forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

Policy Paper

Das versteckte Internet

Empfehlungen an Wirtschaft und Politik

IMPRESSUM

Kontakt:
Peter Zoche
Koordinator Sicherheitsforschung und Technikfolgenabschätzung

Telefon +49 721 6809-152
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

www.isi.fraunhofer.de
www.forum-privatheit.de

Schriftenreihe:
Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt
ISSN-Print 2199-8906
ISSN-Internet 2199-8914

1. Auflage, Juni 2015

Das versteckte Internet – Herausforderungen für den Privatheitsschutz

Immer mehr alltägliche Geräte werden in Zukunft sowohl mit dem Internet verbunden sein als auch untereinander kommunizieren können. Infolge dieser Entwicklung wird auch die Menge der anfallenden Daten weiter zunehmen, was zahlreiche Privatheitsrisiken mit sich bringt.

Alltagsgegenstände erhalten zunehmend Datenverarbeitungs- und Kommunikationsfunktionen

Die Erweiterung von herkömmlichen Fernsehern, Autos und Brillen um internetbasierte Zusatzfunktionen, etwa die Kommunikation des Fernsehers mit Internetdiensten, fügt sich dermaßen unsichtbar in die Benutzung ein, dass den Nutzern kaum noch ersichtlich ist, wie viele Daten wo, wann und zu welchem Zweck erhoben, genutzt und wem diese persönlichen Informationen zugänglich gemacht werden. Hier äußert sich zunächst ein eklatanter Mangel an Transparenz, den das Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt mit dem White Paper „Das versteckte Internet" adressiert.

Zunehmende Komplexität und Erosion der Selbstbestimmung

Der kaum wahrnehmbaren Einführung internetbasierter Zusatzfunktionen folgt ihre Integration in zunehmend komplexer ausgestaltete Systeme. Diese Systeme wiederum vollziehen eine langsame, aber kontinuierliche Wandlung von Produkten hin zu Services. So gehören die in einem Smart Car anfallenden personenbezogenen Daten nicht uneingeschränkt dem Fahrzeughalter, sondern können in den Verantwortungsbereich der Fahrzeughersteller fallen, wodurch die Selbstbestimmung der Fahrzeughalter beeinträchtigt wird.

Eingriff in die Rechte von Nutzern

In anderen Fällen äußert sich die fehlende Selbstbestimmung in Form einer mangelnden Konfigurierbarkeit der Geräte, beispielsweise dem Zwang, ständig online sein zu müssen, um bestimmte Services nutzen zu können. Während einige der im Hintergrund stattfindenden Datenübertragungen für den Betrieb neuer Funktionalitäten notwendig sein können, stellen sie in vielen Fällen überflüssige Eingriffe in die Rechte der Nutzerinnen und Nutzer dar.

Suboptimale Lösungen

Die verwendeten Lösungen bleiben hinter den technischen Möglichkeiten und den geforderten Anforderungen des Privatheitsschutzes zurück. Auf Hersteller- bzw. Anbieterseite verweist dies – gerade in den Bereichen Fernsehen und Automobilität – auf das Fehlen einer Datenschutz-Kultur, die den datenschutzrelevanten Herausforderungen vernetzter Technologien und daraus resultierenden Erfordernissen gerecht wird.

Intransparente Datenmärkte

Hat eine beabsichtigte oder unbeabsichtigte Datenübertragung erst einmal stattgefunden, lässt sich kaum noch erschließen, was mit den personenbezogenen Daten geschieht.

Selbstschutz für Bürger fast unmöglich

In zunehmend komplexeren und weniger konfigurierbaren Systemen gestaltet sich auch die Realisierbarkeit von Selbstdatenschutzmaßnahmen, wie sie bei klassischen IT-Systemen zumindest in Ansätzen realisierbar sind, als noch schwieriger.

Diese Eingriffe wiederum haben Auswirkungen nicht nur auf die Privatheit der Nutzer selbst, sondern zunehmend auch auf die Privatheit anderer, sich in Sensornähe aufhaltender Menschen und ermöglichen sowohl die gezielte Ausspähung einzelner Nutzer als auch eine Massenausspähung aller Nutzer.

Handlungsoptionen

Systemgestaltung

Bereits heute existiert eine Reihe von Möglichkeiten, die Hersteller und Anbieter bei der Technikgestaltung berücksichtigen sollten:

Mehr Transparenz über Internetfunktionalitäten

■ Die Integration von Internetfunktionalitäten in bislang nicht vernetzte Geräte muss transparent erfolgen

Ziel der Hersteller und Anbieter sollte die Herstellung von Vertrauen sein, indem Datenübertragungen nicht ohne das Wissen der Nutzer im Hintergrund stattfinden. Dazu ist eine klare Kommunikation gegenüber Nutzerinnen und Nutzern darüber erforderlich, welche Daten wann, für wie lange und zu welchem Zweck gesammelt werden und welche diesbezüglichen Rechte die Betroffenen besitzen.

■ Das Datenschutz-Ziel der Transparenz bedarf einer Erweiterung durch weitere Datenschutzprinzipien

Die Schaffung von Transparenz darf nicht dazu führen, dass eine Verlagerung der Verantwortung in den Verantwortungsbereich der Einzelnen stattfindet oder Einzelne durch überbordende Informationsmengen und Entscheidungsmöglichkeiten überfordert werden.

Konsequente Nutzung von Privacy by Design …

■ Privacy by Design

Viele Datenschutzrisiken können vermieden oder minimiert werden, wenn proaktiv, also schon bei der Technikgestaltung, Maßnahmen mitgedacht und implementiert werden, die ein angemessenes Datenschutzniveau garantieren.

… und Privacy by Default

■ Privacy by Default

Eine sinnvolle Nutzung von Geräten und Anwendungen muss bereits in der datenschutzfreundlichen Grundeinstellung gewährleistet werden. Daten müssen zweckgebunden erhoben und eine über den spezifischen Zweck hinausgehende Erhebung vermieden werden.

■ Nutzern echte Entscheidungsmöglichkeiten anbieten

Kennzeichnung und Zertifizierung

- Viele Menschen erwarten nicht, dass ein Smart TV regelmäßig personenbeziehbare Daten über das Internet kommuniziert. Hinweise, die auf etwaige Datenübertragungen aufmerksam machen, müssen auf die Aufnahmefähigkeit und -bereitschaft der Nutzer abgestimmt werden. Schon beim Kauf eines Gerätes muss eine umfassende und allgemeine Information über die Funktionen des zu erwerbenden Gerätes erfolgen. Hilfreich und zugleich eine Herausforderung diesbezüglich ist die Einführung von einheitlichen, zertifizierten Kennzeichnungen (z.B. in Symbolform) in den Produktbeschreibungen, die darauf hinweisen, welche Art von Daten wofür gesammelt wird und welche Privatheitsrisiken damit verbunden sein können.

Datensparsame Wahlmöglichkeiten, Berichtigung und Löschung anbieten

- Ausgehend von der datenschutzfreundlichen Grundeinstellung sollten Nutzer selbst entscheiden können, welche der weiteren Funktionen, die über die Grundeinstellung hinausgehen und u. U. Privatheitsgefährdungen mit sich bringen, sie benutzen wollen. Ebenso wie die Möglichkeit der Nutzung zusätzlicher Funktionen auf Wunsch, muss Nutzern die Möglichkeit eingeräumt werden, zuvor erteilte Einwilligungen zurückzunehmen bzw. freigeschaltete Funktionen wieder zu deaktivieren.

- Darüber hinaus sollte Nutzern Berichtigung und Löschung auf einfache Weise ermöglicht werden.

Kontroll- und Eingriffsmöglichkeiten für Nutzer schaffen

- Hinweise, die auf Datenübertragungen aufmerksam machen, sollten nicht nur vorab, sondern, sofern dies im konkreten Fall erforderlich ist, auch während des Betriebs in Form situationsbezogener Informationen per visuellem oder akustischem Signal erfolgen und je nach Ausmaß der Datenübertragung auch eine erneute Einwilligung erforderlich machen.

Bildung und Aufklärung

Datenschutz als Bestandteil von Unternehmens- und Ingenieurkultur

- Herstellern und Anbietern, die vergleichsweise wenige Erfahrungen im Bereich datenverarbeitender Technologien mitbringen, ist empfohlen, ihr Selbstverständnis und ihre Geschäftsmodelle auf die Verträglichkeit mit Datenschutzprinzipien zu überdenken. Dies erfordert zunächst den entsprechenden Willen, darüber hinaus aber auch materielle Ressourcen und Zeit.
- Es ist nötig, Datenschutzthemen fest in die berufliche Aus- und Weiterbildung von Ingenieuren und Informatikern zu integrieren.

Regulierung

Darüber hinaus existieren auch Möglichkeiten der politisch-rechtlichen Regulierung:

Staatliche Gewährleistung des Rechts auf informationelle Selbstbestimmung

- Dem Staat kommt die Aufgabe zu, über die Ausgestaltung datenschutzfreundlicher Maßnahmen zu wachen. Dazu zählt insbesondere die Gewährleistung angemessener Schutzmaßnahmen und im Falle von Datenschutzverstößen die Einführung entsprechender Strafmaßnahmen, aber auch die Zurverfügungstellung geeigneter Selbstschutzmaßnahmen.

Rechtsrahmen bürgerfreundlich und zukunftsfest gestalten

- Insbesondere in den Kommissions- und EU-Parlamentsentwürfen der momentan verhandelten EU-Datenschutz-Grundverordnung sind die oben besprochenen Datenschutzprinzipien verankert: Data Protection by Design, Data Protection by Default, Zweckbindung, Einführung von Zertifizierungsverfahren und Gütesiegeln, Strafmaßnahmen bei Verstößen und Berichtigungs- sowie Löschungsansprüche.

Nach etwa dreieinhalb Jahren der Verhandlungen hat der EU-Ministerrat seine Verhandlungsposition veröffentlicht, die nun in den Trilog-Verhandlungen zwischen Rat, Kommission und Parlament beraten werden. Mit der EU-Datenschutz-Grundverordnung bietet sich die Möglichkeit, die Verwendung personenbezogener Daten nachhaltig zu regulieren. Diese Chance sollte insbesondere durch die deutsche Verhandlungsdelegation im Rat dazu genutzt werden, ein hohes Datenschutzniveau zu etablieren, indem Datenschutz nicht als Geschäftsrisiko, sondern in einer zunehmend durch Datenmissbrauch geprägten Umwelt vielmehr als Geschäftsvorteil hervorgehoben wird.

Regulierungsbedarf bei internetbasierten Technologien

- Die schon jetzt auf den Markt gebrachten internetbasierten Services und Produkte in wichtigen Bereichen wie Straßenverkehr, Stromversorgung etc. schaffen Pfadabhängigkeiten, welche eine spätere Regulierung immer schwieriger machen. Deshalb besteht schon heute Handlungsbedarf.

Ein verantwortungsbewusster Umgang mit modernen Technologien kann dann gelingen, wenn sich der Staat seiner Schutzpflichten bewusst ist, wirtschaftliche Akteure ihren Gestaltungsspielraum zur Herstellung sicherer Technologien gewissenhaft nutzen, und Nutzerinnen und Nutzer ihr Bewusstsein im Umgang mit ihren Daten schärfen.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft
UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT HOHENHEIM
LEHRSTUHL FÜR MEDIENPSYCHOLOGIE

EBERHARD KARLS UNIVERSITÄT TÜBINGEN
INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein