Deutscher Bundestag **Protokoll Nr. 17/15**
17. Wahlperiode

Unterausschuss Neue Medien (22)
Wortprotokoll*
15. Sitzung

Berlin, den 24.10.2011, 13:00 Uhr
Sitzungsort: Paul-Löbe-Haus
Konrad-Adenauer-Straße 1
10557 Berlin
Sitzungssaal: E.800

Vorsitz: Sebastian Blumenthal, MdB

TAGESORDNUNG:

Öffentliches Expertengespräch zum Thema „Datensicherheit bei Facebook und anderen sozialen Netzwerken in Anbetracht einer Entschließung der Datenschutzbeauftragten der Länder und des Bundes“

Experten:

Richard Allan, Facebook, Director EU-Policy, Dublin
Per Meyerdierks, Google Germany GmbH, Datenschutzbeauftragter, Hamburg
Peter Schaar, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn
Dr. Thilo Weichert, Der Landesbeauftragte für den Datenschutz Schleswig-Holstein, Kiel

* Redaktionell überarbeitete Bandabschrift

Anwesenheitsliste*

Mitglieder des Ausschusses

Ordentliche Mitglieder des Ausschusses	Stellvertretende Mitglieder des Ausschusses
CDU/CSU	
Brandl, Dr. Reinhard	
Jarzombek, Thomas	
Selle, Johannes	
Wanderwitz, Marco	
SPD	
Dörmann, Martin	Özoğuz, Aydan
Klingbeil, Lars	
Zypries, Brigitte	
Reichenbach, Gerold a. G.	
FDP	
Blumenthal, Sebastian	
Schulz, Jimmy	
DIE LINKE.	
Behrens, Herbert	
Sitte, Petra, Dr.	
BÜNDNIS 90/DIE GRÜNEN	
	Notz, Konstantin von, Dr.

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

Bundesregierung

Bender	BMWi
Batt	BMI
Maiwald	BMI
Neumann	BMJ
Ewe	BMELV
Maass	BMWi
Altmeppen	BMWi
Schwarz	BMWi

Bundesrat

Ommen	LV Niedersachsen
Denove	LV Bayern

Fraktionen und Gruppen

Tigges	SPD
Fröhlich	DIE LINKE.
Frey	B90/GRÜNEN
Dobeneck	B90/GRÜNEN
Scheele	DIE LINKE.
Leberl	CDU/CSU
Kühnau	CDU/CSU
Grünhoff	FDP
Göllnitz	FDP

Öffentliches Expertengespräch zum Thema „Datensicherheit bei Facebook und anderen sozialen Netzwerken in Anbetracht einer Entschließung der Datenschutzbeauftragten der Länder und des Bundes“

Der Vorsitzende: Meine Damen und Herren, ich darf Sie bitten, die Plätze einzunehmen und eröffne hiermit die 15. Sitzung des Unterausschusses Neue Medien. Wir haben heute ein Expertengespräch zum Themenschwerpunkt „Datensicherheit bei Facebook und anderen sozialen Netzwerken“. Ich beginne mit einigen formalen Erläuterungen, bevor wir in die eigentliche Sitzung eintreten. Zunächst zwei erfreuliche Ereignisse. Wir hatten zwei Kollegen aus diesem Kreis, die vor Kurzem ihr Wiegenfest feiern durften. Im Namen der Kolleginnen und Kollegen aus dem Unterausschuss darf ich zum einen Marco Wanderwitz nachträglich zum Geburtstag gratulieren und zum anderen Jimmy Schulz, der vorgestern Geburtstag hatte. Auch hier noch einmal herzlichen Glückwunsch im Namen der Kolleginnen und Kollegen des Unterausschusses zu diesem außerordentlich erfreulichen Ereignis.

Wir haben uns für die heutige Sitzung ein Zeitfenster von 90 Minuten vorgenommen. Den Ablauf werden wir so gestalten, dass zunächst die Sachverständigen jeweils Eingangsstatements von zirka drei Minuten halten. Anschließend, bevor wir in die Fragerunden eintreten, werden wir auch die Vertreter der Bundesregierung zu dem Themenschwerpunkt um Eingangsstatements bitten, damit wir bereits zu Beginn ein möglichst breites Spektrum abdecken können.

Die Übertragung der Sitzung, die heute zeitgleich stattfindet, läuft über Livestream unter www.bundestag.de, und wird als Aufzeichnung später in der Mediathek des Deutschen Bundestages verfügbar sein. Das Wortprotokoll der heutigen Sitzung, das unter anderem nach Übersetzung der englischsprachigen Teile von den Sachverständigen freizugeben ist, wird der Öffentlichkeit ebenfalls im Nachgang zu der heutigen Sitzung im Internet zugänglich gemacht werden.

Meine Damen und Herren, im Unterausschuss Neue Medien haben wir als mitberatendes Gremium zu anderen Fachausschüssen immer wieder Vorlagen und Gesetzesinitiativen auf der Agenda. Zu Beginn der Wahlperiode haben wir aber auch interfraktionell vereinbart, uns vorzubehalten, zu tagesaktuellen Themen im Wege der Selbstbefassung Expertenanhörungen und Expertengespräche durchzuführen. Der heutige Themenschwerpunkt „Datensicherheit und Datenschutz in sozialen Netzwerken“ gehört dazu. Und es gibt dafür einen ausgesprochen aktuellen Hintergrund. Wir möchten mit dem Gremium einen Beitrag dazu leisten, aktuelle Themen in die parlamentarische Debatte im Deutschen Bundestag zu tragen.

In die heutige Sitzung haben wir insgesamt vier Sachverständige bzw. vier beteiligte Parteien geladen. Ich stelle sie kurz alphabetisch vor: Zum einen Facebook, das vertreten ist durch Herrn Richard Allan, Director EU-Policy und in dieser Funktion auch ranghöchster Ansprechpartner von Facebook in Europa.

Herzlich willkommen, Herr Allan, hier im Unterausschuss. Wir haben ferner Vertreter von Google eingeladen, gerade im Hinblick auf Google+ als Angebot im Bereich der sozialen Netzwerke. Uns wurden zwei Vertreter benannt, die für Fragen zur Verfügung stehen. Das ist einmal Herr Per Meyerdierks, Datenschutzbeauftragter für Google Deutschland, und dann noch Herr Jan Kottmann, der ggf. zu weiteren Themen, die nicht unmittelbar den Datenschutzaspekt berühren, antworten kann. Wir haben als Sachverständigen von Seiten der beteiligten Datenschützer Herrn Peter Schaar, den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, eingeladen. Herr Schaar, herzlich willkommen im Unterausschuss Neue Medien. Sie werden flankiert vom Datenschutzbeauftragten des Landes Schleswig-Holstein, Herrn Dr. Thilo Weichert. Da gab es ja in der letzten Zeit, insbesondere mit Facebook, einen, sagen wir, intensiven Austausch von Positionen und Informationen. Das Ganze wird möglicherweise heute hier fortgeführt. Wir sind schon sehr gespannt.

Abschließend möchte ich noch die Vertreter der beteiligten Ministerien begrüßen. Wir haben aus dem Bundesministerium des Innern Herrn Abteilungsleiter Hans-Heinrich von Knobloch heute hier und ihn begleitend den IT-Direktor, Herrn Peter Batt. Ich begrüße ferner von Seiten des Bundeministeriums für Ernährung, Landwirtschaft und Verbraucherschutz Herrn Abteilungsleiter Dr. Christian Grugel. Auch Sie sind uns herzlich willkommen.

Ausgangspunkt der heutigen Sitzung zu dem Thema „Datensicherheit in sozialen Netzwerken“ ist nicht nur die öffentliche Debatte, sondern unter anderem auch die Arbeit der Datenschutzbeauftragten der Länder und des Bundes. Diese haben auf ihrer 82. Konferenz am 28. und 29. September 2011 in München ein Thesenpapier verfasst mit dem Titel „Datenschutz bei sozialen Netzwerken jetzt verwirklichen“. Wir hatten an alle Sachverständigen die Bitte gerichtet, vorab einen Fragenkatalog zu beantworten. Hier nur der Information halber der Hinweis, dass wir bislang lediglich einen Rücklauf haben. Insofern, Herrn Dr. Thilo Weichert, besonderen Dank für die Fleißarbeit, denn er hat den Fragenkatalog beantwortet. Die Antwort liegt hier auch aus. Die anderen Sachverständigen bitte ich, die Fragen, die wir an sie gerichtet haben, im Rahmen der Eingangsstatements zu thematisieren, damit wir auf der Grundlage dieser Punkte in die Thematik einsteigen können.

Die Fragerunden werden nachher so ablaufen, dass wir gemäß der Größenverhältnisse der Fraktionen vorgehen. An alle Beteiligten jetzt schon die Bitte, sich kurz, präzise und prägnant zu fassen, damit wir umso mehr Möglichkeiten haben, Fragen zu stellen. Das Prozedere sieht so aus, dass bitte eine Frage an zwei Sachverständige oder zwei Fragen an einen Sachverständigen gerichtet werden, damit wir eine Struktur in die Fragerunden bekommen. Soweit der Vorrede. Ich bitte darum, nun mit den Eingangsstatements zu beginnen. Von Seiten der Fraktionen war der Wunsch geäußert worden, dass Herr Dr. Thilo Weichert beginnen möge. Anschließend dann Herr Schaar. Ich bitte deshalb Herrn Dr. Weichert um sein Eingangsstatement.

Dr. Thilo Weichert (Der Landesbeauftragte für den Datenschutz Schleswig-Holstein, Kiel): Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren Abgeordnete. Vielen Dank für die

Einladung. Ich hoffe, dass unsere schriftliche Stellungnahme nicht nur eine Fleißarbeit war, sondern hinreichend Qualifikation aufweist, um sich mit dem Thema auseinanderzusetzen. Ich darf mich bzw. das Unabhängige Landeszentrum für Datenschutz kurz vorstellen. Das ULD ist die Datenschutzaufsichtsbehörde für Schleswig-Holstein. Wir haben, nachdem wir eine Vielzahl von Anfragen und Beschwerden bekommen hatten, eine technische Prüfung von Insight, der Webanalyse von Facebook, vorgenommen, die insbesondere dann ausgelöst wird, wenn Fanpages oder so genannte Social Plugins genutzt werden, wie der „Gefällt mir"-Button. Auf der Basis dieser Analyse haben wir am 19. August 2011 die Öffentlichkeit über unsere Ergebnisse informiert und festgestellt, dass die beiden Angebote Fanpages und Social Plugins weder mit dem deutschen noch dem europäischen Datenschutzrecht in Einklang zu bringen sind. Wir haben folglich die Website-Betreiber aufgefordert, in Bezug auf Schleswig-Holstein, für das wir ausschließlich zuständig sind, entsprechende Anwendungen bis Ende September 2011 abzustellen. Im Oktober haben wir dann eine kleine Zahl von öffentlichen und privaten Stellen aufgefordert, schriftlich dazu Stellung zu nehmen, weshalb von ihnen Social Plugins und Fanpages weiterbetrieben werden. Dazu gehörten u.a. die Industrie- und Handelskammer Schleswig-Holstein und die Staatskanzlei des Landes Schleswig-Holstein. Da die Frist noch bis Ende Oktober läuft, haben wir dazu bis heute auch noch keine Stellungnahme erhalten. Von einigen der Adressaten haben wir allerdings in der Zwischenzeit das Signal bzw. die Umsetzung, die jeweilige Anwendung abzuschalten.

Für November 2011 plant das ULD eine weitere Eskalation. Wenn die Anwendungen bis dahin nicht abgeschaltet sein sollten, werden wir entsprechende Sanktionen aussprechen. Anders als das mancherorts dargestellt wird, werden wir aber keine Bußgelder erlassen, sondern unser Ziel ist eine verwaltungsgerichtliche Klärung, weil diese im Vergleich zu einem Bußgeldverfahren eine höhere Verbindlichkeit haben würde. Wir führen parallel dazu Gespräche mit Facebook, mit der Staatskanzlei Schleswig-Holstein, der Industrie- und Handelskammer sowie dem Verein „Digitale Wirtschaft in Schleswig-Holstein". Diese Gespräche finden zwar in einer freundlichen Atmosphäre statt, sind aber bisher leider ohne Ergebnis geblieben. Nach unserer Überzeugung sind die Zustände, die wir derzeit bei sozialen Netzwerken – insbesondere von US-Anbietern – haben, rechtswidrig und nicht zu halten. Es folgt daraus, insbesondere gegenüber deutschen Anbietern, auch eine Wettbewerbsverzerrung. Deshalb sind wir der Meinung, dass es dringend notwendig ist, die notwendigen Klarstellungen herbeizuführen. Dazu dienen die Aktivitäten des ULD. Keine Frage, wir begrüßen als einen möglichen Schritt auch die Selbstverpflichtung. Diese kann im Rahmen von § 38a Bundesdatenschutzgesetz (BDSG) erfolgen, d. h. bei Anbietern, die reguliert sind im Sinne einer Prüfung durch die zuständigen Aufsichtsbehörden. Eine andere Form der Selbstregulierung kann darin bestehen, dass die sozialen Netzwerke ihre Anwendungen zertifizieren lassen. Das ULD bietet solche Zertifizierungen sowohl nach europäischem als auch nach deutschem Recht an. Soweit erst einmal eingangs. Vielen Dank für Ihre Aufmerksamkeit.

Der Vorsitzende: Hervorragend, drei Minuten auf den Punkt genau, Herr Dr. Weichert, das setzt schon einmal Maßstäbe. Wir fahren fort mit dem Bundesdatenschutzbeauftragten. Herr Schaar. Sie haben das Wort.

Peter Schaar (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn): Vielen Dank, Herr Vorsitzender. Ich möchte zunächst einmal zum grundlegenden Problem des Datenschutzes bei sozialen Netzwerken etwas sagen. Bei sozialen Netzwerken handelt es sich um Dienste, die man üblicherweise als Web 2.0-Dienste bezeichnet. Das heißt, es sind solche, bei denen die klare Trennung zwischen den verschiedenen datenschutzrechtlichen Rollen, die wir klassischerweise in anderen Bereichen haben, nicht mehr so einfach ist: Anbieter, Nutzer und Betroffene, die verschiedenen Rollen können sich überschneiden. Die Nutzer sind zugleich Mitglieder und können Inhalte publizieren, für die sie selbst die Verantwortung tragen. Andererseits sind sie aber auch Betroffene der Datenverarbeitung, weil im Hinterzimmer der Netzwerke, ich nenne das mal so, im technischen Umfeld natürlich eine Vielzahl von personenbezogenen Daten verarbeitet werden, die eben von den Betroffenen selbst nicht eingestellt wurden. Um diese Daten geht es hier in erster Linie, die so genannten Nutzungsdaten. Diese sind deshalb von besonderem Interesse, weil sie über das publizierte Maß hinaus Einblick geben in persönliche Interessen, in Beziehungen und Verhaltensweisen. Deshalb sind diese Daten, insbesondere wenn sie mit den Inhalten, die die Nutzer selbst einstellen, verknüpft werden, besonders sensibel.

So lässt sich zum Beispiel aus dem persönlichen Umfeld eines Betroffenen und seinem Clickstream sehr viel herauslesen und zwar auch hinsichtlich der Angaben, die er bewusst nicht über sich veröffentlich hat. Zum Beispiel über seine Religionszugehörigkeit, seine politischen Interessen oder seine sportlichen Aktivitäten. Auch wenn das nicht im Profil des Nutzers steht und insofern nicht von ihm veröffentlicht wurde, lässt sich aus diesen bei der Nutzung nebenbei anfallenden Daten so manches extrahieren. Deshalb ist es um so wichtiger, dass die datenschutzrechtlichen Regelungen hier auch eingehalten werden. Das gilt insbesondere für die so genannte Profilbildung. Für diese ist eine ausdrückliche Einwilligung des Betroffenen erforderlich, wenn sie personenbezogen stattfindet. Findet sie per Pseudonym statt, das ist aber bei Facebook und vergleichbaren Plattformen nicht der Fall, würde eine Information mit einem Opt out ausreichen. Bei der personalisierten Profilbildung braucht man dagegen eine ausdrückliche Einwilligung. Ich habe eine solche nirgendwo in den Nutzungsbedingungen sehen können, wo nur mitunter sehr allgemeine Umschreibungen stehen. Ich kann nicht bestätigen, dass das eine Rechtsgrundlage für eine Profilbildung wäre.

Ich möchte nun noch kurz zu den von Ihnen zum Anlass dieser Anhörung genommenen Konfliktfeldern etwas sagen. Bei den ‚Gefällt mir"-Buttons stimme ich dem ULD Schleswig-Holstein vollständig zu, dass diejenigen, die auf Websites „Gefällt mir"-Buttons anbringen – ich meine jetzt nicht die auf Facebook, sondern die, die auf externen Websites angebracht werden – datenschutzrechtlich die Verantwortung dafür tragen, mithin die Stelle, die die Website betreibt. Das kann zum Beispiel bei einer Handelskammer oder auch einem Bundesministerium der Fall sein, und dementsprechend muss auch dafür gesorgt werden, dass die einschlägigen datenschutzrechtlichen Vorgaben eingehalten werden.

Hinsichtlich der Fanseiten bin ich noch nicht zu einem endgültigen Ergebnis gekommen. Ich frage mich, ob die bisherige Konstruktion, die wir bei Website-Betreibern üblicherweise zugrundelegen, nämlich

einem Auftraggeber- und Auftragnehmerverhältnis, wie vom ULD angenommen, hier vorliegt, da es sich um eine besondere Art von interaktiven Diensten handelt. Außer Frage steht für mich aber, dass es auch eine datenschutzrechtliche Verantwortung derjenigen gibt, die eine Fanpage betreiben. Zum Beispiel, wenn eine Krankenkasse eine Fanpage unterhält und dazu animiert, dort Fragen in Bezug auf Krankheiten, Ärzte und mögliche Therapien einzustellen und für alle Nutzer öffentlich nachvollziehbar unter dem Namen diskutieren zu lassen. Wenn man dazu einlädt, dann trägt man meines Erachtens auch ein Stück weit eine Verantwortung. Ich möchte es hiermit erst einmal bewenden lassen, weil meine Zeit schon vorüber ist.

Der Vorsitzende: Vielen Dank, Herr Schaar. Wir fahren fort mit Google. Herr Meyerdierks wird das Eingangsstatement halten. Noch einen Hinweis. Für den englischsprachigen Redebeitrag von Herrn Allan haben wir eine Simultanübersetzung. Wählen Sie bitte Kanal 2 für Deutsch.

Per Meyerdierks (Google Germany GmbH, Datenschutzbeauftragter, Hamburg): Vielen Dank, Herr Vorsitzender, vielen Dank, meine Damen und Herren Abgeordnete für die Einladung, dass wir heute hier zu diesem Thema sprechen können. Es handelt sich bei den Themen, die wir heute besprechen, sicherlich nicht um rein US-amerikanische Themen bzw. Themen, die US-amerikanische Firmen ausschließlich betreffen. Das hat Herr Dr. Weichert auch anfangs bereits klargestellt. Gleichzeitig handelt es sich insbesondere bei den Social Plugins, die angesprochen wurden, wie dem „Gefällt mir“-Button oder dem „+1“-Button, auch nicht um Fragen, die für derartige Plugins spezifisch wären. Vielmehr geht es bei den Fragen, die angesprochen werden im Zusammenhang mit Social Plugins, um Fragen, die die Einbindung jedweder Drittinhalte auf einer Website betreffen. Denn eine solche Einbindung führt stets zu einer Übertragung von Daten und ist im Internet allgegenwärtig. Ich glaube, es ist ganz wichtig, sich diesen Umstand klarzumachen.

Und dennoch stehen US-amerikanische Anbieter bzw. global operierende Internetanbieter, insbesondere soziale Netzwerke, vor einer besonderen Herausforderung im Hinblick auf den Datenschutz. Sie bedienen eine globale Nutzerschaft, die aus unterschiedlichen Ländern kommt, dennoch aber auf ein und derselben Plattform miteinander interagiert und kommunizieren möchte. Deshalb ist es notwendig, dass die Plattform technisch gesehen einheitlich gestaltet ist. Gleichzeitig sehen sich Betreiber solcher Plattformen verschiedenen Rechtsordnungen mit unterschiedlichen Datenschutzregelungen gegenüber, welche nebeneinander Geltung beanspruchen. Das ist eine Konstellation, die wir im Internet bei international operierenden Diensten sehr häufig antreffen.

Im Bereich des Datenschutzes ist es daher aus der Perspektive von Google und auch nach meiner Ansicht von enormer Bedeutung, den Nutzer ins Zentrum der Überlegungen bezüglich des Datenschutzes zu stellen. Für ihn muss Transparenz geschaffen werden darüber, wie Daten verarbeitet werden. Dem Nutzer müssen Mittel an die Hand gegeben werden, um Entscheidungen bezüglich der Datenverarbeitung zu treffen. Das heißt, die Transparenz und die Kontrollmöglichkeiten sind

entscheidend, um einen Datenschutz, der unterschiedlichen Vorstellungen in verschiedenen Ländern gerecht werden soll, auf einer einheitlichen Plattform zu realisieren.

Google hat für seine Dienste von Anbeginn an auf diese beiden Säulen des Datenschutzes gesetzt: Transparenz und Kontrollmöglichkeiten. Insbesondere gilt das für das noch recht junge Netzwerk Google+, welches erst seit drei Wochen in einer öffentlichen Beta-Version zur Verfügung steht. Dort war es von vornherein im Design- und im Entwicklungsprozess ein zentraler Bestandteil, die beiden Aspekte des Datenschutzes zu gewährleisten. Es würde mich freuen, später auf Einzelheiten noch eingehen zu können. Vielen Dank.

Der Vorsitzende: Vielen Dank, Herr Meyerdierks. Von Seiten der Sachverständigen schließt Herr Richard Allan. Bitteschön.

Richard Allan (Facebook, Director EU-Policy, Dublin): Vielen Dank, Herr Vorsitzender. Zunächst möchte ich Ihnen für die Einladung danken und Ihnen zu dieser sehr wichtigen und zeitnahen Anhörung heute vor einem "ausverkauften Haus" gratulieren. Ich bin beindruckt, wie viel Aufmerksamkeit diesem Ausschuss bei Debatten um Technologiefragen zuteil wird und kann Ihnen nur wünschen, dass all Ihre Sitzungen so gut besucht sind.

In meinen einführenden Bemerkungen möchte ich kurz drei Punkte ansprechen und dafür die Fragen aufgreifen, die Sie uns freundlicherweise bereits im Vorfeld haben zukommen lassen. Dann möchte ich Ihnen gerne weiteres Material präsentieren, das ich mitgebracht habe, insbesondere bezüglich unserer Reaktion auf den Bericht des ULD. In Absprache mit dem ULD haben wir entschieden, es der Öffentlichkeit zugänglich zu machen, und ich werde Sie hierzu gerne aufgrund Ihrer Fragen näher informieren.

Bei den drei Punkten, die ich eingangs erwähnte, möchte ich zunächst über zwei Probleme und dann über einen möglichen Lösungsansatz sprechen. Die Probleme liegen zum einen im ULD-Bericht an sich begründet. Ich denke, es ist kein Geheimnis, dass wir große Teile des Materials, das dort verwendet wird, zurückweisen – insbesondere wenn Annahmen über mögliche Verhaltensweisen von Facebook getroffen werden, ohne dass diese stichhaltig nachgewiesen werden. Das trifft ganz besonders auf das entscheidende Thema des Profiling zu. Hier geht der Bericht davon aus, dass Facebook Nutzerdaten zur Erstellung von Nutzerprofilen verwendet. Wir haben ganz klar erklärt, dass wir so etwas nicht machen. Momentan befinden wir uns in einer etwas festgefahrenen Situation: Das ULD hat etwas behauptet und wir haben das zurückgewiesen. Wir möchten gerne eine Möglichkeit finden zu zeigen, dass dies der Fall ist. Genau darum geht es uns bei einer konstruktiven Zusammenarbeit mit dem ULD, sowie darum, Bereiche zu finden, wo wir mehr Transparenz und Entscheidungsfreiheit – auf die wir uns alle, glaube ich, als positive Werte einigen können – schaffen können.

Ich möchte hier noch einmal deutlich machen, dass es nicht darum gehen kann, Sonderlösungen für Schleswig-Holstein zu kreieren. Auch wenn wir die dazu nötigen technischen Mittel hätten, wäre das unserer Meinung nach kein zufriedenstellendes Ergebnis. Vielmehr geht es darum, die Bedenken einer bestimmten Datenschutzbehörde zur Kenntnis zu nehmen und zu sehen, wie wir ihnen mit unserem Produkt Rechnung tragen können. Und ich denke, aus unserer jüngsten Geschichte wird ersichtlich, dass wir genau so mit Datenschutzbehörden auf der ganzen Welt vorgegangen sind, einschließlich der Hamburger Datenschutzbehörde hier in Deutschland. In letzterem Fall haben wir eine Einigung bezüglich des "Freunde-Finden"-Dienstes erzielt, mit dem unsere Nutzer Kontakte importieren können. Darüber hinaus haben wir Änderungen eingeführt, deren Bedeutung eigentlich noch viel weitreichender ist. Wir möchten also gerne weiter gemeinsam mit dem ULD spezifische Fragen aus dem Bericht klären.

Das zweite Problem ergibt sich eigentlich aus dem ersten, denn, wie mein Kollege von Google ganz richtig gesagt hat, einige der Interpretationen – und das haben auch Ihre Fragen noch einmal deutlich gemacht – beziehen sich auf alle nutzergenerierten Internetdienste und möglicherweise sogar auf alle Web-Plugins. Für Firmen und Privatpersonen in Deutschland, die die unter dem Begriff Web 2.0 zusammengefassten Dienste nutzen möchten, stellt es ein viel größeres Problem dar, wenn ihre Möglichkeit dazu rechtlich in Frage gestellt wird – in einer Welt, in der sich ihre Konkurrenten und andere Menschen genau dieser Technologien bedienen. Das ist meiner Meinung nach ein Thema von großer Bedeutung für die Politik und die Öffentlichkeit. Ich bin dem Ausschuss daher sehr dankbar, dass er dies in der heutigen Sitzung berücksichtigt.

Nach diesen Problemen möchte ich nun einige mögliche Lösungsansätze aufzeigen. Nur um das ganz deutlich klarzustellen: Ich bin heute hier als Vertreter von Facebook Ireland Ltd, dem Unternehmen, mit dem die Nutzer des Dienstes in Deutschland einen Vertrag eingegangen sind. Ich fliege unmittelbar nach der Sitzung von hier aus weiter, um bei einem Prüfungsverfahren der Irischen Datenschutzkommission dabei zu sein. Ich halte das für sehr wichtig, weil es aufzeigt, dass die Nutzer von Facebook in Deutschland den Schutz ihrer Daten unter dem EU-Rahmenbeschluss zum Datenschutz und der Auslegung der gemeinsamen Datenschutzrichtlinie im europäischen Recht erfahren. Im Übrigen nehmen Menschen in ganz Europa ihre in der Richtlinie festgelegten Rechte wahr. Wie Sie vielleicht gehört haben, hat sich ein Student aus Wien damit hervorgetan, die ihm in der Richtlinie zugesicherten Rechte auf besonders forsche Art und Weise wahrzunehmen, und hat seine Beschwerden bei der Irischen Datenschutzkommission eingereicht. Wir nehmen diesen Vorgang äußerst ernst und werden dazu der Reihe nach noch Stellung nehmen.

Ich meine also, es ist wichtig zu bedenken, dass wir nicht in einem luftleeren Raum operieren und Firmen wie die unsere nach europäischem Recht bereits eine klar umrissene rechtliche Verantwortung haben. Wir ziehen jedoch zusätzlich Möglichkeiten zur freiwilligen Selbstkontrolle in Betracht, um den speziell in Deutschland angemeldeten Bedenken Rechnung zu tragen. Zudem sind wir der Meinung, dass die Kombination einer allgemeinen Rechtsgrundlage mit einer auf die örtlichen Besonderheiten zugeschnittenen freiwilligen Selbstkontrolle uns alle unserem, wie wir denken, gemeinsamen Ziel ein

gutes Stück näherbringen kann, Einzelpersonen und Organisationen in Deutschland die volle Bandbreite der modernen Internetdienste in Anspruch nehmen zu lassen, und zwar als Bürger, die Teil jener Unternehmen und Organisationen sind, und als Bürger, die solche Dienste nutzen und einen Anspruch darauf haben, dass ihr Recht auf Privatsphäre geschützt wird.

Der Vorsitzende: Soweit zur Einführung. Vielen Dank Herr Allan. Wir fahren fort mit den beteiligten Ministerien auf Ebene der Bundesregierung und ich bitte zunächst um ein Eingangsstatement von Herrn Dr. Grugel, zuständig für den Bereich des Verbraucherschutzes. Bitteschön.

Dr. Christian Grugel (Leiter der Abteilung 2, Verbraucherpolitik, Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz): Vielen Dank, Herr Vorsitzender. Meine sehr geehrten Damen und Herren Abgeordnete. Für immer mehr Menschen sind soziale Netzwerke ein wesentliches Mittel für ihre persönliche Kommunikation. Die hier eingestellten und ausgetauschten Informationen geben häufig tiefen Einblick in die Privatsphäre und in die Persönlichkeit. Daher haben soziale Netzwerke eine große Verantwortung für den Schutz der Privatsphäre. Datenschutzverstöße sind hier besonders gravierend. Deshalb hat auch Bundesministerin Aigner dieses Thema von Anfang an zu einem ihrer Schwerpunkte der Verbraucherpolitik im Internet gemacht. Die öffentliche Debatte bekam durch ihren Austritt aus Facebook deutlichen Rückenwind. Für eine effektive Rechtsdurchsetzung und klare Regelung setzen wir vor allem auf die europäische Ebene. Was wir auf europäischer Ebene regeln können, sollten wir angesichts der globalen Dimension des Internets auch dort regeln. Es gibt, wenn ich das ergänzen darf, keine globalere Einrichtung als das Internet. Unter anderem halten wir klare Löschungsrechte für erforderlich. Es muss die Möglichkeit bestehen, insbesondere selbsteingestellte Informationen, jederzeit endgültig zu löschen. Auch die Prinzipien der datenschutzfreundlichen Voreinstellungen und des Datenschutzes durch Technik, also „Privacy by default“ und „Privacy by design“, sollten verankert werden. Die Selbstregulierung kann eine sinnvolle Ergänzung sein. Voraussetzungen einer wirksamen Selbstregulierung sind unter anderem die effektive Kontrolle und Sanktionierung bei Verstößen sowie die Einbeziehung von Verbraucherverbänden in die Ausgestaltung, wie dies auch bei der aktuell in den USA diskutierten Entwicklung einer Selbstverpflichtung zum Schutz der Privatsphäre im Internet der Fall ist. Eine Selbstverpflichtung muss das geltende Datenschutzrecht konkretisieren bzw. ergänzen. Sie kann dieses selbstverständlich nicht ersetzen. Eine Selbstverpflichtung muss zu konkreten Änderungen in der Ausgestaltung der sozialen Netzwerke führen, soweit diese den Anforderungen nicht entsprechen. Im Übrigen hoffen wir, heute viele gute Anregungen in diesem Bereich zu erhalten. Vielen Dank, Herr Vorsitzender.

Der Vorsitzende: Vielen Dank, Herr Dr. Grugel. Wir fahren fort mit dem Zuständigkeitsbereich des BMI. Herr von Knobloch, bitteschön.

MD Hans-Heinrich von Knobloch (Leiter der Abteilung Staats-, Verfassungs- und Verwaltungsrecht, Bundesministerium des Innern): Vielen Dank, Herr Vorsitzender. Ich kann mich im

Wesentlichen den Ausführungen von Herrn Dr. Grugel anschließen. Recht hat er, dass wir unter anderem hier sind, um zu lernen und zuzuhören.

Ich möchte einige wenige Aspekte noch einmal herausgreifen. Selbstverständlich sind die sozialen Netzwerke ebenso wie für das BMELV auch für das BMI eine Wirklichkeit, der sich die Bundesregierung zu stellen hat. Eine Wirklichkeit, die für Millionen Menschen eine große Errungenschaft bedeutet. Herr Allan hat allerdings auch Probleme angedeutet, indem er danach fragte, welches Recht eigentlich anwendbar sei. Vor diesem Problem stehen wir auch und es ist aus unserer Sicht ein entscheidendes, das wir angehen müssen, um eine überzeugende Lösung zu finden, die sich nicht auf Inseln beschränkt. Inseln könnten sein, dass man sagt: „Wir gestalten Recht, das sich nur für bestimmte Gebiete eignet." Inseln könnten sein, dass man sagt: „Wir kümmern uns nur um die Profilbildung." Es ist aus unserer Sicht erforderlich, dass wir eine überzeugende Gesamtlösung hinbekommen. An dieser Stelle möchte ich anmerken, dass wir glauben, dass dies auch für den Datenschutz als solchen gilt, der eine geradezu gigantische Herausforderung ist und just an diesem Punkt im Internet an seine Grenzen stößt.

Die EU-Kommission hat angekündigt, im Januar des kommenden Jahres einen Rechtsakt diesbezüglich herausgeben zu wollen. Zunächst als Entwurf, über den dann zu sprechen sein wird. Aber es ist bereits durchgesickert, dass dieser Rechtsakt sich auch um die Bildung von Profilen kümmern will. Das begrüßt die Bundesregierung außerordentlich. Sie sagt allerdings auch, dass es hier abzuwägen gilt. Es geht nicht nur allein um die Interessen des Einzelnen, um Profilbildung und so weiter, sondern es geht auch um andere Interessen wie den Informationsanspruch der Allgemeinheit und so weiter. Das wird man sich in diesem Bereich alles genau ansehen müssen. Zum Thema Selbstregulierung hat Herr Dr. Grugel soeben bereits einiges gesagt. Aus Sicht des BMI ist die Selbstregulierung der naheliegende Schritt vor gesetzlichen Regelungen. Wir sind bezüglich der Selbstregulierung dabei, Gespräche zu führen. Herr Batt kann vielleicht noch ein, zwei Worte dazu sagen. Diese Selbstregulierungsgespräche sind angelaufen. Sie werden fortgeführt und sollen dazu dienen, mit den Sozialen Netzwerken zunächst einmal auf eine Grundlage zu kommen, die ohne gesetzliche Zwänge und so weiter auskommt. Vielen herzlichen Dank.

Der Vorsitzende: Vielen Dank, Herr von Knobloch. Wir steigen dann jetzt ein in die Fragenrunde und beginnen mit der Fraktion CDU/CSU. Herr Dr. Brandl stellt die erste Frage, bitteschön.

Abg. Dr. Reinhard Brandl (CDU/CSU): Auch von unserer Seite zunächst einmal herzlich willkommen hier im Unterausschuss Neue Medien und vielen Dank, dass Sie sich die Zeit nehmen. Danke auch für Ihre Eingangsstatements. Meine erste Frage geht an Herrn Allan. Sie haben vorhin gesagt, Facebook sei nicht das einzige Unternehmen, das Profilbildung im Internet betreibe. Es mag da sicher noch eine ganze Reihe weiterer Unternehmen geben, aber Facebook ist an einer Stelle doch etwas Besonderes. Erstens, weil es sichtbar und ein sehr großes und umfassendes soziales Netzwerk ist. Und zweitens, weil Facebook die Daten, die aufgezeichnet werden anlässlich der Nutzung des Internets durch User, kombiniert mit privaten Daten, die diese selbst ins Internet stellen. Das ist ja auch von Herrn Schaar kurz angesprochen worden. Jetzt haben Sie, wenn ich Sie richtig verstanden habe, gesagt, Sie nutzen diese

Kombination von Daten nicht zur Profilbildung. Wenn dem so ist, frage ich mich, was Sie dann damit machen. Wofür brauchen Sie die Daten, wenn keine Profile erstellt werden sollen auf deren Basis dann Werbung eingeblendet werden soll? Ansonsten verstehe ich die Ratio dahinter nicht. Meine zweite Frage geht an Herrn Dr. Weichert. Sie haben vorhin angesprochen, dass Sie insbesondere mit Verwaltungsgerichtsverfügungen etwas gegen die Verwender des „Gefällt mir"-Buttons erreichen wollen. Ich würde da gerne etwas mehr zum Hintergrund erfahren, auf welche Grundlage Sie sich dabei stützen, wie lange das voraussichtlich dauern wird und was Sie sich davon erhoffen. Was soll dort genau untersucht werden? Es gibt in Bezug auf die Technik ein Gutachten, zu dem Facebook ja eine andere Meinung vertritt. Wie soll das Verwaltungsgericht das prüfen? Für welchen Kreis an Unternehmen, öffentlichen Organisationen und Einrichtungen soll das alles dann gelten? Herzlichen Dank.

Der Vorsitzende: Wir fahren fort mit der Fraktion der SPD, Lars Klingbeil, bitte.

Abg. Lars Klingbeil (SPD): Es ist ja schon erstaunlich, dass wir seit einigen Wochen eine Debatte führen, wonach es anscheinend nicht möglich zu sein scheint, innovative Dienste mit datenschutzrechtlichen Bestimmungen in Einklang zu bringen. Ich bin dankbar, dass diesbezüglich Gespräche geführt werden. Wir haben aber auch gerade gehört, dass die Aktivitäten der Bundesregierung darin bestehen, Facebook-Profile zu löschen.

An Herrn Schaar habe ich die Frage, wie Sie das Zwei-Klick-Modell von Heise bewerten. Es ist damit ein Modell vorgeschlagen worden, das sowohl die Bedürfnisse eines innovativen Dienstes als auch den Datenschutzstandard berücksichtigt.

Herrn Allan möchte ich die Frage stellen, welche Position die Bundesregierung gegenüber Facebook eingenommen hat, um Differenzen anzugehen, die es bezüglich der Auffassung Ihres Unternehmens mit den deutschen Datenschutzbehörden gibt. Interessieren würde mich, ob Sie konsultiert worden sind bzw. gemeinsam mit der Regierung nach Lösungen gesucht wurde. Danke.

Der Vorsitzende: Es fährt fort Jimmy Schulz für die Fraktion der FDP.

Abg. Jimmy Schulz (FDP): Meine erste Frage geht an Herrn Dr. Weichert. Wir haben ja gerade von Herrn Allan gehört, dass es keine Sonderregelung für Schleswig-Holstein geben wird. Ich hatte Ihrem Statement entnommen, dass es vielleicht doch so sein soll. Ich möchte Sie bitten, das noch einmal zu erläutern, weil die Presse in dieser Hinsicht auch etwas unklar war.

Dann habe ich noch eine Frage an Herrn Allan ergänzend zu dem, was der Kollege von der Union fragte. Mich interessiert, welche Daten genau von Nicht-Facebook-Nutzern bzw. nicht eingeloggten Nutzern gespeichert werden können, ob diese gespeichert werden und wenn ja, zu welchem Zweck. Es geht dabei auch um eine größere Transparenz im Hinblick auf den Status des nicht eingeloggten Mitglieds bzw. des Nicht-Mitglieds, welche Daten da erfasst werden und wo sie ggf. verarbeitet werden. Es ist für

uns ganz wichtig zu wissen, ob diese Daten in Europa bleiben oder in die USA übermittelt werden und was ggf. dort genau mit ihnen geschieht.

Der Vorsitzende: Für die Fraktion DIE LINKE. hat sich Herr Behrens gemeldet.

Abg. Herbert Behrens (DIE LINKE.): Ich habe eine Frage an Herrn Schaar bezüglich der EU-Datenschutzrichtlinie. Wir haben eben gehört, dass die Bundesregierung eher darauf setzt, über freiwillige Vereinbarungen bzw. Selbstverpflichtungen weiterzukommen. Wir meinen, dass über die Freiwilligkeit von bestimmten Regeln hinaus Rechtsgrundlagen zentral wichtig sind, gerade in diesem Bereich, um den Schutz der User zu garantieren. Den Ausführungen von Herrn Allan konnten wir entnehmen, dass es sich bei Facebook um ein europäisches Unternehmen handelt, das selbstverständlich die europäischen Datenschutzstandards einzuhalten hat. An dieser Stelle sind allerdings durchaus auch andere Erfahrungsberichte zu hören. Von daher interessiert mich insbesondere, was es heißt, wenn zwischen Europa und den USA eine Datenschutzvereinbarung abgeschlossen wurde, die regelt, wie mit den jeweiligen Datenschutzstandards umzugehen ist, wir aber dann doch ein Unternehmen haben, das außerhalb der EU steht. Und mir wäre noch einmal wichtig zu wissen, wie mit dem Sachverhalt umzugehen ist, dass die Datenschutzregelungen im Safe-Harbour-Abkommen unter Umständen nicht einheitlich gesehen werden zwischen Anbietern und Datenschützern. Ich würde es begrüßen, Sie könnten uns sagen, woran sich der Konflikt an dieser Stelle entzündet, um möglicherweise als Gesetzgeber Ansatzpunkte für eine Lösung zu finden.

Der Vorsitzende: Den Abschluss macht Herr von Notz für die Fraktion BÜNDNIS 90/DIE GRÜNEN.

Abg. Dr. Konstantin von Notz (Bündnis 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. Herzlichen Dank, meine Herren für Ihre Eingangsstatements. Ich habe zwei Fragen. Zunächst eine an Herrn Allan und dann eine an Herrn Dr. Weichert. Herr Allan, wenn ich Ihre Ausführungen bezüglich des Sitzes Ihres Unternehmens richtig verstanden habe, dann spielen Sie darauf an, wie das auch schon Facebook-Vizepräsident Elliot Schrage getan hat, letztlich seien 95 Prozent des irischen Datenschutzrechts identisch mit dem deutschen. Wenn dem so ist, frage ich, warum Sie angesichts des Umstands, wie nachgefragt das Sachverständigengespräch hier heute ist, im Hinblick auf die äußerst schlechte PR, die Ihr Unternehmen aufgrund der fehlenden 5 Prozent erhält, keine andere Strategie wählen und auf die Kritik eingehen. Unter rein ökonomischen Gesichtspunkten muss es da einen Haken geben, sonst würden Sie doch den naheliegenden Weg gehen und diese 5 Prozent umsetzen, was das Unternehmen sicherlich problemlos könnte.

Meine zweite Frage geht an Herrn Dr. Weichert. Bisher ist in dem gesamten Bereich Datenschutz in der digitalen Welt auf Ebene des Bundes leider viel zu wenig geschehen. Halten Sie es für den richtigen Weg, jetzt, wo die Diskussion auch die europäische Ebene erreicht hat und wir darüber reden, Datensicherheit in sozialen Netzwerken zu gewährleisten, zu warten, bis auf europäischer Ebene etwas

passiert? Sehen Sie nicht vielmehr Handlungsdruck auch auf nationaler Ebene, gesetzliche Regelungen zu erlassen, notfalls auch im Hinblick darauf, dass das andere vielleicht noch etwas dauern kann?

Der Vorsitzende: Das war die erste Fragenrunde. Wir kommen nun zur Beantwortung durch die Sachverständigen. Ich würde, auch damit wir die Reihenfolge einhalten, Herrn Dr. Weichert bitten, mit der Beantwortung zu beginnen. Es gab Fragen von den Kollegen Dr. Brandl, von Herrn Schulz und von Herrn Dr. von Notz.

Dr. Thilo Weichert (Der Landesbeauftragte für den Datenschutz Schleswig-Holstein, Kiel): Das Gutachten des ULD vom 19. August 2011 basiert ausschließlich auf eigenen Recherchen. Gegenstand der Untersuchung war nicht die interne Datenverarbeitung bei Facebook. An die kamen wir nicht heran und konnten sie daher auch in keinster Weise bewerten. Wir waren insofern auf das Reich der Mutmaßung angewiesen und tatsächlich verlassen. Das, was von uns festgestellt wurde, ist objektiv richtig, es wurde von Facebook auch bestätigt. Bezüglich der rechtlichen Bewertung und der Vermutung der Profilbildung für Werbezwecke bei Nicht-Mitgliedern konnten wir nur Mutmaßungen anstellen. Cookies zum Beispiel zwei Jahre lang aufzubewahren, obwohl sie für Sicherheitszwecke nicht mehr benötigt werden, muss wohl einen bestimmten Grund haben. Insofern nehmen wir gerne zur Kenntnis, dass Facebook keine Datenverarbeitung vornimmt. Das hatten wir nämlich vermutet. Noch besser wäre, das haben wir gefordert und ist uns von Facebook auch zugestanden worden, den Vorgang anhand von aussagekräftigen Dokumenten prüfen zu dürfen. Uns geht es um die Profilbildung bei Nicht-Mitgliedern. Mitglieder werden profiliert und dort wird Werbung auch entsprechend geschaltet, was bei Nicht-Mitgliedern nicht der Fall zu sein scheint. Die Hintergründe unserer Kontrollen waren zunächst einmal Beschwerden. Unsere Zuständigkeit ergibt sich aus § 38 BDSG. Wir sind die zuständige Aufsichtsbehörde für den Datenschutz im öffentlichen und nicht-öffentlichen Bereich im Bundesland Schleswig-Holstein. Die materiell-rechtlichen Regelungen, die wir als Prüfungsgrundlage genommen haben, sind vielfältige. Im Vordergrund steht insbesondere Art. 5 Abs. 3 E-Privacy-Richtlinie, der Nachfolgeregelung der vormaligen Datenschutzrichtlinie für elektronische Kommunikation. Darin ist geregelt, dass das Setzen von Cookies, die nicht zur Diensterbringung erforderlich sind, der expliziten Einwilligung der Nutzerinnen und Nutzer bedarf. Diese Regelung ist leider noch nicht in nationales Recht umgesetzt, was wir eigentlich seit zwei Jahren, seit diese Richtlinie gilt, fordern. Es gibt zwar einen entsprechenden Entwurf des Bundesrates, aber den scheint die Bundesregierung nicht weiterverfolgen zu wollen. Wir sind von Seiten der ULD der Meinung, und ich glaube, das ist auch die Meinung aller Aufsichtsbehörden, dass wegen des Nicht-Umsetzens dieser Richtlinie seit Mai 2011 die unmittelbare Anwendbarkeit gegeben ist, weshalb wir sie auch als Grundlage unserer Bewertung herangezogen haben. Die anderen rechtlichen Regelungen sind spezielle nationale Regelungen, insbesondere § 15 Abs. 3 Telemediengesetz (TMG), wonach die Profilbildung in pseudonymer Form nur dann erlaubt ist, wenn eine hinreichende Information darüber erfolgt und ein Opt out, also eine Widerspruchsmöglichkeit, besteht. Auch das wurde weder bei Goolge+ noch bei Facebook eingehalten.

Weitere Regelungen betreffen die Datenübermittlung in die USA. Gesetzt den Fall, dass Facebook Ireland tatsächlich die verantwortliche Stelle ist, dann findet eine Datenübermittlung an einen Auftragnehmer, nämlich Facebook Inc. in den USA statt. Auch diese Datenübermittlung muss legitimiert werden. Nach der einhelligen Überzeugung aller Aufsichtsbehörden für den Datenschutz in Deutschland kann diese Datenübermittlung nicht auf der Grundlage des Safe-Harbour-Abkommens legitimiert werden, weil dieses lediglich eine Selbstzertifizierung vorsieht. Insofern muss nach herrschender Auffassung bei jeder Datenübermittlung noch einmal separat durch die verantwortliche Stelle geprüft werden, ob tatsächlich die materiellen Anforderungen von Safe-Harbour gegeben sind. Wir kommen zu dem Ergebnis, dass dies bei Facebook offenkundig nicht der Fall ist, wenngleich in einigen wenigen Fällen, Herr Allan hat gerade auf einen Wiener Studenten verwiesen, Auskunft erteilt worden ist. In vielen anderen Fällen, die auch als Beschwerden bei uns vorgelegen haben, wurde entweder gar keine Auskunft erteilt oder nur eine unbefriedigende, so dass auch die materiellen Anforderungen des Safe-Harbour-Abkommens nicht erfüllt sind. Unser Ziel ist es, diesen Umstand erst einmal gegenüber der Öffentlichkeit zu thematisieren, um dann Verstöße gegen den Datenschutz abzustellen. Das können wir natürlich nur vor dem Hintergrund der begrenzten Zuständigkeit des ULD. Aus diesem Grund gehen wir den Weg, per Anordnung auf der Grundlage von § 38 Abs. 5 BDSG, mithin technische, organisatorische oder materiell-rechtliche Anordnungen zur Änderung der Datenverarbeitung, zunächst eine Anfechtungsklage anzuregen, um also das Verwaltungsgericht bzw. Oberverwaltungsgericht Schleswig-Holstein anzurufen. Wie lange das dauern wird, lässt sich nur schwer prognostizieren. Unsere Erfahrung in einem ähnlichen Verfahren, bei dem es um die hausärztliche Versorgung ging und ein einstweiliger Rechtschutz erforderlich war, ging da hin, dass man mindestens ein Jahr als Verfahrenszeit hinnehmen muss.

Ich glaube, an solch einem Verfahren führt kein Weg vorbei, solange sich die Betreiber von sozialen Netzwerken und die Aufsichtsbehörden bezüglich der datenschutzkonformen Umsetzung der geltenden Regelungen nicht einigen können. Es besteht nach meiner Überzeugung ein massiver Handlungsdruck auf nationaler Ebene. Wir haben hier in Deutschland nicht nur die intensivste Debatte bezüglich des Datenschutzes bei sozialen Netzwerken, sondern vermutlich auch den vielleicht größten Sachverstand überhaupt. Ich könnte mir sehr gut vorstellen, wenn eine Bundesrepublik Deutschland hier hinsichtlich der Regulierung von sozialen Netzwerken voranginge, dass die Europäische Kommission mit Begeisterung folgen würde. Das ULD sowie die anderen deutschen Aufsichtsbehörden in Sachen Datenschutz überhaupt, sind in einem engen Meinungsaustausch mit den Mitgliedern der Artikel-29-Datenschutzgruppe der Europäischen Union, also den anderen Aufsichtsbehörden in Sachen Datenschutz in Europa. Wir sind auch in einem engen Meinungsaustausch mit dem irischen Datenschutzbeauftragten und stellen fest, dass die von uns thematisierten Probleme in den anderen Ländern ähnlich gesehen werden und insofern eine nationale Regelung äußerst wünschenswert wäre. Tatsächlich gibt es auch schon Vorarbeiten, nämlich den Entwurf des Bundesrates zur Änderung des Telemediengesetzes, um unter anderem Art. 5 Abs. 3 E-Privacy Richtlinie umzusetzen. Allerdings gibt es Hinweise, dass dieser Entwurf weder von der Bundesregierung noch dem Deutschen Bundestag weiterbehandelt werden soll. Was im nationalen Recht fehlt, ist die Regelung des Umgangs mit den

Inhaltsdaten bei sozialen Netzwerken. Dazu hat das ULD bereits im Oktober 2010 einen Regelungsvorschlag gemacht, den es lohnt, weiter zu diskutieren und zu überarbeiten. Eine Kombination der beiden Vorschläge, des Änderungsentwurfs des Bundesrates und desjenigen des ULD wäre, glaube ich, eine gute Grundlage für die weitere Diskussion. Man könnte dann auch relativ zügig innerhalb eines Jahres zum Abschluss des Gesetzgebungsverfahrens kommen und Rechtssicherheit hinsichtlich des Datenschutzes und der Datenverarbeitung bei sozialen Netzwerken erhalten.

Der Vorsitzende: Vielen Dank Herr Weichert. Als nächstes Herr Schaar, bitte. Es gab Fragen der Kollegen Klingbeil und Behrens.

Dr. Thilo Weichert (Der Landesbeauftragte für den Datenschutz Schleswig-Holstein, Kiel): Verzeihung, offensichtlich gab es ein Missverständnis zwischen Herrn Allan und dem ULD. Wir hatten das Gespräch mit Facebook so verstanden, dass tatsächlich auch versucht werde, eine Speziallösung für Schleswig-Holstein zu finden. Eine solche Lösung ist nun wohl doch nicht angedacht, wenngleich sie zur Folge gehabt hätte, dass wir schadlos und klaglos gestellt worden wären. Aber ich glaube, es ist für niemanden von Interesse, hier für Schleswig-Holstein einen Sonderweg vorzusehen.

Der Vorsitzende: Vielen Dank für die Klarstellung. Ich denke, es hätte auch gewisse technische Hindernisse gegeben bei der eindeutigen Filterung von IP-Adressen, insbesondere im Hinblick auf die Mobilfunknetze. Umso besser, dass das nun noch einmal klargestellt wurde.

Peter Schaar (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn): Herr Abg. Klingbeil, Sie sprechen ein Thema an, das in der Tat nicht nur diesen speziellen Service betrifft, sondern auch andere. Sie fragten nach der so genannten Zwei-Klick-Lösung, die vom Heise-Verlag wohl erstmalig vorgestellt worden ist. Grundsätzlich ist es ja so, dass man fremde Inhalte auf verschiedene Art und Weise in eine Website einbinden kann. Es gibt die schlichten normalen Links, die von Anbeginn des Webs an seit es HTML und entsprechende Standards gibt, implementiert werden. Diese Links werden normalerweise vom Nutzer dadurch aktiviert, dass er eben dem Link folgt und auf einer anderen Website landet. In einem solchen Fall findet eine Verbindung zu einem anderen Server erst statt, wenn der Betroffene aktiv geworden ist. Es gibt verschiedene andere Techniken, wie man fremde Inhalte einbinden kann. Früher gab es sehr viele so genannte Frames. Heute wird das teilweise über Skripte auf andere Art gelöst, indem es teilweise schon eine Kontaktaufnahme zu Drittservern gibt, ohne dass der Betroffene selbst zusätzlich aktiv werden muss. Das heißt, ich rufe eine bestimmte Seite auf und werde zugleich mit einem oder unter Umständen mehreren anderen Servern verbunden. Jeder dieser Server baut technisch gesehen einen Kontakt bzw. eine Verbindung auf mit dem Nutzer und ist auch in der Lage, jeweils bestimmte Interaktionen auszuführen. Zum Beispiel Cookies zu setzen, die IP-Adressen zu speichern und diese Informationen weiterzugeben. Dafür gibt es Protokolle und Konventionen, die das Verfahren festlegen. Beispielsweise das so genannte Common-Logfile-Format, das auch den Referrer enthält, also die Spur, woher der Betreffende Nutzer gerade kommt, auf welcher Website er zuvor war. Das gibt den Anbietern dieser anderen Services, seien es nun solche, die Werbung vermitteln oder soziale Netzwerke,

zusätzliche Informationen über den Nutzer, ohne dass dieser selbst aktiv wird oder ohne dass dieser davon etwas weiß. Das ist in der Tat ein Problem, das nicht auf Facebook allein beschränkt ist, sondern eine Vielzahl von Services betrifft und dementsprechend ist es auch unser Anliegen, hier Lösungen zu finden, die den Nutzern wieder die Hoheit über ihre Daten geben. Das setzt im Grunde genommen zweierlei voraus: Einmal die Informiertheit des Nutzers, die nur dadurch erzeugt werden kann, dass man ihm gezielt die Informationen bereitstellt und zweitens eine echte Wahlmöglichkeit, mithin, dass der Betroffene selbst aktiv wird. Der Heise-Verlag hat mit seiner Zwei-Klick-Lösung einen Weg in diese Richtung gewiesen. Es wird zunächst eine Aktivität des Betroffenen vorausgesetzt, ehe überhaupt ein Kontakt zu einem Drittserver, nämlich z.B. von Facebook, hergestellt wird. Das Vorgehen würde uns schon ein Stück weit voranbringen. Ob das Verfahren allen rechtlichen Anforderungen gerecht wird, vermag ich nicht ad hoc zu beurteilen, ich denke aber, dass es gegenüber der früheren Lösung, die von Facebook auch nach wie vor beworben wird, auf jeden Fall einen Fortschritt darstellt. Und deshalb würde ich es sehr begrüßen, wenn man schon ein solches Social Plugin verwendet, es dann so gestaltet, dass die Betroffenen selbst entscheiden, ob sie praktisch eine Verbindung zu diesem Drittanbieter – einem sozialen Netzwerk oder einem anderen – aufbauen. Insofern denke ich, käme man damit eine gehöriges Stück weiter. Wie gesagt, eine vollständige Lösung scheint es noch nicht zu sein, vielleicht gibt es auch gar keine allumfassende Lösung dafür.

Herr Behrens, Sie haben eine Problematik angesprochen, die mir von grundlegender Bedeutung zu sein scheint. Es geht um die Frage, wie die Datenverarbeitung in sozialen Netzwerken in einem europäischen Kontext zu sehen ist. Und hier sehe ich im Grunde genommen zwei wesentliche Punkte. Einmal denke ich, dass es anzustreben ist, – und da stimme ich auch mit der Bundesregierung überein – auf europäischer Ebene ein möglichst hohes Schutzniveau zu gewährleisten. Je höher dieses gemeinsame Schutzniveau ist, desto einfacher ist der Datentransfer innerhalb Europas. Insofern gibt es ein starkes Interesse an einer solchen Vereinheitlichung auf einem hohen Niveau. Darüber hinaus habe ich den Eindruck, dass die EU-Kommission, speziell EU-Kommissarin Viviane Reding, die für Datenschutzfragen zuständig ist, auch versucht, das in dem neuen Rechtsrahmen zu implementieren. Das Problem ist, dass dieser neue Rechtsrahmen noch nicht existiert, sondern wir einen haben, der noch aus einer anderen Zeit stammt, als es soziale Netzwerke zum Beispiel noch nicht gab. Und auch die so genannte E-Privacy-Richtlinie, die Herr Dr. Weichert angesprochen hat, ist leider nicht gerade auf der Höhe der Zeit. Aber in diesem einen Punkt, was das Tracking anbelangt, denke ich, ist das wesentliche Element eines neuen europäischen Datenschutzstandards schon vorhanden, indem solch ein Tracking nicht hinter dem Rücken der Betroffenen stattfinden darf.

Es gibt einen zweiten Aspekt bei diesen europäischen Fragestellungen, nämlich die Frage, wie sich die Datenverarbeitung innerhalb Europas zwischen den Mitgliedstaaten untereinander und den Mitgliedstaaten und Staaten außerhalb Europas, beispielsweise den USA, auf der anderen Seite verhält. Innerhalb Europas gilt bei Diensten, die in diesem Kontext angeboten werden, grundsätzlich, dass Diskriminierungsfreiheit gegeben sein muss. Das bedeutet, dass der Datenschutz weder die Erbringung von Diensten der Informationsgesellschaft noch von sonstigen Dienstleistungen erschweren darf, weil es

da ansonsten ein Gefälle zwischen den Mitgliedstaaten gäbe. Tatsache ist aber, dass es da bereits ein Gefälle gibt. Wir haben das Telemediengesetz. Dementsprechend ist das auch der Maßstab, an dem sich die deutschen Datenschutzbehörden zu orientieren haben, wie im Übrigen auch alle anderen, die Dienste anbieten oder nutzen. Und da gibt es bestimmte Vorgaben hinsichtlich der Aufzeichnung des Nutzungsverhaltens. Dass Facebook nun postuliert, kein amerikanischer Dienst zu sein, sondern den Dienst von Irland aus anzubieten, ist in gewisser Weise eine Frage, die man über die Vertragsgestaltung regeln kann. Ich frage mich allerdings, ob diese Vertragsgestaltung tatsächlich nur zwischen den Nutzern und Facebook anzusehen ist oder ob hier nicht auch, wie Herr Dr. Weichert schon angedeutet hat, vielmehr das Vertragsverhältnis zwischen Facebook USA und Facebook Europa zu betrachten ist. Ich gehe davon aus, dass nur in dem Fall, dass Facebook Europa die alleinige Steuerung und Kompetenz über die Datenverarbeitung besitzt, unterstellt werden kann, dass es sich um einen europäischen Dienst handelt. Ob dies der Fall ist, wird derzeit vom irischen Datenschutzbeauftragten untersucht. Ich bin gespannt, wie das Ergebnis dieser Untersuchung ausfallen wird. Unabhängig davon stellt sich immer noch die Frage, auf welcher Rechtsgrundlage Daten in die Vereinigten Staaten übertragen werden. Welche technischen Einrichtungen werden in Irland betrieben? Sind das irische Rechenzentren, auf denen diese Daten liegen, oder liegen sie irgendwo in den Vereinigten Staaten oder anderswo in einer Cloud? Diesen Sachverhalt muss man noch einmal genau anschauen und erst im Anschluss daran kann man beurteilen, was rechtskonform ist.

Lassen Sie mich noch kurz auf die Frage eingehen, an wen man sich richten sollte. Ich finde es richtig, dass sich diejenigen Akteure, die in Deutschland handeln, an deutsches Recht halten und dementsprechend auch diese Vorgaben akzeptieren. Es ist unsere Aufgabe als Datenschutzbehörden das deutsche Recht durchzusetzen. Unabhängig davon denke ich, dass es gerade bei solchen Diensten, wie wir sie hier sehen, die sehr viele Mitglieder auch außerhalb Europas haben, wichtig ist, die Dienste dazu zu bringen, ihr Angebot rechtskonform zu gestalten. Das ist für mich das Entscheidende. Die Handelskammern in Berlin oder Schleswig-Holstein scheinen mir nicht das entscheidende Problem zu sein, sondern das zentrale Problem sind die Dienste selbst und deshalb würde ich gerne auch an die anwesenden Vertreter dieser Dienste appellieren, sich zu bewegen. Ich weiß, dass es zum Beispiel bei Google sehr viel Bewegung gegeben hat. Da gab es ja auch eine sehr intensive Debatte zwischen den Datenschutzbehörden und dem Unternehmen bezüglich der Reichweitenmessung. Da hat es Bewegung gegeben und wir haben das, glaube ich, auch zu einem guten Ergebnis gebracht. Ich könnte mir auch vorstellen, dass man bei Facebook noch ein Stück weiterkommt. In Bezug auf die Einbindung von externen Adressbüchern in Facebook im Sinne eines Uploads ist meines Wissens die Hamburgische Datenaufsichtsbehörde auch schon sehr weit gekommen. Ich denke, diesen Weg müssen wir weiter gehen.

Der Vorsitzende: Vielen Dank, Herr Schaar. An Google+ gab es jetzt in der ersten Fragerunde keine Rückfragen. Deshalb kommen wir gleich zu Herrn Allan. Bitteschön.

Richard Allan (Facebook, Director EU-Policy, Dublin): Vielen Dank. Ich möchte in der positiven Stimmung fortfahren, die Herr Schaar gesetzt hat, und auf die Fragen von Herrn Brandl, Herrn Klingbeil und Herrn Schulz zum "Gefällt mir"-Button und zu Social Plugins antworten. Herr Schaar hat die Entwicklung im Internet sehr genau beschrieben: Viele Websites greifen beim Öffnen auf Funktionen von verschiedenen Service-Providern zurück. Wir sollten uns einmal vergegenwärtigen, warum das so ist. Bevor es diese Art der Technologie gab, musste man, um eine soziale Funktion einzubringen, die betreffenden Personen selbst registrieren. Wenn man geografische Funktionen einbeziehen wollte, musste man seinen eigenen Map Service erstellen. Für die Einbindung von Videos musste man einen eigenen Video-Streaming-Service erstellen. Dafür hatten die meisten Websites aber weder die technischen noch die finanziellen Mittel. Und deshalb haben wir ein Ökosystem von Providern für diese Services geschaffen, sodass jetzt politische Parteien, jedes Unternehmen und jede Organisation in Deutschland mit sehr geringem technischem und finanziellem Aufwand einen fantastischen Web-Service erstellen kann. Und das ist der eigentliche Grund.

Von der Seite des Datenschutzes aus kann man jetzt auf verschiedene Arten darauf reagieren. Eine bestünde darin, diese Services von Drittanbietern komplett zu verbieten, was meiner Ansicht nach den Interessen der Organisationen in Deutschland, die diese Services verwenden, eher schaden würde. Andere wollen eine weitere komplexe technische Schicht hinzufügen, die so genannte "Zwei-Klick-Lösung". Aus Datenschutzgründen wäre das eine legitime behördliche Auflage, aber Sie müssen wissen, dass dies mit erheblichen Kosten verbunden wäre. Da gibt es die technischen und Engineering-Kosten, aber vor allem würden dabei Funktionen verloren gehen, weil die meisten dieser Plugins sofort Informationen liefern, sobald Sie eine Website betreten. Wenn Sie bei einem Social Plugin, wie dem von Facebook, Inhalte auf einer Website ansehen, erkennen Sie sofort, wem von Ihren Freunden diese Website gefällt. Das wiederum erhöht die Wahrscheinlichkeit, dass Sie sich selbst mit diesen Inhalten beschäftigen. Wenn man also diese Funktion entfernen möchte – und das tut die Zwei-Klick-Lösung, kann man natürlich anführen, dass dies den Datenschutz verbessert, aber eben auf Kosten der Funktionalität. Ich halte es für legitim, dass die Behörden sich zwischen diesen beiden Optionen entscheiden. Wir würden es am liebsten sehen, wenn dieser Weg nicht weiter verfolgt würde. Unserer Meinung nach würde man dann immer zuerst eine tote Website aufrufen und muss 15-mal klicken, um sie zum Leben zu erwecken. In der Realität würden dann viele Benutzer versuchen, dies irgendwie zu umgehen, weil es frustrierend ist, auf der Website nicht die benötigten Funktionen sehen zu können. Wir halten es für einen besseren Weg, diesem Dialog und vielleicht dieser Herausforderung zu folgen, vor die uns Herr Schaar gestellt hat. Also nach Möglichkeiten zu suchen, wie wir als Anbieter dieser Plugins für die Websites, die sie einsetzen, akzeptable Normen erfüllen können. Und diese Normen können verschiedene Bereiche der Verwendung bereitgestellter Daten betreffen, z. B. wie wir sie speichern und nach einem angemessenen Zeitraum löschen. Lassen Sie mich unsere Vorgehensweise beschreiben, um auf verschiedene Einzelheiten einzugehen.

Zuerst einmal unterscheiden wir klar zwischen Nutzern und Nichtnutzern unseres Service. Mit eingetragenen Facebook-Nutzern haben wir einen Vertrag. In diesem Vertrag, unseren

Nutzungsbedingungen, wird ganz eindeutig erklärt, dass wir diese Art von Daten sammeln und wofür wir sie verwenden – genau wie in unseren Datenschutzrichtlinien. Sowohl die Nutzungsbedingungen als auch die Datenschutzrichtlinien sind auf jeder einzelnen Facebook-Seite verlinkt. Außerdem ist es offensichtlich, was passiert, wenn man eine Webseite über das Plugin besucht. Und vergessen wir nicht, dass der Besucher einer Seite sehen kann, dass seinen Freunden dieselben Inhalte gefallen, dass die Verbindung also sofort hergestellt ist. Wir denken, das ist für jeden klar erkennbar. Aber auch hier prüfen wir gerne, wie wir die Transparenz weiter verbessern können, wenn das in der aktuellen Debatte hilfreich ist.

Es dient also dem Benutzer. Sobald ein Benutzer auf den "Gefällt mir"-Button klickt, wird ein Eintrag im Profil erstellt, so als wenn er in Facebook selbst etwas anklickt. Er hat also explizit erklärt, dass ihm die CDU-Website oder die CDU-Seite auf Facebook gefällt. Beide sind gleichwertig. Tut er das nicht, wird eine gewisse Datenmenge in einem so genannten "Impression Log" gespeichert, einem Standard-Webprotokoll, das erfasst, wenn jemand eine bestimmte Seite einer Website besucht hat.

Bei Nichtnutzern haben wir auf das in Deutschland heikle Thema der IP-Adressen reagiert und uns vor einigen Monaten beraten lassen. Wir hatten bereits eine technische Maßnahme implementiert, damit in den Protokolldateien keine IP-Adressen von Personen gespeichert werden, die keine Facebook-Benutzer in Deutschland sind und die eine Seite mit einem "Gefällt mir"-Button besuchen. Ich halte dies für eine sehr wichtige Entwicklung. Das bedeutet, dass die Art von Profiling nach IP-Adressen, die uns vorgeworfen wurde, überhaupt nicht möglich ist, weil es diese IP-Adressen von Nichtnutzern in den Facebook-Protokolldateien überhaupt nicht gibt. Es gibt einen kurzen Durchlaufzeitpunkt, wenn sie unseren Server erreichen, damit wir die Inhalte zurückschicken, aber in die spätere Protokolldatei schreiben wir eine generische IP-Adresse – dieselbe Adresse für jeden Zugriff aus Deutschland.

Es wurde gefragt, was wir dann mit diesen Daten machen – eine berechtigte Frage. Nun, wir nutzen diese Daten zu Sicherheitszwecken. Wir sind stolz darauf, dass unsere Website zu den sichersten im Internet gehört. Wir verwenden sehr viel Zeit und Energie darauf, sicherzustellen, dass Ihnen auf unserer Website niemand erzählt, er sei in London gestrandet und Sie sollten ihm doch bitte 50 Dollar per FedEx schicken. Diese Leute arbeiten so, dass sie viele Konten auf Facebook erstellen. Anhand eines Protokolls, wer von wo aus auf die Website zugegriffen hat, können wir diese Leute fernhalten.

Wir verwenden die Daten außerdem zur Verbesserung der Leistungsfähigkeit. Wenn jemand einen unserer Buttons auf seine Website setzt, möchte er auch wissen, welche Auswirkungen dies hat – und manchmal diskutieren wir sogar mit den Leuten darüber, welchen Einfluss der Button auf ihre persönliche Website hatte. In den meisten Fällen ist der Button sehr wertvoll. Er hilft, ihre Inhalte zu verbreiten, aber manchmal wollen die Benutzer mit uns auch darüber diskutieren. Anhand der Protokolldatei können wir erkennen, wann, von wo aus und mit welcher Reaktionszeit auf unseren Service zugegriffen wurde.

Die Daten verwenden wir in diesem temporären Sinne, um statistisch analysieren zu können, was sie für die Sicherheit unserer Services bedeuten. Und nach 90 Tagen löschen wir sie. Ich halte die Fragen "Wie lange bewahren Sie die Daten auf?", "Wofür verwenden Sie sie?", "Wie sicher sind sie?" für sehr wichtige Fragen an Plugin-Anbieter, die wichtige Wege für die Zukunft aufzeigen können.

Entgegen gewisser Behauptungen verwenden wir die Daten *nicht* für Werbung gegenüber Nichtnutzern. Das kann ich Ihnen ganz einfach beweisen: Wenn Sie als Nichtnutzer auf Facebook gehen, sehen Sie keinerlei Werbung. Es gibt keinen Platz, auf dem wir Nichtnutzern Werbung anzeigen könnten. Werbung wird nur angemeldeten Facebook-Nutzern angezeigt. Sie können mir also glauben, dass wir diese Daten nicht zu Werbezwecken nutzen, aber Sie können das auch selbst überprüfen. Können Sie mir zeigen, wo diese Werbung für Nichtnutzer von Facebook angezeigt wird? Ich halte das für einen wichtigen Aspekt.

Zur Frage von Herrn von Notz bezüglich des Gerichtsstandes: Das ist ein sehr spannender Punkt. Lassen Sie mich nur kurz die Statistik heranziehen: In der Europäischen Union gibt es 27 verschiedene staatliche Datenschutzbehörden. In Deutschland gibt es auch noch 16 Landesdatenschutzbeauftragte; im europäischen Wirtschaftsraum noch einige weitere. Ich komme so schnell auf ca. 50 verschiedene Datenschutzbehörden, die wir berücksichtigen müssen. Und wenn jede von ihnen einmal pro Woche mit uns sprechen und vielleicht eine Anhörung durchführen will, reicht ein Vollzeit-Job dafür nicht aus. Für uns bei Facebook ist das Realität. Unser Unternehmen ist relativ groß, aber denken Sie einmal an Unternehmen nicht weit von hier in Berlin, die 30, 40 oder 50 Mitarbeiter beschäftigen, die heute Internetfirmen aufbauen und im gleichen globalen Umfeld tätig sind wie wir bei Facebook. Diese Unternehmen haben – ganz realistisch gesehen – keine Möglichkeit, die vielen verschiedenen Auflagen vollständig zu erfüllen, also tun sie, was wir tun: Sie entscheiden sich für ein Land als ihre Hauptniederlassung und befolgen von diesem Land aus die Prinzipien des Binnenmarktes, die ganz richtig in den Richtlinien niedergelegt und in deutsches Recht umgesetzt wurden. Und solange sie die gesetzlichen Vorschriften des Landes ihrer Niederlassung erfüllen, können sie frei in der Europäischen Union Handel treiben. Ich sage nur, dass dies ein sinnvolles Arrangement für Facebook ist. Warum Irland? Nun, dort ist eben unsere Firmenzentrale angesiedelt, und dort beschäftigen wir über 400 Mitarbeiter. Das sind rund 15 Prozent unserer gesamten Mitarbeiter weltweit. Und wenn Sie als deutscher Nutzer ein Problem mit Ihrem Service hier haben oder Sie als deutscher Kunde einen Service in Deutschland nutzen möchten, tun Sie dies über unsere Mitarbeiter in Dublin. Ein anderer Firmensitz wäre für uns ein Problem, weil es nicht der Realität unseres Unternehmens entsprechen würde.

Nachdem wir uns also für das Land unserer Zentrale entschieden haben, ist es doch ganz richtig, dass wir zunächst hart an unserer Compliance [in Irland] arbeiten. Herr Schaar hat recht: Der irische Datenschutzbeauftragte prüft alle unsere Verträge und unsere gesamte Dokumentation. Wir wollen zunächst alle diese Auflagen erfüllen, dann können wir Ihnen das gleiche Niveau auch hier in Deutschland bieten. Natürlich sind wir bereit, direkt mit Ihnen zu besprechen, ob es im deutschen Recht weitere Facetten gibt, die wir bei unserer Arbeit berücksichtigen müssen.

Der Vorsitzende: Vielen Dank, Herr Allan. Soweit zur Beantwortung. Wir haben damit die erste Fragerunde abgeschlossen. Es verbleiben jetzt noch 20 Minuten für die zweite Fragerunde. Das sollte ein subtiler Hinweis darauf sein, sich möglichst kurz und knapp zu fassen. Wir beginnen mit der Fraktion der CDU/CSU. Thomas Jarzombek, bitte.

Abg. Thomas Jarzombek (CDU/CSU): Vielen Dank, Herr Vorsitzender. Meine Damen und Herren. Der erste Punkt, den ich ansprechen möchte, ist noch einmal die Speicherung von Daten ohne ein Kundenverhältnis als Grundlage zu haben. Ich würde gerne von Herrn Allan wissen wollen, welche Auskünfte denjenigen zu erteilen wären, die bislang noch nicht auf Facebook registriert sind, bezüglich dessen, was dort über sie gespeichert wird. Zumal Sie ja darauf hinweisen, dass man solche Auskünfte erhalten könne. Ich wüsste ebenfalls gerne, an wen man sich in einem solchen Fall wenden muss.

Die Aufklärung des Kunden ist für mich der zweite Punkt. Ich würde gerne wissen, was Facebook den Kunden als Aufklärung über die Dinge zu präsentieren gedenkt, die über sie gespeichert werden. Ich erinnere mich, bei Bild online gelesen zu haben, dass der österreichische Student eine Klage von mehreren 100 Seiten einreichte. Als ich das gelesen habe, muss ich ehrlicherweise sagen, war ich sehr erschrocken. Ich habe Freunden und Bekannten davon berichtet, die ähnlich reagierten. Deshalb möchte ich wissen, welche Vorschläge Sie haben, Ihre Kunden besser darüber zu informieren, dass wohl nahezu unendliche Datenmassen gespeichert werden. Der Staat hat ja ansonsten auch schon einmal Warnhinweise auf Produkte kleben lassen, um damit vor bestimmten Risiken zu warnen. Ich bin grundsätzlich kein Freund von Verboten und Ähnlichem, aber unter diesen Umständen müssen wir uns vielleicht auch einmal überlegen, wie man Warnhinweise anbringt und Musterdatenauskünfte bereitstellt. Das könnten vielleicht ja auch einmal Ministerien exemplarisch tun, um Nutzer darauf hinzuweisen und aufzuklären.

Meine dritte Frage, auch an Herrn Allan gerichtet, betrifft die regulierte Selbstregulierung. Mich würde interessieren, was Sie davon halten und ob Facebook in irgendeiner Art und Weise bereit ist, sich in freiwillige Verpflichtungen zu begeben, wie wir sie bei vielen anderen Dingen erlebt haben. Ich frage das auch vor dem Hintergrund, dass es überhaupt keine Präsenz von Facebook hier in Deutschland gibt. Es gibt zwar ein Sekretariat, das weiß ich sehr wohl, aber es gibt überhaupt keinen Ansprechpartner in Berlin für die Politik, für die Verbraucherschutzverbände, für die Ministerien. Es gibt also noch nicht einmal jemanden, mit dem man hier reden könnte von Ihrem Unternehmen. Sie kommen zuweilen zu uns, was ich sehr schätze. Allerdings ist das natürlich auch kein vernünftiger Dialog, einen Ansprechpartner zu haben, der in Irland sitzt und nur alle paar Wochen nach Deutschland kommt. Ich finde, ehrlich gesagt, so wie Sie hier derzeit aufgestellt sind, ist es kein guter Zustand, um zu irgendeiner Form der Selbstregulierung zu kommen.

Meine vierte Frage richtet sich an die Vertreter der Bundesregierung. Es wird immer wieder darauf hingewiesen bzw. behauptet, es gebe bei Facebook keine Datenverarbeitung in Deutschland, sondern nur in Irland. Es gibt allerdings Mietrechenzentren, deren Kapazitäten man variabel nutzen kann, so dass

es in technischer Hinsicht nahe liegt, zu vermuten, dass auch Plattformbetreiber wie Facebook solche Anbieter nutzen. Es ist insofern nicht auszuschließen, dass Daten in Deutschland gespeichert werden. Mich interessiert, ob Sie hier einen Ansatz sehen für künftige Gesetzesnovellen, genauere und weitergehende Auskunftsrechte vorzusehen, so dass solche Anbieter dann auch erklären müssten, ob sie Daten von bestimmten Unternehmen in Deutschland verarbeiten.

Der Vorsitzende: Vielen Dank. Die Anzahl der eigentlich zulässigen Fragen wurden eben verdoppelt. Ich bitte, die folgenden Kollegen das nicht als Beispiel zu nehmen. Für die SPD-Fraktion Herr Reichenbach, bitte.

Abg. Gerold Reichenbach (SPD): Ich habe zwei Fragen. Die erste Frage bezieht sich noch einmal auf die IP-Adresse. Sie haben darauf hingewiesen, dass Sie die IP-Adresse nicht speichern, sondern eine numerische Zahl. Das Vorgehen haben Sie damit begründet, dass es der Sicherheit diene. Vor diesem Hintergrund würde ich gerne von Ihnen wissen, ob Sie ein Interesse an dem Account haben, der sich einloggt und ob Sie das auswerten. Offenkundig geht das über die entsprechenden Zahlen bzw. Daten, die Sie generieren auch, ohne die tatsächliche IP-Adresse zu haben.

Die zweite Frage geht an die beiden Herren Datenschutzbeauftragte. Wäre das nicht einer IP-Adresse gleichzustellen, wenn die Zahlen bzw. Daten entsprechend ausgewertet werden, weil sie auch da wieder rückverschlüsselbar wären?

Dann habe ich noch eine weitere Frage sowohl an die Datenschützer als auch an Sie, sehr geehrter Herr Allan. Sie haben von Selbstregulierung gesprochen. Glauben Sie, dass Sie über die Selbstregulierung das Problem des unterschiedlichen Landesrechts und der zuständigen Landesanstalten für den Datenschutz gelöst bekommen, denn das würde ja heißen, dass Sie davon ausgehen, dass die Selbstregulierung an die Stelle der Auslegung der bestehenden Gesetze tritt? Ich frage deshalb die Datenschutzbeauftragten, ob es überhaupt möglich ist, ihre Kontrollfunktion in eine Selbstregulierung abzugeben.

Der Vorsitzende: Wir fahren fort mit der Fraktion der FDP und der Bitte an den Kollegen Schulz, nur eine Frage zu stellen, damit das Kontingent dann wieder etwas ausgeglichen erscheint.

Abg. Jimmy Schulz (FDP): Ich werde das gerne tun. Vorhin tauchte die Frage auf, nach welchem Recht – insbesondere bei Facebook – überhaupt gehandelt werden kann, mithin, ob das BDSG hier überhaupt Geltung hat. Ich hatte diese Frage im Zusammenhang mit der automatischen Gesichtserkennung, dem Auto Tracking, an die Wissenschaftlichen Dienste des Deutschen Bundestages gerichtet und zur Antwort bekommen, da Facebook keinen richtigen Sitz in Deutschland besitze und auch die irische Niederlassung weisungsgebunden an die US-Zentrale sei, müsse man feststellen, dass Facebook als nicht innerhalb der EU gelegenes Unternehmen in Deutschland personenbezogene Daten erhebe, nutze und speichere und somit gemäß § 1 Abs. 5 S. 2 BDSG unter Anwendung des Territorialprinzips den deutschen Bundesdatenschutzvorschriften unterliege. In Anbetracht dieser Schlussfolgerung möchte ich

Herrn Allan fragen, wie Facebook mit dem Auto Tracking umgeht. Sie sind damals ein wenig zurückgerudert und haben das dann nicht mehr als „default“ genommen. Ich möchte gerne wissen, was wirklich geschieht. Sie bieten das zwar nicht mehr an, betreiben aber gleichwohl im Hintergrund Gesichtserkennung, wenngleich vermutlich nur zu rein internen Zwecken.

Nur weil wir das nicht sehen, heißt das noch lange nicht, dass Sie das nicht machen. Geschieht das im Hintergrund trotzdem? Wenn dem so wäre, hätte das dann ja auch eine Auswirkung auf die Anwendung des deutschen Datenschutzrechts. Insofern würde ich das schon gerne wissen.

Der Vorsitzende: Für die Fraktion DIE LINKE. Frau Dr. Sitte, bitte.

Abg. Dr. Petra Sitte (DIE LINKE.): Ich möchte direkt an die Frage des Kollegen von der SPD anschließen, in Bezug auf die Selbstregulierung. Unlängst hat sich Herr Allan mit dem Bundesminister des Innern, Herrn Dr. Hans-Peter Friedrich, getroffen. Nun gibt es da offenkundig auch einen gewissen Streit, wer von Seiten der Bundesregierung wirklich Ihr Ansprechpartner ist. Der Bundesminister des Innern ist es offensichtlich nicht wirklich. Wenn Sie mit ihm eine Regelung zur Selbstregulierung verbreden wollten, müsste diese Bestand haben in der Akzeptanz gegenüber den Ländereinrichtungen. Insofern richtet sich meine Frage genau in gleicher Weise, aber nicht nur an die Vertreter der Datenschutzbehörden, sondern auch an Sie, als Repräsentant von Facebook, was Sie sich in Bezug auf den Mehrwert einer solchen Selbstregulierung erhoffen, wenn wir in Betracht ziehen, das es das Angebot der Lizensierung nach europäischen Datenschutzrichtlinien bzw. den deutschen Kriterien gibt. Zugegebenermaßen ist Schleswig-Holstein da als Grundanbieter am weitesten.

Insofern ist die Feststellung des Bundesministers des Innern, man habe etwas entschärft, für mich nicht so ganz klar geworden. Ich würde es begrüßen, wenn Sie uns das aus der Sicht eines Unternehmensvertreters noch einmal erklären könnten. Ebenso, was Sie von Selbstregulierung und ähnlichem erwarten.

Meine zweite Frage richtet sich an Herrn Meyerdierks. Unlängst hat ein Vertreter des Google-Vorstandes zur Kenntnis gegeben, dass man die Pseudonymisierung und andere Formen der Identität zulassen werde. Mich interessiert ab wann das gelten soll und wie es sich mit der Klarnamenregistrierung verhält bezogen auf die Positionierung von Herrn Allan, der anlässlich eines Gesprächs im Juni diesen Jahres in meiner Fraktion sagte, für Facebook komme das nicht in Frage, weil es die Grundidee des Unternehmens tangiere und insofern auf andere Anbieter verwies. Wie bewerten Sie das aus der Sicht eines anderen Anbieters? Dankeschön.

Der Vorsitzende: Für die Fraktion BÜNDNIS 90/DIE GRÜNEN Herr Dr. von Notz.

Abg. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, Herr Allan ich möchte Ihnen an dieser Stelle noch einmal sagen, von allen zwischenmenschlichen Sympathien mal ganz abgesehen, dass ich

immer weniger Verständnis dafür habe, wie Facebook agiert. Dass wir hier solche Anhörungen machen müssen, weil einzelne Landesdatenschutzbeauftragte die Auseinandersetzung suchen, dass das sozusagen der Weg ist, den der Gesetzgeber hier gehen muss, weil es eben keine richtige Vertretung von Facebook in Deutschland gibt und hier sozusagen versucht wird, sich um die Dinge herumzudrücken, dafür habe ich kein Verständnis und finde, das geht so nicht mehr. Insofern kann man nur dankbar sein, dass man jetzt einen Aufhänger hat, hier einmal miteinander zu sprechen. Sie sind ein global agierendes Unternehmen und keine Garagenklitsche mehr, sondern Facebook ist ein milliardenschweres Unternehmen und es gibt auch nicht nur sieben User in Deutschland, sondern inzwischen sind es 22 bis 23 Millionen Menschen in diesem Land, die Ihre Dienste in Anspruch nehmen. Deswegen möchte ich Ihnen an dieser Stelle noch einmal in aller Ernsthaftigkeit sagen, dass wir uns wünschen, dass Sie sich an deutsches Recht halten.

Anknüpfend an Ihre Beantwortung meiner ersten Frage möchte ich Ihnen nahelegen, wenn Sie sich jetzt an diesem irischen Recht festmachen und das mit den vielen Datenschutzbeauftragten auf dem Kontinent und so weiter derart kompliziert ist, entscheiden Sie sich doch einfach für das verbraucherfreundlichste, welches das deutsche ist, und entsprechen Sie diesem. Dann sage ich Ihnen voraus, haben Sie in Irland auch keine Probleme und müssen sich nur danach richten. Ganz unkompliziert und völlig kostengünstig.

Die zweite Sache, anknüpfend an den Gedanken des Kollegen Jarzombek, betrifft Daten, die Sie speichern. Auch wenn Sie sagen, Sie würden Nichtmitglieder nicht bewerben, so ist es doch trotzdem eine interessante Frage, ob Sie die Daten von Nichtmitgliedern speichern, weil sie irgendwann einmal Mitglieder werden könnten, um dann ggf. einen Pool zu haben, den Sie bewerben können. Der Gedanke liegt ja gar nicht so fern bei inzwischen 23 Mio. Menschen in diesem Land. Dass Sie die Leute nicht, wenn Sie zum ersten mal auf die Facebook-Site gelangen, gleich mit Werbung eindecken, das macht unter vielen Gesichtspunkten Sinn. Aber sammeln Sie nicht die Daten und halten sie vor, um dann, wenn Menschen Mitglied geworden sind und ein Profil anlegen, nicht erst mühsam über Jahre hinweg ihre Daten sammeln zu müssen? Vielen Dank.

Der Vorsitzende: Wir kommen in die Antwortrunde und beginnen erneut mit Herrn Dr. Weichert. Da gab es eine Frage des Kollegen Reichenbach.

Dr. Thilo Weichert (Der Landesbeauftragte für den Datenschutz Schleswig-Holstein, Kiel): Ich glaube, ich kann es auch sehr kurz machen. Die IP-Adresse kann nach der neusten Rechtsprechung des Bundesverfassungsgerichtes zur Vorratsdatenspeicherung ein personenbezogenes Datum sein. Das ist in der Zwischenzeit unbestritten. Aber es gibt natürlich auch andere Identifikatoren. Facebook und auch Google nutzen Cookies und deren IDs, die dann auch bei den jeweiligen Unternehmen gespeichert werden und eine Zuordnung der jeweiligen Aufrufe und das Tracking möglich machen.

Was die Selbstregulierung betrifft, ist es natürlich klar, dass eine solche nur reguliert Sinn macht, damit sie die gesetzlichen Regelungen nicht außer Kraft setzen kann. Aus diesem Grund haben wir im § 38a BDSG eine ganz klare Regelung, wie das funktioniert. Zuständig dafür sind die Aufsichtsbehörden in dem Bundesland, in dem der jeweilige Verband seinen Sitz hat. Bei Bitkom wäre das wahrscheinlich Berlin, aber im Vorweg findet natürlich eine Abstimmung unter den Aufsichtsbehörden im so genannten Düsseldorfer Kreis statt. Ich bin darin Vorsitzender des Arbeitskreises Versicherungswirtschaft und kurz vor dem Abschluss einer solchen Selbstregulierung, die sehr umfassend und erfolgreich ist. Ich kann insofern bestätigen, dass so etwas möglich ist, vor allem im Dialog zwischen den Verbraucherschützern, den Aufsichtsbehörden und den jeweiligen Unternehmen. Das Bundesministerium des Innern bzw. ein Landesinnenministerium hat dort überhaupt nichts verloren. Die sind zuständig für die Gesetzgebung und sollten ausschließlich diese Aufgabe wahrnehmen. Wenn noch irgendwelche anderen Geschichten laufen, dann ist das alles unverbindlich und vielleicht nett, aber das hat alles keinerlei rechtliche Wirkung.

Zur Identifizierungspflicht bei sozialen Netzwerken kann ich im Prinzip nur § 13 Abs. 6 TMG zitieren, wonach „der Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen hat, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren“. Da dies der Fall ist, handelte Google+ richtig, indem man verkündete, auch Pseudonyme zu erlauben. Facebook wäre gut beraten, eine solche Möglichkeit auch für Deutschland vorzusehen.

Der Vorsitzende: Vielen Dank, Herr Dr. Weichert. Herr Schaar fährt fort. Da gab es ebenfalls eine Frage von Herrn Reichenbach.

Peter Schaar (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn): Vielen Dank. Es geht in der Tat nicht nur um die IP-Adresse, sondern es geht generell um die Frage, eine Person mittels eines Merkmals zu identifizieren. Gerade die europäische Datenschutzrichtlinie enthält hier eine ganz klare Definition. Wenn entsprechende Merkmale, die zur Identifikation einer Person herangezogen werden können, verwendet werden, handelt es sich um personenbezogene Daten. Diese sind immer auch der Prüfmaßstab für Datenschützer gewesen. Deshalb sind wir auf europäischer Ebene zu dem Ergebnis gekommen, IP-Adressen in der Regel als personenbezogen anzusehen, selbst wenn sie nicht in jedem Fall zur Identifikation der Person führen, weil zum Beispiel jemand in einem Hotel das Internet benutzt hat oder in einem Internetcafé von einem freien Hot Spot aus. Insofern kann eine Rückverfolgung auf die Person zwar im Einzelfall nicht möglich sein, gleichwohl gehen wir davon aus, dass die IP-Adresse hier als personenbezogenes Datum, mithin Identifikationsmerkmal, anzusehen ist.

Außerdem gibt es eine ganze Reihe von Trackingmechanismen, die teilweise sehr viel schwieriger für den Betroffenen zu erkennen sind, unter Umständen schwieriger noch als Cookies. Wir sprechen zwar immer noch von Cookies, es gibt aber bereits eine Vielzahl von Trackingmechanismen, die sich zum Beispiel nicht über einen Browserklick oder eine Browserkonfiguration ohne weiteres abschalten lassen,

sondern es werden im Hintergrund Daten gespeichert und man muss tief in das System eingreifen, um diese Trackinginformationen loszuwerden. Besonders der neue HTML-5-Standard, der jetzt zunehmend zum Einsatz kommt, enthält entsprechende Möglichkeiten, an den verschiedensten Stellen im System ein Identifikationsmerkmal zu speichern. Wenn das auch nur an einer dieser Stellen nicht gelöscht wird, ist eine Rekonstruktion dieses Identifikationsmerkmals jederzeit wieder möglich. Man bewegt sich also weit jenseits dessen, was wir von Cookies her kennen. Flash Cookies gehören auch dazu. Das heißt, entscheidend ist letztlich nicht, ob durch Cookie oder IP-Adresse, sondern Nutzer können auch anders identifiziert werden und die gewonnen Informationen können über diese Identifikationsmechanismen jederzeit wieder aktiviert werden. Das ist, glaube ich, das Entscheidende dabei und da geht es mir und meinen Kolleginnen und Kollegen in ganz Europa darum, diese Mechanismen so weit wie möglich transparent zu machen und der Steuerung durch die Betroffenen wieder zu unterwerfen.

Ich muss sagen, wir sind da im Übrigen in Europa nicht allein. Ich bin im engen Kontakt mit der Federal Trade Commission in den USA, die das ganz genauso sieht, dass gegen den Willen des Betroffenen kein Tracking stattfinden darf. Wir sind gerade dabei, Mechanismen zu diskutieren, die es ermöglichen, die Kontrolle dem Nutzer wieder zu geben. Insofern geht es da nicht um die schleswig-holsteinische Insellösung, sondern es geht auch um globale Prozesse. Wir werden uns in der kommenden Woche in Mexico City mit der Federal Trade Commission zusammensetzen, die seit dem vergangenen Jahr auch Mitglied der internationalen Datenschutzkonferenz ist, und die Frage angehen, den neuen Internetprotokollstandard IPv6 datenschutzgerecht zu gestalten. Dazu werden wir dann wahrscheinlich auch etwas beschließen. Ich werde Sie davon zu gegebener Zeit unterrichten.

Zum Thema Selbstregulierung möchte ich nur eine Ergänzung anbringen. Selbstregulierung ist natürlich ein wirksames, ergänzendes Mittel zur Fremdregulierung durch den Gesetzgeber. Aber Selbstregulierung kann den Gesetzgeber nicht ersetzen, wenn es um Grundrechtsschutz geht und um elementare Richtungsentscheidungen. Der frühere Innenminister de Maizière hat in diesem Zusammenhang davon gesprochen, dass es bestimmter roter Linien bedarf. Manche meiner Kolleginnen und Kollegen sind der Auffassung, die roten Linien reichen nicht aus. Aber ich wäre schon froh, wenn man die roten Linien mal updaten und an die heutigen Anforderungen anpassen könnte, insbesondere was das Profiling angeht. Dazu besteht Gelegenheit, wenn die Novelle des Telekommunikationsgesetzes den Bundestag durchläuft. Das soll ja in dieser Woche der Fall sein. Wenn man da jetzt schnell arbeitet, könnte man vielleicht auch noch etwas machen.

Der Vorsitzende: Wir fahren fort mit Google+. Da gab es eine Frage von Frau Dr. Sitte. Herr Meyerdierks übernehmen Sie bitte die Antwort.

Per Meyerdierks (Google Germany GmbH, Datenschutzbeauftragter, Hamburg): In der Tat gibt es mit § 13 Abs. 6 TMG, der von Herrn Dr. Weichert zitiert wurde, eine Vorschrift im deutschen Recht, auf deren Grundlage für jeden Dienst einzeln zu beurteilen ist, ob das Anbieten unter Pseudonym oder sogar

anonym zumutbar ist für den Dienstanbieter. Google bietet eine ganze Reihe von Diensten an, die anonym oder unter Pseudonym genutzt werden können. Google+ hingegen, welches, wie ich eingangs erwähnte, noch ein recht junges Netzwerk ist, wurde bewusst für die Nutzung unter Klarnamen an den Markt gebracht. Sinn und Zweck einer solchen Plattform ist eben auch, schnell ein Netzwerk aufbauen zu können. Man identifiziert Mitmenschen, die man auf diesem Netzwerk unter Umständen kontaktieren möchte, üblicherweise mit dem Klarnamen. Darüber hinaus führt die Verwendung von Klarnamen auch zu einem anderen Umgang miteinander. Ich denke das ist intuitiv verständlich. Gleichzeitig ist es aber ein Netzwerk, welches sich nach wie vor in der Entwicklung befindet. Viele Dinge werden im laufenden Betrieb angepasst und dazu gehört auch, die Erwägung, Pseudonyme zuzulassen. Ich kann allerdings nähere Zeiträume oder wie das konkret ausgestaltet werden wird, schlicht und einfach derzeit nicht mitteilen, weil das eine Option ist, die derzeit noch evaluiert wird.

Der Vorsitzende: Den Abschluss macht noch einmal Herr Allan. Es gab Fragen von allen Fraktionen an Sie.

Richard Allan (Facebook, Director EU-Policy, Dublin): Vielen Dank. Zunächst zu Herrn Jarzombeks Frage: Ich finde die Frage, in welchem Umfang wir Informationen über unsere Datenerfassungspraktiken offenlegen, durchaus legitim. Ich halte uns in Sachen Datenschutz durchaus für führend auf dem Markt. Wenn Sie sich die kürzlich veröffentlichten neuen Datenschutzrichtlinien von Facebook ansehen, stellen Sie fest, dass sie verständlicher und einfacher geworden sind – ob auf Englisch, Deutsch oder Französisch oder jeder anderen Sprache, in der sie angeboten werden – als die meisten anderen Datenschutzrichtlinien. Sie gehen auch auf Punkte wie unsere Werbepraxis ein, damit Benutzer genau wissen, wie sie funktionieren. Sie haben speziell nach Informationen für Nichtnutzer gefragt. Ich glaube, in diesem Bereich könnten wir uns tatsächlich noch verbessern. Wir haben festgestellt, dass einige unserer Partner, die unsere Services auf ihren Websites einsetzen, in ihrer Datenschutzrichtlinie klar und für jeden verständlich erklären, was passiert, wenn Sie eine Website mit Plugins besuchen. Ich finde, das ist einer der Bereiche, die wir mit Kollegen in der Regulierungs- und Selbstregulierungs-Community in Deutschland besprechen müssen: Wie stellen wir diese vollständige Transparenz für Websites in Deutschland sicher? Ich möchte auf die Frage der Ansprechpartner zum Schluss im Zusammenhang mit der Beantwortung der Fragen von Herrn von Notz zurückkommen.

Was die Frage von Herrn Reichenbach betrifft, glaube ich, war es Herr Schaar oder Herr Dr. Weichert, der ganz richtig darauf hingewiesen hat, dass es nicht nur um IP-Adressen, sondern auch um Cookies geht. Beide können auf unterschiedliche Weise als Kennung verwendet werden. Über Cookies hat der Benutzer natürlich eine viel bessere Kontrolle, er kann sie jederzeit aus seinem Browser löschen und sie sind rechner- und browserspezifisch. Doch es sind eben diese Cookies, die die Grundlage unserer Sicherheitsmaßnahmen bilden. Dem Sicherheitsteam wäre es lieber, auch die zugehörige IP-Adresse zu haben, und wir haben sogar darum gestritten, weil die IP-Adresse einen klaren Sicherheitswert hat. Aber bei all diesen Entscheidungen gilt es, die richtige Balance zu finden: genügend Informationen, um für Sicherheit des Service zu sorgen, aber nicht zu viele Daten zu sammeln, die man nicht benötigt. Und

nach meinem Verständnis ist in den europäischen Datenschutzgrundsätzen und dem deutschen Recht klar festgelegt, dass keine derartige Auswertung stattfinden darf. Im Übrigen werden die Auswertungen ständig aktualisiert. Jetzt, wo das ULD diese Praktiken kritisiert hat, werden wir uns diesem Bereich selbstverständlich noch genauer widmen, um sicherzustellen, dass die Daten, die wir rechtmäßig speichern, ordnungsgemäß behandelt werden und wir dies auch begründen können.

Nun zu der Frage von Herrn Schulz bezüglich "Tag-Suggest". Ich möchte nur einen wichtigen Punkt betonen: Es geht nicht um automatisches Tagging. Facebook hat in sehr begrenztem Umfang die Gesichtserkennungstechnologie umgesetzt. Diese schlägt Tags nur zwischen Freunden vor. Wenn ich also der Facebook-Freund von Herrn Schulz wäre, der Tags für 50 Fotos oder eine große Anzahl von Fotos von sich gesetzt hat, könnte mir beim Hochladen eines Fotos vom heutigen Meeting angezeigt werden, dass es sich eventuell um Herrn Schulz handelt. Aber das muss ich bestätigen, bevor das Tag gesetzt wird. Es gibt also kein automatisches Tagging. Das halte ich für einen sehr wichtigen Punkt. Auch hier halten wir unser Vorgehen für absolut legal, zumal wir es rechtzeitig angekündigt hatten. Im Dezember 2010 war auf den Titelseiten verschiedener Zeitungen auch in Deutschland zu lesen, dass wir diesen Service einführen. Wir halten dies im Rahmen unserer aktuellen Bestimmungen für legal. Die hamburger Datenschutzbehörde hat Bedenken angemeldet, die wir gerade prüfen. Es gibt also noch keine abschließende Entscheidung, aber ich glaube, Herr Dr. Caspar von der hamburger Datenschutzbehörde erwartet bis zum 7. November eine abschließende Entscheidung. Er hat uns eine klare und angemessene Frist gesetzt. Wir befinden uns in der abschließenden Phase dieser Diskussion, wobei bis zum Ende dieser Verhandlungen weiter Foto-Tags vorgeschlagen werden.

Was die Frage von Frau Dr. Sitte bezüglich der Verwendung von Pseudonymen und des Gesprächs mit dem Bundesminister der Innern angeht, kann ich sagen, dass sich die Lage dadurch in einem gewissen Umfang zwar, aber noch nicht vollständig entspannt hat. Ich finde, wir sollten unbedingt konstruktiv darauf hinarbeiten, zu Ergebnissen zu kommen. Wir befürchten, ehrlich gesagt, dass potenzielle Nutzer in Deutschland vor einer Nutzung unserer Services zurückschrecken könnten, weil ihnen gerichtliche Schritte drohen könnten. Es ist doch klar, dass dies Anlass zur Sorge bereitet. Wir finden, dass dies voreilig war, und würden es auch hier sehr begrüßen, wenn die Behörden lieber versuchen würden, Mechanismen zu finden, wie Organisationen in Deutschland unsere Services legal nutzen können, bevor man eine Klage gegen sie anstrengt, und dass der vom Innenministerium eingeleitete Prozess hier eine effektive Möglichkeit sein könnte, dass die Industrie und die Behörden in Deutschland sich zusammensetzen und entscheiden, wie eine gute Praxis für die von uns verwendeten Technologien aussieht, die wir dann branchenweit einsetzen würden. Ich glaube, das wird auch den deutschen Organisationen und Unternehmen helfen, weil wir nicht immer und immer wieder dieselben Argumente durchkauen müssen, wenn neue Services entwickelt werden, was in dieser Branche unvermeidbar ist. Das erhoffen wir uns von diesem Prozess.

Zur möglichen Verwendung von Pseudonymen habe ich dem Fraktionsvorstand der Bündnisgrünen im Deutschen Bundestag eine lange Antwort geschickt. Ich sende Ihnen separat die entsprechenden

Argumente, damit Sie sich ein Bild machen können. Lassen Sie mich nur so viel sagen: Wir hegen große Sympathie für Menschen, die Services unter einem Pseudonym nutzen möchten – speziell Menschenrechtsaktivisten usw., aber wir haben noch keine Möglichkeit gefunden, wie wir einen Service bereitstellen können, in dem wir die Integrität der Menschen schützen, die dort mit anderen realen Menschen interagieren (was zahlreiche sicherheitsbezogene und wertvolle Vorteile bietet) und gleichzeitig bestimmte Ausnahmen von dieser Richtlinie zulassen können. Bei jeder Ausnahme müssen wir entscheiden, wer die Guten und Bösen sind – wer also ein Pseudonym verdient oder, wie beispielsweise Geheimdienste, nicht verdient. Bisher haben wir dafür keinen praktikablen Weg gefunden, also bleiben wir bei unserem Grundsatz, dass auf Facebook die wahre Identität zu verwenden ist. Es wird interessant sein zu sehen, was unsere Kollegen bei Google sich im Hinblick auf eine Änderung ihrer Richtlinien ausdenken. Ich werde Ihnen die gesamte ausführliche Argumentation schicken, wofür uns jetzt leider die Zeit fehlt.

Zurück nun zur Frage von Herrn Dr. von Notz und Herrn Jarzombek, ob wir genug getan haben, um uns mit Ihnen zu verständigen: Ein klares Nein. Bisher haben wir uns noch nicht genug mit Ihnen befasst. Wird sich das ändern? Ja. Meine Kollegin Frau Kirschsieper befindet sich bereits als Ihre Ansprechpartnerin in Berlin, und vielleicht haben Sie auf Facebook die Ausschreibung für eine zweite politische Position gesehen. Wir verbreiten über unsere Plattform gezielt Informationen für Menschen in der Hauptstadtregion, die sich für Politik interessieren könnten, also wahrscheinlich auch an einige von Ihnen. Wir wollen wirklich enger mit Ihnen zusammenarbeiten. Ich weiß allerdings, dass ich a) nicht in Deutschland lebe und b) kein Deutsch spreche und Ihnen deshalb nur in eingeschränktem Umfang nützlich sein kann, also möchte ich dies wettmachen. Bitte schicken Sie mir Ihre Vorschläge. Wir wissen sehr wohl, dass wir bei der Einführung eines neuen Services, der naturgemäß Bedenken weckt, unbedingt dafür sorgen müssen, dass Sie die nötigen Informationen erhalten, um politische Entscheidungen fundiert treffen zu können. Deshalb verspreche ich Ihnen hier und heute, noch mehr zu tun.

Wäre es am einfachsten, unsere Aktivitäten nach Deutschland zu verlagern? Das kann ich heute nicht sagen. Es ist sicher nicht zu erwarten und eher unrealistisch. Wie zuvor gesagt, haben wir eine Struktur geschaffen, eine europäische Struktur mit Firmensitz in einem bestimmten Land, und das muss sich auch in unseren rechtlichen Praktiken widerspiegeln.

Der Vorsitzende: Es gab noch Fragen von Thomas Jarzombek an die Vertreter der Ministerien. War das an beide Häuser gerichtet? Gut, dann bitteschön.

MD Hans-Heinrich von Knobloch (Leiter der Abteilung Staats-, Verfassungs- und Verwaltungsrecht, Bundesministerium des Innern): Es handelt sich sicherlich hier um das Problem der Auftragsdatenspeicherung. Das ist ein Komplex, wie viele andere auch in dem Zusammenhang, weshalb wir ihn bei den weiteren Überlegungen berücksichtigen werden. Vielen Dank.

Der Vorsitzende: Soweit die Antworten. Ich möchte mich bei den Sachverständigen und auch den Vertretern der Bundesregierung bedanken. Insbesondere bei den Sachverständigen, denn Sie hatten teilweise eine weite Anreise. Herr Allan, ein Zweitwohnsitz in Berlin oder Kiel wäre wahrscheinlich empfehlenswert, denn Sie sind ein gefragter Mann. Das wird sich sicher auch in den kommenden Monaten nicht ändern. Als Kieler kann ich Ihnen Schleswig-Holstein auch in dieser Hinsicht besonders ans Herz legen. Herr Dr. Weichert freut sich auch schon, genau. Danke an die Kolleginnen und Kollegen, dass sie noch die Geduld aufgebracht haben, denn wir haben leicht überzogen. Ich denke, dass zwar einige Fragen beantwortet werden konnten, viele aber auch noch offen geblieben sind und wir deshalb im Gespräch bleiben werden. Dazu wollte der Unterausschuss Neue Medien heute einen Beitrag leisten. Danke nochmals für Ihre Teilnahme. Die Sitzung ist hiermit geschlossen.

Schluss der Sitzung: 14:40 Uhr

Sebastian Blumenthal, MdB
Vorsitzender