. (Dept. of Computer Science, Princeton University), 2003, *Privacy Management for Ubiquitous Recording* (Draft); <http://www.cs.princeton.edu/~felten/privman.pdf>.

Iachello, G., 2003, Protecting Personal Data: Can IT Security Management Standards Help? *19th Annual Computer Security Applications Conference*, Dec. 2003, Las Vegas <http://www.acsac.org/2003/papers/20.pdf>.

Jiang, X., 2002, Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces: Bridging the Technical and the Social, *Ubicomp 2002 Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing*, 29.9., Göteborg <http://guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/jiang-privacyworkshop.pdf>.

Lessig, L., 1998, The Architecture of Privacy, *Taiwan Net '98*, March 1998, Taipei <http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf>.

OECD, 1980, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* <http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>.

OECD, 2003, *Kurzfassung OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten* <http://www.oecd.org/dataoecd/16/7/15589558.pdf>.

Shell, J. S., 2002, Taking Control of the Panopticon: Privacy Considerations in the Design of Attentive User Interfaces, *CSCW 2002 workshop Privacy in Digital Environments: Empowering Users*, 16.11., New Orleans.

Whitaker, R., 1999, *The End of Privacy: How Total Surveillance is Becoming a Reality*, New York: New Press.