

Vernehmlassungsantwort zum Fernmeldegesetz (FMG)

Swiss Internet User Group (SIUG)

14. Oktober 2002

Die SIUG ist eine Non-Profit-Organisation, die sich aus Internetexperten verschiedener Stufen zusammensetzt. Dazu gehören Akademiker aus verschiedenen Fachgebieten, Experten aus dem ISP-Bereich, selbständige Informatiker und Anwender. Das Ziel der SIUG ist es, sich für eine vernünftige Anwendung, Entwicklung und Reglementierung des Internets und verwandter Technologien einzusetzen, ohne dabei den ursprünglichen offenen Geist und die Tradition des Mediums übermässig einzuschränken.

Swiss Internet User Group (SIUG)
Postfach 1908
8021 Zürich
Mail siug@siug.ch
Web <http://www.siug.ch/>

Kontakt:

Matthias Leisi
Zürichweg 5, 8153 Rümlang
Telefon 043 211 03 55, Fax 043 211 03 56
Mail matthias.leisi@siug.ch

Inhaltsverzeichnis

1 Allgemeiner Teil	3
2 Besonderer Teil	3
2.1 Artikel 4, Meldepflicht	3
2.2 Artikel 11 <i>b</i> , Verbot der Bündelung von Diensten	4
2.3 Artikel 12 <i>a</i> , Informationen über die Qualität der Dienste	4
2.4 Artikel 12 <i>b</i> , Preise für Mehrwertdienste	5
2.5 Artikel 12 <i>d</i> , Verzeichnisse	6
2.6 Artikel 13 <i>a</i> , Datenverarbeitung; 13 <i>b</i> , Amtshilfe	6
2.7 Artikel 16, Umfang der Grundversorgung	7
2.8 Artikel 19 <i>a</i> , Auskunftspflicht des Bundesamtes	7
2.9 Artikel 21, Zugang zu den Verzeichnissen	7
2.10 Artikel 28, Zuteilung und Verwaltung	8
2.11 Artikel 29, Auskunftspflicht	8
2.12 Artikel 38, Finanzierung der Grundversorgung	8
2.13 Artikel 44 <i>a</i> , Standortdaten	9
2.14 Artikel 45, Auskunft	9
2.15 Artikel 45 <i>a</i> , Unerwünschte Mitteilungen; UWG Artikel 3 Bst. n	9
2.16 Artikel 46, Persönlichkeitsschutz	12
2.17 Artikel 48 <i>a</i> , Sicherheit und Verfügbarkeit	13
2.18 Artikel 49, Fälschen oder Unterdrücken von Informationen	13
2.19 Verordnung über die Adressierungselemente im Fernmeldebereich, Artikel 9	14
3 Schlussbemerkungen	14

1 Allgemeiner Teil

Die SIUG begrüsst die allgemeine Stossrichtung der Änderung des Fernmeldegesetzes in Richtung der Angleichung an den europäischen Rechtsrahmen und erhöhter Transparenz und mehr Wettbewerb. Insbesondere im Bereich des Internets sollten aus Sicht der SIUG jedoch einige Differenzierungen vorgenommen werden, um den Spezifika dieses Mediums gerecht zu werden.

Insbesondere unterstützt die SIUG die angestrebten Verbesserungen im Konsumentenschutz. Neben einer graduellen Neupositionierung der marktbeherrschenden Anbieterin hin zu mehr Wettbewerb sieht die SIUG in der Schaffung einer Schlichtungsstelle einen entscheidenden Beitrag zur Erreichung der Ziele der Gesetzesrevision.

Der SIUG ist es ein besonderes Anliegen, dass die Bekämpfung von unerwünschten Mitteilungen im Rahmen der Revision berücksichtigt wird. Insbesondere per E-Mail und im Usenet ist "Spamming" mittlerweile nicht mehr nur eine Lappalie, sondern eine ernsthafte Einschränkung der Nutzbarkeit.

Der Mail-Dienstleister GMX hat für seinen eigenen Dienst festgestellt, dass jedes siebte Mail ein Spam-Mail ist.¹ Die technisch vertretbaren Massnahmen sind längst in Kraft, können aber prinzipbedingt nie ausreichend sein. Die Menge an unerwünschten Mitteilungen ist mittlerweile so weit angewachsen, dass kaum mehr zumutbare Massnahmen getroffen werden müssen, um der Flut Herr zu werden.²

Die SIUG schlägt deshalb einige Präzisierungen und Erweiterungen vor, die sich auch an den Erfahrungen mit anderen Gesetzgebungen zu Spam respektive anderen laufenden Gesetzesvorhaben orientieren (EU Direktive 2002/58/EG, Novellierung von §101 des österreichischen Telekommunikationsgesetz, Spam-Gesetze einiger us-amerikanischer Bundesstaaten³).

Neben der Regelung von Spam auf der Ebene von Gesetz und/oder Verordnung muss das Problem auch international angegangen werden. Es sollte Aufgabe des Bundesamtes und der Kommission sein, sich in internationalen Gremien für eine möglichst einheitliche Regelung stark zu machen.

2 Besonderer Teil

2.1 Artikel 4, Meldepflicht

Es ist zu klären, inwiefern Anbieterinnen von Internetdienstleistungen (Zugangsprouder, Webhoster, Anbieterinnen von Shell-Zugängen u.a.) von der Neuformulierung erfasst werden. Es ist zu beachten, dass eine zu weite Definition eine grosse Zahl von Hobby-Anbietern erfassen würde, was sowohl mit einem grossen administrativen Aufwand als auch mit noch unklaren Konsequenzen für diese Anbieterinnen verbunden wäre. Gerade mit den sich stark verbreitenden ADSL- und TV-Kabel-Anschlüssen wird es für private Personen immer leichter, kleine

¹Quelle: Pressemitteilung der GMX AG, München, vom 13. August 2002, <http://www.gmx.net/de/cgi/presse.cms?AREA=200208131>

²Als Beispiel: Die Moderation der internationalen Newsgroup news.answers erhielt in der Woche vom 4. bis 11. August 500 Spam-Mails, d.h. über 70 Stück pro Tag.

³Quelle: <http://www.spamlaws.com/>

eigene Dienstleistungen für ihren Freundes- und Bekanntenkreis anzubieten. Das Gesetz sollte diesen Hobby-Anbietern nicht die gleichen Pflichten auferlegen wie professionellen Anbieterinnen.

2.2 Artikel 11b, Verbot der Bündelung von Diensten

Es ist zu prüfen, inwieweit gemeinsame Werbe- und Marketingaktionen sowie das Cross-Selling von marktbeherrschenden Anbieterinnen und von ihr beherrschter Drittunternehmen eingeschränkt werden sollen. Zu denken ist etwa an Rechnungen der Swisscom Fixnet, denen Werbematerial für Dienste von Swisscom-Tochterunternehmen (Bluewin, Swisscom Mobile, ...) beiliegen.

Die SIUG schlägt deshalb im Sinne des Konsumentenschutzes und der Eindämmung von unerwünschten Werbesendungen einen neuen Absatz 3 in Artikel 11b vor:

Art. 11b Verbot der Bündelung von Diensten

...

³ Sie stellt sicher, dass im Rahmen von Korrespondenz mit Kundinnen und Kunden über Geschäfte der Grundversorgung keine Werbe- und Marketingmassnahmen für Drittunternehmen, auf die sie einen beherrschenden Einfluss hat, durchgeführt werden.

2.3 Artikel 12a, Informationen über die Qualität der Dienste

Die Anbieterinnen von Internetdiensten haben verschiedene technische Optionen zur Ausgestaltung ihrer Dienstleistungen, etwa durch Filterung und Umleitung von Datenströmen. Diese Einschränkungen von ungehindertem Internet-Zugang sind für den Endkunden nicht immer im Voraus zu erkennen, können aber zu Einschränkungen in der Nutzung führen. Beispiele für solche Einschränkungen:

- *Verwenden von privaten IP-Adressen.* Die Anbieterin erspart sich damit offizielle IP-Adressen, während die Kundinnen einige Dienste (FTP, diverse Chat-Funktionen) nur mehr eingeschränkt nutzen können.
- *Zwangsproxies,* die den ganzen Web-Datenverkehr über ein zusätzliches Gateway lenken. Die Anbieterin kann dadurch allenfalls Kosten für übertragene Datenvolumen sparen, Werbung einblenden, und sonst in den Datenverkehr eingreifen. Kundinnen und Kunden haben kaum praktikable Möglichkeiten, einen Zwangsproxy zu umgehen.
- *Sperren von einzelnen Ports.* Anbieterinnen können den Datenverkehr zu / von einzelnen Ports⁴ sperren, um so gewisse Dienste gänzlich unzugänglich zu machen. Kundinnen und Kunden erhalten meist unspezifische oder technische Fehlermeldungen, die von Laien kaum richtig interpretiert werden können. Zudem erwecken diese Fehlermeldungen bei den Kunden oftmals den Anschein, dass ein entfernter Dienstleistungsanbieter technische

⁴Ports sind "Unteradressen" von Internetadressen. In der Regel ist jedem Dienst eine Portnummer zugeordnet, dem Web (http) beispielsweise der Port 80, oder dem Mailverkehr die Ports 25 (smtp, zum Versenden) und 110 (pop3, zum Empfangen).

Probleme aufweist. Dies kann den entfernten Dienstleistungsanbieter in ein schlechtes Licht rücken.

- *Sperren von einzelnen IP-Adressen.* Anbieterinnen können den Datenverkehr zu / von einzelnen IP-Adressen⁵ sperren, um so mehrere Dienste von bestimmten Rechnern unzugänglich zu machen. Kundinnen und Kunden erhalten meist unspezifische oder technische Fehlermeldungen ("Verbindung abgelehnt" oder ähnlich), die von Laien kaum richtig interpretiert werden können. Weiters kann die gleiche Argumentation wie bei Portsperrern angewendet werden.

Im Gesetz ist daher eine Informationspflicht der Anbieterinnen von Internetdienstleistungen über die *Einschränkungen* gegenüber einem vollwertigen und unmodifizierten Internetzugang vorzusehen. Die SIUG schlägt deshalb einen neuen Absatz 3 in Artikel 12b vor:

Art. 12a Informationen über die Qualität der Dienste

...

³ Die Anbieterinnen von fernmeldetechnischen Übertragungen von Daten werden verpflichtet, Informationen über die Einschränkungen von Datenübertragung und -verbindungen gegenüber internationalen Normen zu veröffentlichen. Das Bundesamt legt Inhalt und Form der Veröffentlichung fest.

2.4 Artikel 12b, Preise für Mehrwertdienste

Preisobergrenzen zur Bekämpfung des Missbrauchs von Mehrwertdiensten sind zu begrüßen. Wie die Erfahrungen mit sogenannten Dialern (Programme, welche unbemerkt Verbindungen zu Mehrwertdiensten aufbauen) insbesondere in Deutschland zeigen, sind Preisobergrenzen pro Zeiteinheit respektive pro Anruf nicht ausreichend. Vielmehr muss eine Obergrenze des gesamten Rechnungsbetrags für Mehrwertdienste vorgesehen werden.

Die Anbieterinnen haben gegenüber den Kundinnen und Kunden erhebliche Druckmittel durch die Androhung einer Anschlussperre. Dieses Mittel sollte nicht bei Streitigkeiten um Mehrwertdienste eingesetzt werden können, da sonst Kundinnen und Kunden zum Akzeptieren strittiger Rechnungen gedrängt werden könnten. Die Formulierung eines entsprechenden Absatzes 3 lässt die SIUG offen.

Die SIUG schlägt ansonsten die folgende Formulierung von Artikel 12b vor:

Art. 12b Preise für Mehrwertdienste

¹ Zur Verhinderung von Missbräuchen kann der Bundesrat Preisobergrenzen für auf Fernmeldediensten aufbauende Mehrwertdienste festsetzen, die von Dritten erbracht werden und von Anbieterinnen von Fernmeldediensten in Rechnung gestellt werden.

² Die Anbieterinnen müssen ihren Kunden die Möglichkeit geben, Betragsobergrenzen für Mehrwertdienste festzulegen. Die Kommission kann Betragsobergrenzen festlegen, die bis auf den Änderungswunsch der Kundinnen und Kunden zu gelten haben.

⁵IP-Adressen sind technisch die "eigentlichen" Adressierungselemente im Internet. Jeder an das Internet angeschlossene Rechner, auch Endkunden, verfügen zumindest für die Dauer einer Verbindung über eine solche Adresse.

³ (Formulierung offen)

2.5 Artikel 12d, Verzeichnisse

Die Anbieterinnen von Mehrwertdiensten sind im Missbrauchsfall durch Unter-(unter)vermietung von Nummern(blöcken) schwierig zu eruieren. Es sollte daher eine zentrale Stelle respektive ein zentrales Verzeichnis vorgesehen werden, um den Kundinnen und Kunden einen vereinfachten Zugriff auf die Anbieterinnen zu ermöglichen. Um eine Anbieterneutralität sicherzustellen, sollte dieses Verzeichnis unter der Aufsicht des Bundesamtes stehen.

Sollte eine Anbieterin in der Schweiz nicht belangbar sein, sollte ersatzweise die vorangehende Anbieterin in der "Vermietungskette" belangt werden können. Als Konsequenz müsste jede Anbieterin, die Nummern(blöcke) für Mehrwertdienste direkt zugewiesen bekommt in der Schweiz domiziliert sein.

Die SIUG verzichtet auf einen Formulierungsvorschlag, da dieses Anliegen allenfalls nicht in Artikel 12d alleine berücksichtigt werden kann.

Die SIUG steht dem Absatz 2 wohlwollend gegenüber, möchte allerdings noch einen Schritt weiter gehen: Die Eintragung in öffentliche Verzeichnisse sollte nicht der Standardfall sein, sondern nur auf besonderen Wunsch der Kundinnen und Kunden erfolgen (siehe auch die Anmerkungen zu Artikel 21, Seite 7, und zu Artikel 45a, Seite 11).

Für Absatz 2 ist allenfalls zu prüfen, ob die Kundinnen und Kunden die einzutragenden Daten gänzlich frei bestimmen dürfen, oder ob gewisse Einschränkungen bezüglich Korrektheit von Adressierungselementen vorzusehen sind.

Die Europäische Union geht in der Richtlinie 2002/58/EG in Artikel 12 [sic] detailliert auf Teilnehmerverzeichnisse ein. Dabei wird den Kundinnen und Kunden insbesondere das Recht auf die gebührenfreie Bestimmung über die Nutzungszwecke ihrer Daten gegeben; darüber hinaus wird eine Auskunftspflicht über Suchmöglichkeiten festgelegt. Die SIUG unterstützt die Zielrichtung und die Ausgestaltung von Artikel 12 der Richtlinie und empfiehlt eine sinngemässe Regelung für das Fernmeldegesetz.

2.6 Artikel 13a, Datenverarbeitung; 13b, Amtshilfe

Die SIUG kann die uferlose Ausweitung der Verletzung der Persönlichkeitsrechte, wie er in den Artikeln 13a und 13b zum Ausdruck kommt, in keiner Weise unterstützen.

Weder die Kommission noch das Bundesamt benötigen im Rahmen des FMG die Kompetenz, Personendaten, und schon gar nicht Persönlichkeitsprofile, von Kundinnen und Kunden zu bearbeiten.

Es geht nicht an, dass zusätzliche Überwachungskompetenzen quasi über die Hintertüre eingeführt werden; wenn schon, dann sind solche Kompetenzen in BÜPF/VÜPF (SR 780.1 und 780.11) vorzusehen.

Die SIUG bemängelt zudem, dass keinerlei Bestrebungen ersichtlich sind, die Verletzungen der Persönlichkeitsrechte durch eine unabhängige Stelle zu kontrollieren und dass keine öffentliche Rechenschaft über die Sammelaktivitäten vorgesehen sind.

Die in Artikel 13a Absatz 1 nur schwach eingeschränkte Kompetenz („... unerlässlich ist.“) ist inakzeptabel.

Die Absätze 2 und 3 ergeben sich eigentlich schon aus dem Datenschutzgesetz (DSG, SR 235.1); die Präzisierung in Absatz 3 sollte aber auch auf der Stufe des FMG festgelegt werden.

Es ist nicht einzusehen, warum die Kommission und das Bundesamt die Kompetenz erhalten sollen, besonders schützenswerte Personendaten (DSG Art. 3 Bst. c.) weiterzugeben (und damit implizit auch zu beschaffen). Damit erhalten Kommission und Bundesamt eine Blankoerlaubnis zum Sammeln von zum Beispiel religiösen und politischen Ansichten, über die Intimsphäre, und so weiter.

2.7 Artikel 16, Umfang der Grundversorgung

Neben den grundlegenden Telefondiensten und den Möglichkeiten zur Datenübertragung sollte auch der Zugang zu breitbandigen Datenverbindungen in die Grundversorgung aufgenommen werden, wo dies technisch möglich ist. Daher schlägt die SIUG die folgende Formulierung von Art. 16 Bst. a vor:

Art. 16 Umfang der Grundversorgung

¹ ...^a den öffentlichen Telefondienst, [...] Übertragung von Daten mit Datenraten *des mehrfachen* wie sie über die Übertragungswege für Sprache geleitet werden können ...

In Buchstabe d wird das Führen von Verzeichnissen der Grundversorgung der Grundversorgungskonzessionärin übertragen. Um den möglichen Missbrauch der marktbeherrschenden Stellung auch bei Verzeichnisdiensten von vornherein auszuschliessen ist zumindest eine Aufsicht durch das Bundesamt / die Kommission vorzusehen. Idealerweise würde dieses Verzeichnis aber vom Bundesamt selbst geführt, um einen diskriminierungsfreien Zugang zu den Verzeichnisdaten sicherzustellen. Die SIUG schlägt hier keine konkrete Formulierung vor, da dieses Anliegen allenfalls im Zusammenhang mit den Artikeln 12d und 21 eingebracht werden muss.

2.8 Artikel 19a, Auskunftspflicht des Bundesamtes

Aus dem Wortlaut von Artikel 19a ist nicht ersichtlich, ob die "Rechte und Pflichten" auch finanzielle Abgeltungen und Berechnungsgrundlagen umfasst. Es muss auf jeden Fall sichergestellt werden, dass in diesem (ehemaligen Monopol-) Bereich Transparenz geschaffen wird.

2.9 Artikel 21, Zugang zu den Verzeichnissen

Verzeichnisse sollten grundsätzlich "Opt-In" sein, das heisst Eintragungen erfolgen nur dann, wenn der Kunde oder die Kundin dies explizit wünschen. Umso mehr gilt dies aufgrund des hohen Missbrauchpotentials für E-Mail-Verzeichnisse. Die Verbindung von Namen, Adressen und Kommunikationsparametern ist im Hinblick auf den Datenschutz und auf automatisierte Suchmöglichkeiten mit Vorsicht anzugehen.

Insofern gehen "Mehrwertverzeichnisse" weit über den Bereich der Grundversorgung hinaus; eine Regulierung muss über die Grundsätze des DSGVO (SR 235.1) erfolgen, namentlich bei der Zweckgebundenheit der Beschaffung. Eine Präzisierung ist insofern wünschenswert, als dass verhindert werden muss, dass

1. sich die Grundversorgungskonzessionärin durch Verzeichnisse der Dienste der Grundversorgung einen Wettbewerbsvorteil gegenüber Mitbewerberinnen verschafft;
2. Einträge in Verzeichnisse der Grundversorgung von der Zustimmung zur weiteren Nutzung und Verknüpfung von Daten abhängig gemacht wird; und
3. die Daten missbräuchlich verwendet werden können (etwa zum Adressieren von unerwünschten Werbemittelungen, Spam).

Gerade E-Mail-Adressen fallen nicht unter den Bereich der Grundversorgung, da es sich um Dienste in höheren Protokollschichten handelt, die nicht ortsgebunden sind. Ein generisches Verzeichnis "schweizerischer" E-Mail-Adressen, oder gar ein Zwang, Daten zu einem solchen zu liefern, ist nicht praktikabel.

2.10 Artikel 28, Zuteilung und Verwaltung

Die vorgeschlagenen Änderungen werden von der SIUG begrüsst; sie sind im Einklang mit der Position der SIUG zu Domainnamen.⁶

2.11 Artikel 29, Auskunftspflicht

Der aktuelle Wortlaut von Artikel 29 könnte im Hinblick auf Domainnamen klarer formuliert werden, da er die Inhaber von Second-Level-Domains⁷ verpflichten könnte, Informationen über die weitere Verwendung von Adressierungselementen, also Third-Level-Domains usw., der zuständigen Behörde bekanntzugeben.

2.12 Artikel 38, Finanzierung der Grundversorgung

Je nach Anwendung der Meldepflicht gemäss Artikel 4 (Seite 3) ist zu klären, inwiefern auch Internetprovider zur Finanzierung der Grundversorgung beigezogen werden. Zu denken ist hier insbesondere an nicht gewinnorientierte Anbieterinnen; zudem ist zu bedenken, dass gewisse Internetprovider aufgrund ihres Angebotes (zum Beispiel Anbieterinnen von Mailedienstleistungen) vor allem mit ausländischen Internet Providern konkurrenzieren und durch die Pflicht zu Beiträgen an die Grundversorgung Wettbewerbsnachteile zu tragen hätten.

Die Kosten, die den Anbieterinnen von Fernmeldediensten respektive deren Kundinnen und Kunden entstehen, müssen gegenüber den Kundinnen und Kunden transparent nachweisbar sein.

⁶<http://www.saug.ch/positionen/SIUG-Domain.shtml>

⁷Eine Top-Level-Domain ist z.B. ".ch", eine Second-Level-Domain "admin.ch.", eine Third-Level-Domain "uvek.admin.ch." usw.

2.13 Artikel 44a, Standortdaten

Die SIUG unterstützt die eng gefasste Formulierung dieses Artikels. Eine Verdeutlichung gemäss folgender Formulierung wäre wünschenswert:

Art. 44a Standortdaten

... oder an Dritte weitergeben.

Analog Artikel 20 sollte auch hier eine Ausnahme für Notrufe und ähnliches vorgesehen werden.

2.14 Artikel 45, Auskunft

Im Sinne des Konsumentenschutzes sollten Auskünfte gemäss Artikel 45 kostenfrei erfolgen; die "kann"-Formulierung sollte jedoch aus Sicht des Datenschutzes beibehalten werden.

2.15 Artikel 45a, Unerwünschte Mitteilungen; UWG Artikel 3 Bst. n

Die SIUG begrüsst grundsätzlich den neuen Spezialtatbestand in UWG Art. 3 Bst. n und in FMG Art. 45a betreffend "Spamming". Gleichzeitig ist sich die SIUG bewusst, dass die vorgeschlagene Regelung nur von beschränktem Nutzen ist, da Verursacher und Profiteure von Spam ihren Sitz in vielen Fällen nicht in der Schweiz haben.

Die unten begründete und vorgeschlagene Formulierung von Art. 45a deckt sich konzeptionell mit Artikel 13 der EG Direktive 2002/58/EG, insbesondere im "Opt-In"-Gedanken sowie im Verbot der Verschleierung von Absenderinformationen.

Die Änderungsentwurf vorgeschlagene Regelung ist in dieser Form allerdings nicht praktikabel, da die Anbieterinnen von Fernmeldedienstleistungen nicht wissen können, welche ihrer Kundinnen untereinander oder mit fremden Dienstleistungsanbietern bereits bestehende Geschäftsbeziehungen unterhalten oder dem Empfang von Werbemitteilungen ihre Zustimmung gegeben haben. Die Rolle der Internetprovider kann sich nur auf das Verhindern des Missbrauchs ihrer Daten-netzwerke und Dienstleistungen beschränken.

Seit der Einreichung der Motion Sommaruga⁸ haben einige technische Neuerungen Einzug gehalten, die zusätzlich berücksichtigt werden müssen, um das Gesetz effizient anwenden zu können. Dazu zählen der Missbrauch von fremden Systemen und Adressierungselementen beim Spamming sowie weitere Medien neben Mail, namentlich Usenet, Web-basierte Mitteilungsdienste (Formmail-Scripts), Instant Messaging (IRC, ICQ, ...) und nicht zuletzt SMS.

Anbieterinnen von Fernmeldediensten tragen *immer* zur Übermittlung unerwünschter Werbemitteilungen an ihre Kundinnen und Kunden bei, und sei es nur durch das Zurverfügungstellen von z.B. Mailservern zum Empfang. Die Betreiber von Mailservern können zwar die Menge von Werbemitteilungen etwas einschränken (zum Beispiel durch den Einsatz von Listen bekannter "offener" Mailserver, die zum Spamming missbraucht werden können). Solche *Blocklisten* sind jedoch nicht

⁸00.3393: Elektronische Massenwerbesendungen. "Spamming", AB 2000 N 1196 und AB 2001 E 109

vollständig zuverlässig und können auch *false positives* erzeugen, d.h. es können auch erwünschte bzw. erwartete Mails geblockt werden. Von daher dürfen die Betreiber von Mailservern nicht *verpflichtet* werden, solche technischen Mittel zu ergreifen; natürlich können die Anbieterinnen solche Blocklisten bereits heute und in Zukunft im Rahmen ihrer vertraglichen Beziehungen mit den Kundinnen und Kunden einsetzen. Es ist wünschenswert, dass solche Filtersysteme den Kunden wahlweise zur Verfügung gestellt werden; daraus eine Pflicht abzuleiten geht aber über das wünschenswerte hinaus.

Hingegen sollten Anbieterinnen von Fernmeldediensten verpflichtet werden, aktives Spamming von ihren Systemen aus zu unterbinden. Verantwortungsvolle Anbieterinnen wenden heute schon entsprechende Massnahmen an (z.B. Verwarnung respektive Kündigung von Zugängen bei Spamming, festgehalten in öffentlich einsehbaren AGBs oder technische Massnahmen).

Auch Gehilfschaft zu Spamming (Hosten von per Spam beworbenen Webseiten, Betreiben von Nameservern für beworbene Domains, ...) sollte im Art. 45a aufgeführt sein. Zudem sollten indirekte Dienstleistungen (z.B. Anbieterinnen von Wählzugängen) mit einbezogen werden. Da die Verursacher und Profiteure von Spam häufig technische und administrative Lücken in fremden Systemen ausnutzen, sollten zudem Vorkehrungen gegen die Verfälschung von Identität und Herkunft vorgesehen werden. Diese Vorkehrungen sollten umgekehrt nicht so weit gehen, dass anonyme Mitteilungen von privaten Personen nicht mehr möglich sind. Speziell in Foren (z.B. im Usenet oder im WWW) zur Selbsthilfe kann es angebracht sein, Diskussionen in anonymisierter Form zu führen, da ansonsten den Beteiligten schwere persönliche Probleme oder Nachteile entstehen könnten. Es ist hier wichtig darauf hinzuweisen, dass auch bei der herkömmlichen Briefpost nach wie vor anonyme Sendungen möglich und akzeptiert sind, trotz einiger damit verbundener Nachteile. Die Regelung sollte deshalb darauf beschränkt werden, im *kommerziellen* Umfeld (also z.B. für Werbesendungen) und für *Massenwerbesendungen* keine falschen Adressierungselemente verwendet werden dürfen.

Hauptproblem von "Spamming" ist die Kostenverschiebung, d.h. dass der Empfänger (respektive die Anbieterinnen) die Kosten für Übertragung, Verarbeitung und Speicherung zu tragen haben. Ein hartnäckiges Problem bei der Eindämmung von Spam ist die mangelnde Kooperationsbereitschaft seitens mancher Anbieterinnen, sei es aus Unkenntnis oder um den spammenden Kunden zu decken. Die SIUG schlägt deshalb die folgende Formulierung von Art. 45a vor (Alternativformulierungen in Klammern):

Art. 45a Unerwünschte Mitteilungen

¹ Anbieterinnen von Fernmeldediensten verhindern mit geeigneten und zumutbaren Massnahmen die (alternativ: wiederholte) Übermittlung von unerwünschten Massenmitteilungen zu Werbezwecken an Dritte durch ihre Kundinnen und Kunden, zu denen die Dritten keine ausdrückliche Zustimmung gegeben haben oder zu denen keine Geschäftsbeziehung besteht.

² Wer Fernmeldedienste zur Übermittlung unerwünschter Mitteilungen gemäss UWG Art. 3 Bst. n missbraucht, hat die Kosten der Anbieterinnen der Fernmeldedienste und der Empfänger zu tragen. Die Anbieterinnen der Fernmeldedienste (alternativ: und die Empfänger) können zu diesem Zweck angemessene, kostendeckende Pauschalen festlegen.

³ Auf keinen Fall dürfen Mitteilungen zu Werbzwecken versendet werden, bei denen die Identität des Absenders (alternativ: Verantwortlichen), in dessen Namen die Nachricht übermittelt wird, verschleiert oder verheimlicht werden. Ebenso dürfen keine fremden Adressierungselemente, Namens- und Nummernräume zur Verschleierung der wahren Identität verwendet werden.

⁴ Das Bundesamt regelt unter Beizug der Kommission und unter Berücksichtigungen aktueller Entwicklungen und des Stands der Technik Einzelheiten in einer Verordnung.

Absatz 1 definiert den Missbrauch analog dem vorgeschlagenen UWG Art. 3 Bst. n. Er soll Internetprovider dazu verpflichten, Spammer aus ihren Netzen auszuschliessen. Da Spam durch die Provider nicht im Voraus nebenwirkungsfrei erkannt werden kann, können die Provider auch erst nachträgliche Massnahmen gegen Spamer ergreifen. Diese umfassen z.B. Ermahnungen, das Kündigen des Vertrags, das Sperren des Internetzugangs oder das Einschränken von Dienstleistungen (namentlich das Sperren des Mailversands).

Absatz 2 berücksichtigt die Kostenverschiebung, indem den Missbrauchern die sog. "Cleanup Fees" aufgebürdet werden. Da diese im Einzelfall schwierig zu belegen sind, sollten Anbieterinnen die Möglichkeit haben, angemessene Pauschalen festzulegen. Beispielsweise legt die Spam-Gesetzgebung des US-Bundesstaates Kalifornien dazu einen Betrag von 50 US-Dollar pro Mail oder 25'000 US-Dollar pro Tag fest (California Business and Professions Code Section 17538.45).

Absatz 3 entspricht grösstenteils Artikel 13, Absatz 3 der EU Direktive 2002 / 58 / EG. Da es immer Grauzonen geben wird, was die Definition von "unerwünscht" betrifft, muss zumindest sichergestellt werden, dass die Fälschung der Identität unstatthaft ist. Spam-Versender verwenden in der Regel fremde Kennungen (d.h. Domainnamen und Absenderadressen) für ihr Tun.⁹ Die Schweizer Justizbehörden tun sich mit diesem offensichtlichen Missbrauch schwer und behandeln entsprechende Fälle nur sehr zögerlich. Analog ist auch der neue Buchstabe *m* von UWG Art. 3 (s. unten) sowie die vorgeschlagene Änderung in Artikel 49 (s. unten) zu begründen.

Absatz 4 dient dazu, eine gewisse Flexibilität in einem Umfeld zu erlangen, das einem schnellen Wandel unterworfen ist.

Den Anforderungen dieses Artikels kann eine Anbieterin z.B. durch eine entsprechende Gestaltung ihrer Allgemeinen Geschäftsbedingungen und durch ex-post Massnahmen bei erfolgtem Spamming (Mahnung, Kündigung) genügen.

Elektronische Teilnehmerverzeichnisse bieten sich als Quelle für automatisierte unerwünschte Werbemitteilungen besonders an. Als Verstärkung von Art. 45a bietet sich daher ein zusätzlicher Absatz in Art. 12d, Verzeichnisse, an (siehe auch 6).

Art. 12d Verzeichnisse

...

³ Die veröffentlichten elektronischen Verzeichnisse dürfen nicht für automatisierte Kontaktaufnahmen mit den verzeichneten Personen verwendet werden, sofern zuvor keine geschäftliche Beziehung bestand.

⁹Professionelle Spammer gehen noch einen Schritt weiter, indem sie "Routinginformationen", d.h. Beschreibungen für die "Datenwege" im Internet fälschen.

Die Vorgeschlagene Änderung von UWG Art. 3 zielt zwar in die richtige Richtung, verhindert aber *gezielte* persönliche Anrufe zu Werbezwecken. Solange diese gezielt und in *kleinem* Umfang erfolgen, sollten sie nicht unbedingt grundsätzlich verboten werden. Das Ziel des Gesetzes sollte es daher sein, automatisierte Werbemethoden mit Telekommunikationsmitteln zu unterbinden.

Gemäss dem oben gesagten sollte UWG Art. 3 wie folgt geändert werden:

UWG Artikel 3, Bst. n und m

Unlauter handelt insbesondere, wer:

n. Telekommunikationsmittel *automatisiert* zu Werbezwecken bei Personen verwendet, die dem nicht ausdrücklich zugestimmt haben und mit denen er oder sie nicht schon in einer Geschäftsbeziehung steht, *Daten zu diesem Zweck sammelt oder anbietet.*

o. Mitteilungen zu Werbezwecken unter Verwendung fremder Adressierungselemente oder von fremden Namens- und Nummernräumen versendet.

Alternativ-Vorschläge

In der Debatte um die Bekämpfung von Spam wird manchenorts vorgeschlagen, ein "Opt-Out"-Modell statt der im ursprünglichen Entwurf und in den obigen Absätzen vorhandenen "Opt-In"-Regelung vorzusehen. Eine Opt-Out-Regelung ist dadurch gekennzeichnet, dass Adressierungselemente grundsätzlich mit unerwünschten Mitteilungen bedient werden können, bis ein Widerspruch erfolgt.

Die SIUG ist vehement gegen eine Opt-Out-Regelung, da eine solche den Empfängerinnen und Empfängern zusätzliche Umtriebe und Kosten verursacht. Sog. "Robinson-Listen" haben sich im Umfeld von Spam nicht bewährt: über kurz oder lang wurden diese Listen als besonders wertvolles Adressmaterial verwendet oder verkauft. Zudem würde eine Opt-Out-Regelung zu grossen Massen von Werbemitteilungen führen und den Empfängern grosse Umtriebe zum Abbestellen der Mitteilungen auflasten.

Auch die von interessierten Marketingkreisen vorgeschlagenen Kennzeichnungen von unerwünschten Mitteilungen sind unzureichend. Einerseits werden sie von einschlägigen Spammern regelmässig ignoriert. Andererseits ist durch die am häufigsten propagierte Methode der Kennzeichnung (im Betreff einer Mail) kein effizientes Aussortieren von Mailsendungen auf dem Mailserver notwendig, da dazu jedes Werbemail vom Empfänger zuerst empfangen werden muss.¹⁰

2.16 Artikel 46, Persönlichkeitsschutz

Die Daten, welche Anbieterinnen von ihren Kundinnen und Kunden im Zug der Erbringung von Kommunikationsdienstleistungen erheben, bieten ein erhebliches

¹⁰Das SMTP-Protokoll, RFC 2822 ff. definiert lediglich zwei Abschnitte der Datenübertragung: im sog. "Envelope" (Umschlag) werden lediglich eine Serverkennung und die Absender- resp. Empfänger-Adresse übermittelt. Im "Data"-Abschnitt wird der ganze Rest der Mail übermittelt, inklusive der Betreff-Zeile. Das bedeutet, dass man ein Mail auf jeden Fall annehmen muss, auch wenn man kein Interesse an Werbemails hat, und somit die Kosten für die Übertragung und Verarbeitung zu tragen hat.

Potential zur Verletzung des Persönlichkeitsschutzes. Nach der Meinung der SIUG sollte der Umgang mit Log-Dateien und ähnlichen Aufzeichnungen im Grundsatz im FMG geregelt werden, wobei konkretere Anforderungen als etwa beim Datenschutzgesetz (SR 235.1) zu stellen sind.

Die zum Beispiel in Deutschland geltenden Regeln bedeuten in der Praxis, dass Daten nur soweit zu speichern sind, wie sie für die Rechnungslegung erforderlich sind; Detaildaten (zum Beispiel Informationen über Zeit und Ziel von Verbindungen) sind nach 80 Tagen zu löschen, sofern keine Gründe für eine längere Aufbewahrung sprechen; solche Gründe können zum Beispiel bestrittene Rechnungen/Forderungen oder hängige juristische Verfahren sein.

Log-Dateien und ähnliches sind, soweit sie zu technischen Gründen wie Performance-Messung, Feststellen von Netzmissbrauch und ähnlichem überhaupt notwendig sind, sollten in prinzipiell in anonymisierter Form angelegt werden, sofern das sinnvoll ist.

Die SIUG schlägt daher vor, den Artikel 46 in zwei Absätze aufzuteilen:

Art. 46 Persönlichkeitsschutz

¹ (bisheriger Artikel 46)

² Aufzeichnungen über das Kommunikationsverhalten der Kundinnen und Kunden sind nur dann persönlich zuordenbar anzulegen, sofern es für die Abrechnung oder aus technischen Gründen unabdingbar ist. Die Aufzeichnungen müssen nach drei Monaten gelöscht werden. Vorbehalten bleibt die Aufbewahrung aufgrund laufender Rechtsverfahren.

2.17 Artikel 48a, Sicherheit und Verfügbarkeit

Sicherheit und Verfügbarkeit sind nicht rein technische, sondern ganz besonders auch organisatorische und administrative Probleme. Insofern sollte der neue Artikel 48a ergänzt werden:

Art. 48a Sicherheit und Verfügbarkeit

Der Bundesrat kann für die Sicherheit und Verfügbarkeit der Fernmeldeanlagen oder -dienste technische *und organisatorische* Vorschriften erlassen.

2.18 Artikel 49, Fälschen oder Unterdrücken von Informationen

Es ist gängige Praxis von Spammern via E-Mail und per SMS, ihre Identität durch Missbrauch fremder Adressierungselemente zu verschleiern. Es ist zu erwarten, dass diese "Taktik" auch von anderen Versendern unerwünschter Mitteilungen angewendet werden wird. Dem gleichen Zweck dienen E-Mail-Spammern auch schlecht gesicherte Server und Proxies, nach denen diese das Internet systematisch und automatisiert absuchen. Die SIUG schlägt daher eine Ergänzung von Artikel 49 vor (siehe unten).

Zudem begrüsst die SIUG das Verbot des Fälschens und Unterdrückens von Informationen. Gerade im Zuge der grossen Unsicherheit unter den Internet Providern bzgl. illegaler Inhalte im Ausland, den daraus erfolgten Internetsperren durch

verschiedene Schweizer Provider mit den resultierenden Kollateralschäden drängt sich hier eine klare Regelung auf. Dies wäre auch im Sinne der Motion Pfisterer¹¹, die eine Straffreiheit für das bloss Übermitteln von Informationen vorsieht. Der hier vorgeschlagene weitergehende Schritt ist deshalb sehr zu begrüssen. Im Sinne der Anmerkungen zu Artikel 12a (Seite 4) ist jedoch eine weitere Anpassung angebracht.

Art. 49 Fälschen oder Unterdrücken von Information

...

a. Informationen fälscht oder unterdrückt und dies nicht gem. Art. 12a bekanntgibt;

...

³ Wer Adressierungselemente fälscht oder Vorbereitungshandlungen dazu trifft wird mit Busse oder Gefängnis bestraft.

Unter "Vorbereitungshandlungen" muss etwa die systematische Suche nach schlecht gewarteten Rechnern im Internet verstanden werden, die ein vom Besitzer nicht autorisiertes Versenden von Spams ermöglichen. Dieses "Scanning" erfolgt in der Regel vollautomatisiert und liefert Listen von zu Spam-Zwecken missbrauchbaren Rechnern. Eine solche Vorbereitungshandlung sollte nicht zulässig sein.

2.19 Verordnung über die Adressierungselemente im Fernmeldebereich, Artikel 9

Die SIUG begrüsst die vorgeschlagene Änderung, da gerade im Bereich der Telekiosnummern mit versteckt auf Computern von Internetbenutzern installierten Einwahlprogrammen (sog. *Dialer*) Missbrauch betrieben wird. Bei der Bekämpfung dieses Missbrauchs ist es sehr hilfreich, wenn die Betroffenen die Bekanntgabe der Identität der Nummerninhaber erwirken und gegen diese vorgehen können.

3 Schlussbemerkungen

Die SIUG erhofft sich durch die Änderung des Fernmeldegesetzes Verbesserungen in mehreren Punkten:

1. Mehr Transparenz für die Kundinnen und Kunden;
2. Griffige Massnahmen gegen unerlaubte Werbemitteilungen, sofern deren Urheber in der Schweiz domiziliert sind;
3. Mehr Wettbewerb zu Gunsten der Kundinnen und Kunden in Bereichen, die bisher aus verschiedenen Gründen die Stellung der marktbeherrschenden Anbieterin weiter verstärkt haben;
4. Für die Kundinnen und Kunden bessere Möglichkeiten, sich gegen Missbräuche im Bereich von Mehrwertdiensten zur Wehr zu setzen.

¹¹00.3714: Netzwerkkriminalität. Änderung der rechtlichen Bestimmungen, AB 2001 S 27 und AB 2001 N 1087

Wir sind der Überzeugung, dass die von uns vorgeschlagenen Änderungen und Ergänzungen diese Ziele ausgewogen im Gesetz verankern.

Besonders die Bekämpfung der verschiedenen Formen von "Netzmissbrauch" – zu denken ist da an unerwünschte Werbemittelungen und die Dialer-Seuche – muss eine hohe Priorität haben. Eine Studie der Europäischen Kommission geht von volkswirtschaftlichen Schäden von 10 Mia. Euro pro Jahr durch Spam aus, und andere Untersuchungen schätzen, dass die Hälfte des Mailvolumens aus unerwünschten Werbemittelungen besteht.

Um das Medium E-Mail nutzbar zu erhalten, ist ein entschiedenes Vorgehen dringend notwendig, auch und gerade gegen Spammer in und aus der Schweiz. Nicht nur die SIUG, sondern auch andere Organisationen sind in der Bekämpfung von und Aufklärung über Spam aktiv, und jeder Netzwerkverantwortliche kann den Ärger mit Spam – verstopfte Mailboxen, belastete Datenleitungen, Missbrauch eigener und fremder Domainnamen sowie technische Systeme – bestätigen.