

Unterausschuss Neue Medien (22)
Wortprotokoll *
2. Sitzung

Berlin, den 07.06.2010, 13:00 Uhr
Sitzungsort: Paul-Löbe-Haus
Konrad-Adenauer-Str. 1
10557 Berlin
Sitzungssaal: 4.400

Vorsitz: Sebastian Blumenthal, MdB

TAGESORDNUNG:

Vor Eintritt in die Tagesordnung S. 4

Tagesordnungspunkt 1 S. 7

Informationsgespräch mit Sachverständigen
Aktuelle Fragestellungen im Zusammenhang mit Sozialen Netzwerken

Dr. Clemens Riedl, Geschäftsführender Vorstand, VZ net, Netzwerke Ltd., Berlin
Dr. Alexander Dix, Berliner Beauftragter für Datenschutz und Informationsfreiheit

Tagesordnungspunkt 2a S. 24

Bericht gem. § 56a GO-BT des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung

Technikfolgenabschätzung (TA)
Zukunftsreport - Ubiquitäres Computing

BT-Drucksache 17/405

Peter Zoche (Fraunhofer-Institut für System- und Innovationsforschung)

* Redaktionell überarbeitete Bandabschrift

Tagesordnungspunkt 2b **S. 32**

Unterrichtung durch die Bundesregierung

Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie

BT-Drucksache 16/7891

Tagesordnungspunkt 3a **abgesetzt**

Gesetzentwurf der Abgeordneten Jörn Wunderlich, Dr. Petra Sitte, Agnes Alpers, weiterer Abgeordneter und der Fraktion DIE LINKE.

Entwurf eines Gesetzes zur Aufhebung von Zugangsbeschränkungen in Kommunikationsnetzen

BT-Drucksache 17/646

Tagesordnungspunkt 3b **abgesetzt**

Gesetzentwurf der Abgeordneten Dr. Konstantin von Notz, Volker Beck (Köln), Birgitt Bender, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Gesetzes zur Aufhebung des Gesetzes zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen und Änderung weiterer Gesetze

BT-Drucksache 17/772

Tagesordnungspunkt 3c **abgesetzt**

Gesetzentwurf der SPD

Entwurf eines Gesetzes zur Aufhebung des Gesetzes zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen

BT-Drucksache 17/776

Tagesordnungspunkt 4 **abgesetzt**

Antrag der Abgeordneten Dr. Konstantin von Notz, Wolfgang Wieland, Jerzy Montag, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Keine Vorratsdatenspeicherungen über den Umweg Europa

BT-Drucksache 17/1168

Tagesordnungspunkt 5 **S. 32**

Verschiedenes

Anwesenheitsliste*

Mitglieder des Ausschusses

Ordentliche Mitglieder des Ausschusses

Stellv. Mitglieder des Ausschusses

CDU/CSU

Brandl, Reinhard, Dr.
Jarzombek, Thomas
Schipanski, Tankred
Selle, Johannes
Wanderwitz, Marco

Bär, Dorothee

SPD

Klingbeil, Lars
Zypries, Brigitte

FDP

Blumenthal, Sebastian
Schulz, Jimmy

DIE LINKE.

Behrens, Herbert
Sitte, Petra, Dr.

BÜNDNIS 90/DIE GRÜNEN

Rößner, Tabea

Notz, Konstantin von, Dr.

*) Der Urschrift des Protokolls ist die Liste der Unterschriften beigegefügt.

Bundesregierung

Bleek
Heinrich
Engers

BMWi
BFDi
BMJ

Bundesrat

Georgi
Denove
Dombrowski

LV Sachsen-Anhalt
LV Bayern
LV Berlin

Fraktionen und Gruppen

Gießmann
Sobolewski
Scheele
Dobeneck
Leberl
Göllnitz
Kollbeck
Richter
Sauer

B90/GRÜNE
B90/GRÜNE
DIE LINKE.
B90/GRÜNE
CDU/CSU
FDP
SPD
FDP
FDP

Vor Eintritt in die Tagesordnung

Vorsitzender: Ich bitte Sie, die Plätze einzunehmen. Liebe Kolleginnen und Kollegen, sehr geehrte Damen und Herren, liebe Gäste und Besucher, ich eröffne hiermit die zweite Sitzung des Unterausschusses Neue Medien. In Bezug auf die Tagesordnung der heutigen Sitzung gilt es zunächst, eine Abstimmung vorzunehmen, da es unter den Obleuten zuvor darüber keine Einigung gab. Es gibt den Wunsch der Oppositionsfraktionen, das hier noch einmal zu thematisieren. Bevor wir aber zu den Formalitäten kommen, möchte ich die Gelegenheit nutzen, zwei erfreuliche Ereignisse zu verkünden. Ich möchte im Namen des Kollegiums ganz herzlich nachträglich zum Geburtstag gratulieren, einmal dem Kollegen Behrens von der Fraktion DIE LINKE. und Herrn Jarzombek, CDU/CSU-Fraktion. Dann noch ein weiterer Punkt zu dem Thema Formalia. Da es heute eine öffentliche Sitzung ist und wir externe Gäste haben, bitte ich darum, die Hausordnung des Deutschen Bundestages zu berücksichtigen. Demnach soll von spontanen Beifalls- bzw. Missfallensbekundungen Abstand genommen und sollen weder Transparente noch irgendwelche Hilfsmittel hier eingesetzt werden. Aber ich denke, die Themen, die wir heute hier haben, sind derart interessant und spannend, dass man einfach auch einmal konzentriert zuhören kann.

Abg. Tabea Rößner (BÜNDNIS 90/DIE GRÜNEN): Es geht mir darum, dass Sie zu Anfang gesagt hatten, dass es um eine Abstimmung bzw. um einen Tagesordnungspunkt gehe. Es geht aber um zwei, die wir auch beide getrennt voneinander abstimmen möchten.

Vorsitzender: Das ist richtig. Ich habe den Vorgang als solchen, dass über die Tagesordnung abgestimmt wird, in der Singularform benutzt. Im Detail sind es zwei Tagesordnungspunkte, die auch getrennt voneinander aufgerufen werden. Es geht zunächst um den Tagesordnungspunkt 3a in Verbindung mit 3b und 3c der vorläufigen Tagesordnung für die heutige Sitzung. Hier gab es das Mehrheitsvotum aus der Besprechung der Obleute, den gesamten Tagesordnungspunkt abzusetzen. Und das gleiche betrifft den Tagesordnungspunkt 4. Auch hier gab es aus der Obleuterunde das Mehrheitsvotum der Koalitionsfraktionen, diesen Tagesordnungspunkt ebenfalls heute nicht zu behandeln, sondern ggf. zu einem späteren Zeitpunkt wieder aufzurufen. Ich bitte um Wortmeldungen, weil insbesondere die Oppositionsfraktionen signalisiert haben, das auf jeden Fall noch einmal thematisieren zu wollen.

Abg. Herbert Behrens (DIE LINKE.): Gerade dieser Punkt war in unserer ersten Obleutebesprechung ein wichtiges Thema, auf das sich alle Fraktionen verständigt hatten. Und darum ist es auch unser Wunsch, sich zügig mit dem Thema auseinanderzusetzen. Dieses Einvernehmen hat sich nun aufgelöst. Unserer Auffassung nach ist es formalistisch, darauf zu verweisen, es sei vom federführenden Ausschuss noch kein Votum angefordert, andere Ausschüsse hätten die Beratung zurückgestellt und würden sich ebenfalls noch nicht damit befassen. Ich finde, der Unterausschuss sollte so autonom in seiner Arbeit sein, sich unter Umständen mit bestimmten Fragen etwas intensiver auseinanderzusetzen, als das in der Regel im Ausschuss der Fall ist. Vor diesem Hintergrund hatten

wir in der Obleutebesprechung dafür plädiert, es bei der Tagesordnung zu belassen, wie sie von den Obleuten in der letzten Besprechung vereinbart worden war. Also, unser Votum ginge auf jeden Fall in diese Richtung.

Vorsitzender: Als Nächster Herr Kollege Konstantin von Notz, bitte.

Abg. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Ich kann mich dem anschließen. Wir finden es ausgesprochen ärgerlich, dass jetzt selbst bis in die Unterausschüsse die sozusagen unliebsamen Themen von der Tagesordnung verschwinden sollen. Ich vermute, dass einige, die an solchen Beschlüssen mitwirken und dafür die Hand heben, bei anderen Anlässen wie z. B. Podiumsdiskussionen sagen, wie dringend es erforderlich sei, sich zu den Themen auszutauschen und darüber zu beraten. Insofern habe ich überhaupt kein Verständnis dafür, dass sowohl das Thema Aufhebung von Zugangsbeschränkungen in Kommunikationsnetzen als auch das Thema Vorratsdatenspeicherung von der Tagesordnung genommen werden soll und das in einem Unterausschuss. Was bereits in einem normalen Ausschuss zu beanstanden wäre, wird noch befremdlicher, wenn es in einem Unterausschuss stattfindet, wo eigentlich eine etwas offenere und auch etwas großzügigere Diskussion zum Selbstverständnis gehören sollte. Insofern appelliere ich dringend, zumal wenn gerade diesem Unterausschuss ein Liberaler vorsitzt, sich dieser Verweigerungshaltung nicht anzuschließen, sondern die Dinge hier offen zu diskutieren, denn in der Bevölkerung und überhaupt spielen sie eine große Rolle. Und da ist kein Platz für zeitliches Taktieren.

Vorsitzender: Als nächstes habe ich Lars Klingbeil auf der Rednerliste.

Abg. Lars Klingbeil (SPD): Ich unterstelle einmal, dass die Absetzung nichts mit Differenzen innerhalb der Koalitionsfraktionen zu tun hat, denn man arbeitet ja ansonsten auch wohl sehr harmonisch zusammen.

Auch meine Fraktion plädiert dringend dafür, die Themen zu beraten und keinesfalls mehr als die Hälfte der Beratungsgegenstände von der Tagesordnung abzusetzen. Wir haben – und das war eine Einigung bzw. ein gemeinsamer Wille aller Fraktionen – gemeinsam zum Ausdruck gebracht, wie wichtig uns dieser Unterausschuss ist und waren uns einig in der Einschätzung, dass Themen der Netzpolitik hier prominenter und intensiver behandelt werden sollten, als es ansonsten im Deutschen Bundestag der Fall ist. Das galt meiner Wahrnehmung nach insbesondere für das Thema Netzsperrern, das ein ganz zentraler Punkt der netzpolitischen Diskussion in den letzten Monaten und im letzten Jahr war. Und deshalb wäre es wichtig und richtig, diesen Punkt heute zu behandeln, die Gesetzentwürfe zu beraten und einen Sachstandsbericht der Bundesregierung darüber zu bekommen, zumal der Presse zu entnehmen war, dass der Entwurf eines Löschgesetzes schon fertiggestellt sei. Bereits im Februar dieses Jahres hat die SPD-Fraktion ihre Position zu dem Thema festgelegt und wartet seither auf eine Gelegenheit, angemessen darüber sprechen zu können. Es ist uns unverständlich, wieso das nicht gewünscht sein soll, wo doch diese Woche im Ausschuss für Familie, Senioren, Frauen und

Jugend ein Vertreter der Bundesregierung zu dem Thema sexuelle Misshandlung von Kindern Rede und Antwort stehen wird. Für uns ist nicht nachvollziehbar, weshalb der Tagesordnungspunkt hier heute abgesetzt werden soll, wenn er in anderen Ausschüssen beraten werden kann.

Vorsitzender: Marco Wanderwitz bitte, danach Jimmy Schulz.

Abg. Marco Wanderwitz (CDU/CSU): Es ist ja bereits erwähnt worden, dass wir zu den Tagesordnungspunkten 3a bis c die ursprünglich angeforderten Voten durch den federführenden Ausschuss explizit durch Absetzung nicht angefordert sehen. Darüber hinaus ist es in der Tat so, dass wir uns in den Koalitionsfraktionen eingehend beraten. Das tun wir regelmäßig mit allen Themen. Mehr würde ich da nicht hineininterpretieren.

Ich möchte noch kurz auf das Argument der Kollegen Behrens und von Notz, den Arbeitsauftrag der Unterausschüsse betreffend, eingehen. Ich sehe die Aufgabe der Unterausschüsse nicht darin, gezielt Themen aufzurufen, die in den Hauptausschüssen vertagt wurden.

Im Übrigen sehe ich es als ein völlig normales Verfahren nach unserer Geschäftsordnung an, das auch in jedem Ausschuss regelmäßig praktiziert wird, Dinge zu schieben, wenn Fraktionen, die nun einmal Mehrheitsfraktionen sind, den Bedarf dazu geltend machen. Deswegen beantrage ich noch einmal förmlich für die Koalitionsfraktionen, die Tagesordnungspunkte 3a, b und c sowie 4 zu vertagen.

Vorsitzender: Abg. Jimmy Schulz für die Fraktion der FDP, bitte.

Abg. Jimmy Schulz (FDP): Die Argumente haben wir ja gerade auch schon in der Obleuterunde ausführlich ausgetauscht. Deswegen plädiert auch meine Fraktion dafür, die Tagesordnungspunkte 3a, b und c sowie 4 zu verschieben.

Vorsitzender: Damit sind von allen Fraktionen die Argumente vorgetragen worden. Wir stimmen jetzt getrennt über die Absetzung des Tagesordnungspunktes 3a, b und c ab. Dort gab es den Antrag, diese von der heutigen Tagesordnung abzusetzen.

Der Unterausschuss beschließt mit der Mehrheit der Stimmen der Fraktionen der CDU/CSU und der FDP gegen die Stimmen der SPD-Fraktion, der Fraktion DIE LINKE. und der Fraktion BÜNDNIS 90/DIE GRÜNEN die Tagesordnungspunkte 3a, b und c abzusetzen.

Als Nächstes rufe ich auf den Tagesordnungspunkt 4 und möchte über den Antrag abstimmen lassen, diesen von der Tagesordnung abzusetzen.

Der Unterausschuss beschließt mit der Mehrheit der Stimmen der Fraktionen der CDU/CSU und der FDP gegen die Stimmen der SPD-Fraktion, der Fraktion DIE LINKE. und der Fraktion BÜNDNIS 90/DIE GRÜNEN Tagesordnungspunkt 4 abzusetzen.

Tagesordnungspunkt 1

Informationsgespräch mit Sachverständigen

Aktuelle Fragestellungen im Zusammenhang mit Sozialen Netzwerken

Vorsitzender: Wir treten nun ein in die Tagesordnung, die in den weiteren Punkten unstrittig gewesen ist und fahren mit dem Thema Datenschutz und Privatsphäre in sozialen Netzwerken fort. Dazu haben wir Sachverständige eingeladen. Zunächst kurz zum Verfahrensablauf. Es war Konsens eben in der Obleuterunde, dass die Sachverständigen jeweils Eingangsstatements von maximal 10 Minuten halten und danach die Fraktionen in der Reihenfolge der Größe Fragen stellen. Meine Bitte wäre, da wir uns zeitlich jetzt schon ein wenig im Verzug befinden, dass wir uns möglichst kurz fassen. Ich würde es begrüßen, wenn die Referenten die Vorgabe von maximal 10 Minuten auch nicht als maximal auslegen, da wir so ggf. ein paar Minuten einsparen können. Bevor wir in die Vorträge einsteigen, möchte ich es nicht versäumen, Ihnen unsere Gäste persönlich vorzustellen. Zum einen begrüßen wir Dr. Alexander Dix, Berliner Beauftragter für Datenschutz und Informationsfreiheit. Herzlich willkommen bei uns im Unterausschuss. Und von der VZnet-Gruppe, Dr. Clemens Riedl, Geschäftsführender Vorstand der VZnet Netzwerke Ltd., Berlin. Herzlich Willkommen. Sie haben noch zwei Kollegen aus Ihrem Unternehmen mitgebracht: Frau Jana Moser, Rechtsanwältin und Datenschutzbeauftragte sowie Herrn Philippe Gröschel, Jugendschutzbeauftragter bei VZnet Netzwerke. Herzlich willkommen auch Ihnen bei uns im Unterausschuss.

Zu Ihrer Information möchte ich darauf hinweisen, dass wir auch Facebook zu der heutigen Sitzung eingeladen haben. Facebook ist ja eines der Netzwerke, in deren Zusammenhang die strittige Diskussion in den vergangenen Wochen in der Öffentlichkeit geführt wurde. Die Anfrage ist zwar mit einem zeitlich zumutbaren Vorlauf auf der Arbeitsebene hier durch die Verwaltung des Deutschen Bundestages erfolgt, Facebook hat sich aber nicht in der Lage gesehen, eine sprachfähige Vertretung zu uns in den Unterausschuss zu entsenden. Ich möchte – das habe ich zuvor in der Obleuterunde als Konsenswunsch vernommen – gegenüber Facebook offiziell unser Befremden darüber zum Ausdruck bringen, dass man offenbar vereinzelt Termine hier in Berlin wahrnehmen kann, aber, wenn ein Gremium des Deutschen Bundestages zu einem Informationsgespräch bittet und eine Einladung ausspricht, trotz ausreichenden zeitlichen Vorlaufs, sich nicht in der Lage sieht, der Einladung zu folgen oder zumindest eine Stellungnahme abzugeben.

Nun beginnen wir mit den Vorträgen unserer Gäste und ich würde gerne Herrn Dr. Dix als erstem das Wort erteilen. Bitteschön, Herr Dr. Dix.

Dr. Alexander Dix (Berliner Beauftragter für Datenschutz und Informationsfreiheit): Vielen Dank, Herr Vorsitzender, für die Einladung, die ich gern angenommen habe. Ich möchte mich auf einige kurze grundsätzliche Bemerkungen beschränken, ohne zu sehr ins Detail zu gehen. Es ist allgemein bekannt, dass die sozialen Netzwerke rasant an Bedeutung gewinnen. Vielfach werden soziale Netzwerke – jedenfalls das größte soziale Netzwerk weltweit mit den größten Nutzerzahlen:

Facebook, ebenso wie Google – bereits als ein Teil der Infrastruktur des Internets angesehen. Zweifellos bieten soziale Netzwerke auch die Chance – ich betone bewusst: Chance – den Nutzern eine größere Kontrolle über ihre Daten zu geben, als dies der Fall wäre, wenn die Daten auf eigenen Webseiten im offenen Internet publiziert würden.

Einige Anbieter, und da muss ich Facebook an allererster Stelle nennen, nutzen diese Chance allerdings bisher nicht. Ich würde sogar so weit gehen, auch wenn das vielleicht sehr drastisch klingen mag, dass sie ihre Nutzer weitgehend entmündigen, also im Moment genau das Gegenteil von informationeller Selbstbestimmung umsetzen. Der Gründer des Unternehmens, Mark Zuckerberg – das ist ja durch die Medien gegangen – vertritt offenbar die Auffassung, dass die Privatsphäre gewissermaßen ein Auslaufmodell sei und das Unternehmen lediglich diesen sozialen Veränderungen Rechnung trage. Das ist nicht richtig, sondern das Unternehmen macht den Nutzern detaillierte Vorgaben. Ich habe aber den Eindruck, das Unternehmen lernt gerade aufgrund der Entwicklung in den vergangenen Wochen, dass dies eine Fehleinschätzung war. Die Konsequenzen, die daraus gezogen werden, halte ich allerdings immer noch für unzureichend. Meiner Ansicht nach haben Betreiber sozialer Netzwerke, und das gilt jetzt für alle – Facebook ist zwar das größte Unternehmen, der größte Spieler auf diesem Markt, aber keineswegs der einzige – zwei zentrale Aufgaben aus Datenschutzsicht. Erstens müssen sie ihre Plattformen sicher machen vor Angriffen von außen. Das war lange Zeit nicht der Fall. Facebook und auch deutsche Netze – auch die VZ-Netzwerke – haben in dem Bereich in der Vergangenheit Lehrgeld zahlen müssen. Es gibt immer noch Pannen in diesem Bereich, gerade auch bei Facebook. Ich betone, dass es wichtig ist zu unterscheiden, inwieweit sich Plattformen gegen Hackerangriffe, mithin kriminelle Angriffe von außen, schützen und inwieweit sie da Lücken aufweisen. Zum Zweiten – und das ist eigentlich die schwierigere Aufgabe – müssen die Plattformbetreiber ein Geschäftsmodell entwickeln, das sich am europäischen und deutschen Datenschutzrecht orientiert und mit diesem kompatibel ist. Insbesondere bei dem großen amerikanischen Netzwerk ist das jedenfalls bisher nicht der Fall.

Ich möchte kurz präzisieren, welche Anforderungen das im Wesentlichen sind. Erstens müssen die Grundeinstellungen für diese Plattformen von vornherein datenschutzfreundlich sein. Es muss dem Nutzer ein Kommunikationsdienst angeboten werden, bei dem von seinen hochgeladenen, teilweise sehr persönlichen Informationen, bis hin zu Fotos, zunächst einmal so wenig wie möglich plattformweit veröffentlicht wird. Der Nutzer sollte in einem ersten Schritt die Möglichkeit haben zu entscheiden, welche dieser Daten er welchen Teilnehmern bekanntgeben will.

Zum Zweiten muss eine pseudonyme Nutzung der Daten möglich sein und als Option angeboten werden. Das ist in Deutschland nach dem Telemediengesetz zwingend erforderlich. Soziale Netzwerke sind Plattformen und bieten Telemedien an. Folglich muss von ihnen die Möglichkeit einer pseudonymen Nutzung eröffnet werden. Auch wenn natürlich jeder Nutzer die Möglichkeit hat „nein“ zu sagen und auf der Plattform mit seinem wirklichen Namen erscheinen kann, muss er die faktische und rechtliche Möglichkeit haben, das anders zu handhaben. Möglicherweise auch, wenn er auf verschiedenen Plattformen tätig ist, was wir sogar empfehlen würden.

Drittens, und das ist ein grundsätzlicher Aspekt, der über das Rechtliche hinausgeht, bin ich der Meinung, dass die Anbieter von sozialen Netzwerken alles daran setzen müssen, um das Bewusstsein der Nutzer für Datenschutzmöglichkeiten zu schärfen. Sie bieten ja durchaus Einstellmöglichkeiten im Sinne des Datenschutzes an, so dass sie auch die Verantwortung wahrnehmen sollten, die Nutzer von Anfang an auf diese Möglichkeiten hinzuweisen. Ich würde sogar so weit gehen zu sagen, in der Vergangenheit haben viele soziale Netzwerke so etwas wie eine Illusion von Intimität erweckt. Sie haben nämlich den Eindruck erweckt, wer sich auf den Plattformen bewegt, findet alles schön kuschelig, bewegt sich nur unter Freunden, niemand sonst erfährt etwas. In Wirklichkeit aber besteht immer die technische Möglichkeit – ich betone: die technische Möglichkeit –, dass jeder Nutzer massenweise Daten aus diesen Netzwerken exportiert ins offene Internet.

Das ist in aller Regel durch die Nutzungsbedingungen zwar verboten, aber es ist technisch nicht auszuschließen. Und auf dieses Risiko müssen meiner Ansicht nach die Nutzer frühzeitig hingewiesen werden. Es gibt immer wieder Vorfälle, bei denen Nutzer im großen Umfang Profildaten maschinell einsammeln und exportieren. Das kann von Seiten der Plattformbetreiber erschwert werden, und das ist auch besser geworden in der letzten Zeit. Man hat zwar neue Techniken entwickelt, um das schwieriger zu machen, aber technisch lässt sich das immer noch nicht gänzlich unterbinden. Es handelt sich dabei auch um etwas völlig anderes, als das, was ich vorhin als Hackerangriffe von außen bezeichnet habe. Die Insidertätigkeit hier ist – wie auch in Unternehmen – sehr viel schwieriger zu kontrollieren als Angriffe von außen.

Mark Zuckerberg, der Gründer und Chef von Facebook, um ihn noch einmal zu zitieren, hat gerade kürzlich wieder betont, dass nach seiner Auffassung der Trend im Internet – und speziell auch bei solchen Communities – hin zur Personalisierung gehe. Das ist eine Feststellung, die auch andere schon getroffen haben; daran scheint mir prinzipiell nichts falsch zu sein. Etwas völlig anderes ist die Annahme – und der scheint Herr Zuckerberg immer noch anzuhängen – diese Personalisierung könne ggf. fremdbestimmt erfolgen. Personalisierung sollte immer nur selbstbestimmt erfolgen, indem jeder einzelne Nutzer die Möglichkeit hat zu entscheiden, welche seiner Daten für Werbezwecke genutzt werden dürfen und welche Werbung ihm zugespielt werden darf. Also auch soziale Netzwerke sollten dem Prinzip des Permission Marketing Rechnung tragen und nicht erst auf Widersprüche warten, die Werbung dann unmöglich machen. Die Grundeinstellung auch solcher Dienste sollte datenschutzfreundlich sein. Das haben die Datenschutzbeauftragten des Bundes und der Länder kürzlich in einem Eckpunktepapier für ein modernes Datenschutzrecht für Internetdienste gefordert. Das ist also keine Forderung, die sich auf die sozialen Plattformen beschränkt.

Wichtig ist aus meiner Sicht darüber hinaus, dass auch außereuropäische Anbieter wie Facebook anerkennen müssen, dass sie sich, wenn sie sich auf dem europäischen Markt bewegen und insbesondere Nutzer mit deutschsprachigen Angeboten ansprechen und ggf. auch auf Mittel der Datenverarbeitung im europäischen Raum zugreifen, an europäisches Datenschutzrecht halten müssen. Anderenfalls würden deutsche Anbieter in die missliche Situation kommen, dass sie gegenüber außereuropäischen Wettbewerbern im Nachteil wären, weil diese massive wirtschaftliche

Vorteile dadurch hätten, das deutsche Datenschutzrecht umgehen zu können. Es muss jetzt alles daran gesetzt werden, dass diese datenschutzrechtlichen Vorgaben einheitlich durchgesetzt werden. Facebook unterliegt nach unserer Auffassung eindeutig dem deutschen Datenschutzrecht genauso wie andere ausländische Anbieter in Deutschland. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist im Moment dabei, Maßnahmen gegen Facebook zu prüfen. Er ist wie ich der Auffassung, dass so manche Grundeinstellung auf Facebook selbst nach den neuesten Änderungen eindeutig unvereinbar ist mit deutschem Datenschutzrecht. Das haben auch die europäischen Datenschutzbeauftragten in einem Arbeitspapier zum Ausdruck gebracht und Facebook mitgeteilt, dass sie die Praxis von Facebook in Europa als rechtswidrig ansehen und Änderungen fordern.

Dr. Clemens Riedl (Geschäftsführender Vorstand, VZnet, Netzwerke Ltd., Berlin): Herzlichen Dank für die Einladung zum Informationsgespräch im Unterausschuss Neue Medien. Ich möchte erwähnen, dass wir in der Vergangenheit immer gut mit der Politik zusammengearbeitet haben. Hinweisen möchte ich in diesem Zusammenhang auf unser Programm zur Bundestagswahl 2009, in dessen Rahmen wir Millionen Leute aufgefordert haben, zur Wahl zu gehen. Wir haben dabei auch umfangreiche Aktionen gegen die Politikverdrossenheit unternommen. Erwähnen möchte ich auch die 512 Politikerprofile, die gegenwärtig in den VZ-Netzwerken mit vielen Tausenden von Anhängern vorzufinden sind; an der Spitze die Bundeskanzlerin mit über 70.000 Freunden. Meine Firma nimmt am IT-Gipfel und an den sonstigen Aktivitäten der Bundesregierung teil. Wir halten den Dialog zwischen der Wirtschaftspolitik und der IT-Industrie für zentral wichtig. Es ist ein Milliarden-Markt, von dem wir fürchten, dass er Deutschland verlorenght. Die Erfolge von sozialen Netzwerken in anderen Ländern, allen voran Facebook, und von Suchmaschinen wie Google haben sehr viel zu tun mit dem zweitgrößten Werbemarkt der Erde hier in der Bundesrepublik.

Gestatten Sie drei, vier erläuternde Punkte zu den VZ-Netzwerken. Wir haben 16,8 Millionen Bundesbürger auf unserer Plattform. Diese besteht aus SchülerVZ, StudiVZ und MeinVZ. Wir beschäftigen 300 Mitarbeiter in Berlin im Stadtteil Prenzlauer Berg und halten uns zu 100 Prozent an deutsches Recht.

Zu dem Thema Datenschutz bzw. Datensicherheit möchte ich sagen, dass wir absolut strengste Voreinstellungen präferieren, wie sie Dr. Dix eben angesprochen hat. Wir sprechen uns ganz klar gegen eine Auslesbarkeit von Profilen auf Suchmaschinen aus und haben deshalb eine Löschfunktion, mit der die Profile endgültig löscher sind. Bei uns werden auch Urheberrechte, wie zum Beispiel das Recht aufs eigene Bild, beachtet. Unser Geschäftsmodell haben wir in den letzten Jahren so verändert, dass wir auf keine Datenweitergabe an Dritte angewiesen sind. Das ist ganz entscheidend in dieser Industrie.

Zu allen weiteren Details würde ich gerne auf Frau Jana Moser, die für den Datenschutz unserer Angebote zuständig ist, verweisen. Zur Datensicherheit möchte ich erwähnen, dass wir einen sogenannten Alarmbutton implementiert haben, wie er von der Politik gefordert wurde. Wir

beschäftigen allein 130 Mitarbeiter, um in vielen Sprachen zu den unterschiedlichsten Themen Stellungen nehmen zu können, die unsere User bewegen. Ein solcher Service ist zwar teuer, uns aber sehr wichtig, weshalb wir an dieser Stelle gerne diesen Support bieten.

Wir gehen offensiv in die Öffentlichkeit, insbesondere auch an Schulen und betreiben sehr viel Nutzeraufklärung. Es gibt Telefonsprechstunden für Eltern und Lehrer, es werden Unterrichtsmaterialien vorgehalten, die auch herunterladbar sind. All das halten wir für einen pädagogisch sehr wichtigen Auftrag, den wir aufgrund unserer Größenordnung zu liefern haben.

Zum Thema Wettbewerb möchte ich sagen, dass wir es kritisch finden, dass deutsches Recht nicht auf internationale Mitbewerber angewendet wird, weil uns das in diesem Markt einen Wettbewerbsnachteil bereitet, der kaum zu kompensieren ist. Bei unseren ausländischen Mitbewerbern gibt es Dinge wie Adressbuchablage, den Aufbau von Schattennetzwerken zu weiteren Mitarbeitergenerierungen und ähnliches, millionenfach Tag für Tag. Es gibt keine Einwilligungen, nicht einmal geringste Häkchen haben User bei unseren Mitbewerbern zu setzen. All das macht es enorm schwierig für uns, in dem Markt zu bestehen. Uns ist auch klar, dass wir weder von Seiten der Öffentlich-Rechtlichen noch der Politik eine Erleichterung bzw. ein Entgegenkommen zu erwarten haben. Wir sehen es jeden Tag, dass ARD und ZDF den privaten, internationalen, amerikanischen Internetkonzernen die Nutzer nur so zutreiben. Auch sind die meisten deutschen Politiker sehr aktiv auf Facebook und werben insofern für diese Plattform.

Zum Thema Regulierung ist zu sagen, dass weitere Gesetze es für die wenigen verbleibenden deutschen Mitspieler in diesem globalen Markt nur erschweren würden, weiter zu bestehen. Es gibt zu wenige Anwendungen auf Seiten der amerikanischen Mitbewerber, so dass sie nur deutsche Betreiber treffen würden. Wir hoffen vielmehr auf die internationale Durchsetzbarkeit deutschen Datenschutzrechts, damit wir gleiche Rahmenbedingungen für die deutschen Nutzer schaffen.

Als Fazit möchte ich zusammenfassen, dass wir immer Ansprechpartner der deutschen Politik bleiben werden. Unsere Gesellschafter haben sich mehrmals dagegen ausgesprochen, den Firmensitz in ein anderes Land zu verlegen, wo es ggf. für uns ganz andere Möglichkeiten geben würde. Wir halten den Datenschutz und den Jugendschutz für sehr wichtig und werden immer 100 Prozent konform mit deutschem Recht sein. Ich betone aber noch einmal: Wir halten es nicht für richtig, neue Gesetze zu schaffen, sondern vielmehr bestehende durchzusetzen für alle Marktteilnehmer, insbesondere dort, wo 90 Prozent der deutschen User unterwegs sind, nämlich auf amerikanischen Plattformen. Vielen Dank.

Vorsitzender: Vielen Dank, Herr Dr. Riedl. Das wären dann die Eingangsstatements und Kurzvorträge. Ich würde dann eintreten in die Fragerunde, beginnend mit der Fraktion CDU/CSU.

Abg. Marco Wanderwitz (CDU/CSU): Zunächst vielen Dank auch von meiner Seite für die Stellungnahmen. Insbesondere Ihnen Herr Dr. Riedl, für die deutliche Aussprache mancher Dinge, so

wie Sie sie bewerten. Das hilft uns weiter. Ich hätte eine Nachfrage zum Stichwort Werbung. Werbekunden sind ja sehr wichtig zur Finanzierung einer Plattform. Wie wirkt sich darauf eine eventuell große Zurückhaltung der Nutzer aus, in den Einstellungen die Werbung ausschließenden Wahlmöglichkeiten anzukreuzen. Wenn angenommen eines Tages die übergroße Mehrzahl Ihrer User, ich weiß nicht, inwieweit Sie das vielleicht jetzt schon unterscheiden können und uns diese Zahlen möglicherweise zur Verfügung stellen können, sich dem Werbeangebot verschließt, wie sieht es dann mit der Finanzierung Ihres Netzwerks aus? Das scheint mir ein Konfliktfeld zu sein. Einerseits finanzieren sich Plattformen durch Werbung, auf der anderen Seite haben die User ein zunehmendes Interesse, so wenige Daten wie möglich an potenzielle Werbekunden von Ihnen fließen zu lassen.

Vorsitzender: Ich würde vorschlagen, dass wir, wenn die beiden Referenten damit einverstanden sind, einmal die Runde durch die Fraktionen machen mit den Fragen, um dann gesammelt zu antworten. Wir machen dann weiter mit der ersten Frage der SPD-Fraktion.

Abg. Lars Klingbeil (SPD): Auch ich möchte Ihnen für die deutlichen Worte danken. In Sachen Rechtsprechung würde ich gerne nachfragen wollen. Man hat in der aktuellen deutschen Debatte manchmal den Eindruck, dass wir als Politik gar nichts anderes machen können, als unsere Profile zu löschen, weil wir im Prinzip machtlos sind, da nationalstaatlich nichts regelbar zu sein scheint und auch neue Gesetze schnell an Grenzen stoßen. Andererseits konnte ich einer von mir in Auftrag gegebenen Ausarbeitung des Wissenschaftlichen Dienstes des Deutschen Bundestages zum Persönlichkeitsschutz in sozialen Netzwerken entnehmen, dass Anbieter, die eine Niederlassung in Deutschland haben und deutsche User ansprechen, sich an deutsche Gesetze zu halten haben. Insofern sehe ich das Problem nicht darin, dass die Gesetze fehlen, sondern die Durchsetzung dieser Gesetze fehlt. Hierzu hätte ich gerne Ihre Einschätzung.

Vorsitzender: Wir fahren fort mit den Fragen der FDP.

Abg. Jimmy Schulz (FDP): Gestatten Sie erst einmal meinen Dank dafür, dass Sie gekommen sind, denn das zeigt ja auch Ihr hohes Interesse an dem Thema. Die VZnet-Netzwerke möchte ich loben, da sich Ihr Unternehmen meiner Ansicht nach - im Gegensatz zu so manch anderem Unternehmen - ausdrücklich und sichtbar zum Datenschutz bekennt. Nichtsdestotrotz haben Sie natürlich auch hier und da mit Problemen zu kämpfen und es ist jetzt noch gar nicht so lange her, dass massenhaft Userdaten ausgelesen wurden. Mich interessiert, mit welchen Maßnahmen Sie dies – insbesondere das massenhafte Datenauslesen über mehrere, verschiedene Accounts – verhindern wollen.

Vorsitzender: Wir schließen diese erste Fragerunde mit den Fragen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.

Abg. Herbert Behrens (DIE LINKE.): Herr Dr. Riedl, Sie haben von Ihrem großen Einsatz gesprochen, den Sie zum Schutz Ihrer Teilnehmerinnen und Teilnehmer aufbieten und hatten auch die

personellen Kapazitäten erwähnt, die das in Anspruch nimmt. Gleichwohl ist Ihr Angebot ja wohl kommerziell orientiert, möchte ich einmal unterstellen. Ich würde Ihren Hinweis gerne aufgreifen, von Industrie zu sprechen. Insofern möchte ich von Ihnen als kommerziellem Anbieter wissen, wie Sie die weitere Entwicklung der Branche sehen. Einige Rahmenbedingungen haben Sie bereits genannt, die für Sie erfüllt sein müssen, um auch in Zukunft erfolgreich sein zu können. Darüber hinaus würde mich interessieren, wo Sie künftige Geschäftsfelder für sich sehen innerhalb der bestehenden Gesetze, die wir hier in der Bundesrepublik bzw. auf Ebene der Europäischen Union haben.

An Herrn Dr. Dix möchte ich eine Frage in Bezug auf die informationelle Selbstbestimmung richten. Sie erwähnten, dass insbesondere dieses Recht ein zentrales Problem bei sozialen Netzwerken jeder Art im Internet darstelle. Sie wiesen auf die bestehende Rechtslage hin und erwähnten die kritische Prüfung sowohl des Hamburgischen Datenschützers als auch durch Sie, von anderem Boden aus agierende andere Anbieter stärker in die Pflicht zu nehmen. Welche Notwendigkeit sehen Sie noch im Hinblick auf die gesetzgeberische Seite, wo nachgearbeitet werden müsste, um diesen neuen Entwicklungen in den sozialen Netzwerken angemessen begegnen zu können?

Abg. Konstatin von Notz (BÜNDNIS 90/DIE GRÜNEN): Herzlichen Dank für beide Ausführungen. Ich hätte zwei Fragen an Herrn Dr. Dix. Es ist interessant und in der Tat bedauerlich, dass man heute hier nicht vergleichend hören konnte, wie andere Netzwerkbetreiber das künftig angehen wollen. Ich frage mich, ob ich Ihre Ausführungen richtig deute, dass es auf klarere gesetzliche Regelungen ankommt und der Status quo, den wir haben, nicht ausreichend ist und es zudem an einer Durchsetzbarkeit mangelt. Daran anknüpfend möchte ich gerne wissen, ob der Datenschutzbereich ausreichend ausgestattet ist, um diesem Bereich, der ja tatsächlich in den vergangenen Jahren enorm angewachsen ist gerade im Bereich der sozialen Netzwerke, personell und von der sachlichen Seite her gesehen, auf Augenhöhe zu begegnen.

Vorsitzender. Gut, das wäre die erste Fragerunde. Ich schlage vor, dass wir mit der Beantwortung durch Herrn Dr. Dix beginnen und Herr Dr. Riedl daran anknüpft.

Dr. Alexander Dix (Berliner Beauftragter für Datenschutz und Informationsfreiheit): Danke sehr. Zunächst zu der Frage die rechtlichen Möglichkeiten betreffend, die es im Moment gibt, sich gegenüber Angeboten, gegenüber Netzbetreibern, die sich offenbar nicht an geltende rechtliche Bestimmungen halten, zu wehren. Zum Einen gibt es eindeutig gesetzliche Vorschriften, die hier verletzt werden, das ist eine grundlegende Feststellung. Strittig war bisher, wer für die Ahndung zuständig ist. Erst seit Kurzem gibt es beispielsweise für die Aktivitäten von Facebook eine zuständige deutsche Datenschutzbehörde, seit Facebook in Hamburg eine Niederlassung eröffnet hat. Bei den anderen Netzwerken gibt es diese Probleme nicht, weil es eindeutig deutsche Anbieter sind. Im Hinblick auf Facebook war es bis dato so, dass - ähnlich wie bei Google - lange Zeit von den Unternehmen die Anwendbarkeit deutschen und europäischen Rechts grundsätzlich in Abrede gestellt wurde. Mittlerweile gibt es diesbezüglich unterschiedliche Signale. Trotzdem ist der Hamburgische

Datenschutzbeauftragte jetzt für die Durchsetzung deutschen Datenschutzrechts zuständig und er ist dabei, die entsprechenden Schritte einzuleiten.

Man muss darüber hinaus feststellen, dass es bisher ein gewisses Durchsetzungsdefizit gab. Es ist ganz klar, um Ihre Frage direkt zu beantworten, dass die Datenschutzbehörden, und das gilt für die Kollegen in Hamburg genauso wie für andere auch, große Schwierigkeiten haben mit ihrer bisherigen personellen Ausstattung. Einem Unternehmen vom Kaliber Facebooks Paroli zu bieten, das ist nicht so einfach, aber es wird mit all den zur Verfügung stehenden Möglichkeiten versucht und unter Umständen auf eine gerichtliche Auseinandersetzung hinauslaufen. Es gibt bisher keine Rechtsprechung, die hierzu eindeutige Antworten geben würde, aber unsere Rechtsauffassung ist ja klar. Gleichwohl meine ich, um zunächst noch einmal auf die Frage nach der Gesetzgebung zu antworten, dass es auch einen Gesetzgebungsbedarf, und zwar unabhängig von Facebook und den sozialen Netzwerken, gibt, der entstanden ist aufgrund europäischen Rechts, dem sogenannten Telekompaket, das im vergangenen Dezember beschlossen worden ist. Insbesondere durch die Verschärfung der Richtlinie zur elektronischen Kommunikation. Deren Art. 5 Abs. 3 verlangt nach unserer Auffassung auch eine Verschärfung des Telemediengesetzes was die Kontrolle der Nutzer über Cookies betrifft. Das gilt für soziale Netzwerke wie auch für andere Anbieter von Internetdiensten und muss verbessert werden. Nach allem, was ich bisher aus der Bundesregierung höre, ist man dort zwar anderer Auffassung, aber wir diskutieren das und hoffen, dass eine Anpassung des Telemediengesetzes ins Auge gefasst wird. Unabhängig davon besteht aber vor allem im Moment die Aufgabe, geltendes Recht schon jetzt umzusetzen und durchzusetzen. Das ist die Aufgabe, der sich die Aufsichtsbehörden jetzt schon stellen müssen.

Ich meine aber darüber hinaus, dass es trotzdem richtig ist, und deshalb begrüße ich auch die Haltung der Bundesverbraucherschutzministerin ausdrücklich, dass man hier als individueller Nutzer abstimmen sollte und einem Netzwerk seine Sympathien entziehen sollte, wenn man mit ihm nicht einverstanden ist. Das geht schneller als Gesetze zu machen und durchzusetzen und da ist jeder Nutzer in der Tat aufgefordert, die Anbieter zu vergleichen und sich anzusehen wie der Datenschutz bzw. die Datenverwendung aufgebaut sind und angemessen gewährleistet sind. Diesbezüglich haben die deutschen Anbieter eindeutig einen Standortvorteil, mit dem sie auch argumentieren sollten. Das unterstützen wir nach Kräften. Das sind also zwei Seiten: Einerseits eine rechtliche Bestimmung durchzusetzen - das ist unter Umständen schwierig und bedarf eines langen Atems, es muss aber gemacht werden - und zum Zweiten müssen in einzelnen Punkten gesetzliche Regelungen auch präzisiert und verbessert werden. Daneben sollten aber die Nutzer auch jetzt schon ihre Möglichkeiten nutzen, nämlich erstens die Einstellmöglichkeiten ausschöpfen, und wenn ihnen die nicht reichen oder wenn die Informationspolitik der Anbieter, die auch teilweise sehr zu wünschen übrig lässt, gerade bei Facebook, unzureichend ist, sollten sie einfach sagen, wir haben ein besseres Angebot im Netz gefunden und gehen lieber da hin.

Vorsitzender: Wir fahren fort mit den Antworten von Dr. Riedl.

Dr. Clemens Riedl (Geschäftsführender Vorstand, VZnet, Netzwerke Ltd., Berlin): Es gab vier Fragen an uns. Die erste beantwortete ich wie folgt. Werbung wird man sich bei uns anschauen müssen genauso wie bei RTL, genauso, wie Sie sie sonst in den Printmedien wie den Zeitungen vorfinden. Die Refinanzierbarkeit über den Werbemarkt ist für uns entscheidend. Ich glaube, es kommt Ihnen, Herr Abgeordneter, auf zwei andere Aspekte an. Erstens, dass keine Daten der Nutzer zur Vermarktung der Werbung weitergegeben werden, was ganz entscheidend ist, und zweitens dass die Nutzer selbst entscheiden sollen, personalisierte, auf sie gemünzte Werbung ansehen zu wollen. Das können sie bei uns mit einer spezifischen Einstellung in der Tat selbst entscheiden.

Jana Moser (VZnet, Netzwerke Ltd., Berlin): Die Frage, ob die Politik denn tatsächlich machtlos ist, wird zurzeit in Anbetracht der Reaktion von Frau Ministerin Aigner in Bezug auf unseren amerikanischen Konkurrenten, das Profil zu löschen, heftig diskutiert. Klar könnte man natürlich denken, das ist die einzige Möglichkeit, das Profil zu löschen. Da gibt es allerdings zwei Probleme. Erstens ist beachtlich, mit welchem Ziel und unter welchen Modalitäten die Anmeldung erfolgte. Da gibt es zentrale Unterschiede, wenn man die Plattformen vergleicht, wobei das nicht nur für soziale Netzwerke gilt. Der Begriff „Opt-in“, der für eine aktive Zustimmung zu einer Verarbeitung der Daten steht, die über den eigentlichen Zweck der Plattform hinausgeht, nimmt eine wichtige Rolle ein. Es handelt sich um eine aktive Zustimmung, so dass irgendwo einmal ein Häkchen gesetzt worden sein muss. Wenn ich mich allerdings irgendwo anmelde und nirgends ein Häkchen gesetzt habe und mich im Nachhinein wundere, dass meine Daten seltsam verarbeitet werden, dann fehlt mir teilweise schon ein wenig das Verständnis, warum dann im Nachhinein die Löschfunktion gesucht wird, wo das doch ein frühzeitiger aktiver Vorgang ist. Also, da ist quasi vorher schon etwas schiefgelaufen und nicht erst bei der Profillöschung.

Wenn man nun Gedanken anstellt, wie man das besser machen kann in Bezug auf das Opt-in, das Einholen des Häkchens, dann verweise ich auf das Beispiel unserer Plattform, unserer Registrierung, wo man zahlreiche Abfragen vorfindet. Zu beachten sind dabei natürlich die Datenschutzerklärung und sind die Allgemeinen Geschäftsbedingungen sowie der Verhaltenskodex. Aber überall dort, wo ein Häkchen gesetzt werden muss, bedeutet das zugleich für uns mit einer nennenswerten Quote von Abbrechern konfrontiert zu werden. Wir verlieren allein bei der Registrierung 45 Prozent derjenigen, die auf unsere Plattform kommen. Ein hoher Prozentsatz dieser Abbrecher wird mit hoher Wahrscheinlichkeit auf andere Seiten, auf denen Sie keine Häkchen setzen müssen, weil das schlichtweg einfach weniger Klicks bedeutet, ausweichen. Und da sind wir wieder bei den Hinweisen von Herrn Dr. Dix, der vorhin empfahl, die Nutzer mögen doch bitte per Klick entscheiden. Wenn man dem beipflichtet, dann soll bitte auch die Politik per Klick entscheiden.

Ein anderer Punkt sind die Datenschutzgesetze, die bereits angesprochen wurden, ihre Anwendbarkeit und Durchsetzbarkeit. Aus meiner juristischen Sicht sehe ich das ebenso wie Herr Dr. Dix, dass der Nutzer nicht merkt, ob der Plattformbetreiber ein deutsches Unternehmen ist. In der Regel ist die Seite in deutscher Sprache, es gibt eine deutsche Domain, die zumeist umgeleitet wird auf die übersetzte Dotcom-Seite. Der Nutzer sieht nicht, woran er ist. Ich muss an dieser Stelle aber auch sagen, dass

die Gesetze teilweise interpretationsbedürftig sind. Ausländische, insbesondere amerikanische Unternehmen – es muss jetzt nicht Facebook sein – nutzen das zu ihren Gunsten aus. Oft ist es so, dass die juristischen Meinungen weit auseinanderliegen. Ja, und wenn dann etwas unklar ist, lege ich es als kommerzieller Anbieter verständlicherweise so aus, dass es meinem Geschäftsmodell dient und Hindernisse dann nicht anwendbar sind. Oftmals gibt es zwar eine Niederlassung in Deutschland. Wenn die aber selbst kein Telemediendienst-Angebot bietet, sondern eine reine Werbefirma ist, dann kann man sich auch auf die Seite stellen und sagen, es sei gar nichts anwendbar. Aber das kann meiner Ansicht nach doch nicht intendiert sein. Also denke ich auch wie Herr Dr. Dix, dass es auf jeden Fall einer Korrektur im Telemediengesetz bedürfte, um die Gesetzeslage an die Realität anzupassen und deutlicher zu machen, für wen die Gesetze gelten, damit es nicht auf eine reine Regulierung deutscher bzw. europäischer Unternehmen hinausläuft, sondern wirklich dem Schutz der informationellen Selbstbestimmung der Nutzer dient.

Dr. Clemens Riedl (Geschäftsführender Vorstand, VZnet, Netzwerke Ltd., Berlin): Die nächste Frage, auf die ich eingehen möchte, betraf Aktivitäten gegen das maschinelle Auslesen von Nutzerdaten. Es scheint mir in diesem Zusammenhang noch einmal der Hinweis ganz wichtig – Herr Dr. Dix hat das auch schon gesagt –, dass es zwei Anwendungen zu unterscheiden gilt: den Angriff von außen und das Datenleck, so wie es in den Medien transportiert wurde. Letzteres hat bei VZnet Gott sei Dank bislang noch nie stattgefunden. Im Hinblick auf das maschinelle Auslesen von Nutzerdaten innerhalb der Plattformen sollte man sich einmal konkret vor Augen führen, jemand legt z. B. 800 unterschiedliche Accounts mit falschem Namen an und liest dann darüber Daten aus und veruntreut diese. Was können wir dagegen tun? Die Wahrheit ist, dass es eine Menge gibt, was man dagegen unternehmen kann. Klar kann man schlecht feststellen, ob die Nutzer ihre Namen wahrheitsgemäß angeben oder nicht. Wir könnten aber prüfen, von welchen Rechnern aus Anmeldungen stattfinden und ob dies massenhaft erfolgt. Für eine solche sinnvolle Prüfung muss uns der Gesetzgeber bzw. der Datenschutz aber erst einmal die Möglichkeit geben, das zu verfolgen.

Jana Moser (VZnet, Netzwerke Ltd., Berlin): Die Frage lautet: Was erlaubt uns der Staat in diesem Zusammenhang? Selbstverständlich können wir aufzeigen, was wir gerne dagegen unternehmen würden, aber das wären überwiegend technische Aspekte. Wir versuchen an dieser Stelle zunächst einmal Spezialisten in das Unternehmen zu nehmen, die sich nur damit beschäftigen. Und wir sind um eine enge Zusammenarbeit mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit bemüht. Aufgrund der letzten Vorfälle, die natürlich auch wieder in den Medien waren, suchen wir nach einer einvernehmlichen Lösung auf Basis der geltenden Gesetze. Um nur einmal ein kleines Beispiel zu nennen: Würden wir einen kostenpflichtigen Mediendienst anbieten, dürfte man Daten untersuchen und verarbeiten, um zu sehen, ob man betrogen bzw. angegriffen wird. Sobald man einen Dienst kostenlos anbietet, gibt es dafür keinerlei gesetzliche Grundlage.

Dr. Clemens Riedl (Geschäftsführender Vorstand, VZnet, Netzwerke Ltd., Berlin): Das hat mit der Diskrepanz zu tun, wie lange man Daten speichern darf, um zu sehen, wie lange jemand auf der

Plattform unterwegs ist. Und dazu gibt es auch unterschiedliche Haltungen an dieser Stelle. Soll man alles ganz schnell löschen und nicht speichern? Dann muss man viel Zeit aufwenden, um zu klären, wie lange diese Leute bei uns eigentlich unterwegs waren und was sie dort tun. Das stellt uns vor Herausforderungen, die wir oftmals nicht lösen können. Aber wir sind sehr dankbar, dass Herr Dr. Dix ein offenes Ohr an dieser Stelle für unsere Problematik hat.

Auf die Frage, ob es eine Industrie ist, kann ich nur sagen, dass es sich um eine der größten Industrien handelt, die wir zurzeit haben. Es geht um den Werbemarkt, der hier in Deutschland mit zirka 20 Mrd. Euro der zweitgrößte der Welt ist. Online sind davon zirka 2 Mrd. Euro. Google zieht davon 50 Prozent an sich. Es gibt tausende Anbieter in diesem Markt, auch online. Von www.spiegel.de bis zu winzigen Portalen und es ist deshalb sehr schwierig auf diesem Markt, als deutsche Firma zu bestehen. Etwas leichter haben es die Medien bzw. Verlage, die den Schutz der deutschen Sprache haben und damit weniger global relevant sind. Dann gab es noch eine Frage, die die Rahmenbedingungen und evtl. künftigen Geschäftsfelder betraf.

Jana Moser (VZnet, Netzwerke Ltd., Berlin): Zu dem Thema Geschäftsfeldentwicklung ist zu sagen, dass wir soziale Netzwerke anbieten, auf denen unter anderem auch Werbung eine große Rolle spielt. Mit der Werbung erzielen wir momentan hauptsächlich unseren Umsatz. Wichtig ist uns dabei, die Nutzer danach zu fragen, ob sie persönlich angepasste Werbung erhalten möchten, ohne dass wir Daten von ihnen weitergeben. Man kann natürlich überlegen, mit Anwendungen von Dritten, wie Applikationen (Apps) bzw. Spielen, Einkünfte zu generieren. Es würde sich dabei allerdings um Angebote von Dritten handeln, die selbst Telemediendiensteanbieter sind und in die Plattform zu integrieren wären. Indem wir uns diesbezüglich um größtmögliche Transparenz bemühen, müssen wir hier auch eine vergleichsweise hohe Abbrecherquote feststellen. Wie kann das sein? Zur Erläuterung möchte ich Ihnen mitteilen, dass wir nicht wünschen, dass die Drittanbieter – beispielsweise bei einem einfachen Onlinespiel – direkt an die Nutzer- bzw. Profildaten kommen, weshalb wir an dieser Stelle eine Schnittstelle – so etwas wie eine Firewall – dazwischengeschaltet haben und es den Nutzern anheimstellen, z. B. nur unter einem Pseudonym zu spielen. Dann gilt es, eine Visitenkarte zu wählen, in die der Nutzer seine Daten, die er möchte und für wichtig hält, eintragen kann. Je nach Spiel mag das eine oder andere Sinn machen. Dieses teilweise sehr komplizierte Verfahren bzw. Konzept, das wir uns in einem Zeitraum von über einem Jahr überlegt haben, dem Nutzer für jedes Spiel eine Identität an die Hand zu geben, reicht schon an so etwas wie Identitätsmanagement heran. Oftmals empfinden die Nutzer das System an dieser Stelle als zu kompliziert und dem Anlass nicht angemessen und brechen den Vorgang ab, obwohl das System gerade den Schutz der Nutzer und ihrer Daten im Blick hat.

Vorsitzender: Das wären die Fragen auf die erste Fragerunde gewesen. Wir steigen nun ein in die zweite Fragerunde.

Abg. Martin Jarzombek (CDU/CSU): Danke, Herr Vorsitzender. Meine sehr geehrten Damen und

Herren. Wir haben von Seiten aller im Deutschen Bundestag vertretenen Fraktionen eine Initiative ergriffen, was das Thema Datensicherheit und Privatsphäre bei Facebook betrifft. Und insofern ist das schon ein spannendes Thema, dem wir uns heute hier widmen.

Was das Thema Abbrecherquote betrifft, so würde mich bei der Erstregistrierung interessieren, ob die Abbrecher später noch einmal wiederkommen. Es gibt ja auch Fälle, in denen man Nutzer zunächst zwar verunsichert, diese sich es dann aber in Ruhe noch einmal überlegen und erst einmal jemanden fragen. Bei Schülern stelle ich mir das so vor, dass die am nächsten Tag in der Pause erst ihre Kumpels fragen und dann vielleicht wiederkommen. Was mich aber viel mehr beschäftigt, ist die Handhabe. Facebook ist insofern ja ein Phänomen, das wird ja nicht das Letzte geblieben sein. In zwei Jahren haben wir einen ähnlichen Anbieter, der uns mit vergleichbaren Dienstleistungen beglückt und die ganze Datenschutzdebatte erneut lostritt. Sie haben, Herr Dr. Dix, vorhin angeführt, dass Sie Ihre Zuständigkeit daraus ableiten, dass Facebook irgendwann und viel später als der Betrieb hierzulande begonnen hat, eine Niederlassung in Hamburg gegründet hat. Wenn man sich jetzt die technische Struktur dieses Netzes ansieht, dann kann man erahnen, dass zirka 40.000 Server betrieben werden. Es gibt Rechenzentren an den verschiedensten Standorten in Deutschland – sehr große sogar. Ein solches Netz ist technisch gar nicht realisierbar, wenn ich 40.000 Server in den USA betreibe, sondern es sind dezentrale Aufbauten erforderlich. Deshalb stellt sich für mich die Frage, ob das alleine nicht schon eine gewisse Handhabe ermöglicht, weil wir damit ein ganz anderes Prinzip haben würden und bei künftigen Anbietern auch viel schneller agieren könnten, wenn wir sagen, dass es reicht, wenn ein Betreiber auf deutschem Boden eine entsprechende Infrastruktur bereithält.

Vorsitzender: Vielen Dank. Frau Bär, bitte.

Abg. Dorothee Bär (CDU/CSU): Vielen Dank. Herr Jarzombek hat ja die Initiative schon erwähnt, darum finde ich es, Herr Dr. Dix, schon ein wenig merkwürdig, wenn Sie die Verbraucherschutzministerin loben, dass sie ihr Profil bei Facebook gelöscht hat. Das kann ja immer nur die Ultima Ratio sein, etwas zu löschen und sich damit aus der Verantwortung zurückzuziehen. Gerade als Politiker haben wir die Verantwortung, uns um die Nutzer zu kümmern. Und die Erfahrung zeigt eben auch, dass diejenigen, die sich für ein soziales Netzwerk entscheiden, nicht danach entscheiden, wer den besten Datenschutz bietet, sondern in erster Linie, wo die meisten Freunde, also diejenigen sind, mit denen man zusammen sein möchte. Deshalb stellt sich für mich die Frage, wo können Sie Herr Dr. Riedl den Nutzern einen Mehrwert bieten, lieber zu Ihnen zu kommen als zu Facebook zu gehen. Sie haben schon verschiedene Aspekte angesprochen, wie Spiele beispielsweise, das haben Sie von der wirtschaftlichen Seite beleuchtet, aber es muss ja auch eine andere Möglichkeit geben. Vielleicht stellen Sie ja schon Überlegungen in die Richtung an, sich derart als die bessere Alternative anzubieten, dass es nicht allein am Datenschutz festgemacht wird, denn für Jugendliche unter 18 Jahren scheint mir das völlig irrelevant zu sein.

Abg. Brigitte Zypries (SPD): Mich interessiert, ob es Überlegungen von Seiten der

Datenschutzbeauftragten gibt, auch einmal eine Werbung im Sinne des Datenschutzes zu machen, wie wir das seinerzeit beim Urheberrecht gemacht haben mit der Kampagne: "Kopien brauchen Originale". Die Wirtschaft hat damals auch mitgemacht und nennenswerte Kampagnen betrieben, so dass sich mir die Frage stellt, ob es eigentlich Sinn macht, gezielt an Schulen zu gehen und da für den Datenschutz zu werben.

Meine zweite, an Dr. Riedl gerichtete Frage betrifft eventuelles Lehrermaterial auf den Plattformen der Firma. Ich würde es mir gerne einmal ansehen und prüfen, ob es brauchbar ist für unsere Arbeit im Wahlkreis, z. B. an den Schulen, mit denen man es zu tun hat.

Ich habe den Beiträgen sowohl des Datenschutzbeauftragten als auch der Firmenvertreter entnommen, dass Sie ähnliche Anforderungen an die Politik richten. Wäre es möglich, dass Sie diese schriftlich formuliert noch einmal nachreichen? Es kann ja nicht sein, dass es nur darum geht, dass die Politiker ihre Konten bei Facebook löschen, wofür ich aber vollstes Verständnis habe, sondern es geht ja auch um mehr. Und es wäre wichtig zu wissen, wo Sie konkret einen Bedarf sehen.

Abg. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, ich wollte mich auch noch einmal zu diesem Problem äußern, auch weil Sie es so direkt angesprochen haben, Herr Dr. Dix, ob man als politischer Mensch in der Pflicht steht, da nun auszutreten und ob das nun tatsächlich ein leuchtendes Beispiel ist, das die Verbraucherschutzministerin abgegeben hat. Ich habe da starke Zweifel und kann mir niemanden vorstellen, dem das helfen soll, dass eine politische Person, die all das, was sie einstellt, ja sowieso aus Gründen der Öffentlichkeit einstellt, nun austritt, um ein Signal zu setzen.

Wie ist es um ein deutsches Netzwerk bestellt, das sich ganz toll an die deutschen Gesetze hält und deswegen als das Gute dasteht? Ich habe große Sympathien für StudiVZ, da bin ich auch, aber es muss ja letztlich sich dasjenige durchsetzen, das ein qualitativ hochwertiges Angebot hat und die Nutzer deswegen anspricht, weil die Beachtung des Datenschutzes ein wesentlicher Bestandteil der Geschäftsidee ist. Ich frage, was wir gesetzlich zum Beispiel Facebook direkt vorschreiben können, was die harten Kriterien sind, die man einfordern muss und wie können wir sie vor allen Dingen effektiv durchsetzen, um aus dieser Bittstellersituation herauszukommen. Es scheint mir ein Armutszeugnis zu sein, wenn die deutsche Verbraucherschutzministerin die Segel streicht und austritt aus dem sozialen Netzwerk und die Bevölkerung, ich sage das jetzt einmal zugespitzt, darin alleine lässt.

Vorsitzender: Wir haben noch Wortmeldungen von Herrn Schulz, Herrn Behrens und Frau Rößner. Herr Schulz, bitte.

Abg. Jimmy Schulz (FDP): Dankeschön. Herr Dr. Dix, Sie hatten angesprochen, dass Mark Zuckerberg das Ende der Privatsphäre angekündigt hat. Wir alle hoffen, dass das nicht eintreten wird, weil wir alle großen Wert auf den Datenschutz legen, was sich in den Gesetzen ausdrückt und auch in den Firmen, die in Deutschland tätig sind. Nichtsdestotrotz sehe ich sehr wohl auch einen Trend – vor allem bei jungen Menschen – eine gewisse Laxheit in der Einstellung an den Tag zu legen, mit den

eigenen Informationen weniger streng umzugehen. Und da möchte ich nicht nur auf Facebook einprägen, das haben wir heute ausgiebig genug getan, sondern da gibt es noch andere Firmen, die sehr viel weitreichendere Privatsphäreninformationen in Zukunft zugänglich machen werden, Bewegungsdaten beispielsweise oder die Verwendung von Bildern. Also, ich sehe da Entwicklungen, die weit über das hinausgehen, was wir hier heute auch schon angesprochen haben. Deswegen interessiert mich die Einstellung der jungen Generation, ob die jungen Menschen im Web 2.0 bzw. in den sozialen Netzwerken freiwillig dazu neigen, persönliche Daten preiszugeben. Ist da eine erhöhte Sensibilität oder eher eine bewusste Freigabe feststellbar? VZnet hat vermutlich ja den Kontakt zu den jungen Menschen und kann beurteilen ob da ein Trend feststellbar ist, aktiv die Sicherheitseinstellungen bewusster vorzunehmen.

Vorsitzender: Herr Behrens, bitte.

Abg. Herbert Behrens (DIE LINKE): Dass es darum geht, sich mit kommenden Problemen auseinanderzusetzen, hätten wir ja gerne getan mit den Tagesordnungspunkten, zu denen uns eine Debatte verwehrt worden ist. Ich meine auch, dass wir uns sehr intensiv mit solchen Fragen beschäftigen müssen, damit wir als Politiker auch rechtzeitig unterwegs sind und nicht im Nachklapp die sich auftuenden Löcher bearbeiten müssen. Meiner Ansicht nach kommt es darauf an, dass wir die datenschutzrechtlichen Dinge sehr ernst nehmen, damit nicht Missbräuche zu beklagen sind, wie wir sie aus der Vergangenheit kennen, als sowohl durch vorsätzlichen und kriminellen Zugriff auf Daten Missbrauch betrieben worden ist bzw. ein laxer Umgang mit dem Datenschutz dazu führte. Frau Moser, Sie hatten dargestellt – für Sie zumindest als kommerziellen Anbieter – dass, wenn sich ein Nutzer durchhangeln muss durch verschiedene datenschutzrechtlich notwendige Dinge und Häkchen setzen muss, am Ende nur 59 Prozent übrigbleiben und sich die anderen ausklicken, weil es ihnen zu umständlich wird. Das deute ich als Plädoyer, dass man eben nicht mehr diesen Weg gehen möchte, sondern es ein wenig einfacher haben möchte, damit einem nicht die Kundschaft abhanden kommt. Ist es Ihnen nicht möglich, mit den Anmeldedaten so umzugehen, diese so zu übersetzen, dass ein entnervtes wegklicken der Leute entbehrlich ist? Auf der anderen Seite wäre natürlich auch die Frage zu stellen, inwieweit es eine sinnvolle Sensibilisierung sein könnte, durch verschiedene Schleusen gehen zu müssen, um sich dann zu einem bestimmten Zeitpunkt auch klar zu machen: „Halt, da gehe ich ja wohl ziemlich offen mit sensiblen Daten um“, und es durchaus eine bewusste Entscheidung sein kann zu sagen: „Das breche ich lieber ab.“

Abg. Tabea Rößner (BÜNDNIS 90/DIE GRÜNEN): Meine Frage richtet sich an Herrn Dr. Riedl. Sie haben betont, dass Ihnen wichtig ist, gerade Kinder und Jugendliche zu schützen. Mich interessieren die möglichen Auswirkungen des in Kürze in Kraft tretenden Jugendmedienschutzstaatsvertrags auf Ihr Angebot. Inwieweit werden Sie sich für eine Alterskennzeichnung Ihrer Angebote im Netz entscheiden und wie werden Sie dann mit den Userinhalten umgehen?

Vorsitzender. Das wäre die zweite Fragerunde. Wir können mit der Beantwortung beginnen. Herr Dr.

Riedl bitte und dann Herr Dr. Dix.

Dr. Clemens Riedl (Geschäftsführender Vorstand, VZnet, Netzwerke Ltd., Berlin): Ein soziales Netzwerk hat damit zu tun, dass man sich einander mitteilt und sich austauscht. Da haben Sie recht, Frau Abgeordnete Bär. Und desto leichter und bequemer das geht, umso weniger Häkchen man setzen muss, desto besser funktioniert der Dienst und wird das Angebot wahrgenommen. Für den Gesetzgeber mag der Standort der Server interessant sein, für die Industrie ist es das nicht. Im Ausland produzierte Personenkraftwagen beispielsweise müssen selbstverständlich, weil sie auf deutschen Straßen unterwegs sind, deutschen Schutzbestimmungen entsprechen. Es kann folglich nicht darauf ankommen, auf welchem Server die Inhalte produziert bzw. gehostet werden. Das ist eigentlich Vergangenheit, die in unserer Industrie keine Rolle mehr spielt, weil die Server, wie Sie zu Recht sagen, auf der ganzen Welt verbreitet sind. Das vielleicht ganz grundsätzlich dazu.

Es ist für uns nicht einfach, im Wettbewerb zu bestehen, obwohl wir genau wissen, was wir alles tun könnten, aber im Detail scheitern unsere Ansätze an Gesetzen, die wir einzuhalten haben. Bewegungsmeldungen und Aktivitäten, die live mitgesendet werden beispielsweise, wenn Sie das alles – in Feeds, und all diesen Sachen – jedes Mal erst durch eine einzelne Einwilligung ermöglichen wollen, dann funktioniert das einfach nicht mehr. Man kann den Dienst dann nicht benutzen. Um dafür dem deutschen Gesetzgeber eine Brücke zu bauen, stehen wir auf dem Standpunkt, die Minimalforderung, die wir gegenüber einem Staat erfüllen würden, ist die, gleiche Rahmenbedingungen für alle zu schaffen, anstatt uns Gedanken machen zu müssen, welche Gesetze wir einhalten müssen, ausländische Mitbewerber aber ohne Schutzbedingungen und Gesetzesauflagen auf der Datenautobahn unterwegs sein können. Das fällt uns sehr schwer.

Jana Moser (VZnet, Netzwerke Ltd., Berlin): Zu der von Ihnen aufgegriffenen Abbrecherquote möchte ich sagen, dass es uns nicht ohne Weiteres möglich ist, die genauer zu analysieren. Sie wollten wissen, ob wir Leute, die vielleicht wiederkommen, sich eines Besseren besonnen haben, alles vielleicht als gar nicht so schlimm ansehen und sich vielleicht doch die Seiten durchklicken und die Häkchen überall machen, wiedererkennen. Dazu müssten wir erst in die Lage versetzt werden. Wir dürfen sie aber nicht wiedererkennen, weil es dafür bislang keine Rechtsgrundlage gibt. Momentan gehen Abbrüche lediglich in unsere anonyme Statistik ein, und dementsprechend wissen wir, dass die Leute weggebrochen sind, aber nicht, ob sie noch einmal wiederkommen.

In diesem Zusammenhang möchte ich gerne die Frage aufgreifen, an welcher Stelle man die jugendschutzrelevanten Dinge im Netz findet. Wir haben im Bereich SchülerVZ auch eine Elternseite, die man auf der Plattform vergleichsweise einfach findet, auch ohne dass man sich einloggen muss. Dort sind sehr viele Unterlagen und wenn ansonsten jemand Interesse hat, noch vertiefte Unterlagen zu bekommen, dann stehen wir natürlich jederzeit zur Verfügung und bieten gerne entsprechendes Material an.

Philippe Gröschel (VZnet, Netzwerke Ltd., Berlin): Die Informationsseite richtet sich an Lehrer und Eltern. Sie ist etwas unterteilt. Auf der einen Seite sind es Informationen, die sich an die Familie wenden. Wie spricht man beispielsweise über das Thema Privatsphäreneinstellung am Frühstückstisch? Der zweite Bereich richtet sich gezielt an Lehrer. Darin geht es um Unterrichtsmaterial, das man sich herunterladen, aber auch postalisch bestellen kann. Das sind Mappen, die wir auch Ihnen gerne zusenden, wenn Sie daran Interesse haben. Wir betreiben aber auch ein Programm namens „SchülerVZ macht Schule“. Das ist ein Projekt, bei dem wir zirka 30 Schulen pro Jahr an Projekttagen besuchen und an großen Veranstaltungen durch die Klassenzimmer gehen, um das Unternehmen vorzustellen, aber auch zu dem Thema Privatsphäre etwas zu sagen und mit den Klassen und den Lehrern zu diskutieren. Das ist ein Teil, mit dem wir als Unternehmen auch dazu beitragen können, Medienkompetenz an Schulen zu stärken. Aber da es mehr als 10.000 Schulen in Deutschland gibt, können wir als verhältnismäßig kleines Unternehmen nicht alle abdecken.

Die Frage nach dem Jugendmedienschutzstaatsvertrag und den Altersklassifizierungen möchte ich wie folgt beantworten. Wir haben in den vergangenen Jahren zwei recht umfangreiche Selbstverpflichtungserklärungen ausgearbeitet. Die eine unter dem Dach der EU-Kommission mit dem Titel „Safer Internet Programme“ und die zweite unter dem Dach des Vereins der Freiwilligen Selbstkontrolle der Multimediadienstanbieter (FSM). Der Entwurf des neuen Jugendmedienschutzstaatsvertrags sieht in § 5 Abs. 3 eine explizite Privilegierung für Großunternehmen vor, die sich solchen Selbstverpflichtungserklärungen unterwerfen. VZnet-Netzwerke hat seinerzeit aktiv an dem runden Tisch zum Jugendmedienschutzprogramm mitgewirkt, der vom Beauftragten der Bundesregierung für Kultur und Medien (BKM) gemeinsam mit den Ländern organisiert worden war, und da wurden diese Themen auch sehr intensiv diskutiert. Aus unserem Blickwinkel wird uns die Klassifizierung so wie sie vorgesehen ist, gar nicht treffen, weil wir eben im Rahmen dieser Privilegierung bereits den Beweis antreten, dass unsere Angebote jeweils für die Altersklassen geeignet sind. Entsprechend müssten keine Einzelseiten klassifiziert werden, sondern das Angebot wurde einmal auf 12 klassifiziert und damit ist das Thema für uns erledigt.

Vorsitzender: Dann würde ich gerne das Wort an Herrn Dr. Dix geben, weil einige der Fragen an Sie gerichtet waren.

Dr. Alexander Dix (Berliner Beauftragter für Datenschutz und Informationsfreiheit): Zunächst die Frage nach den Servern bzw. den Datenverarbeitungskapazitäten, auf die außereuropäische Anbieter zugreifen. Nach unseren Informationen gibt es bisher in Deutschland keine speziellen Rechenzentren für Facebook, in denen Facebook-Nutzerdaten verarbeitet werden. Natürlich werden die Backbones und gängige Kommunikationsnetze genutzt, das ist bei jedem Internetanbieter so. Aber die europäische Richtlinie gibt eindeutig vor, dass europäisches Recht – und das gilt dann auch für das Bundesdatenschutzgesetz – nur dann auf außereuropäische Anbieter anzuwenden ist, wenn und soweit auf Mittel der Datenverarbeitung in Deutschland zugegriffen wird. Solange es solche Serverfarmen, wie Sie sie angesprochen haben, nicht gibt, können das nur die Computer der

einzelnen Nutzer sein. In dem Moment, wo dort ein Cookie abgelegt wird – und wenn es auch nur ein Session-Cookie ist –, greift deutsches Datenschutzrecht. Das war schon so, bevor Facebook eine Niederlassung in Hamburg gegründet hat, insofern war materiell deutsches Datenschutzrecht schon immer anwendbar. Es gab lediglich keine örtliche Zuständigkeit einer Datenschutzbehörde. Das sieht jetzt anders aus, weil Facebook, übrigens dem Beispiel von Google folgend, eine – allerdings mehr mit Marketing befasste – Dependence in Hamburg gegründet hat. Es gibt jetzt also Ansprechpartner, an die man sich wenden kann. Das materielle Recht aber, das war schon vorher anwendbar. Ich habe so meine Zweifel, ob man das deutsche Recht in dem Punkt entscheidend ändern bzw. verschärfen kann, denn die Vorgaben macht das europäische Datenschutzrecht, die Datenschutzrichtlinie, die allerdings im Moment ihrerseits von der EU-Kommission überprüft und modernisiert wird. Also, möglicherweise kann man auf europäischer Eben da auch für mehr Klarheit sorgen, was ich sehr begrüßen würde.

Gestatten Sie mir eine Anmerkung zu der Abbrecherquote, die Frau Moser erwähnt hat. Ich würde sehr davor warnen, daraufhin das Datenschutzniveau in Deutschland abzusenken. Das wäre das verkehrte Signal, sondern, wie gesagt, man sollte das stringente Datenschutzrecht in Deutschland als Argument und geradezu als Wettbewerbsmerkmal einsetzen. Ich kann verstehen, dass man auf Seiten der Betreiber bemerkt, dass die Komplexität offenbar Unlust bei den Nutzern erzeugt. Da sind die Anbieter möglicherweise stärker in der Pflicht, den Nutzern zu erläutern, warum diese Klicks erforderlich sind. Und gerade in dieser Hinsicht haben die VZnet-Netzwerke meiner Wahrnehmung nach auch eine positive Entwicklung durchgemacht. Sie erklären das inzwischen sehr viel besser als am Anfang. Wir waren da nicht immer hundertprozentig einer Meinung in der Vergangenheit, aber das hat sich mittlerweile geändert. Auch heute sind im Einzelnen zwar noch gewisse Wünsche offen, aber im Großen und Ganzen ist das Angebot der VZnet-Netzwerke mittlerweile datenschutzkonform. Da ist eine Vermittlungsleistung zu erbringen, die sich auch nicht darauf beschränken sollte zu sagen: „Das ist in Deutschland eben gesetzlich vorgeschrieben“, sondern die Nutzer sollten auch vor Augen geführt bekommen, was für Konsequenzen es hat, wenn sie das nicht interessiert oder sie es einfach ignorieren. Ich stimme auch nicht mit der Einschätzung mancher Mitglieder des Unterausschusses überein, dass Datenschutz für Minderjährige irrelevant sei. Ich bin selbst nicht Mitglied in einem sozialen Netzwerk, aber ich erzähle gerne das Beispiel eine Lehrers, der sich auf SchülerVZ einladen ließ, sich anmeldete, obwohl das formal eigentlich gar nicht zulässig wäre, und dann alle Profilseiten seiner Schülerinnen und Schüler ausgedruckt und in der großen Pause an eine Wand in Klassenzimmer gehängt hat. Als die Schülerinnen und Schüler aus der Pause zurückkamen und ihre Profile aushängen sahen, ist für sie eine Welt zusammengebrochen, weil sie der irrigen Meinung waren, SchülerVZ sei für sie so etwas wie ein vertraulicher, privater Raum. Diesen Eindruck bestätigen auch Gespräche mit Jugendlichen – ich bin viel in Schulen und versuche das auch zu vermitteln –, dass Datenschutz in einer anderen Weise wahrgenommen wird, als Ältere ihn verstehen. Die Haltung bzw. Einstellung zur Privatsphäre ändert sich ganz zweifelsohne. Aber trotzdem ist Privatsphäre für Jugendliche nicht uncool. Das Gegenteil erlebe ich ständig auch im Gespräch.

Ich bin selbstverständlich gerne bereit, Ihnen meine Empfehlung an den Gesetzgeber noch einmal

separat schriftlich mitzuteilen. Wir haben, letzter Punkt zum Thema Öffentlichkeitsarbeit, gemeinsam mit dem Jugendnetz Berlin eine Broschüre herausgegeben mit dem Titel: „Ich suche dich“ (<http://www.datenschutz-berlin.de/content/veroeffentlichungen>). Die füge ich auch gerne noch einmal für die Mitglieder des Unterausschusses bei.

Dr. Clemens Riedl (Geschäftsführender Vorstand, VZnet, Netzwerke Ltd., Berlin): Eine Frage scheint mir noch nicht beantwortet, die nicht untergehen sollte. Es geht darum, wie junge Menschen mit dem Schutz ihrer Daten umgehen. Ganz grundsätzlich: Wir glauben, Datenschutz ist eher ein Hygienefaktor im Herzbergerschen Sinne, indem er zwar nicht stört, aber auch keinen besonderen Nutzen erkennen lässt. Im täglichen Betrieb sehen wir das. Junge Menschen haben in Deutschland eigentlich einen sehr laxen Umgang mit dem Thema Datenschutz, mit der Freigabe von privaten Daten. Darum halten wir auch die deutschen Datenschutzbestimmungen unter dem Gesichtspunkt der Schutzbedürftigkeit für relevant. Die Wettbewerber betreffend gibt es natürlich den Punkt, dass jeder Deutsche bzw. Jugendliche weiß, wenn er Daten ins Internet einstellt, dass diese dort so ganz sicher nicht sind. Also die sind da sozusagen nicht blind, sondern wissen, was alles schon passiert ist. Aber sie haben das Gefühl, sie sind hier in Deutschland, sie werden geschützt, hier gibt es Gesetze und Datenschützer, die auftreten, und was auch immer. Unbekannt mag sein, dass 90 Prozent derer, die im Internet auf amerikanischen Seiten surfen, sich in einem aus deutscher Sicht völlig rechtsfreien Raum bewegen. Niemand schützt sie. Und ich bezweifle sehr stark, dass die deutsche Bundesregierung dafür jemals die Zuständigkeit haben wird, und auch die Durchsetzbarkeit – und da kennen wir nun die amerikanischen Kollegen auch ganz gut – in dem Sinne, einen Bußgeldbescheid in Palo Alto zuzustellen, nicht einfach sein dürfte.

Vorsitzender: Wir wären dann mit der Beantwortung der Fragen durch die Sachverständigen und mit den beiden Fragerunden von Seiten der Fraktionen durch. Ihnen allen möchte ich dafür danken, dass Sie sich die Zeit genommen haben, hierher zu kommen und mit uns teilweise kontrovers, aber auch sehr informativ für alle Beteiligten das Gespräch zu führen. Ich wünsche Ihnen weiterhin gutes Gelingen im Sinne des Datenschutzes. Gestatten Sie mir noch den Hinweis, ergänzende Informationen bitte an das Sekretariat zu senden, da das Material von dort aus zentral an uns alle weitergegeben wird.

Tagesordnungspunkt 2a

Bericht gem. § 56a GO-BT des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung

Technikfolgenabschätzung (TA)
Zukunftsreport - Ubiquitäres Computing

BT-Drucksache 17/405

Vorsitzender: Ich rufe dann auf den Punkt 2 der Tagesordnung und zwar haben wir dort vorliegen einmal den Punkt 2a, den TAB-Bericht: Technologiefolgenabschätzung, Zukunftsreport – Ubiquitäres

Computing – auf der Bundestagsdrucksache 17/405 und den Punkt 2b: Unterrichtung durch die Bundesregierung – Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie.

Dazu begrüße ich zwei weitere Gäste. Zum einen ist das Herr Peter Zoche vom Fraunhofer-Institut für System- und Innovationsforschung (Karlsruhe). Herzlich Willkommen, Herr Zoche. Und es war mit angekündigt Herr Dr. Peter Bleeck aus dem Bundesministerium für Wirtschaft und Technologie. Der Punkt 2b ist eine reine Unterrichtung und muss nur hier zur Kenntnis gereicht werden. Gleichwohl besteht die Möglichkeit, hier noch Nachfragen an den Vertreter der Bundesregierung zu stellen. Wenn Sie einverstanden sind, würde ich aber zunächst jetzt Herrn Zoche das Wort erteilen, damit er uns kurz in den TAB-Bericht einführt. Herr Zoche, Sie haben das Wort.

Peter Zoche (Fraunhofer-Institut für System- und Innovationsforschung): Vielen Dank, Herr Vorsitzender. Meine Damen und Herren, die Studie ist mittlerweile auch als Buch erschienen und auf den Webseiten des Büros für Technikfolgen-Abschätzung zu finden. Ich bin Koordinator für unser Institut, das institutioneller Partner des TAB ist. Insofern stelle ich zwar heute eine Studie vor, die ich nicht selbst als Projektleiter verantwortet habe, aber ich bemühe mich gleichwohl gerne, Ihnen nachher so gut es geht, Detailfragen zu beantworten. Der Projektleiter ist im Ausland in diesen Tagen und unabkömmlich, weshalb ich ihn entschuldigen möchte.

Was ist die Vision des ubiquitären Computing?

Informationstechnik und Computer umgeben uns in allen möglichen Lebensbereichen und werden zunehmend allgegenwärtig. Sie haben das Potenzial, sich allmählich in Alltagsgegenständen festzusetzen und so unseren Alltag zu durchdringen. „Ubiquitäres Computing“ – so wird diese Entwicklung genannt – kann damit auf einem neuen Niveau Daten in vielen gesellschaftlichen Bereichen erfassen, verarbeiten und zur Verfügung stellen. Das geschieht nicht nur im privaten Bereich – der ist gegenwärtig eher unterentwickelt – sondern Vorreiter ist die industrielle Produktion neben vielen Bereichen des konventionellen Geschäftslebens.

Technische Geräte, aber auch Alltagsgegenstände, werden allmählich smart, indem sie mit Informationstechnologie zum Sammeln, Verarbeiten, Speichern und Kommunizieren von Daten ausgestattet werden. Gegenüber ihrem ursprünglichen Zweck erhalten sie damit eine erweiterte Funktionalität und insofern auch eine neue Qualität.

Smarte Alltagsgegenstände und ubiquitäres Computing können grundsätzlich einen hohen gesellschaftlichen Nutzen stiften und den Komfort im privaten Bereich erweitern. Es bestehen Möglichkeiten, sie im Bereich des Umweltschutzes einzusetzen und so beispielsweise zu einem effizienteren Energieverbrauch beizutragen. „Intelligente“ Fahrzeuge – Sie kennen das – können Verkehrswege sicherer machen. Es gibt lernfähige persönliche Assistenzsysteme, die

Arbeitsproduktivität im Büro steigern können. Im medizinischen Bereich können Sensoren implantiert und damit Kleinstcomputer aktiviert werden, die den Gesundheitszustand von Patienten überwachen und in kritischen Situationen Informationen übermitteln.

Die technologische Grundlage des ubiquitären Computings ist letztlich die Zusammenführung sehr unterschiedlicher Technologien. Als typische Querschnittstechnologie nutzt das ubiquitäre Computing die gesamte Breite der informationstechnischen Systeme – Information und Kommunikation – wobei vor allen Dingen die Fortschritte in der Kommunikationstechnik, der Mikroelektronik zu Beginn eine wesentliche Rolle gespielt haben. Heute kommen hinzu Aspekte der Energieversorgung, Benutzerschnittstellen und Sensorik für die Lokalisierungstechnik, um Anwendungen differenzierter weiterzuentwickeln. Das sind Kennzeichen und Herausforderungen gleichermaßen, unter denen die Technologie des ubiquitären Computings, kurz UbiComp, derzeit steht.

Ein bekanntes Beispiel für Lokalisierungstechniken ist die Radio-Frequenz-Identifikation (RFID) – über die hier auch gesprochen werden soll – mit der sich die Identität von Dingen aus der Distanz feststellen lässt. Vorreiter in der Anwendung von RFID ist die Logistik. Ohne manuelle Eingriffe kann eine lückenlose Verfolgung der Warenströme über die gesamte Lieferkette sichergestellt werden und zwar sicher sichergestellt werden, so zumindest das Ziel.

Die Anwendung der RFID-Technologie stellt momentan eigentlich den ersten großen Schritt zur Realisierung des ubiquitären Computing dar, das letzten Endes eher eine Vision ist für die nächsten zwei Dekaden und dessen Potenzial auch deutlich über diese Anwendung hinausgeht.

Was sind nun die ersten Einsatzbereiche und die Funktionen des ubiquitären Computings? Die Vision geht vor allen Dingen von Verbesserungen für jeden einzelnen Bürger aus. Es handelt sich allerdings weitgehend um eine industrielle Technik, was der aktuellen Dominanz von RFID-Anwendungen letztlich auch geschuldet ist. Anwendungen finden sich im Handel, in der industriellen Produktion, der Materialwirtschaft und der Transportlogistik. Weitere Anwendungen liegen zukünftig vor allen Dingen in der Personenidentifikation, im Gesundheitswesen sowie im Bereich der Mobilität und des Verkehrs.

In der Perspektive wird das ubiquitäre Computing eine Vielzahl neuer Funktionen ermöglichen. Gestatten Sie mir nur ganz knapp einige Stichworte dazu. Beispielsweise können smarte Gegenstände miteinander kooperieren. Es kann beispielweise Zutritt zu gefährlichen Bereichen am Arbeitsplatz nur gewährt werden, wenn eine bestimmte Ausrüstung mitgeführt wird und diese elektronisch erfasst wurde. Es kann also auch darauf geachtet werden, dass bestimmte Arbeitsplätze mit Schutzkleidung und dergleichen betreten werden und ansonsten nicht. Smarte Umgebungen erlauben das Einbringen kommunikationsfähiger Sensoren in die physische Welt. Dadurch wird es dann möglich, Umweltzustände zu überwachen oder Informationen in die Umwelt einzubetten. Der Zugriff zu Services kann durch einfaches Berühren mit smarten Endgeräten – das sozusagen auch virtuell erfolgen kann – initiiert werden. Es können auf diese Weise z. B. Produktinformationen abgerufen werden durch Blickkontakt auf ein bestimmtes Produkt, aber auch durch Berühren des Produktes.

Gegenstände oder Personen können leichter lokalisiert werden. Das gilt nicht nur für Postsendungen und Container, sondern auch für Mietautos oder umweltgefährdende Stoffe, die weiterverfolgt werden können. Es ist aber auch eine Überwachung von Kindern in der Diskussion und gibt Überlegungen, Personen zu überwachen. Das ist natürlich alles mit reichlich Zündstoff umgeben und von daher auch Diskussionsgegenstand hier.

Darüber hinaus ist kennzeichnend für diese Entwicklung, dass zunehmend hybride Produkte und Dienstleistungen denkbar sind. Bislang nicht nachvollziehbare Vorgänge werden dadurch mess- bzw. steuerbar. Zum Beispiel könnten Autoversicherungen nach der tatsächlichen Nutzung abgerechnet werden, also dieses Pay-as-you-drive-Modell. Preise könnten abhängig von der Nutzungsdauer und -intensität, aber auch der Person des Nutzers dynamisch ermittelt werden. Sie sehen, das sind Veränderungen, die wir im Prinzip schon kennen, aber noch nicht in dieser automatisierten Form. Was Sie hier auch im Bundestag bereits diskutierten, sind Kreditkarten, aber auch Waffen, die so ausgestattet werden, dass sie nur von autorisierten Personen benutzbar sind.

Wo sehen wir jetzt Beobachtungs- und Handlungsbedarf? Auch das nur ganz schemenhaft kurz angerissen. Insgesamt ist inzwischen eine recht hohe technische Reife gegeben. Das kann man auch an der fortschreitenden Durchdringung von Einsatzfeldern nachvollziehen. Hierbei gibt es in Detailfragen einen erheblichen Forschungs- und Entwicklungsbedarf auch in grundsätzlicher Hinsicht. Ich will auf die einzelnen Felder hier nicht näher eingehen, sondern nur skizzieren, dass es keine fertige Technologie ist, sondern eine, die in konkreten Anwendungszusammenhängen weiter entwickelt werden muss.

Das wirtschaftliche Potenzial ist hoch. Effizienz und Wettbewerbsfähigkeit können mit Hilfe von RFID und ubiquitärem Einsatz von Computertechnologie immens gesteigert werden. Es können neue Dienstleistungen entwickelt werden und auch neue Geschäftsmodelle, Preismodelle auf dieser Grundlage.

Allerdings ist eine ganze Reihe von Voraussetzungen zu schaffen, die insbesondere die internationale Verbreitung von Produkten erst möglich machen. Beispielsweise sind die internationale Frequenzharmonisierung und auch die Standardisierung noch nicht so weit fortgeschritten, dass man international problemlos mit entsprechenden Produkten agieren könnte.

Auch ist es so, dass im mittelständischen Bereich gewisse Defizite gesehen werden – auch experimentell – diese Technologien zu erproben, da sich diese kleinen und mittleren Unternehmen (KMU) in der Regel nicht so eine intensive Forschung und Entwicklung leisten können, um ihre Produkte und Dienstleistungen vorausschauend zu entwickeln; ein generelles Problem. Da ist im Hinblick auf RFID in der letzten Zeit zwar einiges geschaffen worden an Modellvorhaben, auch in der Zuständigkeit und mit Unterstützung des Bundesministeriums für Wirtschaft und Technologie, aber das ist sicher ein Feld, das noch weiter ausbaufähig ist.

Zu beachten ist auch der Ausgleich der Datenschutz- und Verbraucherschutzinteressen von

Anwendern, Bürgern und Kunden: Der ist bislang unzulänglich. Hier wäre gegebenenfalls ein breiterer, moderierter Diskurs zu strittigen Fragen denkbar. Dieser wurde zwar inzwischen in Ansätzen begonnen, aber wir denken, dass da auch in der nächsten Zeit reichlich Diskussionsbedarf fortbesteht bzw. sich neu entwickeln wird und insofern auch Klärungsbedarf vorhanden ist.

Und viertens werden die Modifizierung der Entsorgungs- und Wiederverwertungsprozesse mit Blick auf den erwarteten Masseneinsatz von RFID und gleichzeitig die Entwicklung von umweltverträglicheren Lösungen als offene Punkte gesehen.

Was sind nun die Auswirkungen des ubiquitären Computings?

Die augenfälligste Wirkung liegt sicher im Bereich der Privatsphäre, über die in anderem Zusammenhang zuvor bereits intensiv diskutiert worden ist. Es geht um die Frage der informationellen Selbstbestimmung. Beide erfahren im Lichte der Allgegenwärtigkeit von Daten und Datenverarbeitung eine Neudefinition. Auch hierzu bieten sich in gewisser Weise verstärkte Aktivitäten an.

Einmal geht es um die Anpassung des Datenschutzrechts an die Möglichkeiten des ubiquitären Computings zur Überwachung und zur Gewinnung personenbezogener Daten. Dann wird in der Literatur das Fehlen eines Arbeitnehmerdatenschutzes beklagt. Und drittens ein gesellschaftlicher Diskurs über die Entstehung und Nutzung von Datenspuren im ubiquitären Computing gefordert. Es geht dabei insbesondere um die Datensparsamkeit und Datenvermeidung und Autonomie über die Daten. Und viertens spielt eine systematische Beobachtung und Bewertung von neuen Technologien sowie deren Wirkung auf die informationelle Selbstbestimmung eine besondere Rolle.

Darüber hinaus ist die gesellschaftliche Kompatibilität am besten anhand konkreter Beispiele zu diskutieren. Der Zugang zu neuen Angeboten und die Teilhabe daran sind dabei ebenso wichtig, wie Fragen der Systemabhängigkeit und Entziehbarkeit, des Kontrollverlustes, der Überwachung, sowie verhaltensnormierende Wirkungen.

Konkrete Ansatzmöglichkeiten bestehen in zwei Punkten. Einmal in der frühzeitigen Berücksichtigung von Nutzerinteressen im Entwicklungsprozess. Das könnte z. B. im Rahmen von ethnografischen Studien, sog. „living labs“ geschehen. Und zweitens die Schaffung von tatsächlichen Wahlmöglichkeiten durch Kennzeichnung von UbiComp-Systemen und Etablierung eines Opt-in-Modells, bei dem die Nutzung bestimmter Funktionen explizit bestätigt werden muss. Soweit in aller gebotenen Kürze.

Vorsitzender: Herr Zoche, vielen Dank für die Einführung. Es ist sicher für Sie jetzt keine besonders komfortable Situation dadurch entstanden, dass wir durch die vorhergehenden Punkte etwas in zeitlichen Verzug geraten sind, aber Sie sollten auf jeden Fall die Möglichkeit erhalten, angemessen in das Thema einzuführen, was Ihnen gelungen ist. Ich schlage aus Zeitgründen vor, es bei einer Fragenrunde zu belassen. Frau Kollegin Zypries hat die erste Frage.

Abg. Brigitte Zypries (SPD): Vielen Dank für den umfänglichen Vortrag. Haben Sie zu dem ubiquitären Computing eigentlich Erkenntnisse aus anderen Staaten und wissen Sie, ob es da spezielle rechtliche Regelungen dazu gibt?

Vorsitzender: Wir sammeln erst einmal, würde ich vorschlagen. Herr Jarzombek, bitte.

Abg. Thomas Jarzombek (CDU/CSU): Es ist sicherlich undankbar, ein derart kompliziertes und zukunftsträchtiges Thema zugleich in der Kürze der Zeit zu diskutieren. Ich möchte eine Frage und eine Überlegung mit auf den Weg geben. Sie haben angesprochen, dass das zentrale Thema am Ende wohl wieder Datenschutz und Privatsphäre sein werden. Ich glaube allerdings nicht, dass man bei der Dynamik der Entwicklung, die hier auch festgestellt worden ist, alles auf gesetzgeberische Weise lösen können. Es gibt ja auch andere Politikfelder, in denen das Mittel der regulierten Selbstregulierung ganz gut funktioniert, indem man eine Art Selbstkontrolle einführt. Wenn man beispielsweise RFID im Handel einsetzen möchte und sich vorstellt, dass man die Tags auch deaktivieren können soll – was ja immer eine Voraussetzung ist, die da auch auf dem Weg gegeben ist – und sich dann möglicherweise z. B. Wartezeiten entwickeln und jemand letztendlich definieren muss, was angemessen ist. Da würde mich schon interessieren, ob ein solcher Versuch mit einer regulierten Selbstregulierung über Selbstkontrollen, schon mal angedacht oder diskutiert wurde, und ob Sie den Weg für gangbar halten.

Vorsitzender: Als Nächste habe ich auf der Rednerliste Frau Dr. Sitte.

Abg. Dr. Petra Sitte (DIE LINKE.): Als der Untersuchungsauftrag gegeben wurde, ist man davon ausgegangen, dass sich das in den nächsten Jahren rasant entwickeln würde. Offen scheint mir, ob sich die Erwartungen in jeder Hinsicht erfüllt haben. Wenn man den Bericht liest, wird einem irgendwie unwohl, weil man sich – und Sie beschreiben das ja auch anschaulich – zunehmend weniger all den Möglichkeiten wie Profilbildung und Kontrolle entziehen kann. Ich habe gerade jüngst so ein Beispiel in einer Diskothek erlebt, als junge Leute, kaum dass sie den Eingang hinter sich gelassen haben, am Tresen mit dem Namen angesprochen werden und die Servicekräfte sehen konnten, wie oft die Gäste bereits dort waren, was sie am Liebsten trinken, wie alt sie sind und so weiter. Höchst persönliche Daten, die aufgrund des eingesetzten Systems verfügbar waren. RFID-Chips sind ja nur das eine Potenzial. Das andere sind ja ohnehin alle Möglichkeiten – auch technischer Art – Kleinstcomputer zu vernetzen. So spannend und so zukunftsträchtig das auch für bestimmte Bereiche wie beispielsweise die Medizin sein mag, aber wie gesagt, was mich interessiert, ist die Einschätzung hinsichtlich der Entwicklungsgeschwindigkeit dieser Technologien.

Abg. Jimmy Schulz (FDP): Einerseits ist eine Entwicklung in dem Bereich festzustellen, die viele Chancen bietet, aber natürlich eine ganze Reihe von Herausforderungen mit sich bringt, denen wir uns stellen müssen. Natürlich wollen wir alle an dieser Entwicklung teilhaben und wir wollen auch, dass sie in allen möglichen Bereichen zum Einsatz kommt. Aber, und das halte ich für einen wichtigen Punkt,

die Wahlfreiheit, die Selbstbestimmung, sich darauf einzulassen, die müssen wir den Bürgerinnen und Bürgern zubilligen, das ist meine feste Überzeugung – auch sich zu verweigern und zu sagen „Ich will das nicht.“ Hierzu interessiert mich Ihre Einschätzung.

Vorsitzender: Eine Frage von Herrn Schipanski.

Abg. Tankred Schipanski (CDU/CSU): Ja, eine ganz konkrete Frage: Und zwar haben Sie von Standardisierung gesprochen, die notwendig ist, damit wir die prognostizierten erheblichen wirtschaftlichen Potenziale nutzen können. Denken Sie, dass es klug ist, in dem Bereich gesetzgeberisch tätig zu werden? Oder ist es besser – wie wir es beim digitalen Fernsehen ähnlich hatten – das über den Markt sich regulieren zu lassen? Es bliebe offen, welche Technologie bzw. welcher Standard sich durchsetzt. Das würden wir als Gesetzgeber praktisch nicht stärker beeinflussen.

Vorsitzender: Ich würde vorschlagen, dass wir in die Beantwortung gehen. Herr Zoche, bitte.

Peter Zoche (Fraunhofer-Institut für System- und Innovationsforschung): Die Standardisierungsfrage von Herr Schipanski: Man muss, glaube ich, unterscheiden, um welche Fragen der Standardisierung es geht. Wenn es z. B. um Fragen der Frequenzzuweisung oder dergleichen geht, ist der Staat von vornherein gefordert. Und da kann er zusammen mit den Unternehmen in dem föderalen System und eventuell auch auf europäischer Ebene eine ausgleichende Rolle mit übernehmen, die sicher förderlich ist, um eine Frequenzharmonisierung und Nutzungsharmonisierung geeigneter Frequenzen herbeizuführen. Zum anderen denke ich, dass der Staat eventuell initiativ tätig werden kann, um solche Standardisierungsbemühungen deutlich werden zu lassen, die ja zum Teil durchaus auch im nationalen wirtschaftlichen Interesse bestehen und nicht nur im Interesse eines einzelnen Herstellers. Aber wenn ich das im Moment so richtig beobachte, haben sich bis zur Abgabe der Studie eigentlich die entscheidenden Initiativen herausgebildet, um Standardisierungsprozesse in Gang zu setzen. Ich sehe, dass mir der Vertreter der Bundesregierung beipflichtet.

Die Wahlfreiheit, ist sie realistisch, Herr Schulz? Auch da muss man unterscheiden. Es gibt wahrscheinlich Beispiele, wie das von Frau Sitte mit der Diskothek, wo in einer Grauzone eventuell bestimmte – auch persönliche – Daten, Nutzungsgewohnheiten und dergleichen genutzt werden und Betroffene sich eventuell über die Tragweite dessen nicht immer im Klaren sind und vielleicht auch nicht im Klaren darüber, ab welchem Punkt das vielleicht irgendwann unangenehm werden könnte. Also, da ist sicher eine gewisse Beobachtung erforderlich, eventuell auch eine intensivere Verbraucheraufklärung und ein Diskurs mit den Verbrauchern darüber, was möglich und gewünscht ist. Es gibt andererseits auch in Betrieben Möglichkeiten, bei der Herstellung von Produkten oder Dienstleistungen Prozesse individuell auf einen bestimmten Arbeitnehmer zurechenbar zu machen in einer Weise, wie wir sie bisher noch nicht kennen. Da können sich Arbeitnehmer kaum entziehen nach dem jetzigem Recht, da sie als Arbeitnehmer in die betriebliche Ordnung eingebunden sind und

eigentlich keine tatsächliche Wahlfreiheit haben. Das sind auch Punkte in der juristischen Debatte, die im Hinblick auf die technischen Entwicklungen genauer betrachtet werden sollten mit Blick auf eventuelle neue Lösungen, oder Konkretisierungen bestehender rechtlicher Regelungen, die geeignet wären, das Persönlichkeitsrecht im betrieblichen Umfeld so zu stärken, dass es künftigen technischen Möglichkeiten des ubiquitären Computings präziser entspricht.

Hinsichtlich der Frage der Entwicklungsgeschwindigkeit glaube ich, haben wir generell immer zwei widersprüchliche Entwicklungen zu beobachten. Zunächst ist da die Marktdurchdringung, die mit einem gewissen Heilsversprechen, mit einer teils enormen Euphorie und auch visionären Kraft beschrieben wird von den Entwicklern und anderen Akteuren. Allerdings werden nur allzu oft die Randbedingungen, unter denen sich eine gedeihliche Entwicklung vollziehen kann, übersehen, ob das jetzt datenschutzrechtliche Anforderungen sind oder ob das der Bedarf von Anwendern ist, der auch erst einmal erschlossen werden muss und dessen konkreter Nutzen individuell angezeigt und erfahrbar gemacht werden muss. Es sind im Grunde naheliegende Dinge, die vielfach übersehen werden und deshalb verlaufen solche Innovationsprozesse nicht selten viel langsamer als erwartet. Es wird häufig auch nicht daran gedacht, dass es ja nicht nur um ein einzelnes Produkt geht, sondern dass es um höchst widersprüchliche Akteure auch auf der wirtschaftlichen Seite geht. Wenn es um einen Electronic Product Code geht: Da sind eben unterschiedliche Interessen bei großen Herstellern, Handelskonzernen oder kleinen mittelständischen Unternehmen vorhanden. Und nicht alle Vorteile einer Technologie sind deckungsgleich unter den Akteuren. Also, von daher kommt häufig Sand in das Getriebe. Das ist ja in verschiedenen Studien auch zutreffend beschrieben worden und ist eigentlich bekannt. Die RFID-Technologie entwickelt sich in der Anwendung vielleicht nicht so rasant, insbesondere im privaten Bereich, wie von manchen erhofft und prognostiziert. Gleichwohl gibt es sehr eindrucksvolle Beispiele, wie Hersteller mit dieser Technologie und dem Technologieeinsatz experimentieren und über dieses Experimentierstadium mittlerweile hinaus gekommen sind, Pilotprojekte abschließen und in die klassische Produktionsphase hineingeraten, in denen sie diese Chips nutzen; beispielsweise die großen Hersteller in der deutschen Automobilindustrie oder Fraport, um nur einige wenige zu nennen.

Was die Frage nach der regulierten Selbstregulierung angeht, so muss ich sagen, dass wir uns etwas schwer mit der Einschätzung tun, weil wir weitgehend keine Juristen bei uns im Haus sind. Trotzdem scheint es uns nicht abwegig, dass es ein Weg sein könnte, genau in diese Richtung der regulierten Selbstregulierung zu gehen, für die sich Prof. Dr. Wolfgang Hoffmann-Riem ja auch ausgesprochen hat. Wir schlagen vor, dass man diese rechtlichen Gesichtspunkte mit Blick auf das ubiquitäre Computing noch einmal genauer im Detail betrachten sollte.

Frau Zypries, zum Schluss zu Ihrer Frage, ob es Gesetze in anderen Ländern gibt, die Fragen des ubiquitären Computings regeln. Ich bin da wirklich überfragt. Wir haben zwar international geschaut, welche typischen Entwicklungen vonstatten gehen. Beispielsweise kann man in Japan eine starke Orientierung am Endverbraucher feststellen. In den USA sind Chips teilweise zur Qualitätssicherung von Produkten vorgeschrieben (z. B. bei einzelnen Medikamenten). Doch spezifische gesetzliche

Regelungen anderer Länder, über die vorhin debattiert wurde, waren nicht Untersuchungsgegenstand.

Vorsitzender: Herr Zoche, ich danke für die Beantwortung der Fragen auch hier im Namen der Kolleginnen und Kollegen im Unterausschuss. Danke, dass Sie sich die Zeit genommen haben, uns in den Bericht und das Thema einzuführen.

Der Unterausschuss empfiehlt einvernehmlich Kenntnisnahme.

Tagesordnungspunkt 2b

Unterrichtung durch die Bundesregierung

Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie

BT-Drucksache 16/7891

Der Unterausschuss empfiehlt einvernehmlich Kenntnisnahme.

Tagesordnungspunkt 5

Verschiedenes

Vorsitzender: Ich möchte noch den Ausblick geben auf die weitere Sitzungsterminierung, was den Unterausschuss angeht. Die Obleute haben beschlossen, dass am 28. Juni zunächst ein Obleutegespräch stattfindet. Wir haben das Angebot vom Bundesjustizministerium, dass die Mitglieder des Unterausschusses Neue Medien an einer Anhörung mit externen Experten zum Thema Leistungsschutzrecht teilnehmen können. Das stieß bei den Obleuten von allen Fraktionen auf großes Interesse. Die Anhörung findet statt im Zeitfenster von 10 bis 15 Uhr. Deshalb können wir die nächste Sitzung des Unterausschusses noch nicht konkret terminieren, da wir auch abwarten müssen, wie sich in dieser Woche aufgrund der Bundesversammlung der gesamte Ablauf für die Gremien ändern wird. Wenn es Ihrerseits keine weiteren Anmerkungen zum Punkt „Verschiedenes“ gibt, danke ich für die rege Teilnahme und schließe die Sitzung.

Schluss der Sitzung: 14:50 Uhr

Sebastian Blumenthal, MdB
Vorsitzender