Ubiquitous Computing:
zwischen Privatheit und (Eigen-)Verantwortlichkeit

- Positionspapier ICIE 2008 -
Beitrag zu Schwerpunkt 3: Das Internet ohne Personalcomputer

Autoren:
Stefan G. Weber (sweber@tk.informatik.tu-darmstadt.de)
und Ricarda Drüeke (ricarda.drueeke@sbg.ac.at)

Einleitung

Schlagwörter wie „Web 2.0“ oder „Social Web“ beschreiben einen Wandel des Mediums Internet. Hinzu kommt, dass Anwendungen und Dienste, die unter den Begriff Ubiquitous Computing fallen, einen weiteren Aspekt betonen: „Das Internet“ wird immer nicht mehr nur stationär genutzt, sondern unterschiedlichste IuK-Technologien werden vernetzt, greifen in alle Lebensbereiche ein und lassen sich von vielen Orten aus nutzen – räumliche und zeitliche Dimensionen verändern sich.

Diese Entwicklungen werfen fundamentale Fragestellungen bezüglich Privatsphäre und dem Schutz derselben wieder auf, machen aber auch neue Aspekte erkennbar; sie betreffen Auswirkungen auf die Privatsphäre bei der Entwicklung, praktischen Umsetzung und Nutzung solcher Technologien [1]. Doch in welcher Phase des Entwicklungsprozesses ist eine Reflexion bezüglich möglicher Gefährdungen der Privatheit des Einzelnen von Nöten? Wie kann verhindert werden, dass erst nach der Entwicklung und Nutzung dieser Technologien informationsethische Fragen, die Eingriffe in die Privatsphäre betreffen, Beachtung finden? Welche Interessen spielen eine Rolle, welche verdeckten Widersprüche lassen sich feststellen?

Das vorliegende Positionspapier nimmt sich diesem Hintergrund an und identifiziert fundamentale Diskussionspunkte.

Die Vision des Ubiquitous Computing

Der von Mark Weiser geprägte Begriffe der allgegenwärtigen Informationsverarbeitung (Ubiquitous Computing, kurz UC) steht für eine weitreichende Verlagerung, Verschiebung und Ausweitung der Nutzung von Datenverarbeitungssystemen und elektronischer Kommunikation. In dieser Vision lebt, arbeitet und verbringt der Mensch seine Freizeit in naher Zukunft in einer Umwelt, in die moderne Informationstechnologie nahtlos eingebettet und dort jederzeit verfügbar ist. Der Desktopcomputer verliert seine Funktion als Schnittstelle von virtueller und realer Welt; stattdessen sind diese miteinander eng verwoben. Alltagsgegenstände sind technisiert und vernetzt, in der Lage ihre Umwelt durch Sensoren zu erfassen und zu erfühlen. Aus ihrem Zusammenspiel emergieren intelligente Umgebungen, mit der Zielsetzung, das Alltagsleben auf unaufdringliche Weise zu unterstützen, in dem beispielsweise der Kühlschrank im Zusammenspiel mit dem Arzneischrank den Hausbewohner darauf aufmerksam macht, dass eine bestimmte Kombination von Lebensmitteln und Medikamenten schwere Nebenwirkungen mit sich bringt.
Diese Vision wirft fundamentale Fragen bezüglich der Wahrung der Privatsphäre und der Informationellen Selbstbestimmung des Individuums auf, aber auch bezüglich der Privatheit im weiteren Sinn (nach dem Rösslerchen Trias [2] mit dezisionalen, informativen und lokalen Dimensionen); die allgegenwärtige Sensorerfassung bietet eine flächendeckende Möglichkeit der Überwachung und Kontrolle, auf verschiedensten Ebenen: was passiert, wenn auch Kran-

kenkassen Einblicke in persönliche Ernährungsgewohnheiten nehmen kann [3], wenn der Arbeitgeber jeden Schritt und jede Handlung seiner Angestellten nachvollziehen kann?

Inhärente Konflikte

Es lassen sich in diesem Kontext eine Reihe verdeckter Widersprüche identifizieren. Im Folgenden werden einige dieser Konfliktfelder von allgemein zu speziell aufgeführt und Thesen zum ausgewogenen Umgang damit entwickelt:

I. Durch UC entsteht eine fundamentale Bedrohung der Privatsphäre. Die Möglichkeiten zur technischen, rechtlichen und sozialverträglichen Umsetzung eines Schutzes der Privatsphäre sind aus heutiger Sicht höchst fraglich.

II. Nichtsdestotrotz und um so mehr, muss Privatsphärenschutz bei der Konstruktion von Systemen zur Allgegenwärtigen Datenverarbeitung von Grund auf beachtet werden, sonst kommt es zu großen Akzeptanzproblemen.

III. Insbesondere können Zurechenbarkeiten und Verantwortlichkeiten, beispielsweise durchgeführte oder unterlassene Handlungen, durch UC Systeme im Alltagsleben und in der Arbeitswelt pausenlos festgestellt werden. Die Kontrolle darüber muss den Nutzern von der Technologie in fast allen Bereichen des Lebens zugestanden werden – wenigen Ausnahmen, beispielsweise automatische biometrische Erfassung an Flughäfen, können nur aufbauend auf einer gesetzlichen Basis und gesellschaftlicher Diskussion akzeptiert werden.

IV. Automatische Überwachungs- und Kontrollsysteme können auf dieser Basis etabliert werden. Die „Entscheidungen“ werden allerdings auf einer tiefen technischen/algorithmischen Ebene getroffen. Welche Entscheidungen, insbesondere bis zu welcher Tragweite können, müssen und dürfen abgegeben werden?

V. Auch persönliche Entscheidungen können dem Nutzer im kleinen Maßstab abgenommen werden. Durch pro-aktives, Kontext-bewußtes Verhalten einer intelligenten Umgebungen besteht jedoch die Gefahr, dass der Nutzer verlernt, sich selbstbestimmt zu verhalten. Die Problematik der informationellen Selbstbestimmung, des Datenschutzes und informationellen Privatsphärenschutzes [4] weitet sich durch das Verschmelzen der virtuellen und realen Welten auf die Problematik der persönliche Selbstbestimmung aus [5].

VI. Nicht nur der informationelle Privatsphärenschutz muss somit fundamental bei der Konzeption ubiquitärer Systeme beachtet werden.

VII. Losgelöst davon bleibt aber festzustellen, dass auch der Schutz der Privatsphäre und von weiteren Persönlichkeitsrechten durch UC Technologie verbessert werden kann. Das Feststellen unerwünschter Eindringlinge in einer intelligenten Umgebung ermöglicht die Schaffung von persönlichen Zonen der Anonymität, in denen freie politische Meinungsbildung und –äußerung möglich wird.

VIII. Dadurch ergibt sich aber wieder ein Missbrauchspotential, dem auf geeignete Art und Weise begegnet werden muss.

Schlussfolgerung und Ausblick

Die Entwicklung ubiquitärer IuK Systeme bringt nicht nur technisch enorme Schwierigkeiten mit sich – auch die sozialen Auswirkungen müssen fundamental beachtet werden; eine Veränderung des Nutzerverhaltens, bestimmt durch allgegenwärtige Technik, ist zu befürchten, in vielen Fällen aber nicht wünschenswert. Eine Entwicklung der Systemgestaltung in die Richtung, die vorangehend in Punkt VII. angedeutet wurde, sehen die Autoren im Rahmen der positiven Vision des Ubiquitous Computing und zukünftiger Technikgestaltung (siehe z.B.

[6],[7],[8]) als wünschenswert. Hier spiegelt sich einer der entscheidenden Punkte der geführten Diskussion wieder: Sicherheit und Freiheit stehen in Konkurrenz zueinander; doch wem soll zugestanden werden, dies abzuwiegen?

Literatur

[1] F. Mattern, Ubiquitous Computing: Eine Einführung mit Anmerkungen zu den sozialen und rechtlichen Folgen, Mobilität, Telematik, Recht, Verlag Dr. Otto Schmidt, S. 1-34, 2005

[2] B. Rössler, Der Wert des Privaten, Frankfurt (Suhrkamp), 2001

[3] V. Coroama, Pervasive Computing im Alltag - Realistische Zukunftsanwendungen zur Untersuchung von Chancen und Risiken autonomer, intelligenter Objekte, digma - Zeitschrift für Datenrecht und Informationssicherheit, Vol. 6, No. 03, pp. 106-109, 2006

[4] A. Rossnagel, Datenschutz in der Welt allgegenwärtigen Rechnens (Privacy in a World of Ubiquitous Computing), it - Information Technology: Vol. 49, No. 2, pp. 83-90, 2007

[5] G. Müller, M. Kreutzer, M. Strasser, V. Coroama, T. Eymann, A. Hohl, N. Nopper, S. Sackmann, Geduldige Technologie für ungeduldige Patienten: Führt Ubiquitous Computing zu mehr Selbstbestimmung? Total Vernetzt - Szenarien einer informatisierten Welt. Berlin, Heidelberg, New York: Springer, S. 159-186, 2003

[6] S. G. Weber, S. Ries, A. Heinemann, Inherent Tradeoffs in Ubiquitous Computing Services. INFORMATIK 2007 - Informatik trifft Logistik, Band 1 der Proceedings zur 37. Jahrestagung der Gesellschaft für Informatik GI e.V., 2007.

[7] S. G. Weber, A. Heinemann, M. Mühlhäuser, Towards an Architecture for Balancing Privacy and Traceability in Ubiquitous Computing Environments. Int'l Workshop on Privacy and Assurance (WPA-08) at 3rd International Conference on Availability, Reliability and Security (ARES 2008), p. 958-964, IEEE Computer Society, 2008

[8] C. Patrikakis, P. Karamolegkos, A. Voulodimos, M. H. A. Wahab, N. S. A. M. Taujuddin, C. Hanif, L. Pareschi, D. Riboni, S. G. Weber, A. Heinemann, S.-C. S. Cheung, J. Chaudhari, Security and Privacy in Pervasive Computing, IEEE Pervasive Computing, vol. 6, no. 4, p. 73-75, IEEE Computer Society, 2007.