> Privatheit im Internet

Chancen wahrnehmen, Risiken einschätzen, Vertrauen gestalten

acatech (Hrsg.)

acatech POSITION
Mai 2013

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

Herausgeber:
acatech – DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN, 2013

Geschäftsstelle
Residenz München
Hofgartenstraße 2
80539 München

T +49 (0) 89 / 5 20 30 90
F +49 (0) 89 / 5 20 30 99

Hauptstadtbüro
Unter den Linden 14
10117 Berlin

T +49 (0) 30 / 2 06 30 96 10
F +49 (0) 30 / 2 06 30 96 11

Brüssel-Büro
Rue du Commerce / Handelsstraat 31
1000 Brüssel
Belgien

T +32 (0) 2 / 5 04 60 60
F +32 (0) 2 / 5 04 60 69

E-Mail: info@acatech.de
Internet: www.acatech.de

Empfohlene Zitierweise:
acatech (Hrsg.): *Privatheit im Internet. Chancen wahrnehmen, Risiken einschätzen, Vertrauen gestalten* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2013.

ISSN: 2192-6166 / ISBN: 978-3-642-37979-6 / e-ISBN: 978-3-642-37980-2
DOI: 10.1007/978-3-642-37980-2

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet unter http://dnb.d-nb.de abrufbar.

Springer Vieweg

Koordination: Dr. Karin-Irene Eiermann
Redaktion: Dunja Reulein, Linda Treugut
Layout-Konzeption: acatech
Konvertierung und Satz: Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS, Sankt Augustin

Gedruckt auf säurefreiem Papier

Springer Vieweg ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media
www.springer-vieweg.de

> DIE REIHE acatech POSITION

In dieser Reihe erscheinen Positionen der Deutschen Akademie der Technikwissenschaften zu technikwissenschaftlichen und technologiepolitischen Zukunftsfragen. Die Positionen enthalten konkrete Handlungsempfehlungen und richten sich an Entscheidungsträger in Politik, Wissenschaft und Wirtschaft sowie die interessierte Öffentlichkeit. Die Positionen werden von acatech Mitgliedern und weiteren Experten erarbeitet und vom acatech Präsidium autorisiert und herausgegeben.

> INHALT

KURZFASSUNG

Kaum eine Technologie hat unser Leben schneller und grundlegender verändert als das Internet. Weltweit nutzen heute über 1,5 Milliarden Menschen das Web; in Deutschland sind es mindestens 50 Millionen. Die Nutzerinnen und Nutzer können einfach auf Informationen zugreifen, online einkaufen oder kostenfrei über Videotelefonie kommunizieren. Das Internet lässt neue Geschäftsmodelle und Arbeitsplätze entstehen und verändert die Geschäftsprozesse innerhalb und zwischen Unternehmen sowie öffentlichen Verwaltungen. Es bildet die Infrastruktur für intelligente Stromnetze, die für das Gelingen der Energiewende nötig sind. Über das Web gesteuerte Cyber-Physical Systems helfen in der Fabrik der Zukunft beim effizienten Einsatz von Produktionsressourcen und Energie.

Und besonders wichtig für demokratische Gesellschaften: Das Internet fördert die freie Selbstbestimmung, demokratische Partizipation und wirtschaftliches Wohlergehen. So unterstützen Informations- und Bildungsangebote die Menschen bei der Entwicklung eines selbstbestimmten Lebensentwurfs. Menschen, die eine politische Überzeugung miteinander teilen, können sich in Interessengruppen vernetzen. Prominente Beispiele hierfür sind die Online-Petition gegen die Vorratsdatenspeicherung und die Demokratiebewegungen in den arabischen Staaten. Durch das Internet sind in den vergangenen Jahren viele neue Jobs entstanden. Gleichzeitig können Unternehmen dort ihre Angebote international platzieren und damit ihre Erfolgschancen steigern.

Die Menschen haben sich daran gewöhnt, für Online-Leistungen kein Geld zu bezahlen. Dennoch sind diese nicht kostenlos: Die Währung, in der die Nutzer die Angebote bezahlen, sind ihre persönlichen *Daten*. Neben den Informationen, die sie willentlich an die Dienste weitergeben (Name, Anschrift etc.), hinterlassen sie auch andere Spuren: welche Webseiten sie besuchen oder was sie in Nachrichten schreiben. Nahezu jedes Unternehmen, das seine Dienste im Internet ohne Bezahlung anbietet, verlangt dafür Daten und verdient mit ihnen Geld, zum Beispiel durch ihre Verwendung für gezielte Werbung. So sind persönliche Informationen Ware und Währung. Das schürt Misstrauen, und viele Internetnutzer und -nutzerinnen sind skeptisch, ob die Dienste mit ihren persönlichen Daten im Internet sorgfältig umgehen, und bezweifeln, dass ihre Privatheit stets angemessen geschützt ist.

Privatheit bedeutet die Fähigkeit, selbst definieren und regulieren zu können, wann man sich wem und wie viel man von sich zeigt oder verbirgt. Verbergen kann vollständig sein, zum Beispiel wenn anonym kommuniziert wird. Verbergen kann sich aber auch nur auf bestimmte Aspekte beziehen wie zum Beispiel Alter, Geschlecht oder Aufenthaltsort. Diese Privatheit ist im Internet oft eingeschränkt. Ein Risiko ist die *De-Kontextualisierung*: Persönliche Daten werden in Kontexten verwendet, denen die Besitzer nicht zustimmen würden, wenn sie dies wüssten. Ein zweites Risiko ist die *Persistenz*: Daten werden länger aufgehoben als nötig oder lediglich anonymisiert statt gelöscht. Drittens schränkt die *Re-Identifikation* die Privatheit ein: Mithilfe fortgeschrittener Analysetechniken können anonyme Datensätze wieder einzelnen Personen zugeordnet werden. Welche persönlichen Daten die Internetdienste kennen, nach welchen Regeln sie verarbeitet und an wen sie weitergegeben werden, ist häufig nicht bekannt. Zwar stellen die Anbieter entsprechende Informationen oft zur Verfügung, beispielsweise in Form von AGBs. Diese Informationen sind aber nicht immer zugänglich und teils schwer verständlich.

Die internationale „Internet-Moral", auch Netiquette genannt, ist noch nicht so fortgeschritten, dass sich die Menschen im Web gegenseitig immer als vertrauenswürdig ansehen können. Zum Beispiel könnten andere Nutzer persönliche Daten über sie veröffentlichen, etwa bei der Markierung von Fotos. Gesetzliche Regelungen zum Schutz der Privatheit sind uneinheitlich und orientieren sich teilweise nicht an den aktuellen Herausforderungen. Allgemein anerkannte

Verhaltenskodizes fehlen. Die technische Umsetzung der Regelungen ist mangelhaft, zum Beispiel kann die Verschlüsselung von Daten den Dienst langsam machen.

Wenn Privatheit derart eingeschränkt wird, lassen sich die freie Selbstbestimmung, demokratische Partizipation und ökonomisches Wohlergehen nicht optimal verwirklichen. Menschen, deren persönliche Daten und Informationen umfassend bekannt sind, können sich kaum frei und selbstbestimmt entwickeln und am politischen Diskurs teilnehmen. Privatheit ist also essenziell, um diese Werte zu verwirklichen. Dabei steht die Privatheit allerdings in einem ambivalenten Verhältnis zu ihnen. Denn Internetdienste können die genannten Werte dennoch unterstützen, obwohl sie Privatheit manchmal nicht oder wenig zulassen, beispielsweise indem sie überhaupt Raum für politische Diskussionen zur Verfügung stellen oder Informationsquellen bieten. Privatheit muss also angemessen gestaltet werden, ohne die Chancen des Internets zu sehr einzuschränken.

Drei Bedingungen müssen erfüllt sein, damit angemessene Privatheit im Internet realisiert werden kann: Nutzungskompetenz, Gestaltungsmöglichkeit und Vertrauenswürdigkeit. Dies kann durch eine Kultur der Privatheit erreicht werden, die Bildung, Recht, Wirtschaft und Technik umfasst. Bildung sorgt dafür, dass die Menschen Chancen und Risiken des Internets sowie ihre Rechte kennen. So können sie Präferenzen für ihren Umgang mit Privatheit im Web entwickeln und diese entsprechend gestalten. Das Recht setzt verbindliche Regeln. Diese Regeln müssen technisch umsetzbar sein, um erfüllt werden zu können. Sie richten sich an Wirtschaft, Behörden, Nutzerinnen und Nutzer und so weiter. Die Akteure beachten die rechtlichen Vorschriften und weitere Regeln, die angemessene Privatheit ermöglichen, und werden so vertrauenswürdig.

Mit den Chancen und Risiken des Internets befassen sich in Deutschland die 2010 vom Deutschen Bundestag eingesetzte Enquete-Kommission „Internet und digitale Gesellschaft", aber auch Datenschutzbehörden und Landtage. Der 2012 von der Europäischen Kommission vorgelegte Entwurf einer neuen Datenschutzverordnung will die Datenschutzgesetzgebung von Europa aus weiterentwickeln und trägt so der transnationalen Dimension des Themas Rechnung.

An diesen Diskurs anknüpfend unterbreitet acatech folgende **Empfehlungen**:

BILDUNG

- Internetkompetenz für alle schaffen
- Internetkompetenz einen festen Platz in der (vor-) schulischen Ausbildung einräumen
- Privatheitsschutz in der Fachausbildung und Weiterbildung verankern
- Privatheitsschutz durch öffentliche Kampagnen vermitteln
- Forschung zu Privatheitsvorstellungen und -praktiken ausbauen

RECHT

- Technische Umsetzung den Diensten überlassen
- Privatheitsschutzrecht anwenden, das den Nutzerinnen und Nutzern vertraut ist
- Einwilligung regulieren
- Transparenz schaffen und Kontrolle ermöglichen
- Löschen ermöglichen
- Migration unterstützen
- Datenschutzprinzipien beachten
- Privatheitsschutz-Zertifizierung regeln
- Verhaltensanreize zur Selbstregulierung erforschen

WIRTSCHAFT

- Mehr Privatheitsschutz zur Auswahl stellen
- Verwendung von Privacy-Agenten ermöglichen
- Standards vereinbaren
- Privatheitssiegel und -zertifikate entwickeln

TECHNIK

- Internetdienste nach dem Prinzip „Privacy by Design" entwickeln und betreiben
- Informierte und bewusste Einwilligung unterstützen
- Vergessenwerden im Internet erforschen
- Nutzerfreundlichkeit sicherstellen
- Nutzungskompetenz und Gestaltungsmöglichkeiten unterstützen
- Vertrauenswürdige Auditierung unterstützen
- Data Mining-Verfahren für „Big Data"-Privacy erforschen
- Anonyme und pseudonyme Nutzung von Diensten ermöglichen
- Grundlegende Methoden und Technologien weiterentwickeln

PROJEKT

Diese Position entstand auf Grundlage der acatech STUDIE *Internet Privacy – Eine multidisziplinäre Bestandsaufnahme* (Buchmann 2012) sowie *Internet Privacy – Options for adequate realisation* (Buchmann 2013).

> PROJEKTLEITUNG

Prof. Dr. Dr. h.c. Johannes Buchmann, Technische Universität Darmstadt/CASED/acatech

> PROJEKTGRUPPE

- Prof. Dr. Dr. h.c. Johannes Buchmann, Technische Universität Darmstadt/CASED/acatech
- Prof. em. Dr. Rafael Capurro, ehemals Hochschule der Medien (HdM), Stuttgart
- Prof. Dr. Martina Löw, Technische Universität Darmstadt
- Prof. Dr. Dr. h.c. Günter Müller, Albert-Ludwigs-Universität Freiburg
- Prof. Dr. Alexander Pretschner, Technische Universität München
- Prof. Dr. Alexander Roßnagel, Universität Kassel
- Prof. Dr. Michael Waidner, Technische Universität Darmstadt/Fraunhofer SIT/CASED
- Dr. Wieland Holfelder, Google Germany
- Dr. Göttrik Wewer, Deutsche Post DHL
- Michael Bültmann, Nokia
- Dirk Wittkopp, IBM Deutschland

> AUFTRÄGE/MITARBEITER

- Dr. Karin-Irene Eiermann, acatech Geschäftsstelle
- Martin Peters, Albert-Ludwigs-Universität Freiburg
- Thomas Heimann, Google Germany
- Carsten Ochs, Technische Universität Darmstadt
- Fatemeh Shirazi, Technische Universität Darmstadt
- Hervais Simo, Technische Universität Darmstadt
- Florian Kelbert, Technische Universität München
- Maxi Nebel, Universität Kassel
- Dr. Philipp Richter, Universität Kassel
- Daniel Nagel, Stuttgart, unabhängig
- Dr. Michael Eldred, Köln, unabhängig

> PROJEKTKOORDINATION

Dr. Karin-Irene Eiermann, acatech Geschäftsstelle

> PROJEKTVERLAUF

Projektlaufzeit: 07/2011 – 06/2013

> FINANZIERUNG

Das Projekt wurde vom Bundesministerium für Bildung und Forschung (BMBF) gefördert (Förderkennzeichen: 01.08.2011 – 30.09.2012: 01BY1175, 01.10.2012 – 31.01.2013: 16BY1175).

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Projektträger:
01.08.2011 – 30.09.2012: Projektträger im Deutschen Zentrum für Luft- und Raumfahrt (PT-DLR), Kommunikationstechnologien

01.10.2012 – 31.01.2013: VDI/VDE Innovation + Technik

acatech dankt außerdem den folgenden Unternehmen für ihre Unterstützung:

Google Germany, Deutsche Post AG, Nokia, IBM Deutschland

1 EINLEITUNG

Kaum eine Technologie hat unser Leben, unsere Arbeit und unsere Interaktionen schneller, stärker, nachhaltiger und fundamentaler verändert als das Internet. Weltweit nutzen es heute über 1,5 Milliarden Menschen; in Deutschland sind es mindestens 50 Millionen. Das Internet ermöglicht und vereinfacht den Zugriff auf Informationen und die Nutzung von Diensten wie die Buchung von Flügen, den Online-Einkauf und die Kommunikation in Form von E-Mails oder kostenfreier Videotelefonie. Das Internet beweist sein Innovationspotenzial, indem es neue Geschäftsmodelle und Arbeitsplätze entstehen lässt und so enorm zur gesamtwirtschaftlichen Wertschöpfung beiträgt. In fundamentaler Weise verändert es die Geschäftsprozesse innerhalb und zwischen Unternehmen sowie innerhalb und zwischen öffentlichen Verwaltungen. Das Internet bildet die Infrastruktur für intelligente Stromnetze, die Stromerzeuger, Speicher sowie Verbraucher miteinander vernetzen und steuern und für das Gelingen der Energiewende nötig sind. Es schafft die Voraussetzung für intelligente Verkehrsleitsysteme, die den Straßenverkehr noch sicherer und effizienter machen. Über das Internet gesteuerte Cyber-Physical Systems helfen in der Fabrik der Zukunft beim effizienten Einsatz von Produktionsressourcen und Energie. Neben diesen positiven Aspekten für den Einzelnen und die Wirtschaft ermöglicht das Web auch die Teilhabe an sozialen und politischen Formationsprozessen und begünstigt die gesamtgesellschaftliche Entwicklung sowie die Entfaltung grundlegender Werte, wie diese Position zeigt.

Kennzeichnend für viele Dienste im Internet ist eine „Umsonst"-Kultur. Die Nutzerinnen und Nutzer haben sich daran gewöhnt – und erwarten es geradezu –, für Suchmaschinen, Lexika, Filme, Bilder, Musik, Nachrichten, Zeitschriften, soziale Netzwerke, Foren, Blogs und viele andere Angebote kein Geld zu bezahlen. Dennoch sind diese Angebote nicht kostenlos: Um sie zu erbringen, sind Hardware und Software, Ideen und Energie, Kapital und Arbeit erforderlich. Und die wollen bezahlt sein. Die Währung, in der die Nutzerinnen und Nutzer diese Leistungen bezahlen, sind nicht Dollar oder Euro – sondern ihre *persönlichen Daten*, also Anmeldeinformationen, Suchanfragen, Fotos, Kurznachrichten, Einkäufe, Aufenthaltsorte, soziale Beziehungen und so weiter. Nahezu jedes Unternehmen, das seine Dienste im Internet ohne Bezahlung anbietet, verlangt dafür solche Daten und verdient mit ihnen Geld, zum Beispiel durch ihre Verwendung für gezielte Werbung. So sind persönliche Daten Ware und Währung.

Obwohl viele das Internet als äußerst nützlich erleben, verursacht die Fülle von persönlichen Informationen auch Unsicherheit, die zu Misstrauen führen kann. Sogar sogenannte *Digital Natives*, die mit dem Internet aufgewachsen sind und sich in der Online-Welt deutlich sicherer fühlen als ältere Generationen, befürchten nicht selten, von anderen Nutzerinnen und Nutzern beobachtet und identifiziert zu werden. *Digital Immigrants*, die im Internet gut sozialisiert sind, sind oft skeptisch, ob die Internetdienste mit ihren persönlichen Daten sorgfältig umgehen. *Digital Outsiders*, denen das Netz bis jetzt fremd geblieben ist, fühlen sich den vermeintlichen Gefahren im Internet sogar hilflos ausgesetzt. Das Vertrauen zwischen Nutzern und Diensteanbietern ist aber die Grundvoraussetzung, um das Potenzial des Internets zum Wohl und Fortschritt der Gesellschaft voll auszuschöpfen.[1]

Die beschriebene Spannung zwischen dem Nutzen des Internets einerseits und seinen Risiken andererseits – allgemeiner: das Internet und seine vielfältigen Auswirkungen auf den Einzelnen, die Gesellschaft, Politik und Wirtschaft – hat in den vergangenen Jahren unter dem Oberbegriff „Netzpolitik" einen immensen Bedeutungszuwachs im politisch-gesellschaftlichen Diskurs erfahren. In Deutschland wurde 2010 vom Deutschen Bundestag eine Enquete-Kommission „Internet und digitale Gesellschaft" eingesetzt, die sich mit Themen wie Datenschutz, Urheberrecht, Medienkompetenz und Verbraucherschutz befasst. Heute sprechen sich Expertinnen und Experten sowie Vertreterinnen und Vertreter aller Bundestagsfraktionen dafür aus, die Arbeit dieser Kommission in einen regulären Bundestagsausschuss für

[1] Buchmann 2012; DIVSI 2012.

Netzpolitik zu überführen. Datenschutzbehörden und Landtage beschäftigen sich regelmäßig mit Themen wie dem Recht auf Verwendung von Pseudonymen in sozialen Netzwerken, dem Umgang mit Nutzerprofilen und der Speicherung von Telekommunikationsdaten zur Bekämpfung von Kriminalität. Auch in der europäischen Diskussion spielen Fragen des Schutzes von Daten und Privatsphäre eine wichtige Rolle. Mit dem 2012 von der Europäischen Kommission vorgelegten Entwurf einer neuen Datenschutzverordnung geht erstmals die Initiative für eine Weiterentwicklung der Datenschutzgesetzgebung von Europa aus und trägt so der transnationalen Dimension dieses Themas Rechnung. Wird der Entwurf Realität, gilt die Verordnung – im Gegensatz zu bisherigen Richtlinien – unmittelbar in allen EU-Mitgliedsstaaten und kann dort nicht mehr verstärkt oder abgeschwächt werden. Die Vorschläge der Kommission stellen den nationalen Regierungen die Aufgabe, ihre Datenschutzgesetze zu modernisieren und die gesellschaftliche Debatte über das Verhältnis von Freiheit, Verantwortung und Regulierung im Internet voranzutreiben.

Diese acatech POSITION und ihre Empfehlungen bilden einen Beitrag zum öffentlichen Diskurs über Privatheit im Internet. Sie sind Ergebnis des acatech Projekts „Internet Privacy", das angesichts der großen wirtschaftlichen und gesellschaftlichen Bedeutung des Themas eine intensive interdisziplinäre wissenschaftliche Auseinandersetzung und einen vieldimensionalen Diskurs begonnen hat, den es in dieser Form in Deutschland bisher noch nicht gibt. Die Empfehlungen sollen einen Beitrag zur Etablierung einer *Kultur der Privatheit* im Internet leisten und damit der Auflösung des Spannungsverhältnisses zwischen dem großen Wert des Internets für seine Nutzerinnen und Nutzer einerseits und der Sorge um die Beeinträchtigung ihrer Privatheit andererseits dienen.

Privatheit

Privatheit ist nicht gleich Privatsphäre. Das Wort Privatsphäre erzeugt die Vorstellung von einem geschützten Bereich, in dem man sich vollständig vor der Außenwelt verbirgt. Wenn Menschen im Internet miteinander kommunizieren und interagieren, geht es aber um mehr. Es geht um Privatheit als einen wichtigen Aspekt sozialer Interaktion: Wer mit seinen Freunden politische Diskussionen führt, möchte vielleicht nicht, dass Außenstehende wie Arbeitskollegen mitlesen können. Wer im Internet einkauft, ist möglicherweise nicht daran interessiert, dass andere davon erfahren. In solchen Interaktionen zeigen die Menschen manches und verbergen anderes. Privatheit bedeutet die Fähigkeit, dieses „sich zeigen und verbergen" selbst definieren und regulieren zu können. Verbergen kann vollständig sein, zum Beispiel wenn anonym kommuniziert wird. Es kann sich aber auch nur auf bestimmte Aspekte beziehen, wie zum Beispiel Alter, Geschlecht oder Aufenthaltsort. Ein anderes Beispiel für diese Vorstellung von Privatheit ist, dass Nutzerinnen und Nutzer sich in unterschiedlichen Rollen zeigen können, etwa in beruflich oder eher privat orientierten sozialen Netzwerken. Was so verstandene Privatheit im Einzelnen bedeutet, ist kulturabhängig. In Deutschland und Europa ist Privatheit eng verwandt mit dem Grundrecht auf „informationelle Selbstbestimmung".

Kultur

Kultur bezeichnet im weitesten Sinne alles, was Menschen selbst gestaltend hervorbringen. Sie umfasst Technik und Kunst, aber auch Recht, Werte, Wirtschaft und Wissenschaft. Sie ist ein Gefüge aus expliziten und impliziten Regeln, Regelungen und Vorstellungen. Kultur stabilisiert die Praktiken und Interaktionen der Menschen. Kultur sollte so gestaltet werden, dass angemessene Privatheit möglich wird. Dabei müssen ihre verschiedenen Aspekte aufeinander bezogen und deren vielfältige, wechselseitige Abhängigkeiten berücksichtigt werden. Wenn zum Beispiel das Recht vorschreibt, dass „Vergessenwerden im Internet" möglich sein soll, dann muss ein solches Vergessen technisch realisiert werden können. Tatsächlich ist ein solches Recht im Entwurf der europäischen Datenschutzverordnung vorgesehen, die technische Machbarkeit liegt jedoch, wenn überhaupt jemals realisierbar, noch in weiter Ferne. In einer

Kultur der Internet-Privatheit verlangen Gesetze das, was sinnvoll und technisch möglich ist. Diensteanbieter, Nutzerinnen und Nutzer beachten diese Gesetze und entwickeln auch jenseits der Rechtsprechung angemessene Praktiken und Normen, die zu einem privatheitsfreundlichen Verhalten aller Beteiligten führen. Die Wissenschaft arbeitet daran, die Schutzmöglichkeiten so weiterzuentwickeln, dass sie noch wirksamer werden, ohne den Nutzen des Internets einzuschränken.

Angemessene Privatheit

Eine Kultur der Privatheit soll etabliert werden. Dazu muss entschieden werden, welches Maß an Privatheit angemessen ist. In den pluralen europäischen Gesellschaften und auch darüber hinaus gibt es darauf keine eindeutige Antwort. Während zum Beispiel manche in sozialen Netzwerken mit Hunderten von „Freunden" persönliche Informationen teilen, ist das für andere unvorstellbar. Zusätzlich ist die Vorstellung von angemessener Privatheit auch einem historischen Entwicklungsprozess unterworfen.

In dieser komplexen und dynamischen Situation schlägt acatech einen festen Bezugspunkt vor, der es erlaubt, angemessene Privatheit immer wieder neu zu bestimmen. Angemessene Privatheit soll daran gemessen werden, inwiefern sie grundlegende europäische Werte befördert: (i) freie Selbstbestimmung, (ii) demokratische Partizipation und (iii) wirtschaftliches Wohlergehen, die Rahmenbedingungen für unsere pluralistischen demokratischen westeuropäischen Gesellschaften. acatech betrachtet also Privatheit nicht als Wert an sich, sondern als wertvoll und schutzwürdig nur insofern, als sie zur Erhaltung, zum Schutz und zur Förderung der genannten grundlegenden Werte dient. Die grundlegenden Werte sind unveränderlicher Bestandteil der universell akzeptierten Menschenrechte und unverzichtbar für ein Leben in Würde, frei von Hunger, Angst vor Unterdrückung, Gewalt und Ungerechtigkeit.[2] Deshalb ist acatech davon überzeugt, dass sie über den europäischen Kontext hinaus breite Akzeptanz finden.

Privatheit steht in einem ambivalenten Verhältnis zu diesen Werten. Einerseits können sich Menschen, deren persönliche Daten und Informationen umfassend bekannt sind, kaum frei und selbstbestimmt entwickeln und am politischen Diskurs teilnehmen. Privatheit ist also notwendig, um diese Werte zu verwirklichen. Andererseits können Internetdienste dennoch die genannten Werte unterstützen, obwohl sie Privatheit manchmal nicht oder wenig zulassen, beispielsweise indem sie überhaupt Raum für politische Diskussionen zur Verfügung stellen, Informationsquellen bieten oder gleichgesinnten Menschen ermöglichen, sich zu vernetzen. Eine Kultur der Privatheit im Internet muss daher angemessene Privatheit ermöglichen, ohne die Chancen des Internets zu sehr einzuschränken.

Im nächsten Abschnitt dieser Position werden die genannten grundlegenden Werte näher erläutert, ihr Bezug zur Privatheit dargestellt und analysiert, inwiefern das Internet zu ihrer Verwirklichung beitragen kann. Der dritte Abschnitt beschreibt Bedrohungen, denen die Privatheit im Netz ausgesetzt ist, und diskutiert deren Bedeutung für die drei Werte. Im vierten Abschnitt werden Thesen zur Entwicklung einer Kultur der Privatheit im Internet formuliert. Der fünfte Abschnitt enthält konkrete Handlungsempfehlungen für wichtige Bereiche: Bildung von Kindern, Jugendlichen und Erwachsenen; Recht; Wirtschaft und Technik.

[2] UN 2000.

2 GRUNDLEGENDE WERTE

Die grundlegenden Werte der europäischen Tradition und Gegenwart, die acatech der Entwicklung einer Kultur der Privatheit im Internet zugrunde legt, sind (i) freie Selbstbestimmung, (ii) demokratische Partizipation und (iii) wirtschaftliches Wohlergehen.

Freie Selbstbestimmung

Unter freier Selbstbestimmung wird die Möglichkeit des Einzelnen verstanden, eigene Lebensoptionen zu entwickeln und aus ihnen frei auswählen zu können. Sie bezieht sich zum Beispiel auf Religion, Beruf, Freunde und sexuelle Orientierung. Das Internet mit seinen vielfältigen Anwendungen kann zur freien Selbstbestimmung beitragen. So ist zum Beispiel die Interaktion mit Menschen auf der ganzen Welt leicht möglich. Damit steigt die Möglichkeit, Gleichgesinnte kennenzulernen und sich etwa zu Interessengruppen zusammenzuschließen. Im Netz stehen außerdem qualitativ hochwertige kostenlose Informations- und Bildungsangebote zur Verfügung, die die Menschen bei der Entwicklung eines selbstbestimmten Lebensentwurfs unterstützen.

Gleichzeitig ist Privatheit eine wichtige Voraussetzung für freie Selbstbestimmung. So muss der oder die Einzelne in der globalen Kommunikation und Interaktion über das Internet zum Beispiel wählen können, welche Informationen er oder sie preisgibt und welche nicht. Informationen, die für gute Freunde bestimmt sind, gehören beispielsweise nicht in einen Kontext, wo Menschen ihre beruflichen Qualifikationen präsentieren wollen, wie etwa in sozialen Business-Netzwerken.

Demokratische Partizipation

Demokratische Partizipation bedeutet mehr als das Recht und die Möglichkeit, an freien und fairen Wahlen teilzunehmen. Sie umfasst die Freiheit des Einzelnen, sich in sozialen und politischen Diskursen frei zu äußern und an der gesellschaftlichen Willensbildung teilzunehmen sowie den freien Zugang zu Informationen, die für die politische Willensbildung notwendig sind. Demokratische Partizipation ist ein wichtiger Aspekt freier Selbstbestimmung und setzt diese voraus. Das Internet kann zur politischen Partizipation in hohem Maße beitragen: Menschen, die eine politische Überzeugung oder ein politisches Ziel miteinander teilen, können sich im Web einfach vernetzen; sie können ihre Botschaften sehr viel nachhaltiger verbreiten, als das in einzelnen Veranstaltungen möglich ist; und sie sind dabei nicht auf die etablierten Medien wie Zeitungen oder das Fernsehen angewiesen. Prominente Beispiele für die Rolle des Internets in politischen Prozessen sind die Online-Petition gegen die Vorratsdatenspeicherung, die Plattform Wikileaks, auf der im Namen des öffentlichen Interesses vertrauliche Dokumente von Regierungen und Unternehmen veröffentlicht werden konnten, und die Demokratiebewegungen in den arabischen Staaten. Die Empfindlichkeit, mit der totalitäre Regime auf das Internet reagieren, und ihre Versuche, es zu zensieren, bestätigen seine Relevanz für die politische Meinungsbildung sowie für politische und soziale Aktionen.

Aber auch demokratische Partizipation setzt angemessene Privatheit voraus. Die Meinungsbildung in politischen Gruppen kann nur dann produktiv erfolgen, wenn ihre Mitglieder darauf vertrauen können, dass ihre Beiträge nicht in einen falschen Kontext geraten. Gleichzeitig ist es für die Teilnehmerinnen und Teilnehmer an politischen Diskursen wichtig, dass sie nur diejenigen Aspekte ihrer Persönlichkeit zeigen müssen, die für den Diskurs relevant sind. Was das ist, hängt wieder von den unterschiedlichen Kulturen in den verschiedenen Ländern ab. So wird in Deutschland das Beziehungs- und Familienleben von Politikern als deren Privatsphäre betrachtet und aus dem politischen Diskurs ausgeklammert, während es in den USA wichtiger Bestandteil politischer Selbstdarstellung ist.

Wirtschaftliches Wohlergehen

Eine grundlegende Voraussetzung menschenwürdigen Lebens ist ökonomisches Wohlergehen einschließlich der Absicherung grundlegender materieller Bedürfnisse. Vorbedingungen für ökonomisches Wohlergehen sind sowohl die Erzeugung von Wohlstand als auch seine breite und

gerechte Verteilung. Ökonomisches Wohlergehen bedeutet auch, dass diejenigen, die dazu in der Lage sind, so viel Geld verdienen können, dass sie davon ein angenehmes Leben führen können und gleichzeitig schwächere Mitglieder der Gesellschaft, zum Beispiel Kinder, Alte und Kranke, unterstützt und versorgt werden. Ökonomisches Wohlergehen spielt in den meisten gesellschaftlichen Ordnungen eine wichtige Rolle. Die Meinungen darüber, was Wohlstand im Einzelnen bedeutet, gehen allerdings auseinander – wie jüngst die Debatten in der Bundestags-Enquete-Kommission „Wohlstand, Wachstum, Lebensqualität" zeigten.

Das Internet als zentraler Bestandteil der modernen Wirtschaft trägt wesentlich zum Wohlstand bei. In den modernen Informationsgesellschaften ist dafür der Zugang zum Internet für alle erforderlich, wie gerade in einem Urteil des Bundesgerichtshofs[3] festgestellt wurde. Er ermöglicht zum Beispiel Teilhabe an Bildung, Wissen und Märkten. Durch das Internet sind in den vergangenen Jahren viele neue Berufe und Jobs entstanden. Eine Studie zeigt, dass allein in Europa über 230.000 Arbeitsplätze von sozialen Online-Netzwerken abhängen.[4] Auf dem globalen Marktplatz des Internets können Menschen viele Produkte und Dienstleistungen günstig kaufen. Gleichzeitig können viele Unternehmen ihre Angebote, besonders datenzentrische Dienste, im Web international platzieren und damit ihre Erfolgschancen steigern. Privatheit spielt auch für wirtschaftliches Wohlergehen eine Rolle. Verletzungen der Privatheit, zum Beispiel die Verwendung persönlicher Daten ohne Einverständnis der Nutzer, können das Vertrauen im Netz reduzieren und damit die Entwicklung internetbasierter Wirtschaftszweige einschränken.

Die Entfaltung der grundlegenden Werte „freie Selbstbestimmung", „demokratische Partizipation" und „wirtschaftliches Wohlergehen" wird also durch das Internet signifikant unterstützt und erfordert gleichzeitig den Schutz der Privatheit der Nutzerinnen und Nutzer. Privatheit im Internet muss also so geschützt werden, dass das Internet seine Möglichkeiten, diese Werte zu unterstützen, trotzdem entfalten kann.

3 BGH 2013.
4 Deloitte 2012.

3 PRIVATHEIT IM INTERNET: EINE HERAUSFORDERUNG

Viele Nutzerinnen und Nutzer von Internetdiensten bezweifeln, dass ihre Privatheit stets angemessen geschützt ist. Sind diese Zweifel berechtigt?

Angemessene Privatheit im Internet ist gegeben, wenn zwei Bedingungen erfüllt sind:

Nutzungskompetenz und Gestaltungsmöglichkeit

Die erste Bedingung ist, dass die Nutzerinnen und Nutzer sich der Möglichkeiten des Internets bewusst sind, ihre Selbstentfaltung, die Möglichkeit zur politischen Partizipation und ihren Wohlstand zu unterstützen. Gleichzeitig kennen sie die Risiken, die sich aus möglichen Verletzungen ihrer Privatheit für sie ergeben. Sie sind in der Lage, in Abwägung dieser beiden Aspekte Präferenzen für ihren Umgang mit Privatheit im Internet zu entwickeln, und können diese Privatheit so gestalten, wie es ihren Präferenzen entspricht. Dies bedeutet, dass entsprechende Gestaltungsmöglichkeiten vorhanden und für die Nutzerinnen und Nutzer verständlich und handhabbar sind.

Gelegentlich wird die Auffassung vertreten, Privatheitsschutz falle ausschließlich in den Verantwortungsbereich der Einzelnen. Angesichts der Komplexität des Internets und seiner Dienste sowie der Heterogenität der Nutzergruppen ist es für die Einzelnen jedoch nicht möglich, alle potenziellen Einschränkungen ihrer Privatheit und deren mögliche Konsequenzen einschätzen und adäquat darauf reagieren zu können. Kenntnisse und Gestaltungsmöglichkeiten können sich nur auf einzelne Bereiche beziehen und hängen von Fähigkeiten, Interesse und Bereitschaft der Beteiligten ab. Der Schutz ihrer oder seiner Privatheit kann darum nicht der oder dem Einzelnen überlassen bleiben. Daher ist eine zweite Bedingung zentral:

Vertrauenswürdigkeit des Internets und seiner Akteure

Das Internet, seine Dienste und Teilnehmer müssen unabhängig von den Kenntnissen, Vorlieben und Aktionen der einzelnen Nutzerinnen und Nutzer einen grundlegenden Schutz der Privatheit garantieren. Diese Bedingung bezieht sich einerseits auf die Anbieter von Internetdiensten. Internetteilnehmerinnen und -teilnehmer wollen sich darauf verlassen können, dass angemessene (gesetzliche und nichtgesetzliche) Regeln für den Betrieb von Internetdiensten existieren und die Anbieter sich an diese Regeln halten. Eine solche Regel ist zum Beispiel Datensparsamkeit: Dienste werden so gestaltet, dass sie mit möglichst wenig persönlichen Daten auskommen. Andererseits bezieht sich die Bedingung der Vertrauenswürdigkeit auch auf die anderen Nutzer, also zum Beispiel auf Freundinnen und Freunde in sozialen Netzwerken. Sie sollen sich ebenfalls an Regeln halten, die einen grundlegenden Schutz der Privatheit gewährleisten, auch ohne dass dies technisch erzwungen wird.

Mögliche Einschränkungen

In vielen Bereichen sind die *Nutzungskompetenzen* und *Gestaltungsmöglichkeiten* der Nutzerinnen und Nutzer einerseits und die *Vertrauenswürdigkeit* des Internets andererseits noch nicht so ausgebildet, dass angemessene Privatheit garantiert wäre. acatech fasst hier die möglichen Einschränkungen der Privatheit zusammen, die in den aus dem acatech Projekt „Internet Privacy" hervorgegangenen Studien ausführlicher dokumentiert sind.[5]

Gegenwärtig ist es für Anwenderinnen und Anwender schwierig, ausreichende *Kenntnisse* darüber zu erlangen, welche persönlichen Daten den Internetdiensten bekannt werden und nach welchen Regeln sie verarbeitet und weitergeben werden. Neben den Informationen, die Nutzerinnen und Nutzer willentlich an die Dienste weitergeben (Name, Anschrift, Bestellinformationen usw.), hinterlassen sie auch viele Spuren, derer sie sich möglicherweise nicht bewusst sind: welche Webseiten sie besuchen, welche Freunde sie haben und was sie in Nachrichten schreiben. Aus den gesammelten Daten können mit den modernen Methoden der Informatik weitere Informationen abgeleitet werden. Auch dessen sind sich Nutzerinnen und Nutzer nicht immer bewusst. Es ist möglicherweise nicht klar, welche Informationen

[5] Buchmann 2012; Buchmann 2013.

an Dritte weitergegeben werden, wenn zum Beispiel ein Nutzer ein Online-Spiel im Kontext eines sozialen Netzwerks verwendet. Hier entsteht das Risiko der *De-Kontextualisierung*: Persönliche Daten werden in Kontexten verwendet, denen die Besitzer nicht zustimmen würden, wenn sie dies wüssten. Neben der De-Kontextualisierung besteht auch das Risiko der *Persistenz*: Persönliche Daten werden länger aufgehoben als nötig. Nutzerinnen und Nutzer sind sich nicht immer darüber im Klaren, was mit ihren Daten geschieht, nachdem sie für einen Dienst nicht mehr nötig sind. Werden die Daten in einem sozialen Netzwerk wirklich gelöscht, wenn Nutzer dies wollen? Dies ist nicht immer der Fall. Es kommt vor, dass die Daten trotzdem aufbewahrt oder lediglich anonymisiert werden. Hier entsteht ein drittes Risiko, das der *Re-Identifikation*: Es ist heute mithilfe fortgeschrittener Analysetechniken möglich, viele anonyme Datensätze wieder einzelnen Personen zuzuordnen. Die Kenntnis der Nutzerinnen und Nutzer bleibt unvollständig, obwohl Informationen der Anbieter in erheblichem Umfang zur Verfügung stehen, beispielsweise in Form von AGBs. Diese Informationen sind aber nicht immer zugänglich und teils schwer verständlich.

Auch die *Gestaltungsmöglichkeiten* der Nutzerinnen und Nutzer im Hinblick auf ihre Privatheitspräferenzen sind eingeschränkt. Dienste bieten nicht immer die gewünschten Auswahlmöglichkeiten. So verlangen die meisten E-Commerce-Anbieter im Internet, dass die Nutzer ihnen ihre vollständigen persönlichen Informationen (Geschlecht, Geburtsdatum, Anschrift etc.) zur Verfügung stellen, obwohl dies für die Erbringung des Dienstes nicht immer nötig ist. Manche Dienste, wie zum Beispiel soziale Netzwerke, bieten zahlreiche Gestaltungsmöglichkeiten. Diese sind jedoch nicht immer leicht verständlich und nutzbar. So ist es etwa für Mitglieder von sozialen Netzwerken oft schwierig zu verhindern, dass andere Nutzer persönliche Daten über sie veröffentlichen, zum Beispiel bei der Markierung von Fotos. Außerdem beziehen sich die Gestaltungsmöglichkeiten typischerweise auf die Daten, die der Dienst direkt von den Anwenderinnen und Anwendern sammelt, aber weniger auf Informationen, die aus den Daten abgeleitet werden. Auch haben die Nutzer meist keinen Einfluss darauf, ob die Informationen an Dritte weitergegeben werden oder nicht.

Die internationale „Internet-Moral", auch Netiquette genannt, ist noch nicht so fortgeschritten, dass sich die Nutzerinnen und Nutzer gegenseitig immer als vertrauenswürdig ansehen können. Gesetzliche Regelungen, die zum Schutz der Privatheit beitragen sollen, sind uneinheitlich und orientieren sich teilweise nicht an den Herausforderungen des modernen Internets. Allgemein anerkannte Verhaltenskodizes für das Agieren im Web fehlen. Zudem gehen nicht alle Anbieter mit den persönlichen Daten der Nutzer so um, wie es gesetzlichen Regeln und den Präferenzen der Nutzer entspricht. Selbst wenn die Dienste beabsichtigen, die Regeln einzuhalten, scheitert das Vorhaben teilweise an der technischen Umsetzung, wenn zum Beispiel Daten unverschlüsselt gespeichert werden, um den Dienst nicht zu langsam zu machen. Werden persönliche Daten an Dritte weitergegeben, wird es noch schwieriger, den Schutz der Privatheit durchzusetzen. Inzwischen können fortgeschrittene Informatiktechniken dazu verwendet werden, aus den vorhandenen Daten viele Informationen zu gewinnen, etwa indem anonymisierte Daten wieder Personen zugeordnet werden.

Die mangelnde Vertrauenswürdigkeit von Nutzern und Anbietern kann zu Zweckentfremdung, De-Kontextualisierung, ungewollter Persistenz und Re-Identifikation persönlicher Daten führen. Um ihre Vertrauenswürdigkeit zu steigern, nehmen Anbieter von Internetdiensten an Auditierungsverfahren teil. Der Wert solcher Verfahren ist aber für die meisten Internetnutzer nicht einschätzbar. Daher tragen sie nur wenig zur Vertrauenswürdigkeit der Dienste bei.

Bedeutung der Einschränkungen der Privatheit für die Grundwerte

In Abschnitt 2 wurde gezeigt, dass Privatheit eine wichtige Voraussetzung für die Verwirklichung und den Schutz von freier Selbstbestimmung, demokratischer Partizipation und

wirtschaftlichem Wohlergehen darstellt. In Anbetracht der beschriebenen möglichen Einschränkungen der Privatheit im Internet lässt sich diese Aussage noch konkretisieren. Die De-Kontextualisierung persönlicher Daten hat in zahlreichen Beispielen zur Einschränkung der freien Selbstbestimmung geführt, etwa wenn die sexuellen Präferenzen den Eltern von Internetnutzern bekannt wurden. De-Kontextualisierung, Persistenz und Re-Identifikation können mit erheblichen Risiken für die freie Selbstbestimmung und die demokratische Partizipation verbunden sein. Wird beispielsweise das Wahlverhalten von Menschen, das in internen politischen Diskussionen zum Ausdruck kommt, öffentlich gemacht, beschädigt dies den demokratischen Grundsatz des Wahlgeheimnisses. Neben diesen direkten Risiken gibt es auch indirekte Effekte. Nutzerinnen und Nutzer könnten sich angesichts möglicher Risiken scheuen, das Internet zur Unterstützung ihrer freien Selbstbestimmung und politischen Partizipation zu verwenden. Auch ökonomisches Wohlergehen kann durch mangelnde Privatheit im Netz kompromittiert werden, weil das Vertrauen in die Dienste eingeschränkt und damit ihr wirtschaftlicher Erfolg behindert wird.

Diese Analyse zeigt, dass der Schutz der Privatheit im Internet essenziell für die Verwirklichung der genannten grundlegenden Werte ist.

4 THESEN ZUR ENTWICKLUNG EINER KULTUR DER PRIVATHEIT IM INTERNET

Aus den vorherigen Abschnitten lassen sich folgende Schlussfolgerungen ziehen, die die Grundlage für konkrete Handlungsempfehlungen bilden:

a) Das Internet unterstützt die Verwirklichung der grundlegenden Werte „freie Selbstbestimmung", „demokratische Partizipation" und „wirtschaftliches Wohlergehen".

b) Mangelnde Privatheit schränkt die Verwirklichung dieser Werte ein.

c) Privatheit im Internet soll so gestaltet werden, dass die grundlegenden Werte optimal verwirklicht werden können.

d) Dies kann durch eine Kultur der Privatheit erreicht werden, die Bildung, Recht, Wirtschaft und Technik umfasst.

5 HANDLUNGSEMPFEHLUNGEN

Die Handlungsempfehlungen in diesem Abschnitt zielen darauf ab, Bildung, rechtliche Rahmenbedingungen, Wirtschaft und Technik so zu entwickeln, dass Privatheit im Internet möglich wird und gleichzeitig das Internet sein Potenzial zur Unterstützung von Selbstbestimmung, demokratischer Partizipation und Wohlstand entfalten kann.

Es wurde in Abschnitt vier gezeigt, dass Privatheit im Internet unter zwei Voraussetzungen möglich ist: Zum einen müssen die Nutzerinnen und Nutzer über entsprechende Kenntnisse verfügen und sich der Möglichkeiten des Internets bewusst sein; zum anderen müssen sie darauf vertrauen können, dass Internetdienste und die anderen User ihre Privatheit respektieren. Die folgenden Empfehlungen tragen zur Erfüllung dieser Bedingungen bei. Sie betreffen die Bereiche Bildung, Recht, wirtschaftliche Akteure (Dienstanbieter) und Technik. Durch das Zusammenspiel dieser Bereiche entsteht die Kultur der Privatheit im Internet. Bildung sorgt dafür, dass die Nutzerinnen und Nutzer Chancen und Risiken des Internets sowie ihre Rechte kennen und ihre Privatheit gemäß ihren eigenen Präferenzen gestalten können. Das Recht setzt verbindliche Regeln. Diese Regeln müssen technisch umsetzbar sein, um erfüllt werden zu können. Sie richten sich an Wirtschaft, Behörden, Anwender etc. Diese beachten die rechtlichen Vorschriften und weitere Regeln, die angemessene Privatheit ermöglichen.

Jede dieser Handlungsempfehlungen erfordert eine Abwägung zwischen der Stärkung von Privatheit einerseits und den möglichen Einschränkungen von Internetdiensten und ihrer Unterstützung der grundlegenden Werte andererseits. Diese Abwägung ist nicht einfach und wurde im acatech Projekt „Internet Privacy" kontrovers diskutiert. An vielen Stellen bedarf sie weiterer Forschung und Diskussion und kann deshalb nicht als abgeschlossen angesehen werden. Insofern bilden die Empfehlungen einen Ausgangspunkt für den weiteren Diskurs.

5.1 BILDUNG

Bildung spielt eine entscheidende Rolle bei der Entwicklung einer Kultur der Privatheit. Das Internet und allgemeiner die Informationstechnologie gehören zu den wichtigsten Kulturtechniken der Gegenwart. Der Umgang mit dem Internet erfordert umfangreiche Kenntnisse und Handlungskompetenzen: Internetkompetenz. Bildungsziel muss es sein, diese zu entwickeln.

Im Kontext dieser Position bezieht sich Internetkompetenz darauf, den Nutzen des Internets für das eigene Leben, besonders für die freie Selbstbestimmung, die demokratische Partizipation und das ökonomische Wohlergehen, einschätzen und einsetzen zu können. Dies umfasst, dass die Nutzerinnen und Nutzer wichtige Geschäftsmodelle des Internets kennen („ich bezahle mit meinen Daten, die Anbieter sind profitorientierte Unternehmen" etc.) sowie relevante Privatheitsrisiken („Daten werden an möglicherweise nicht vertrauenswürdige Dritte weitergegeben", „was einmal im Netz ist, bleibt im Netz – was heute eine harmlose Information ist, kann morgen problematisch sein").

Anhand dieser Kenntnisse können sie ihre Privatheitspräferenzen immer wieder neu bestimmen (etwa „mir ist egal, dass der Anbieter weiß, was ich kaufe"). Sie wissen, wie sie angebotene Möglichkeiten (Monitoring-Werkzeuge, Privatheitseinstellungen etc.) nutzen können, um ihre Privatheitspräferenzen zu realisieren.

Die Anwender kennen ihre Pflichten (etwa „üble Nachrede ist auch im Internet nicht zulässig, die Gesetze der analogen Welt gelten auch in der digitalen Welt") und ihre Verantwortung für sich und andere. Sie wissen, dass Privatheit keine individuelle Angelegenheit ist, sondern dass alle für die Gewährleistung der Privatheit aller verantwortlich sind.

Die Bildung von Internetkompetenz ermöglicht also den bewussten Umgang mit Privatheit im Internet, eröffnet Handlungsmöglichkeiten und macht gleichzeitig Nutzer füreinander vertrauenswürdig.

> Internetkompetenz für alle schaffen

Internetkompetenz ist wichtig für alle. Daher muss es entsprechende Bildungsangebote für viele Zielgruppen geben, zum Beispiel Kinder und Jugendliche, Studierende und Auszubildende – besonders diejenigen, die später im Beruf mit dem Thema Privatheit zu tun haben –, Erwachsene aller Altersstufen und Bildungsschichten mit geringerer oder größerer Internetaffinität. Für Berufsgruppen, die besonders mit dem Thema Privatheit zu tun haben – sei es als Multiplikatoren wie Erzieherinnen und Erzieher, Lehrerinnen und Lehrer oder als IT-Spezialisten etc. –, sind spezielle Weiterbildungsmaßnahmen nötig.

> Internetkompetenz einen festen Platz in der (vor-)schulischen Ausbildung einräumen

acatech empfiehlt, dass Internetkompetenz als Teil von Medienkompetenz einen festen Platz in der vorschulischen und schulischen Ausbildung erhält. Nur so können Kinder und Jugendliche solche Kompetenz erlangen. In der Schule soll der Umfang des Unterrichts in Internet- und Medienkompetenz dem eines etablierten Schulfachs entsprechen. Der Unterricht kann als eigenes Schulfach angeboten oder in die bestehenden Schulfächer als Querschnittsthema integriert werden. Unabhängig davon erfordert er die Entwicklung und Verwendung innovativer Lehrformen und -inhalte. Denkbar wäre eine Medien-Werkstatt mit verschiedenen Formaten: „Schüler lehren Lehrer": Wie funktioniert Selbstorganisation in sozialen Online-Netzwerken? Ebenso können Schüler andere Schüler lehren: Wie funktionieren die Privatheitsregeln der Anbieter, wie bediene ich die Privatheitseinstellungen richtig, woher weiß ich, ob ein Dienst vertrauenswürdig ist? Diskussionen im Sinne „Alle lehren alle" sind auch sinnvoll: Wie viel Privatheit will ich überhaupt und wozu (meine Präferenzen)? Was sind gute Spielregeln für die digital vernetzte Welt? In einem weiteren Format können Schülerinnen und Schüler den Eltern ihre Ergebnisse aus der Medien-Werkstatt präsentieren, gepaart mit Vorträgen externer Expertinnen und Experten. Ergänzt werden können die neuen Formate durch die klassische Lehrform „Lehrer lehren Schüler": Was sind die Geschäftsmodelle im Internet, wie ist die dortige Rechtslage, welche technischen Möglichkeiten der Datensammlung und Nutzung gibt es (was ist ein Cookie, was heißt Inferenz)? acatech empfiehlt auch, dass für Eltern entsprechende Weiterbildungsangebote, etwa von Volkshochschulen, angeboten werden.

> Privatheitsschutz in der Fachausbildung und Weiterbildung verankern

Verschiedene Berufe haben direkt oder indirekt mit dem Thema Privatheit zu tun, zum Beispiel Ärztinnen und Ärzte sowie andere medizinische Berufe oder Informatikerinnen und Informatiker. acatech empfiehlt, dass Privatheitsschutz obligatorischer Bestandteil der Ausbildungen zu diesen Berufen wird und in die entsprechenden Studien- und Ausbildungsgänge integriert wird. Das gilt auch für Studiengänge wie Wirtschaftswissenschaften, in denen zukünftige Führungskräfte ausgebildet werden. Sie werden als Entscheider die für Privatheitsschutz notwendigen Ressourcen bereitstellen müssen und benötigen daher ein Verständnis für dieses Thema. Angesichts der rasanten Entwicklung der Internettechnologie sind auch entsprechende Weiterbildungen für Berufstätige notwendig. Die möglichen Inhalte solcher Weiterbildungen sind vielfältig. Eltern, Lehrerinnen und Lehrer, Erzieherinnen und Erzieher sollen nachvollziehen, wie Kinder und Jugendliche „im Netz leben" und welche besonderen Gruppendynamiken sich dort entwickeln. Gleichzeitig sollen sie lernen, dass die Privatheit der jungen Menschen auch dort gewährleistet sein muss („schnüffelt ihnen nicht nach"). In Weiterbildungen können die Lehrerinnen und Lehrer

zu Internet- und Privatheitsexperten ausgebildet werden. Kurse können die ethischen, rechtlichen und technischen Aspekte des Privatheitsschutzes vermitteln.

> Privatheitsschutz durch öffentliche Kampagnen vermitteln

In den letzten Jahren gab es öffentliche Aufklärungskampagnen zu verschiedenen Themen. Eine Kampagne des Bundesministeriums des Innern informierte zum Beispiel über den neuen elektronischen Personalausweis. Der „Safer Internet Day" ist ein Aktionstag der Europäischen Union für mehr Sicherheit im Web. Das gleiche Ziel verfolgt die Initiative „Deutschland sicher im Netz" von Unternehmen und Verbänden der Internetwirtschaft unter Schirmherrschaft des Bundesministeriums des Innern. acatech empfiehlt, solche Kampagnen auch für den Bereich der Privatheit im Internet zu konzipieren („das Internet ist nützlich, aber achte auf deine Privatheit"). Denkbar sind Kampagnen in den Medien (Rundfunk, Fernsehen, Presse, Kino), über Plakate sowie im Web selbst, also zum Beispiel in sozialen Netzwerken (virales Marketing). acatech schlägt vor, regelmäßig auch beste und schlechteste Praktiken im Bereich der Privatheit zu prämieren.

> Forschung zu Privatheitsvorstellungen und -praktiken ausbauen

Unübersehbar setzt die breite und alltägliche Nutzung des Internets bisherige Privatheitsvorstellungen unter Veränderungsdruck. Bislang ist jedoch noch kaum bekannt, an welchen Punkten mit welchen Veränderungen genau zu rechnen ist. Inwieweit die heutigen Vorstellungen und Praktiken der ersten Generation von „Digital Natives" vom bisherigen Umgang mit Privatheit abweichen und sich darüber hinaus auch dauerhaft als Trend in der Zukunft fortschreiben, kann derzeit kaum gesagt werden. Aus diesem Grund empfiehlt acatech, sowohl diachrone (sozialhistorische) als auch synchrone (gegenwartsbezogene) Forschungsanstrengungen auszubauen. Insbesondere hat sich in den letzten Jahren gezeigt, dass auf Nutzerbefragungen basierende quantitative Studien nur einen ersten Schritt bei der Erforschung der aktuellen Transformationen darstellen können. Eine Untersuchung der alltäglichen Privatheitspraktiken der Nutzerinnen und Nutzer im Internet wäre demgegenüber stärker zu fördern, um so noch konkretere Aussagen über etwaige, zukünftig entstehende Umgangsformen und Problemlagen treffen zu können. In dieser Hinsicht steckt die Forschung in Deutschland im Vergleich etwa zu den angelsächsischen Ländern noch in den Kinderschuhen.

Zudem liegt es in der Natur der Sache, dass Privatheitspraktiken, die gemeinsam mit dem und bezogen auf das Internet entstehen, eine starke technische Komponente aufweisen. Daraus ergeben sich zweierlei Folgen: Zum einen geht mit dem hohen Innovationstempo im Netz ein fast ebenso hohes Veränderungstempo internetbezogener Praktiken einher (einige Anwendungen sorgen erst seit wenigen Jahren für Furore, bringen aber unübersehbar großräumige Transformationsprozesse in Gang); dies macht die Erforschung solcher Praktiken zu einer erforderlichen Daueranstrengung. Zum anderen lassen sich zeitgenössische Sozialforschungen kaum noch sinnvoll durchführen, ohne technische Aspekte zu berücksichtigen. Das Erkenntnisinteresse richtet sich folglich auf Prozesse, deren Beschaffenheit und Konsequenzen ohne eine fest etablierte interdisziplinäre Forschungskultur kaum zu analysieren sind. Die Sozialwissenschaften haben hier von den Technikwissenschaften ebenso viel zu lernen wie umgekehrt. Nur ein Zusammenspiel in diesem Sinne kann es gewährleisten, das Verhältnis und die etwaigen Diskrepanzen zwischen allgemein verbreiteten Privatheitsvorstellungen, tatsächlichen Nutzungspraktiken und technischen Funktionsweisen des Internets zu durchdringen. Nicht zuletzt könnten auf diese Weise auch konkrete Nutzungsprobleme bei der Verwendung bestimmter Tools (Privacy Settings, PETs) sichtbar gemacht werden (Usability-Forschung).

Gleichermaßen besteht dringender Bedarf an gesicherten Erkenntnissen zum Einfluss von Bildungsmaßnahmen auf den Umgang mit Privatheit. An dieser Stelle wäre eine enge

Verzahnung der Medienpädagogik mit der sozialwissenschaftlichen Privatheitsforschung wünschenswert. Wie weiter oben dargestellt, spricht einiges für die systematische Integration der Vermittlung von Internetkompetenz in den schulischen Rahmen. Sinnvollerweise wird die Etablierung solcher Bildungsmaßnahmen von pädagogischen und sozialwissenschaftlichen Forschungsbemühungen begleitet, welche Auskunft über den Erfolg bestimmter Vermittlungsmethoden sowie über den Einfluss dieser Bemühungen auf die Privatheitspraktiken der Nutzerinnen und Nutzer geben.

5.2 RECHT

Die folgenden Vorschläge sollen das Vertrauen der Menschen im Internet stärken, indem sie ihnen einen bewussteren Umgang mit dem Web ermöglichen und dessen Vertrauenswürdigkeit erhöhen. Weil das Internet global ist, wäre dafür eine international gültige Rechtsordnung optimal. Diese Empfehlungen schlagen Eckpunkte für eine solche internationale Rechtsordnung vor. Sie orientieren sich am Entwurf der europäischen Datenschutzverordnung, enthalten aber auch für diese Modifikationen.

> Technische Umsetzung den Diensten überlassen

Alle Gesetze und Verordnungen sollen nur Ziele formulieren (zum Beispiel „Nutzer sollen die Möglichkeit haben, persönliche Daten zu löschen"). Die technische Umsetzung soll den einzelnen Diensten überlassen bleiben, um unnötige Einschränkungen des Dienstes zu minimieren. Mit Auditierungsverfahren kann überprüft werden, ob die Ziele wirklich erreicht werden.

> Privatheitsschutzrecht anwenden, das den Nutzerinnen und Nutzern vertraut ist

acatech empfiehlt, dass für Diensteanbieter das Privatheitsschutzrecht relevant ist, welches dort gültig ist, wo die Nutzerinnen und Nutzer des Dienstes ansässig sind. Das bedeutet zum Beispiel, dass in Europa der europäische Privatheitsschutz auch gewährleistet ist, wenn ein Dienst von einem Staat aus angeboten wird, in dem ein geringerer Privatheitsschutz herrscht. Die Nutzerinnen und Nutzer können darauf vertrauen, dass immer das Recht gilt, das sie kennen, und dass sie sich nicht mit vielen unterschiedlichen Rechtsordnungen auseinandersetzen müssen, wenn sie ihren Privatheitsschutz geltend machen wollen. Damit dies für die Anbieter realisierbar ist, soll das Privatheitsschutzrecht möglichst weiträumig harmonisiert werden und für den harmonisierten Bereich nur eine Behörde zuständig sein, wie das in Europa geplant ist.

> Einwilligung regulieren

Die Erhebung und Verwendung persönlicher Daten setzt im Allgemeinen das bewusste und freiwillige Einverständnis der Betroffenen voraus. Dies gilt besonders dann, wenn Nutzerprofile erstellt werden. Das Einverständnis soll so eingeholt werden, dass die Anwenderinnen und Anwender wissen, wozu sie ihr Einverständnis geben. Damit die Sorgeberechtigten Vertrauen in die Angebote an ihre Kinder gewinnen, sollen nur sie berechtigt sein, in die Verarbeitung der Daten ihrer Kinder einzuwilligen. Weil es im Einzelfall schwierig ist zu entscheiden, ob freiwilliges Einverständnis vorliegt, soll dies durch Regelbeispiele erläutert werden. Die Verarbeitung persönlicher Daten ohne Einwilligung soll nur erlaubt werden, wenn die damit verbundenen Risiken berücksichtigt und entsprechende Schutzmaßnahmen ergriffen werden, zum Beispiel durch Verschlüsselung.

> Transparenz schaffen und Kontrolle ermöglichen

Dienste sollen ihren Kundinnen und Kunden zeitnah und in verständlicher Form darstellen, welche persönlichen Daten sie speichern, was mit diesen Daten geschieht, an wen sie weitergegeben werden (besonders bei Weitergabe in Drittländer mit geringerem Datenschutzniveau), wie lange sie aufbewahrt werden etc. Nutzerinnen und Nutzer sollen die Möglichkeit haben, diese Daten zu korrigieren und zu löschen.

> Löschen ermöglichen

Über die aktive Löschung von persönlichen Daten hinaus sollen Dienste die Möglichkeit bieten, Fristen einzustellen, nach denen persönliche Daten, mindestens aber die von den Nutzerinnen und Nutzern selbst erzeugten, automatisch gelöscht werden. Ein generelles Recht auf Vergessen im Internet erscheint angesichts der gegenwärtigen technischen Möglichkeiten noch nicht realistisch.

> Migration unterstützen

Wer heute über einen längeren Zeitraum einen Internetdienst, zum Beispiel ein soziales Netzwerk oder eine E-Commerce-Plattform, verwendet, ist an diesen Dienst in hohem Maße gebunden, weil die Nutzung über einen längeren Zeitraum personalisiert wurde. In sozialen Netzwerken haben Anwenderinnen und Anwender Freundeskreise etabliert, Bilder hinterlegt, Informationen gepostet und so weiter. E-Commerce-Anbieter kennen die Vorlieben ihrer Kundinnen und Kunden und können auf dieser Grundlage ihr Angebot optimieren. Sie sollten ihnen die Möglichkeit bieten, zu einem anderen Anbieter zu wechseln und dabei ihren persönlichen Kontext mitzunehmen. Eine solche Migrationsmöglichkeit ist nicht nur für die Nutzerinnen und Nutzer wichtig, sondern auch im Interesse des Wettbewerbs zwischen den Anbietern. Gerade privatheitsfreundlichere Anbieter könnten Kundinnen und Kunden überzeugen, zu ihnen zu wechseln.

Die bis jetzt in diesem Abschnitt aufgeführten Empfehlungen dienen dazu, durch rechtliche Rahmenbedingungen sicherzustellen, dass Nutzerinnen und Nutzer sich ausreichend darüber informieren können, welche Konsequenzen die Nutzung eines Dienstes im Internet für ihre Privatheit haben kann, und ihnen die Möglichkeit gegeben wird, die Nutzung gemäß ihrer Präferenzen zu gestalten. Die nun folgenden Empfehlungen zielen darauf ab, die Vertrauenswürdigkeit des Internets, die zweite wichtige Bedingung für einen adäquaten Privatheitsschutz, zu erreichen.

> Datenschutzprinzipien beachten

Internetdienste sollen die zentralen Datenschutzprinzipien Zweckbindung, Datenminimierung, Datensicherheit und privatheitsschutzfreundliche Voreinstellungen beachten. Zweckbindung bedeutet, dass persönliche Daten (sowohl direkt erhobene als auch durch Verarbeitung gewonnene) nur zu Zwecken benutzt werden dürfen, denen die Nutzerinnen und Nutzer zugestimmt haben oder die durch andere Gesetze erlaubt sind. Datenminimierung verlangt, Dienste so zu gestalten, dass sie mit möglichst wenig persönlichen Daten auskommen. Dies kann zum Beispiel bedeuten, dass Dienste anonym oder unter Pseudonymen benutzt werden. Datensicherheit soll unter Verwendung moderner Technologie (zum Beispiel Verschlüsselung) realisiert werden. Privatheitsschutzfreundliche Voreinstellungen sollen gewährleisten, dass Dienste den Erwartungen der Nutzerinnen und Nutzer an den Umgang mit ihrer Privatheit auch dann entsprechen, wenn sie Privatheitsschutzeinstellungen nicht anpassen.

> Privatheitsschutz-Zertifizierung regeln

acatech empfiehlt, dass international oder wenigstens weitreichend geregelte und anerkannte Zertifikate und Prüfsiegel für Privatheitsschutz etabliert werden. Sie erlauben es, dass der Schutz der Privatheit zu einem Wettbewerbsvorteil werden kann. Solche Zertifikate und Prüfsiegel ermöglichen auch Diensteanbietern, die Aufgaben delegieren, zu prüfen, ob ihre Auftragnehmer hinreichenden Schutz der Privatheit gewährleisten. Das Recht soll hier nur einen Rahmen schaffen, der Qualität und Vergleichbarkeit garantiert. Die Ausgestaltung von Zertifizierung und Prüfsiegeln soll der Wirtschaft überlassen bleiben.

> Verhaltensanreize zur Selbstregulierung erforschen

Forschungsbedarf besteht vor allem bei der Frage, wie das Recht, das mit Ge- und Verboten sowie behördlicher Kontrolle arbeitet, durch Mechanismen ersetzt oder ergänzt werden kann, die auf andere Weise geeignete Verhaltensanreize zum Schutz der Privatheit setzen. So muss zum einen untersucht werden, wie Wettbewerb für den Privatheitsschutz genutzt

werden kann. Wie kann dieser zu einem Werbeargument und Wettbewerbsvorteil werden? Wie können die dafür erforderlichen verlässlichen Marktinformationen generiert und verbreitet werden? Zum anderen ist für den Privatheitsschutz bei Internetdiensten eine Allianz von Recht und Technik von zentraler Bedeutung. Sie muss sicherstellen, dass die Betroffenen ihre Privatheit selbst schützen können (Selbstdatenschutz) und dass diese durch den Internetdienst geschützt wird (Systemdatenschutz). Drittens ist zu untersuchen, welche Fragen den Diensteanbietern und ihrer Selbstregulierung überlassen werden können. Welche Rahmensetzung und welche Anreize sind notwendig, um zu gewährleisten, dass die Selbstregulierung rechtzeitig und zielgerecht erfolgt?

Darüber hinaus empfiehlt acatech, zu untersuchen, ob und wie die Einführung der sogenannten Gefährdungshaftung für Internetdienste zur Steigerung des Vertrauens im Internet beitragen kann. Gefährdungshaftung würde garantieren, dass Anbieter von Internetdiensten für Schäden haften müssen, die sie verursacht haben, unabhängig davon, ob sie die Schäden verschuldet haben. Entsprechend empfiehlt acatech zu untersuchen, ob und wie das Privatheitsschutzrecht auch auf die Verarbeitung von Daten zu privaten und persönlichen Zwecken ausgedehnt werden soll, weil heute für alle Internetnutzerinnen und -nutzer mächtige Datenverarbeitungswerkzeuge leicht verfügbar sind.

5.3 WIRTSCHAFT

Diejenigen, die Internetdienste anbieten, sei es mit wirtschaftlichem Interesse oder nicht, sollen zu einer Kultur der Privatheit im Internet beitragen, indem sie Transparenz schaffen, Kontrolle und Migration ermöglichen sowie die Datenschutzprinzipien beachten, wie im vorangegangenen Abschnitt dargestellt. Sie sollen dies unabhängig davon tun, ob dies vorgeschrieben ist oder nicht. Damit steigern sie das Vertrauen in ihren Dienst und verbessern dessen Marktchancen. Sie fördern so auch das Vertrauen im Internet insgesamt und unterstützen damit dessen Entwicklung zum Nutzen von Gesellschaft und Wirtschaft. Entsprechend der acatech Empfehlung sollen Vorschriften sich auf Zielsetzungen, Anreize, Kontrollen und Sanktionen beschränken und den Diensteanbietern ermöglichen, die für sie günstigen Umsetzungen zu wählen. Darüber hinaus empfiehlt acatech Folgendes:

> Mehr Privatheitsschutz zur Auswahl stellen

Gegenwärtig werden viele Internetdienste (zum Beispiel Suchmaschinen und soziale Netzwerke) mit den persönlichen Daten der Nutzerinnen und Nutzer „bezahlt". Die Anwenderinnen und Anwender haben dabei nur eingeschränkte Kontrolle über ihre Daten. acatech empfiehlt, kostenpflichtige Premium-Dienste anzubieten, die restriktiver mit den persönlichen Daten umgehen, also zum Beispiel solche Daten nicht für gezielte Werbung verwenden oder die Verwendung von Pseudonymen oder sogar anonyme Nutzung erlauben. Die Empfehlung richtet sich nicht nur an etablierte Dienstleister. Darüber hinaus sollten Start-ups, die solche Dienste anbieten, entsprechend gefördert werden. Je mehr Nutzerinnen und Nutzer ihre Privatheit schützen wollen, desto interessanter wird dieses Geschäftsmodell für die Diensteanbieter, insbesondere wenn aussagekräftige Privatheitssiegel und -zertifikate etabliert sind.

> Verwendung von Privacy-Agenten ermöglichen

acatech empfiehlt, dass Internetdienste Nutzerinnen und Nutzern die Möglichkeit geben, sich von sogenannten Privacy-Agenten unterstützen zu lassen. Privacy-Agenten sind zum Beispiel Programme, denen User einmalig ihre Präferenzen mitteilen (zum Beispiel „gib bei der Verwendung von Apps niemals meinen Aufenthaltsort preis"), und die diese danach automatisch umsetzen und nur bei wichtigen und kritischen Fragen die persönliche Aufmerksamkeit des Betroffenen beanspruchen. Das setzt voraus, dass relevante Informationen in einem Format bereitgestellt werden, das von Privacy-Agenten ausgewertet werden kann.

> Standards vereinbaren

Unabhängig von möglichen Regulierungen sollen Diensteanbieter selbst Standards vereinbaren, die es Privacy-Agenten erlauben, die Nutzerinnen und Nutzer bei der Gestaltung ihrer Privatheit zu unterstützen, und ihnen die Migration ihrer wesentlichen Daten von einem zu einem anderen Anbieter ermöglichen. Solche Standards sollen sich auch auf die Nutzerschnittstellen von Privacy-Agenten beziehen, damit Anwenderinnen und Anwender einfach ihre Privatheitspräferenzen realisieren können.

> Privatheitssiegel und -zertifikate entwickeln

Anbieter von Internetdiensten sollen gemeinsam unabhängige, qualitätsgesicherte Privatheitssiegel und -zertifikate etablieren und sich zu ihrer regelmäßigen Nutzung verpflichten. Eine regelmäßige, durch unabhängige Institutionen durchgeführte Qualitätsüberprüfung trägt zur Akzeptanz der Siegel und allgemein zum Vertrauensaufbau bei.

5.4 TECHNIK

Die obigen Empfehlungen lassen sich nur mit entsprechender technischer Unterstützung realisieren. Die notwendigen Techniken sind, wenn überhaupt, oft nur ansatzweise vorhanden. Die Weiterentwicklung der Technik erfordert in vielen Fällen erhebliche Forschungsanstrengungen.

> Internetdienste nach dem Prinzip „Privacy by Design" entwickeln und betreiben

Traditionell werden Dienste zunächst im Hinblick auf ihre Funktionalität entwickelt. Maßnahmen, die die Sicherheit und Privatheit des Dienstes gewährleisten, werden später ergriffen. Ein solches Vorgehen macht die Absicherung aufwendig – mit oft unbefriedigendem Resultat. Internetdienste sollten stattdessen nach dem Prinzip „Privacy by Design" entwickelt und in der Folge dann auch betrieben werden.

„Privacy by Design" beginnt mit einer Analyse und öffentlichen Diskussion, welchen Einfluss ein Dienst auf die Privatheit seiner Nutzerinnen und Nutzer hat. Eine solche Analyse erfordert die Definition, quantitative Bewertung und möglichst automatische Analyse von Sicherheit, Vertraulichkeit und Privatheit, insbesondere im Hinblick auf aggregierte und abgeleitete Daten. acatech empfiehlt, die Forschung nach entsprechenden technischen Hilfsmitteln (Checklisten, Erweiterungen von Entwicklungstools, automatisierte Tests etc.) und Referenzarchitekturen (Best Practices für bestimmte Anwendungsfälle) zu intensivieren, die Entwickler und Administratoren für eine effektive und kostengünstige Umsetzung von „Privacy by Design" brauchen.

> Informierte und bewusste Einwilligung unterstützen

Dienstleister dürfen im Allgemeinen die Daten ihrer Nutzerinnen und Nutzer nur mit deren Einwilligung erheben und verwenden, wie in Abschnitt 5.2 erläutert. Dieses Prinzip führt bereits heute zu zahlreichen technischen Herausforderungen, und die meisten davon sind noch nicht ausreichend erforscht und gelöst. acatech empfiehlt, besonders folgende Forschungs- und Entwicklungsfragen zu beantworten. Wie kann man die Einwilligung so gestalten, dass User sie tatsächlich bewusst geben und nicht blindlings einwilligen, um schnell den gewünschten Dienst zu erhalten, oder umgekehrt frustriert eine eigentlich gewollte Transaktion abbrechen? Wie kann man sicherstellen, dass zum Beispiel die Einwilligung von Kindern nur mit Zustimmung der Eltern erfolgt und Kinder auf für sie als ungeeignet erachtete Dienste keinen Zugriff haben? Wie kann die Einwilligung (oder deren Verweigerung) im Fall abgeleiteter Daten erfolgen, also von Daten, an deren Erhebung der oder die Betroffene überhaupt nicht direkt beteiligt ist?

> Vergessenwerden im Internet erforschen

Ein umfassendes „Vergessenwerden im Internet" ist wünschenswert. Dieses muss über das Löschen von solchen Primärdaten, die Dienste direkt von Nutzerinnen und

Nutzern sammeln, hinausgehen. Was „Vergessenwerden" bedeutet, ist aber weder genau verstanden noch kann es bis heute umfassend umgesetzt werden. acatech empfiehlt die Erforschung und Entwicklung von Methoden, die es ermöglichen, weitergegebene Daten und durch Auswertung gewonnene Informationen zu löschen, zum Beispiel mithilfe anbieterübergreifender Daten- und Sicherheitsmodelle („Sticky Policies": die Daten „wissen", wann sie gelöscht werden müssen). Solche Methoden dürften aufwendig und teuer sein. Darum sollten auch praktikable Bewertungsmethoden entwickelt werden, mit denen die Konsequenzen des Nichtlöschens beurteilt werden können. Zum Beispiel besteht kein Grund, tatsächlich anonymisierte Daten zu löschen. Oftmals gelingt es aber später doch, scheinbar anonymisierte Daten wieder Personen zuzuordnen.

> Nutzerfreundlichkeit sicherstellen

Technologien, die Privatheit schützen, werden häufig gar nicht oder nicht so eingesetzt, wie es zur Entfaltung ihrer vollen Wirksamkeit notwendig wäre. Ein Grund dafür ist, dass ihre Verwendung zu kompliziert ist und mit dem Bedürfnis kollidiert, einen Dienst auf möglichst einfache Art und Weise zu nutzen. acatech empfiehlt Forschungsanstrengungen im Bereich der Nutzbarkeit (Usability) von solchen Technologien. Dies umfasst die Untersuchung von Präferenzen von Internetteilnehmerinnen und -teilnehmern, sogenannte mentale Modelle, die zeigen, welche Reaktionen Dienste auslösen.

> Nutzungskompetenz und Gestaltungsmöglichkeiten unterstützen

Nutzungskompetenz der Anwenderinnen und Anwender setzt voraus, dass sie wissen, welche persönlichen Informationen über sie wo vorhanden sind und welche Konsequenzen das für ihre Privatheit hat. Auf der Grundlage dieses Wissens können sie Privatheitspräferenzen entwickeln und umsetzen. acatech empfiehlt die Weiterentwicklung von Werkzeugen (Privacy-Agenten), die Nutzerinnen und Nutzern zeigen, welche persönlichen Informationen ein bestimmter Dienst oder eine Gruppe von Diensten kennt (zum Beispiel alle sozialen Netzwerke, in denen sie aktiv sind), und was das angesichts ihrer Präferenzen für ihre Privatheit bedeutet. Dies ist nicht nur eine große analytische und technische Herausforderung, sondern solche Werkzeuge müssen auch nutzerfreundlich gestaltet werden, zum Beispiel durch nonverbale Informationen wie Ampeln oder Signale. Die Werkzeuge sollen die Anwenderinnen und Anwender auch bei Privatheitsentscheidungen unterstützen, wenn zum Beispiel ein Dienst Informationen über ihren Aufenthaltsort verwenden will.

acatech empfiehlt die Entwicklung von Standards in unterschiedlichen Bereichen. Regeln (Policies), die Anbieter bei der Verarbeitung von persönlichen Daten anwenden, sollen standardisiert werden. Solche standardisierten Regeln können zum einen für die Nutzerinnen und Nutzer leichter verständlich formuliert werden und erlauben zum anderen eine automatische Evaluation. Eine solche automatische Evaluation ist von besonderer Bedeutung, bevor Dienste auf andere Dienste zugreifen. Entsprechend sollen standardisierte Nutzerprofile für den Umgang mit Privatheit entwickelt und angeboten werden. Das erweitert die Gestaltungsmöglichkeiten der Anwenderinnen und Anwender und entbindet sie gleichzeitig von der Notwendigkeit, eigene Profile zu entwickeln. Sie können sich sicher sein, dass solche Profile das angestrebte Ziel erreichen. Standardisierte Nutzerprofile sollen durch Techniken ergänzt werden, die es ermöglichen, formulierte Präferenzen („diese Informationen bitte nicht weitergeben") in automatisch ausführbare Policies zu übersetzen. acatech empfiehlt drittens die Entwicklung von standardisierten Formaten, die die Migration von Nutzerprofilen von einem Dienst in einen anderen Dienst unterstützen. Dies erlaubt es Nutzerinnen und Nutzern, denjenigen Dienst zu wählen, der ihren Präferenzen im Hinblick auf Privatheit am meisten entspricht.

> Vertrauenswürdige Auditierung unterstützen

Für Anwenderinnen und Anwender ist nicht leicht erkennbar, ob ein Dienst ihre Privatheit respektiert. Hier können

Auditierung und entsprechende Zertifikate Abhilfe schaffen. acatech empfiehlt die Entwicklung standardisierter Prozesse, von Bewertungskriterien und Bewertungsverfahren für solche Auditierungen, die nicht nur einen Internetdienst selbst, sondern auch die beteiligten Drittanbieter einbeziehen, wie zum Beispiel die Entwickler von Apps, Werbetreibende, erweiterte Serviceanbieter wie Recommender oder Drittverkäufer bei E-Commerce. Auditierung und Zertifikate werden dadurch vergleichbar und aussagekräftiger. Der IT-Grundschutz und Common Criteria-Schutzprofile können als Vorbild dienen. In diesem Bereich ist die Weiterentwicklung von Softwaresystemen für die automatische Evaluation von besonderer Bedeutung. In Ergänzung zu Zertifikaten, die von unabhängigen Prüfeinrichtungen vergeben werden, sollen auch Empfehlungssysteme weiterentwickelt werden, die bereits aus dem Bereich E-Commerce bekannt sind. Auch sie sollen die Privatheitsfreundlichkeit von Internetdiensten bewerten. Schließlich empfiehlt acatech, Zertifizierungstechniken zu entwickeln, die Nutzerinnen und Nutzern gegenüber bezeugen können, dass Privatheitsagenten korrekt arbeiten.

> Data Mining-Verfahren für „Big Data"-Privacy erforschen

Im Internet werden riesige Datenmengen gespeichert (Big Data) und mit fortgeschrittenen Informatikmethoden (Data Mining) besonders für wirtschaftliche Zwecke analysiert (Business Intelligence). Die Fähigkeit zur Analyse großer Datenmengen hat Rückwirkungen auf die Privatheit. acatech empfiehlt, Methoden zu nutzen und weiterzuentwickeln, die Nutzerinnen und Nutzer über mögliche Privatheitsrisiken aufklären.

> Anonyme und pseudonyme Nutzung von Diensten ermöglichen

Für viele Internetdienste ist es wichtig, stabile Kundenbeziehungen aufzubauen und dazu Nutzerinnen und Nutzer wiederzuerkennen. Viele Dienste könnten aber auch anonym oder zumindest unter einem frei gewählten Pseudonym genutzt werden. Es genügt, wenn sie bestimmte Eigenschaften (sogenannte Attribute) eines Kunden gesichert verifizieren, zum Beispiel die Altersgruppe, den aktuellen Aufenthaltsort oder die Mitgliedschaft in einer bestimmten Gruppe. Eine umfangreichere Identifikation ist nicht notwendig. acatech empfiehlt deshalb der Wirtschaft, Dienste auch anonym oder mit Pseudonymen benutzen zu lassen. Die Umsetzung dieser Empfehlung erfordert besondere technische Lösungen. Es sind Systeme zu entwickeln, mit deren Hilfe Anwenderinnen und Anwender ihre eigenen Identitäten, Pseudonyme und Attribute selbst verwalten und deren Verwendung durch Internetdienste verfolgen können (Personal Identity Management). Entsprechend sollten auch Systeme entwickelt werden, mit deren Hilfe Internetdienste bestimmte Attribute verifizieren können, ohne dazu den Nutzer weiter gehend identifizieren zu müssen. Besondere Herausforderungen für die Forschung und Entwicklung stellen hierbei die Benutzerfreundlichkeit sowie die Verwendung mobiler und eingebetteter (cyber-physical) Endgeräte und die damit verbundenen Attribute dar.

> Grundlegende Methoden und Technologien weiterentwickeln

Wirkungsvoller Privatheitsschutz setzt voraus, dass die verwendeten grundlegenden Techniken hinreichend sicher sind. Das ist aber nicht garantiert. Verfahren, die heute sicher sind, können morgen unsicher sein. Außerdem erfordern die IT-Szenarien der Zukunft neue grundlegende Schutztechniken. acatech empfiehlt deshalb, dass Forschung und Entwicklung im Bereich der grundlegenden Technologien intensiv vorangetrieben werden. Ein wichtiger Bereich ist die Entwicklung kryptographischer Verfahren, die auch neuen Bedrohungen wie zum Beispiel Quantencomputern standhalten und die Ressourceneinschränkungen vieler moderner IT-Komponenten tolerieren. Ein weiteres Beispiel ist die Entwicklung von praktischen kryptographischen Protokollen, die die Privatheit unterstützen, wie etwa „Fully Homomorphic Encryption" und

„Secure Multiparty Computation", also Verfahren, die Berechnungen mit verschlüsselten Daten erlauben, ohne die Daten preiszugeben. Ein letztes Beispiel ist die Entwicklung von Methoden, die einerseits die Privatheit unterstützen, andererseits aber die Zurechenbarkeit von illegalen Handlungen erlauben.

acatech empfiehlt auch zu erforschen, wie Dualitäten wie privatheitsfreundlich/privatheitsunfreundlich oder sicher/unsicher differenziert als „hinreichend für einen bestimmten Kontext" bewertet werden können. Eine solche Differenzierung ermöglicht es, angemessene und wirtschaftlich vertretbare Lösungen zu finden.

6 DER NÄCHSTE SCHRITT

Die Arbeit in der interdisziplinären Projektgruppe hat sich als sehr fruchtbar erwiesen. Es ist den Vertreterinnen und Vertretern der beteiligten wissenschaftlichen Disziplinen und Unternehmen gelungen, auf der Grundlage ihrer intensiven Forschung und Diskussion gemeinsame Empfehlungen für die Etablierung einer Kultur der Privatheit im Internet zu formulieren. Diese Empfehlungen beruhen auf dem Verständnis von Privatheit im heutigen Internet und den Erwartungen für die überschaubare Zukunft. Gerade die Forschung muss aber auch auf Herausforderungen und Chancen eingehen, die jenseits der überschaubaren Zukunft liegen.

acatech empfiehlt daher, Szenarien zu entwerfen und zu erforschen, wie sich die Informationstechnologie, ihre Bedeutung in Gesellschaft und Wirtschaft und ihre Auswirkungen auf Privatheit und die grundlegenden Werte weiterentwickeln können. Dabei können auch zusätzliche Disziplinen, etwa die Psychologie, und weitere gesellschaftliche Gruppen einbezogen werden.

Bereits erwähnt wurden die deutlich erkennbaren und vorrangig durch IT getriebenen Trends zum Cloud und Mobile Computing und zu Embedded IT und Cyber-Physical Systems. Diese technologischen Entwicklungen beschleunigen bedeutende Trends in Gesellschaft und Wirtschaft wie die Verwandlung von Konsumenten in Produzenten von Informationen und Dienstleistungen, die Globalisierung der Arbeitswelt und das vermehrte Auftreten loser und dynamischer Arbeitsbeziehungen, verteilte Energieerzeugung und urbane Produktion, personalisierte und massiv IT-unterstützte Medizin. Gemeinsam ist diesen Trends, dass die IT in einem sehr wörtlichen Sinne immer näher an den Menschen heranrückt und damit der Schutz der Privatheit noch bedeutender wird.

Schreiten die gegenwärtigen Entwicklungen voran und wird immer mehr Privates öffentlich, oder wird sich eine Gegenbewegung bilden? Falls sich eine Gegenbewegung bildet, was könnte dies wiederum für die grundlegenden technischen Trends bedeuten?

Viele der im technischen Sinne wirkungsvollsten Maßnahmen zum Schutz der Privatheit setzen massive, nichtevolutionäre Änderungen an der existierenden IT-Infrastruktur voraus. Zum Beispiel setzt Ende-zu-Ende-Verschlüsselung im globalen Internet eine global vertrauenswürdige Infrastruktur (eine sogenannte PKI) voraus. Technische Lösungen dafür existieren, organisatorisch scheint das unmöglich zu sein. Wie müsste und könnte man aktuelle Entwicklungen – zum Beispiel den Umbau der produzierenden Industrie in Richtung „Industrie 4.0" – steuern, damit mehr Optionen für die Gestaltung und den Schutz der Privatheit entstehen?

Noch etwas fundamentaler gedacht: Kann man mit dem heutigen Internet überhaupt zu vertrauenswürdigen Lösungen kommen? Falls nein, wie könnte ein Netz aussehen, das Vertrauenswürdigkeit ermöglicht, und wie könnte man solche Erkenntnisse in aktuelle Entwicklungen einbringen?

LITERATUR

BGH 2013
Bundesgerichtshof (BGH): *Urteil vom 24.1.2013* (Az. III ZR 98/12), Karlsruhe 2013.

Buchmann 2012
Buchmann, J. (Hrsg.): *Internet Privacy – Eine multidisziplinäre Bestandsaufnahme/A multidisciplinary analysis* (acatech STUDIE), Heidelberg u.a.: Springer Verlag 2012.

Buchmann 2013
Buchmann, J. (Hrsg.): *Internet Privacy – Options for adequate realisation* (acatech STUDY), Heidelberg u.a.: Springer Verlag 2013.

Deloitte 2012
Deloitte: *Measuring Facebook's Impact in Europe. Executive Summary*, London 2012. URL: http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Industries/TMT/uk-tmt-media-facebook-europe-economic-impact-exec-summary.pdf [Stand: 04.02.2013].

DIVSI 2012
Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI): *DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet*, Hamburg 2012.

UN 2000
United Nations (UN): *United Nations Millenium Declaration*, September 2000. URL: http://www.un.org/millennium/declaration/ares552e.htm [Stand: 04.02.2013].

> BISHER SIND IN DER REIHE acatech POSITION UND IHRER VORGÄNGERIN acatech BEZIEHT POSITION FOLGENDE BÄNDE ERSCHIENEN:

acatech (Hrsg.): *Georessource Boden – Wirtschaftsfaktor und Ökosystemdienstleister. Empfehlungen für eine Bündelung der wissenschaftlichen Kompetenz im Boden- und Landmanagement* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2012.

acatech (Hrsg.): *Perspektiven der Biotechnologie-Kommunikation. Kontroversen – Randbedingungen – Formate* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2012. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Faszination Konstruktion – Berufsbild und Tätigkeitsfeld im Wandel. Empfehlungen zur Ausbildung qualifizierter Fachkräfte in Deutschland* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2012.

acatech (Hrsg.): *Anpassungsstrategien in der Klimapolitik* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2012.

acatech (Hrsg.): *Die Energiewende finanzierbar gestalten. Effiziente Ordnungspolitik für das Energiesystem der Zukunft* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2012. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Menschen und Güter bewegen. Integrative Entwicklung von Mobilität und Logistik für mehr Lebensqualität und Wohlstand* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2012.

acatech (Hrsg.): *Biotechnologische Energieumwandlung in Deutschland. Stand, Kontext, Perspektiven* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2012.

acatech (Hrsg.): *Mehr Innovationen für Deutschland. Wie Inkubatoren akademische Hightech-Ausgründungen besser fördern können* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2012. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Georessource Wasser – Herausforderung Globaler Wandel. Ansätze und Voraussetzungen für eine integrierte Wasserressourcenbewirtschaftung in Deutschland* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2012. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Future Energy Grid. Informations- und Kommunikationstechnologien für den Weg in ein nachhaltiges und wirtschaftliches Energiesystem* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2012. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Cyber-Physical Systems. Innovationsmotor für Mobilität, Gesundheit, Energie und Produktion* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2011. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Den Ausstieg aus der Kernkraft sicher gestalten. Warum Deutschland kerntechnische Kompetenz für Rückbau, Reaktorsicherheit, Endlagerung und Strahlenschutz braucht* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2011. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Smart Cities. Deutsche Hochtechnologie für die Stadt der Zukunft* (acatech bezieht Position, Nr. 10), Heidelberg u.a.: Springer Verlag 2011. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Akzeptanz von Technik und Infrastrukturen* (acatech bezieht Position, Nr. 9), Heidelberg u.a.: Springer Verlag 2011.

acatech (Hrsg.): *Nanoelektronik als künftige Schlüsseltechnologie der IKT in Deutschland* (acatech bezieht Position, Nr. 8), Heidelberg u.a.: Springer Verlag 2011.

acatech (Hrsg.): *Leitlinien für eine deutsche Raumfahrtpolitik* (acatech bezieht Position, Nr. 7), Heidelberg u.a.: Springer Verlag 2011.

acatech (Hrsg.): *Wie Deutschland zum Leitanbieter für Elektromobilität werden kann* (acatech bezieht Position, Nr. 6), Heidelberg u.a.: Springer Verlag 2010.

acatech (Hrsg.): *Intelligente Objekte – klein, vernetzt, sensitiv* (acatech bezieht Position, Nr. 5), Heidelberg u.a.: Springer Verlag 2009.

acatech (Hrsg.): *Strategie zur Förderung des Nachwuchses in Technik und Naturwissenschaft. Handlungsempfehlungen für die Gegenwart, Forschungsbedarf für die Zukunft* (acatech bezieht Position, Nr. 4), Heidelberg u.a.: Springer Verlag 2009. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Materialwissenschaft und Werkstofftechnik in Deutschland. Empfehlungen zu Profilbildung, Forschung und Lehre* (acatech bezieht Position, Nr. 3), Stuttgart: Fraunhofer IRB Verlag 2008. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Innovationskraft der Gesundheitstechnologien. Empfehlungen zur nachhaltigen Förderung von Innovationen in der Medizintechnik* (acatech bezieht Position, Nr. 2), Stuttgart: Fraunhofer IRB Verlag 2007.

acatech (Hrsg.): *RFID wird erwachsen. Deutschland sollte die Potenziale der elektronischen Identifikation nutzen* (acatech bezieht Position, Nr. 1), Stuttgart: Fraunhofer IRB Verlag 2006.

> acatech – DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

acatech vertritt die deutschen Technikwissenschaften im In- und Ausland in selbstbestimmter, unabhängiger und gemeinwohlorientierter Weise. Als Arbeitsakademie berät acatech Politik und Gesellschaft in technikwissenschaftlichen und technologiepolitischen Zukunftsfragen. Darüber hinaus hat es sich acatech zum Ziel gesetzt, den Wissenstransfer zwischen Wissenschaft und Wirtschaft zu unterstützen und den technikwissenschaftlichen Nachwuchs zu fördern. Zu den Mitgliedern der Akademie zählen herausragende Wissenschaftler aus Hochschulen, Forschungseinrichtungen und Unternehmen. acatech finanziert sich durch eine institutionelle Förderung von Bund und Ländern sowie durch Spenden und projektbezogene Drittmittel. Um den Diskurs über technischen Fortschritt in Deutschland zu fördern und das Potenzial zukunftsweisender Technologien für Wirtschaft und Gesellschaft darzustellen, veranstaltet acatech Symposien, Foren, Podiumsdiskussionen und Workshops. Mit Studien, Empfehlungen und Stellungnahmen wendet sich acatech an die Öffentlichkeit. acatech besteht aus drei Organen: Die Mitglieder der Akademie sind in der Mitgliederversammlung organisiert; das Präsidium, das von den Mitgliedern und Senatoren der Akademie bestimmt wird, lenkt die Arbeit; ein Senat mit namhaften Persönlichkeiten vor allem aus der Industrie, aus der Wissenschaft und aus der Politik berät acatech in Fragen der strategischen Ausrichtung und sorgt für den Austausch mit der Wirtschaft und anderen Wissenschaftsorganisationen in Deutschland. Die Geschäftsstelle von acatech befindet sich in München; zudem ist acatech mit einem Hauptstadtbüro in Berlin und einem Büro in Brüssel vertreten.

Weitere Informationen unter www.acatech.de