

Antrag

der Abgeordneten Ulrich Kelber, Elvira Drobinski-Weiß, Willi Brase, Petra Crone, Petra Ernstberger, Iris Gleicke, Gabriele Groneberg, Astrid Klug, Ute Kumpf, Thomas Oppermann, Holger Ortel, Heinz Paula, Dr. Wilhelm Priesmeier, Mechthild Rawert, Kerstin Tack, Dr. Frank-Walter Steinmeier und der Fraktion der SPD

Die digitale Welt verbraucherfreundlich gestalten

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

1. Die Digitalisierung bringt Veränderungen für Verbraucherinnen und Verbraucher mit sich, die Eingang in die weitere verbraucherpolitische Diskussion finden müssen. Das Internet globalisiert Verbraucherverhalten. Der Markt ist vielfältiger, aber auch unüberschaubarer und intransparenter, die rechtlichen und technischen Hintergründe sowie der Konsumalltag sind komplexer geworden. Viele Verbraucherinnen und Verbraucher finden sich im Tarifdschungel und im Kleingedruckten nicht zurecht.

Einerseits gilt es die technischen Errungenschaften zu nutzen, andererseits müssen die Interessen der Verbraucherinnen und Verbraucher gewahrt werden. Die Schutzwürdigkeit von Verbraucherinnen und Verbrauchern muss unter zwei Maßgaben besondere Beachtung finden:

- Verbraucherinnen und Verbraucher, die über vernetzte Endgeräte interagieren, haben kein persönliches Gegenüber, dessen Aktionen und Reaktionen sie einschätzen und bewerten können.
- Das Kenntnisniveau und die Umgangserfahrung mit neuen Medien sind unter Verbraucherinnen und Verbrauchern unterschiedlich ausgeprägt. Das jeweilige Schutzniveau muss so angesiedelt sein, dass es alle Verbraucherinnen und Verbraucher erfasst.

Moderne Verbraucherpolitik muss sich in der digitalen wie auch in der analogen Welt an den tatsächlichen Bedürfnissen der Verbraucherinnen und Verbraucher orientieren. Aktuelle empirische Studien zum Verbraucherverhalten, Gutachten und Stellungnahmen des Wissenschaftlichen Beirats Verbraucher- und Ernährungspolitik beim Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV) sowie aktuelle Arbeiten und Positionen des Europäischen Parlaments zum Thema „vulnerable consumers“ bieten eine gute Grundlage für ein modernes Verbraucherleitbild, nach dem es „die“ Verbraucherinnen und Verbraucher oder „den“ Entscheidungstyp nicht gibt. Jede Verbraucherin und jeder Verbraucher hat besondere Kenntnisse. Während eine Verbraucherin Ernährungsexpertin ist, ist ein anderer Verbraucher Computerspezialist.

Der Deutsche Bundestag geht daher von einem differenzierten Verbraucherleitbild aus, wonach sich Verbraucherinnen und Verbraucher grob in drei Kategorien einordnen lassen:

- den „verletzlichen“ Verbraucher, der mit der Angebotsvielfalt und -unübersichtlichkeit überfordert ist,
- den „vertrauenden“ Verbraucher, der aus verschiedensten Gründen (z. B. Zeitmangel, Bequemlichkeit o. Ä.) auf die Sicherheit der Produkte und die Seriosität des Angebots vertraut, sowie
- den „verantwortungsvollen“ Verbraucher, der sich vor einer Entscheidung informiert und bewusst auswählt.

Um den verschiedenen Verbrauchertypen gerecht zu werden, muss es Ziel der Marktgestaltung werden, dass gesunder Menschenverstand ausreichend ist, um bewusste Entscheidungen zu treffen. Verbraucherbezogene Forschung ist hierfür unerlässlich.

2. Informationspflichten sind aus verbraucherpolitischer Perspektive nur dann sinnvoll, wenn die Informationen auch so gestaltet sind, dass sie einen Mehrwert für Verbraucherinnen und Verbraucher bieten. Der Nutzen für die Verbraucherinnen und Verbraucher wird derzeit nicht ausreichend evaluiert. Verbraucherinnen und Verbraucher sollen die richtige Information zum richtigen Zeitpunkt in einer für sie verständlichen Weise erhalten. Sie muss verfügbar sein, wenn sie wirklich benötigt wird und auch im Kontext der digitalen Welt – so beispielsweise bei der Darstellungsform auf mobilen Endgeräten mit ihren vergleichsweise kleinen Displays – zweckdienlich sein.
3. Ob die digitale Gesellschaft eine offene, demokratische, kreative, verbraucherfreundliche sowie eine innovative und wirtschaftlich erfolgreiche sein kann, entscheidet sich nicht zuletzt daran, ob es gelingt, das Internet offen und diskriminierungsfrei zu halten. Grundlage hierfür ist, dass alle Bürgerinnen und Bürger, alle Verbraucherinnen und Verbraucher Zugang zu schnellem Internet haben sowie eine gesetzlich verankerte Netzneutralität. Der gleichberechtigte Transport von Daten und der diskriminierungsfreie Zugang zum Netz und zu dessen Inhalten sind für optimale Teilhabe und niedrige Marktzugangsschwellen konstitutiv. Die Diskriminierungsfreiheit der Infrastrukturen und Inhalte bilden die Grundlage für ein freies und innovationsfreundliches Internet.
4. Aufgabe moderner Verbraucherpolitik ist es, die Grundrechte der Verbraucherinnen und Verbraucher, insbesondere das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, auch in der digitalen Gesellschaft zu wahren. Jeder muss auch in der digitalen Welt das Recht haben, selbst zu entscheiden, was er wann mit seinen personenbezogenen Daten macht und wie diese Daten verarbeitet werden. Das Grundrecht auf informationelle Selbstbestimmung muss zur Geltung kommen. Auch das immer mehr an Bedeutung gewinnende Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – das IT-Grundrecht – dient dem Persönlichkeitsschutz der Verbraucherinnen und Verbraucher. Maßnahmen des Datenschutzes und der Datensicherheit sind besonders wichtige Mittel und ergänzen sich gegenseitig, um den Schutz dieser Grundrechte zu gewährleisten. Hohe Datenschutzstandards sind mehr denn je notwendig, insbesondere weil Verbraucherinnen und Verbraucher immer mehr digitale Technik nutzen und somit immer mehr digitale Spuren hinterlassen, aber auf Grund der immer komplexeren Systeme meist nicht in der Lage sind, ausreichende Selbstschutzmaßnahmen zu ergreifen. Hohe Datenschutz- und Datensicherheitsstandards schaffen das nötige abstrakte Vertrauen in diese Techniken und ermöglichen erst dadurch allen Verbraucherinnen und Ver-

brauchern unabhängig von den eigenen Kenntnissen und Fähigkeiten einen unbefangenen Umgang mit den neuen Techniken und Möglichkeiten. Hohe Datenschutz- und Datensicherheitsstandards tragen auf diese Weise auch dazu bei, dass alle Verbraucherinnen und Verbraucher unabhängig von ihren technischen Kenntnissen an den neuen Entwicklungen teilhaben können.

5. Die Anforderungen an einen wirksamen Datenschutz haben sich durch die zunehmende Nutzung digitaler Techniken verändert. Datenschutz – und somit der Schutz der informationellen Selbstbestimmung der Verbraucherinnen und Verbraucher – lässt sich nicht mehr allein dadurch gewährleisten, dass auf problematische Sachverhalte im Einzelfall gesetzgeberisch reagiert wird. Es sind nicht mehr nur Datenhandel, die Datensammelwut des Staates oder einzelner Unternehmen, illegale Geschäftspraktiken oder in einzelnen Techniken liegende funktionale Besonderheiten, die die Souveränität der Verbraucherinnen und Verbraucher über ihre Daten gefährden. Aus der rasanten Entwicklung neuer Techniken, der Globalisierung von Datenverarbeitung und der Vernetzung sämtlicher Lebensbereiche sowie der Verknüpfung von Alltagsgegenständen mit dem Internet ergeben sich vielmehr auch strukturelle Risiken für die Grundrechte der Betroffenen. Diese Entwicklung wird in den kommenden Jahren zunehmen.

Profilbildung – das Erfassen von Verhalten und Persönlichkeitsmerkmalen zur Berechnung von Vorlieben oder Wahrscheinlichkeiten – ist in vielen Bereichen der digitalisierten Gesellschaft bereits Realität. Auf Profilbildung basierende Dienste können nützliche Helfer im Alltag sein und Verbraucherinnen und Verbraucher mit gewünschten Informationen versorgen. Auf der anderen Seite werden personenbezogene Daten in einem Umfang und in einer Vielfalt gesammelt und ausgewertet, die nicht von allen Verbraucherinnen und Verbrauchern gewollte Einblicke in wesentliche Teile der Lebensgestaltung oder gar aussagekräftige Bilder der Persönlichkeit ermöglichen. Neben einer verbesserten Aufklärung der Verbraucherinnen und Verbraucher über die Notwendigkeit und die Möglichkeiten des Selbstdatenschutzes, bedarf es allgemeingültiger Regelungen, unter welchen Voraussetzungen Profilbildung erlaubt sein soll.

Neue Trends, wie die unter dem Stichwort „Big Data“ bekannten Technologien zur Verknüpfung und Auswertung unstrukturierter Datenmengen aus verschiedensten Quellen – teils in Echtzeit –, stellen den Datenschutz vor Herausforderungen. Big-Data-Technologien bieten Chancen. Sie können etwa im Gesundheitsbereich, der Energieversorgung oder in der Verkehrsplanung wertvolle Erkenntnisse liefern. Es gilt, den gesellschaftlichen Nutzen der Datenverarbeitung von Big-Data-Technologien mit dem Prinzip der informationellen Selbstbestimmung zu vereinen. Datenschutz ist ein grundlegendes Freiheitsrecht. Jede und jeder muss selbst entscheiden können, wie mit ihren/seinen Daten umgegangen wird. Daher kommt dem Datenschutz durch Technik eine grundlegende Bedeutung zu: Anonymisierung und Pseudonymisierung können einen wichtigen Beitrag dazu leisten, Datenanalysen mit den Zielen und den hohen Anforderungen des Datenschutzes vereinbar zu machen. Diese Vereinbarkeit ergibt sich allerdings nicht von alleine – sie muss aktiv politisch gestaltet werden. Vor diesem Hintergrund müssen klare gesetzliche Regelungen bereits beim Erheben von personenbezogenen Daten ansetzen und nicht erst bei deren Nutzung.

Es muss sichergestellt werden, dass der unbestreitbare Nutzen, den z. B. Big-Data-Anwendungen für die Gesellschaft bringen können, nicht zu gläsernen Verbraucherinnen und Verbrauchern führt. Der anonymen Gestaltung von auf Profilbildung basierenden Geschäftsmodellen und der Förderung entsprechender Techniken kommt dabei besondere Bedeutung zu. Anonymisierung und Pseudonymisierung können aber nur dort greifen, wo auf Grund der er-

hobenen und verknüpften Daten ein „single out“, also die eindeutige Identifizierung einer einzelnen Person, nicht möglich ist.

Eröffnen Verbraucherinnen und Verbraucher beispielsweise einen Account bei einem sozialen Netzwerk oder nehmen sie ein neu erworbenes Smartphone in Betrieb, so müssen sie sich durch teils sehr umständliche und breit gefächerte Einstellungsebenen kämpfen, bis sie überhaupt wissen, welche Daten öffentlich zugänglich sind, ob Daten in der Cloud gespeichert werden oder welche Dienste auf die GPS-Funktion oder das Adressbuch ihres Telefons zugreifen. Die Voreinstellungen sind hier in der Regel eben so datenschutzunfreundlich wie undurchsichtig. Damit Verbraucherinnen und Verbraucher bei der Nutzung neuer Techniken oder Dienste zu jeder Zeit volle Kontrolle darüber haben, welche Daten erhoben, verarbeitet oder veröffentlicht werden, muss der Grundsatz „Privacy by default“ gesetzlich verankert werden. Damit wären alle Dienste oder Endgeräte verpflichtend, so datenschutzfreundlich wie möglich voreinzustellen. Es muss den Verbraucherinnen und Verbrauchern überlassen bleiben, und durch einfache bzw. plakative Benutzerführung auch faktisch möglich sein, Apps oder Diensten den Zugriff auf einzelne Daten zu gewähren oder einzelne Daten zur Speicherung in der Cloud freizugeben.

Ebenso ist bei der Entwicklung einer neuen Technik ein präventiver Ansatz erforderlich. Router, intelligente Stromzähler oder Smartphones aber auch Dienstleistungen im Internet wie Suchmaschinen führen zu massenweiser Verarbeitung personenbezogener Daten. Es ist weder zielführend noch ökonomisch sinnvoll, wenn Datenschutzprobleme erst bei der Verwendung beobachtet werden und durch nachträgliche Änderungen oder Nachrüstungen auf diese reagiert wird. Zum einen hat die persönlichkeitsrelevante Datenverarbeitung dann bereits stattgefunden, zum anderen können nachträgliche Korrekturen sehr zeit- und kostenintensiv sein. Nützlich ist ein Konzept, das bereits bei der Herstellung von Endgeräten oder der Programmierung von Anwendungen ansetzt und den Datenschutz über den gesamten Lebenszyklus einer Technologie hinweg – von der Herstellung über die Nutzung bis hin zur Entsorgung – von vornherein mitdenkt. Der Grundsatz „Privacy by Design“ muss gesetzlich geregelt werden.

In der digitalen Welt werden zunehmend unterschiedliche Dienste miteinander verknüpft. Gleichzeitig geht der Trend zu integrierten Systemen, bei den Hardware, Software und Dienste zu einheitlichen integrierten Systemen verbunden werden, die gegenüber Konkurrenzprodukten abgeschottet und inkompatibel sind. Apple hat mit einem solchen geschlossenen System den Anfang gemacht. Zurzeit wird an der Marktreife weiterer, mit bestimmter Hardware und Geräten verknüpfter integrierter Dienstleistungen gearbeitet. Als Beispiel seien „connected car“ oder „connected home“ bzw. „smart home“ genannt. Der Ausbau von Clouddiensten und die Einführung von IPv6 werden diese Entwicklung weiter beschleunigen. Hat der Benutzer sich in diesen Diensten „eingerichtet“, so geht beim Wechsel des Anbieters, des Geräte- oder Fahrzeugherstellers eventuell ein mehr oder weniger großer Teil seiner Daten und damit „Lebenseinrichtung“ verloren. Es entstünde eine Art „digitale Leibeigenschaft“. Darum ist es nicht nur aus Gründen des Verbraucherschutzes, sondern auch zur Aufrechterhaltung des Wettbewerbs und der Wettbewerbsgleichheit, notwendig, das Recht auf Transportabilität eigener Daten gesetzlich zu verankern und einheitliche Standards für den Datenaustausch und den Ex- und Import von Daten zu definieren.

6. Finanztransaktionen finden immer häufiger über digitale Infrastrukturen statt. Dies nicht nur im Bereich des Onlinebanking und der Onlinebezahl-dienste, sondern auch beim alltäglichen Einkaufen im Geschäft. Wenn Verbraucherinnen und Verbraucher an der Kasse mit ihrer Kreditkarte oder per

Lastschriftinzugsverfahren bezahlen, finden internetbasierte Datenverarbeitungen statt. Erste Techniken des mobilen Bezahls via Smartphone stecken bereits in den Startlöchern. Sowohl Internetzahlungsdienste als auch Techniken für mobiles Bezahlen müssen so gestaltet werden, dass Verbraucherinnen und Verbraucher keine Angst vor Betrug im Zahlungsverkehr oder Missbrauch ihrer Zahlungsdaten haben müssen. Der Erfolg von Online- und Mobile-Payment-Diensten hängt entscheidend vom Vertrauen der Verbraucherinnen und Verbraucher in die neuen Techniken und Möglichkeiten ab.

Bei der Nutzung von Onlinebanking und Onlinebezahlssystemen müssen Verbraucherinnen und Verbraucher darauf vertrauen können, dass sie und ihr Vermögen vor unberechtigtem Zugriff geschützt sind. Bevor eine Zahlung online veranlasst werden kann, muss durch starke Authentifizierungsmechanismen die Berechtigung des Nutzers oder der Nutzerin sichergestellt sein.

Derzeit geht der Trend im Internet dahin, dass sowohl Händler als auch Verbraucherinnen und Verbraucher beim selben Zahlungsdienstleister angemeldet sein müssen. Dies führt nicht nur dazu, dass Verbraucherinnen und Verbraucher gezwungen werden, ihre Kontodaten bei etlichen Diensten zu hinterlegen und Händler über etliche dieser Dienste Zahlungen abzuwickeln, es schränkt zudem auch den Wettbewerb unter den Zahlungsdienstleistern ein. Verbraucherinnen und Verbraucher sollten ihren Zahlungsdienstleister frei wählen können. Wenn sie sich bei einer Vielzahl von Zahlungsdienstleistern registrieren müssten, geht ihnen der notwendige Überblick über erfolgte Transaktionen und ggf. auch missbräuchliche Abbuchungen abhandeln. Neue Onlinebezahlformen sollten daher auf standardisierten Verfahren aufsetzen, so dass Verbraucherinnen und Verbraucher ggf. einen anderen Zahlungsdienstleister als den des Händlers nutzen können. Nur durch eine freie Wahl des Zahlungsdienstleisters kann dauerhaft ein funktionierender Preis- und Leistungswettbewerb ermöglicht werden.

Auch Mobiltelefone sind fast ständig online erreichbar und dadurch besonders angreifbar. Sicherheitssoftware hat sich, anders als beim PC, noch nicht durchgesetzt. So kann Schad- oder Spionagesoftware beispielsweise über Apps oder Updates anderer Anwendungen in das Smartphone gelangen. Auch wird es durch die immer mehr werdenden Anwendungen, die zu Marketingzwecken Zugriff auf Daten verlangen, angreifbar. Alle Bezahlformen des Online und Mobile Payments erfordern daher Sicherheitssysteme auf hohem Niveau unter Gewährleistung der Nutzbarkeit. Anbieter sollten IT-Sicherheit stärker in den Produkten implementieren. Dies kann über gesetzliche Anreize wie beispielsweise durch Produkthaftungsregelungen oder eine Beweislastregelung befördert werden.

7. Die digitale Welt zeichnet sich dadurch aus, dass der technologische Fortschritt ständig neue Marktsegmente und -teilnehmer hervorbringt. Zudem bietet der digitale Markt im Vergleich zu anderen Märkten viele scheinbar „kostenfreie“ Angebote, was ihn deutlich von anderen Märkten unterscheidet. Verbraucherinnen und Verbraucher haben es schwer, seriöse von unseriösen Angeboten zu unterscheiden. Analoge Strukturen und Zuständigkeiten verhindern in der Regel sowohl eine umfassende zivilgesellschaftliche Marktbeobachtung wie auch staatliche Marktmissbrauchsaufsicht. Wir brauchen daher einen Marktwächter in der digitalen Welt, der die Marktstrukturen beobachtet, Beschwerden von Verbraucherinnen und Verbrauchern sammelt und systematisch auswertet, Missstände an die zuständigen Aufsichtsbehörden meldet und im Zweifel auch die Rechte der Verbraucherinnen und Verbraucher durchsetzt. Darüber hinaus soll er in der Verbraucherbildung aktiv sein. Der Marktwächter digitale Welt soll nicht nur konkrete Beschwerden aufnehmen, bündeln und überprüfen, ob eine systematische Benachteiligung der Verbraucherinnen und Verbraucher vorliegt, sondern auch allgemeine

Geschäftsbedingungen sowie Verbraucherschützende Vorschriften (bspw. Button-Lösung) im Onlinehandel kontrollieren. Die Überwachung der datenschutzrechtlichen Vorschriften sowie des Umgangs mit Daten im digitalen Bereich von der Onlineplattform bis hin zu Praktiken in Ladengeschäften bspw. mit RFID Chips, gehören ebenso zu seinen Aufgaben. Er sammelt Verbraucherbeschwerden und wertet diese systematisch aus.

8. Unter dem Motto „Vergüten statt verbieten“ vereinen sich die im digitalen Zeitalter scheinbar gegensätzlichen Notwendigkeiten. Auch im digitalen Zeitalter muss den Kultur- und Kreativschaffenden aus der Verwertung geistigen Eigentums eine angemessene Vergütung erwachsen. Auf der anderen Seite muss die reale Nutzung des Netzes zur legalen Nutzung werden. Hierzu müssen moderne – für Urheberinnen und Urheber sowie Nutzerinnen und Nutzer gleichermaßen attraktive – Onlineangebote und Geschäftsmodelle für das Internet etabliert und der Trend zur Nutzung legaler Onlineangebote unterstützt werden. Eine Kulturflattrate lehnt die Fraktion der SPD ab.

Es bedarf neuer Geschäftsmodelle und Vermarktungsstrategien, die sowohl die Rechte der Urheberinnen und Urheber wahren als auch die digitalen Realitäten und Gewohnheiten der Verbraucherinnen und Verbraucher berücksichtigen. Die derzeitige Situation, in der Verbraucherinnen und Verbraucher auf Grund veränderter gesellschaftlicher Rahmenbedingungen mit dem Urheberrecht in Konflikt geraten, ist genauso wenig haltbar, wie daraus resultierende Einnahmeverluste der Urheberinnen und Urheber. Diese neuen Geschäftsmodelle und Vermarktungsstrategien sollen sowohl den Urheberinnen und Urhebern und Verwerterinnen und Verwertern von Rechten dienen als auch zugleich eine einfache und verbraucherfreundliche legale Nutzung geschützter Inhalte ermöglichen, was auch den Nutzerinnen und Nutzern die nötige Rechtssicherheit bietet. Die Entwicklung legaler kommerzieller Geschäftsmodelle sollte daher unterstützt und vorangetrieben werden.

Aus Sicht der Verbraucherinnen und Verbraucher bleibt unklar, warum digitale Werkexemplare im Gegensatz zu Datenträgern nicht weiterverkauft werden dürfen. Der Europäische Gerichtshof hat 2012 in einem Vorabentscheidungsverfahren (Az.: C-128/11) entschieden, dass Softwarehersteller den Weiterverkauf „gebrauchter“ Lizenzen nicht untersagen dürfen, wenn der Käufer diese per Download erworben hat und ihm dabei ein zeitlich unbegrenztes Nutzungsrecht eingeräumt wurde. Körperliche Kopien auf CDs und ähnlichen Datenträgern seien insofern aus dem Internet heruntergeladenen Programmkopien gleichzustellen. Allerdings müsse der Erwerber beim Weiterverkauf die Kopie von seinem eigenen Rechner löschen. Es ist zu prüfen, ob und inwiefern die Grundsätze dieser Entscheidung zu UsedSoft auch auf den Bereich des Handels mit digitalen Mediengütern (beispielsweise Filme, Musik, eBooks) übertragen werden können.

Die Regelungen zur Privatkopie haben sich im Grundsatz bewährt. Sie tragen erheblich zum Rechtsfrieden bei, auch wenn die Rechtsanwendung in der Praxis kompliziert ist. Eine weitere Beschränkung der Zulässigkeit der Privatkopie wäre kontraproduktiv und ist in der Praxis nicht durchsetzbar. Sie darf auch – im Rahmen des rechtlich Erlaubten – nicht durch Nutzungsbedingungen und Lizenzvereinbarungen eingeschränkt werden.

Ein weiteres drängendes Handlungsfeld ist die massenhafte Abmahnung von Privaten auf Grund von Urheberrechtsverstößen im Internet. Familien werden mit überzogenen Gebühren von durchschnittlich 700 bis 800 Euro, mitunter auch deutlich darüber, belastet, wenn ein Kind einen Song ins Internet gestellt hat oder ein Dritter über einen vermeintlich nicht ausreichend gesicherten Internetanschluss unbefugt Dateien hochgeladen hat. Aus der Abmahnung gegenüber Privaten darf kein „Geschäft“ werden. Deshalb müssen

die Abmahnkosten bei Urheberrechtsverstößen im privaten Bereich wirksam begrenzt werden.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. verbraucherbezogene Forschung zu stärken und auszubauen, mit dem Ziel, anhand von validen Erkenntnissen – etwa der Verhaltensökonomie oder zu Marktstrukturen – durch verbraucherpolitische Maßnahmen den Markt so zu gestalten, dass auch verletzte und vertrauende Verbraucherinnen und Verbraucher nicht benachteiligt oder überfordert werden;
2. ein Verbraucherpanel als jährliche und repräsentative Verbrauchererhebung einzurichten;
3. einen Verbrauchercheck im Rahmen von Gesetzgebungsverfahren einzuführen, bei dem die Auswirkungen von gesetzlichen Regelungen auf Verbraucherinnen und Verbraucher in der analogen wie auch digitalen Welt beleuchtet werden;
4. Maßnahmen zur Verbesserung der Qualität von Verbraucherinformationen zu ergreifen. Insbesondere sollen
 - a) die notwendigen und wesentlichen Informationen – aber auch die erforderlichen rechtsverbindlichen Einwilligungserklärungen – dem genutzten Medium angemessen gestaltet und verständlich sein;
 - b) Verbraucherinformationen dahingehend geprüft werden, ob eine Information für den angestrebten Zweck das richtige Mittel ist bzw. ob es sich um einen Bereich handelt, in dem eine Information den Verbraucherinnen und Verbrauchern die Wahlfreiheit erleichtert und somit einen Mehrwert bietet oder eher um einen Bereich, in dem Verbraucherinnen und Verbraucher schutzbedürftig sind und daher andere Instrumente zielführender wären;
 - c) Verbraucherinformationen dahingehend geprüft werden, ob sie verfügbar sind, wenn sie wirklich benötigt werden;
 - d) Verbraucherinformationen dahingehend geprüft werden, ob sie für die unterschiedlichen Verbrauchergruppen verständlich sind;
5. ein Recht auf schnelles Internet für alle über eine Universaldienstverpflichtung gesetzlich abzusichern;
6. Netzneutralität gesetzlich zu verankern;
7. in den Verhandlungen im Europäischen Rat über eine Europäische Datenschutz-Grundverordnung hohe Datenschutzstandards durchzusetzen, damit die Persönlichkeitsrechte der Verbraucherinnen und Verbraucher gewahrt bleiben, insbesondere (zur Datenschutz-Grundverordnung siehe auch Antrag der Fraktion der SPD auf Bundestagsdrucksache 17/11144),
 - das so genannte Marktortprinzip zu verankern, damit bei der Verarbeitung von Daten europäischer Verbraucherinnen und Verbraucher auch europäisches Datenschutzrecht gilt;
 - am Verbot mit Erlaubnisvorbehalt und am Einwilligungsvorbehalt festzuhalten und begleitend Möglichkeiten zu entwickeln, die Einwilligung im Hinblick auf die digitale Welt für datenverarbeitende Stellen und Verbraucherinnen und Verbraucher gleichermaßen praktikabler zu machen;
 - die Begriffe Profiling, Anonymisierung, Pseudonymisierung sowie Datenübertragung zu definieren;

- Datenschutz durch Technik und damit die Möglichkeiten der Anonymisierung und Pseudonymisierung zu fördern, mit dem Ziel, das Erheben von personenbezogenen Daten soweit möglich von vornherein zu vermeiden bzw. zu begrenzen;
 - die Zielvorgaben des Datenschutzes – Datensparsamkeit, Datenvermeidung und die Zweckbindung jeglichen Umgangs mit Daten – stärker zur Geltung zu bringen;
 - mit den Grundsätzen „Privacy by default“ und „Privacy by Design“ einen präventiven Ansatz des Datenschutzes zu etablieren;
 - Regelungen zu Profilbildung zu etablieren, die bereits bei der Erhebung der Daten ansetzen und die Souveränität der Betroffenen über ihre Daten berücksichtigen;
 - den rechtlichen Rahmen zu setzen, damit gut ausgestattete, starke und unabhängige Aufsichtsbehörden eine konsistente Anwendung des Datenschutzrechts in ganz Europa gewährleisten können;
 - durch spürbar hohe Strafen und Bußgelder finanzielle Anreize zu setzen, wirksame Datenschutz- und Datensicherheitsstandards in Unternehmen zu implementieren;
 - ein Recht auf Datentransportabilität festzuschreiben, das in keiner Hinsicht eingeschränkt werden darf, und Regelungen zur Definition von einheitlichen Standards dafür zu treffen;
8. standardisierte Verfahren für Onlinebezahlmodelle zu fördern, so dass Verbraucherinnen und Verbraucher den Zahlungsdienstleister frei wählen können und so dauerhaft ein funktionierender Preis- und Leistungswettbewerb ermöglicht wird;
 9. einen Marktwächter digitale Welt bei den Verbraucherzentralen und ihrem Bundesverband einzurichten, der die Marktstrukturen beobachtet, Beschwerden von Verbraucherinnen und Verbrauchern sammelt und systematisch auswertet, Missstände an die zuständigen Aufsichtsbehörden meldet und im Zweifel auch die Rechte der Verbraucherinnen und Verbraucher durchsetzt;
 10. im Zuge der Einführung eines Marktwächters digitale Welt die Klarstellung im Unterlassungsklagegesetz (UKlaG) vorzunehmen, dass Datenschutzvorschriften, soweit sie Verbraucherrechte betreffen, Verbraucherschutzgesetze im Sinne des UKlaG sind;
 11. zu prüfen, wie der Weiterverkauf von digitalen Gütern rechtlich ermöglicht werden kann;
 12. die Möglichkeit von Privatkopien auch in der digitalen Welt zu erhalten;
 13. massenhafte Abmahnungen von Urheberrechtsverletzungen durch Private einzudämmen, in dem eine Streitwertobergrenze mit klar gefasstem Anwendungsbereich eingeführt wird – insbesondere sind Ausnahmetatbestände mit unbestimmten Rechtsbegriffen abzulehnen. Auch der „fliegenden Gerichtsstands“ bei Urheberrechtsverstößen im Internet muss eingeschränkt werden.

Berlin, den 11. Juni 2013

Dr. Frank-Walter Steinmeier und Fraktion