BAR INFORMATIK

Informatik Service Center ISC-EJPD
Dienst Überwachung Post- und Fernmeldeverkehr
Bereich Recht und Controlling
Patrick Schöpf
3003 Bern

Dienstag, 26. Juli 2011

Stellungnahme VUEPF

Sehr geehrte Damen und Herren.

Als Kleinstunternehmen kämpfen wir seit Jahren für ein faires und sicheres Umfeld im Bereich Internet.
Beides scheint heute aber eher weiter entfernt zu sein, als noch vor einigen Jahren und leider geht die geplante Revision der VÜPF in die falsche Richtung.

Dabei geht es nicht nur um Arbeitsplätze in einem hart umkämpfen Feld in einer Randregion, sondern auch um sinnvolle, verhältnismässige Massnahmen zur Verbrechensbekämpfung und vor allem um die Rechtssicherheit.

Wir unterstützen daher die Stellungnahme der asut (Anhang) vollumfänglich.

Mit freundlichen Grüssen

BAR Informatik AG

Ralf Zenklusen

Anhang: Stellungnahme asut VUEPF

GLISERALLEE 16, CH-3902 BRIG-GLIS, TELEFON 027 922 48 48, FAX 027 922 48 49

info@bar.ch www.bar.ch

VÜPF Änderungsvorlage vom 8. Juni 2011: Stellungnahme der asut

Management Summary

Mit Schreiben vom 8. Juni 2011 eröffnete Bundesrätin Simonetta Sommaruga eine Anhörung zur Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF sowie der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs. Mit dem vorliegenden Papier nimmt der schweizerische Verband der Telekommunikation asut zu den vorgeschlagenen Änderungen kritisch Stellung.

Die folgenden Punkte stehen dabei im Zentrum:

1. Entgegen der Darstellung im Begleitbrief würde die vorgeschlagene Revision nicht nur eine Nachführung der bereits bestehenden Praxis darstellen, sondern eine **massive Ausweitung der staatlichen Überwachung** des Bürgers mit sich bringen, insbesondere eine Vorratsdatenspeicherung des Internetverkehrs. Es handelt sich um einen eigentlichen **Etikettenschwindel,** der im geltenden Bundesgesetz über die Überwachung des Post und Fernmeldeverkehrs BÜPF zudem gar **keine genügende gesetzliche Grundlage** findet und kaum auf statistischen Entscheidgrundlagen basiert.
2. Sodann bringt die Vorlage, anders als in den Erläuterungen dargestellt, **keine Verbesserung der Rechtssicherheit.** Entgegen der Regelung in der geltenden VÜPF soll nämlich der Katalog der Überwachungspflichten in der neuen VÜPF nicht mehr abschliessend sein, sondern die Behörden sollen explizit auch die Kompetenz erhalten, ohne Verordnungsgrundlage neue Überwachungspflichten einzuführen. Anders als unter der geltenden Verordnung haben die Telekom-Unternehmen wie auch die Bürger damit genau *keine* Rechtssicherheit mehr; sie werden nicht mehr wissen, mit welchen Überwachungsmassnahmen sie zu rechnen haben.
3. Die Vorlage soll für die Behörden eine **Kostensenkung** bringen, diese würde allerdings genau besehen **ausschliesslich zu Lasten der Telekom-Unternehmen** gehen. Schon heute werden die Kosten der Telekom-Unternehmen für die Kommunikationsüberwachung nur zu einem Drittel vom Staat entschädigt. Die asut kann nicht nachvollziehen, warum dieser Betrag jetzt zu Lasten der Telekom-Unternehmen und ihrer Kunden noch weiter gesenkt werden soll. Mit der Kostensenkung für die Behörden droht den Telekom-Unternehmen zudem eine massive Steigerung der Zahl von Überwachungsaufträgen, für die sie dann wiederum die Mehrheit der Kosten zu tragen hätten.
4. Die Vorlage **ignoriert das Verhältnismässigkeitsprinzip**: Die Telekom-Unternehmen sollen nicht verpflichtet werden können, teure Überwachungsanlagen zu beschaffen, die sie ohnehin nur in sehr unwahrscheinlichen Fällen überhaupt brauchen werden.

Aus diesen Gründen steht die asut der aktuellen Revision der VÜPF ablehnend gegenüber. Vor allem die geplante Ausweitung der Überwachungsmassnahmen darf nur mit einem demokratisch legitimierten Entscheid und damit nur durch Bundesgesetz erfolgen. **Entsprechend ist mit einer Revision der VÜPF bis zur Verabschiedung des BÜPF zuzuwarten.**

Der asut geht es mit ihrer Opposition gegen die Vorlage keineswegs darum, den Sinn der Telekom-Überwachung zum Zweck der Verbrechensbekämpfung in Frage zu stellen. **Die asut und ihre Mitglieder haben vielmehr schon immer konstruktiv mit den Behörden zusammengearbeitet, um die gesetzlich vorgesehenen Überwachungsmassnahmen umzusetzen.** Die asut wehrt sich allerdings gegen die neuesten Reformpläne, weil derart schwerwiegende Eingriffe in die Privatsphäre des Bürgers und in die Wirtschaftsfreiheit und Eigentumsgarantie der Telekom-Unternehmen nicht durch die Hintertür einer Verordnungsrevision eingeführt werden dürfen.

1 Allgemein

1.1 Teilrevision?

Gemäss dem Begleitbrief vom 8. Juni 2011 zur Vorlage, unterzeichnet durch Frau Bundesrätin Simonetta Sommaruga, soll es bei vorliegender Teilrevision der VÜPF lediglich um eine „Nachführung" gehen, welche für alle Beteiligten „die nötige Bestimmtheit und Rechtssicherheit" schaffe. Dies trifft jedoch nicht zu:

- Zunächst wird mit der Vorlage keineswegs nur die bestehende Praxis nachgeführt, sondern es werden auch diverse neue Überwachungsmassnahmen verankert, wie z.B. eine umfassende Überwachung des Internetverkehrs, zudem sollen internationale Kopfschaltungen analog zur Sprachtelefonie neu auch für SMS- und Internetüberwachungen gemacht werden. Bisher wurden als Folge eines Entscheids des Bundesverwaltungsgerichts internationale Kopfschaltungen lediglich hinsichtlich der Gesprächstelefonie eingesetzt.
- Sodann sollen mit der Revision nicht nur zweifelhafte Massnahmen wie die Kopfschaltungen in den Katalog aufgenommen werden, sondern neu auch eine Massnahme, welche unseres Erachtens illegal ist, nämlich die Antennensuchläufe. Bei solchen Massnahmen existieren keine Verdachtsmomente gegen bestimmte Personen oder Anschlüsse, wie dies von StPO und BÜPF eindeutig gefordert würde, sondern es wird ein Gebiet unspezifisch nach strafrechtlich Verwertbarem abgesucht.
- In den Erläuterungen wird zudem dargelegt, die Revision senke die Kosten: Aus Sicht der Überwachungsbehörden mag dies zwar zutreffen. Denn dadurch dass gewisse nicht vorgesehene Massnahmen in der Verordnung neu typisiert würden, gäbe es für deren Umsetzung für die Fernmeldedienstanbieter (FDA) nur noch eine geringe Pauschalentschädigung gemäss Gebührenverordnung und keine Aufwandsentschädigung gemäss bisherigem Art. 4 der Gebührenverordnung mehr. Eine solche „Kostensenkung" erfolgt aber auf dem Buckel der FDA und entspricht, zumindest nach offizieller Lesart, nicht die Meinung der Revision.
- Weiter ist der verwendete Begriff „Teilrevision" irreführend. Gemäss den Erläuterungen handelt es sich offenbar nur dann um eine Totalrevision der VÜPF, wenn sie im Nachgang einer BÜPF-Revision geschieht. Vom materiellen Gehalt her haben wir es aber bereits vorliegend mit einer Totalrevision der VÜPF zu tun, welche Entscheidungen vorwegnehmen soll, welche eigentlich in den Rahmen der BÜPF-Revision gehören.

1.2 Kein Plus an Rechtssicherheit

Die Vorlage bringt kein Plus an Rechtssicherheit, wie dies in Begleitbrief und Erläuterungen behauptet wird.

Die neueste Praxis des Bundesverwaltungsgerichts vom 21. resp. 23. Juni 2011 bestätigte die Auffassung zweier Mitglieder der asut, dass der Katalog der in der VÜPF geregelten Überwachungsarten abschliessend sei. Art. 17 Abs. 5 und Art. 25 Abs. 5 des Revisionsentwurfs widersprechen diesem Anspruch an die Rechtssicherheit im Sinne der Vorhersehbarkeit, indem sie explizit eine Kompetenz des Dienstes zur Überwachung des Post- und Fernmeldeverkehrs ÜPF zur Einführung weiterer Überwachungsmassnahmen vorsehen.

Aber selbst dann, wenn man der Auffassung ist, der Katalog sei entgegen der Auffassung des Bundesverwaltungsgerichts nicht abschliessend, bringt eine offene Formulierung des Katalogs nichts, da Fernmeldedienstanbieter und Bürger jederzeit damit rechnen müssen, dass entweder die Praxis den Katalog nicht als abschliessend betrachtet oder dass bei Bedarf einfach der Katalog wieder beliebig erweitert wird.

Dass die FDA überdies kein Rechtsmittel besitzen, um sich gegen solche von Gesetz und Verordnung nicht gedeckten Überwachungsmassnahmen zu wehren und ihre verfassungsmässigen Rechte zu wahren, hat die asut bereits in der Vernehmlassung zum VE-BÜPF heftig kritisiert. Sie sieht darin einen wesentlichen konzeptionellen Mangel des BÜPF, der weder durch den VE-BÜPF, geschweige denn durch die nun geplante Verordnungsrevision behoben wird.

Die Erklärung, dass den rechtsstaatlichen Mängeln des BÜPF mit einer VÜPF-Revision nicht beizukommen ist, findet sich im Prinzip in den Erläuterungen zur Vorlage selbst, S. 1 unten:

Nach Ansicht der anordnenden Strafverfolgungsbehörden und der die Überwachungsmassnahmen genehmigenden Zwangsmassnahmengerichte ist die Liste der Überwachungsmassnahmen in der VÜPF nicht abschliessend zu betrachten. Der Dienst und die FDA sind nach dieser Auffassung daher auch verpflichtet, angeordnete und genehmigte Überwachungsmassnahmen durchzuführen, die nicht explizit in der VÜPF aufgeführt sind. Diese Situation führt zu einer grossen Rechtsunsicherheit und dazu, dass sowohl auf Seiten des Dienstes als auch auf Seiten der FDA bei der Durchführung von nicht explizit in der VÜPF aufgeführten Überwachungsmassnahmen erhebliche Kosten entstehen.

Die Problematik, dass aufgrund fehlender Rechtsbehelfe der Provider theoretisch alles durchgeführt werden muss, was Zwangsmassnahmengerichte, welche über kein genügendes technisches Verständnis verfügen, genehmigen, lässt sich mit einer Erweiterung des Massnahmenkatalogs sicher nicht beseitigen, solange dieser derart offen formuliert bleibt.

Damit würde nur erreicht, dass damit insgesamt den FDA die Entschädigungen gekürzt würden, weil die Aufwandsentschädigung gemäss bisherigem Art. 4 der Gebührenverordnung durch pauschal festgelegte Teilentschädigungen ersetzt würde. Weiter würde der neue Art. 1 Abs. 2 bis bewirken, dass pro überwachte Rufnummer unter einem Auftrag sämtliche möglichen Erhebungen verlangt werden könnten und dies nur unter Entschädigung der Basisleistung. Die FDA lehnen dies selbstverständlich ab. Es ist in den Erläuterungen nirgends die Rede davon, dass eine Kürzung der Entschädigungen für die FDA die Absicht wäre. In finanzieller Hinsicht ist in den Erläuterungen auf S. 2 vielmehr die Rede davon, dass es darum gehe, den FDA Investitionssicherheit zu verschaffen.

1.3 Übernahme von bisheriger Rechtssprechung und Praxis:

Oft soll mit Gesetzesrevisionen die in der Zwischenzeit aufgelaufene, „bewährte" Rechtssprechung ins neue Gesetz einfliessen, so auch hier. In diesem Fall ist aber Skepsis angebracht. Einerseits gibt es keine gefestigte Rechtssprechung, sondern nur einige wenige Einzelentscheide, und diese sind meistens nicht hilfreich. Aufgrund der konzeptionellen Fehler im BÜPF, welche zur Folge haben, dass hinsichtlich der Frage, was die Gerichte auf Beschwerde einer FDA hin nun zu prüfen haben, Konfusion herrscht, konnte sich keine Gerichtspraxis entwickeln, welche sich eignen würde, ins Gesetz aufgenommen zu werden.

An dieser Stelle kann nicht auf die Gesamtheit der Unstimmigkeiten und Widersprüchlichkeiten der aufgelaufenen Gerichtsentscheide eingegangen werden, nur soviel: Mit seinen zwei neusten Entscheiden hiess das Bundesverwaltungsgericht zwei Beschwerden von FDA gut, mit der Begründung, die FDA seien in der angefochtenen Verfügung zu Überwachungsmassnahmen verpflichtet worden, welche im Katalog der Überwachungsmassnahmen gemäss VÜPF gar nicht vorhanden sind. Da die Aufzählung der Überwachungsmassnahmen in der VÜPF abschliessend zu verstehen sei, sei eine Verpflichtung der FDA zu Massnahmen ausserhalb des Katalogs nicht zulässig. Gemäss Art. 13 Abs. 1 Bst. a BÜPF darf jedoch der ÜPF eine von Zwangsmassnahmengerichten genehmigte Überwachung nur darauf hin überprüfen, ob die angeordnete Massnahme von einer zuständigen Behörde aus erfolgt ist und ob es um ein Delikt gemäss des Deliktskatalogs des BÜPF geht. Das BVGer hat nun aber darüber hinaus geprüft, ob die angeordneten Massnahmen im Katalog der VÜPF aufgeführt seien. Den FDA ist es zwar durchaus recht, wenn das Bundesverwaltungsgericht in Ausübung einer rechtspolitischen Lückenfüllung über Art. 13. Abs. 1 Bst. a BÜPF hinaus prüft. Es erscheint aber unschlüssig, wenn sich das Gericht einerseits nicht an Art. 13 Abs. 1 Bst. a BÜPF hält und andererseits die von der Beschwerdeführerin angeführten, in diesem Papier auch schon erwähnten, konzeptionellen Fehler des BÜPF in Abrede stellt (A-8267/2010, Erw. 3.2).

Mit dem einzigen höchstrichterlichen Entscheid im Bereich Zulässigkeit von Überwachungsmassnahmen im Fernmeldebereich (BGE 130 II 249ff) wurde überdies eine Überwachungsmassnahme, welche ebenfalls nicht dem VÜPF Katalog angehört (Antennensuchläufe), nicht verhindert. Das Bundesgericht stellte sich dabei auf den Standpunkt, es dürfe die Rechtmässigkeit von Antennensuchläufen gar nicht prüfen. Wenn also in den

Erläuterungen behauptet wird, Antennensuchläufe seien von der Gerichtspraxis als zulässig bestätigt worden, so stimmt das schlicht nicht, denn das Bundesgericht hat die Zulässigkeit von Antennensuchläufen gar keiner Prüfung unterzogen. Es wäre daher nicht gerechtfertigt, den Überwachungstypenkatalog der VÜPF unter Hinweis auf die Bundesgerichtspraxis zu ergänzen.

1.4 VÜPF-Revision im jetzigen Zeitpunkt ist abzulehnen

Aus den diversen oben genannten Gründen, ist diese VÜPF-Teilrevision abzulehnen. Wie dargelegt, ist es nicht möglich, mit dieser Vorlage Rechtssicherheit zu schaffen. Es besteht hingegen die Befürchtung, dass mit dieser VÜPF-Revision im etwas kleineren Kreis und ohne die nötige demokratische Legitimation Forderungen durchgedrückt werden sollen, welche in einer Revision des Gesetzes im formellen Sinn keine Chance hätten. Weiter muss die Befürchtung bestehen, dass mit dieser Verordnungsrevision, welche im Prinzip eine Wunschliste des ÜPF enthält, die längst fällige BÜPF-Revision auf die lange Bank geschoben werden soll.

1.5 BÜPF-Revision abwarten

Die meisten relevanten Änderungen in dieser VÜPF-Revisionsvorlage betreffen Punkte, welche gerade in der parallel laufenden BÜPF-Revision umstritten sind:

- Änderungen, welche die Kosten/Entschädigungen betreffen
- Nicht nur Ausleitung des gesamten Fernmeldeverkehrs von bestimmten Breitbandanschlüssen, sondern auch Überwachungspflichten der Zugangsanbieterinnen auf der Dienste-/Anwendungsebene (allfällige Filterungspflichten der FDA)
- Überwachungsmassnahmen gegen einen unbestimmten Personenkreis (z.B. Antennensuchläufe).

Man kann sich daher des Eindrucks nicht erwehren, der Verordnungsgeber wolle nun die Punkte, die im Rahmen der Vernehmlassung zum BÜPF ins Schussfeld der Kritik geraten sind, am Gesetzgeber vorbei in die VÜPF bringen. Damit würde der von Verfassung und Gesetz vorgesehene Stufenbau (Gesetz – Verordnung – Richtlinien) umgangen, was dem Prinzip der Rechtsstaatlichkeit widerspricht. Es geht nicht an, dass die relevanten Entscheidungen auf einer unteren Normenstufe gefällt werden und sich dann später das Gesetz im formellen Sinn danach richten soll.

Dies gilt insbesondere auch deshalb, weil der Verordnungsgeber die ihm durch Art. 15 (insbes. Abs. 6) BÜPF verliehene Rechtsetzungskompetenz in verschiedener Hinsicht eindeutig überschreitet: So regelt das BÜPF beispielsweise an keiner Stelle die Überwachung von Anwendungen wie VoIP, Instant Messaging oder Multimediadienste, die nicht von Fernmeldediensteanbietern oder Internet-Access-Providern, sondern von Internet-Anwendungsanbietern (Service Provider) angeboten werden (vgl. Hansjakob, Kommentar, N 24 zu Art. 1 BÜPF). Auch hatte der historische Gesetzgeber vor elf Jahren keine Vorstellung, welche neuen Dienstleistungen auf dem Internet zur Verfügung stehen würden, und entsprechend ist der Verordnungsgeber erst durch ein formelles Gesetz zu ermächtigen, Überwachungsarten einzuführen, die zum Zeitpunkt des Erlasses des BÜPF nicht vorstellbar waren (etwa Zugänge über VPN oder „Instant Messaging"). Dies gilt erst recht für eine Vorratsdatenspeicherung für WWW-Internetverkehr (http), die bei einer weiten Auslegung der Verordnung ebenfalls möglich wäre, und die einen schwerwiegenden Eingriff in die Privatsphäre von Bürgern beinhaltete. Ein solcher schwerwiegender Eingriff würde zwingend eine Regelung in einem formellen Gesetz voraussetzen (mehr dazu unten bei den Ausführungen zu Art. 24b des Entwurfs).

Hinzu kommt, dass die Verordnung, wie im Folgenden zu zeigen sein wird, auf technischer Ebene mehr Fragen aufwirft, als sie beantwortet. Anstatt die Verordnung an den Informationsbedürfnissen der Strafverfolgung zu orientieren, wird zudem versucht, technische Lösungen in einem bestimmten technologischen Umfeld zu beschreiben und eine Reihe von Parametern, oft in unklarem Kontext, aufzulisten (dazu den Technischen Annex dieses Dokuments, S. 1).

Da nach Auffassung der asut vor einer Revision der VÜPF der Abschluss der Revision des BÜPF mit dem normalen Durchlauf des Gesetzgebungsverfahrens nötig wäre, wird auf einen detaillierten Änderungsvorschlag verzichtet. Wegen der unklaren, bzw. inexistenten formell-gesetzlichen Grundlage müsste dieser ohnehin nur Stückwerk bleiben. Die asut hat sich bei der BÜPF-Revision schon bisher sehr kooperativ gezeigt und hat mit konstruktiven Vorschlägen an dieser mitgewirkt. Sie wird dies selbstverständlich auch künftig tun und zu einer erfolgreichen Umsetzung jenes Projekts Hand bieten.

1.6 Fehlende Berücksichtigung des Verhältnismässigkeitsprinzips in der Verordnung

Es wäre zu berücksichtigen, dass bei Anbietern mit geringer Kundenzahl, bei Anbietern mit überwiegendem Anteil an Business-Kunden oder aber bei seltenen Überwachungsarten im Hinblick auf die in diesen Fällen nur kleine Zahl von zu erwartenden Überwachungsvorgängen eine Installation von Überwachungsanlagen unverhältnismässig und nicht zumutbar scheint. Die neuen Richtlinien TR TS müssten in diesem Sinne neben den Handover Interfaces (HI), entsprechende Schnittstellen (in ETSI Terminologie Internal Network Interface, INI) spezifizieren, dass der ÜPF in vergleichbaren Fällen ad hoc Ausrüstung installieren kann. In solchen Fällen dürfen die FDA allenfalls verpflichtet werden, die für die Installation der Ausrüstung nötigen Schnittstellen zur Verfügung zu stellen, nicht aber, die Anlagen als solche „auf Vorrat" zu beschaffen.

Ebenfalls eine klare Verletzung des Verhältnismässigkeitsprinzips liegt in der Anforderung von Art. 18 Abs. 3 vor, eine 24x7-Erreichbarkeit sicherzustellen. Viele kleine Provider beschäftigen nur wenige Angestellte und wären durch eine derartige Anforderung überfordert.

1.7 Fehlende Entscheidgrundlage für eine Ausweitung der Überwachungspflichten

Abschliessend ist darauf hinzuweisen, dass die Ausweitung des Anwendungsbereichs der VÜPF offenbar erfolgt, ohne dass über die Wirksamkeit der bisherigen Überwachungsmassnahmen Statistiken erhoben worden wären. Schon die Wirksamkeit der bisherigen Methoden bleibt vielmehr völlig im Unklaren, und erst recht ist nicht gesichert, ob von der geforderten Ausweitung der Überwachungsarten überhaupt die erwünschte Wirkung zu erwarten sei. Umgekehrt betrachtet bleibt also völlig offen, ob für die mit der Vorlage neu eingeführten schweren Eingriffe in die Privatsphäre der Bürger eine sachliche Grundlage besteht.

Auch dies spricht deutlich für die Forderung der asut, die Verordnungsrevision aufzuschieben, bis einerseits die Revision des zu Grunde liegenden Gesetzes erfolgt ist, und andererseits gestützt auf zuverlässiges Datenmaterial über weitere Überwachungsmassnahmen zu entscheiden wäre.

2 Zu einer Auswahl an einzelnen Bestimmungen

2.1 2. Abschnitt: Bearbeitung von Personendaten (...)

Zu Art. 9 Abs. 2: "Übergabepunkt"

Die Frage der Bestimmung der Übergabepunkte ist nach wie vor ungelöst. Damit ist offen, für welchen Abschnitt die Provider genau verantwortlich gemacht werden sollen. Ausserdem ist unklar, welche Aspekte unter Datensicherheit fallen sollen (Confidentiality, Authentication, Availability (DoS), Integrity, Non-repudiation). Zu beiden Punkten vgl. auch den Technischen Annex, S. 4 f.

2.2 4. Abschnitt: Überwachung der „Telefondienste"

Die Abgrenzung des Fernmeldeverkehrs vom Internetverkehr bleibt unklar. Internet-Technologie (damit ist eine Protokollarchitektur gemeint) kann ausserhalb des Internet eingesetzt werden beispielsweise in einem Carrier Class IP Netz (z.B. für VoIP). Vgl. dazu die Anmerkung im Technischen Annex, S. 8.

Zu Art. 16:

In der bisherigen Verordnung wurde unterschieden zwischen „Überwachung des Fernmeldeverkehr mit Ausnahme von Internet" und „Überwachung der Internetzugänge". Neu heisst es nun im 4. Abschnitt nur noch „Überwachung der *Telefondienste*" und später im 6. Abschnitt „Überwachung des Internets".

Die genaue Terminologie müsste nochmals überprüft werden, wird doch im weiteren Verlauf des 4. Abschnitts nicht mehr von „Telefondiensten", sondern wieder von „Fernmeldeverkehr" gesprochen.

Sodann sollten keine Erhebungen gemacht werden über netzinterne Parameter wie IMSI, reale Cell IDs, usw. Solche Erhebungen sind für die Strafverfolgungsbehörden und die Gerichte nicht beweisrelevant. Die Parameter werden nur netzintern verwendet und dienen der Kundensicherheit sowie zur Sicherstellung der Netzintegrität. Bei einigen solcher Daten, wie z.B. den realen Cell IDs, handelt es sich zudem um geschäftsrelevante Daten, welche die FDA nicht herausgeben können, ohne Geschäftsgeheimnisse zu verletzen.

Im Weiteren ist darauf hinzuweisen, dass viele der für die Erhebung vorgesehenen Parameter genau besehen kaum jene Beweissicherheit bieten, die sich der Verordnungsgeber offenbar vorstellt. Vielfach sind die Parameter nämlich durch die Endkunden einfach änderbar (z.B. die MAC-Adresse), sodass sie, weil sehr schwierig verifizierbar, gar keine zuverlässige Beweisführung erlauben. Entsprechend ist deren Erhebung für die Strafverfolgungsbehörden und Gerichte nicht von Nutzen und damit auch unverhältnismässig. Die Erhebung sehr schwierig verifizierbarer Parameter führt im besten Fall zu Beweislosigkeit, im schlechteren Fall zu nicht gerechtfertigten Anschuldigungen oder gar Festnahmen. Entsprechend ist zu fordern, dass Richtlinien zur Verifizierbarkeit von Parametern bestehen und die diesbezügliche Verantwortung einzelner FDA klar umschrieben wird, basierend auf ETSI TR 187 012 clause 5.2 und Draft ETSI TS 187 017 clause 4.

SIM-Nummern sind sodann keine auf dem Netz verfügbaren Parameter, welche zu den Fernmeldeverkehrsdaten gehören. Die Information der SIM-Nummern gehört zu den Auskünften über Fernmeldeanschlüsse und wird heute schon durch eine Anfrage über das CCIS angefragt und die Auskunft durch die FDA erteilt.

In Art. 16 Bst. d Ziff. 2 ist im Weiteren keine klare Zuteilung der Parameter in Klassen gegeben. Zudem erzeugt die Formulierung „(wie die SIM-Nummer, die IMSI-Nummer und die IMEI-Nummer)" Rechtsunsicherheit, da nicht festgelegt ist, welche weiteren Angaben unter dieser Bestimmung herausverlangt werden könnten.

Zu Art. 16 lit. e: Antennensuchlauf:

Diese Ergänzung darf an dieser Stelle keinesfalls gemacht werden, wenn schon müsste die Durchführbarkeit von Antennensuchläufen im Gesetz im formellen Sinn vorgesehen werden, da diese Massnahme klar gegen die geltende Strafprozessordnung verstösst, wonach Fernmeldeüberwachungen nicht zur Suche nach Verdachtsmomenten gegen unbestimmt viele Personen durchgeführt werden dürfen, sondern nur im Falle eines bereits vorliegenden Verdachts und nur betreffend bereits im Voraus klar bestimmter Anschlüsse (dazu schon vorne 1.3).

Darüber hinaus lässt sich sagen, dass es gar nicht möglich ist „an einem bestimmten Standort" rückwirkend „alle mobilen Kommunikationsvorgänge" zu eruieren. Es liesse sich höchstens eine grössere oder kleinere Zahl an Funkzellen ermitteln, welche „einen bestimmten Standort" mit einer gewissen Wahrscheinlichkeit versorgen, und anschliessend die Kommunikationen über diese Funkzellen in einem definierten Zeitraum ermitteln. Ob sich aber die gesuchte Kommunikation darunter befindet, ist nicht gewährleistet.

Zu Art. 16 und 16a vgl. zudem die Anmerkungen im Technischen Annex, S. 9f.

Zu Art. 16b Überwachungsmassnahmen mit Auslandsbezug

Mit der Einfügung dieser Norm sollen die sog. internationalen „Kopfschaltungen" verankert werden, das heisst, die FDA sollen dazu verpflichtet werden, ausländische Rufnummern, respektive schweizerische Rufnummern im

Ausland (outbound Roamer) überwachen zu können, wenn diese mit ihren Kunden kommunizieren. Diese Bestimmung ist abzulehnen, obschon das Bundesverwaltungsgericht vor rund zwei Jahren entschieden hat, eine solche Massnahme sei rechtmässig. Das Bundesverwaltungsgericht (A-2335/2008) stellte sich auf den Standpunkt, dies sei im Prinzip das Gleiche wie die Überwachung einer inländischen Nummer, jedenfalls sei ja die überwachte Nummer klar bestimmt. Allerdings übersah das Bundesverwaltungsgericht die Tatsache, dass es sich

- entweder um eine Überwachung einer Person im Ausland handelt, welche nach Abschluss des Verfahrens nicht, wie von der Gesetzgebung vorgesehen, über die Vornahme der Überwachung informiert werden kann, und die darüber hinaus gegen das Territorialitätsprinzip verstösst,
- im Prinzip auch um eine Überwachung von unbestimmt vielen Personen im Inland handelt, welche Kommunikationen mit der genannten Nummer im Ausland haben. Auch die Kopfschaltung widerspricht damit dem Grundkonzept des BÜPF, wonach Fernmeldeüberwachungen nicht zur Suche nach Verdachtsmomenten gegen unbestimmt viele Personen durchgeführt werden dürfen (Rasterfahndung), sondern nur im Falle eines bereits vorliegenden Verdachts und nur betreffend bereits im Voraus klar bestimmter Anschlüsse. Auch hier ist zudem offensichtlich, dass die unbestimmte Anzahl an Personen im Inland nach Abschluss des Verfahrens nicht über die Überwachung informiert werden kann.

Entgegen der Ansicht des Bundesverwaltungsgerichts gibt es also doch starke Anzeichen dafür, dass Kopfschaltungen nicht ins Konzept des aktuellen BÜPF passen, weshalb auch die Entscheidung über die Zulässigkeit von Kopfschaltungen dem Gesetz im formellen Sinn anheimgestellt werden sollte und nicht im Rahmen einer Revision der VÜPF erfolgen darf.

Zu Art. 16b vgl. zudem die Anmerkungen im Technischen Annex, S. 11 f.

Zu Art. 17 Abs. 4

Es ist unklar was alles mit „Zuleitung" gemeint ist. ETSI spezifiziert die Auslieferungsformate an einem Übergabeinterface (Handover Interface, HI), spezifiziert jedoch die Ausleitungsnetze (Delivery Networks) aus der Infrastruktur des Providers (IIF/MD) zur Infrastruktur von ÜPF (LEMF) nur oberflächlich. Wenn „die Spezifikationen dieser Zuleitung" bedeuten würde, dass ÜPF Delivery Networks spezifiziert, würde dies einen erheblichen Eingriff in die Netzhoheit der Provider bedeuten.

Zu Art. 17 Abs. 5 und Art. 25 Abs. 5

Obschon der Verordnungsgeber (wie auch das Bundesverwaltungsgericht) davon ausgehen will, dass der Überwachungstypenkatalog der VÜPF abschliessend sei, soll diese Bestimmung nun vorsehen, dass auch nicht explizit in der Verordnung aufgeführte Fälle von Überwachungen möglich seien. Damit wird der Katalog der Überwachungstypen offengehalten, und es besteht keine Rechtssicherheit, was vom ÜPF an Überwachungen zu erwarten ist. Dies betrifft die Betreiber im Rahmen der in diesem Zusammenhang zu erwartenden Investitionen und den Normalbürger insofern, als er nicht weiss, wie er vom Staat überwacht werden kann. Gemäss Legalitätsprinzip müsste wenigstens ein Rahmen an zulässigen Überwachungen im Gesetz im formellen Sinn definiert werden. Was darüber hinaus geht, sollen die FDA nicht nur nicht ausführen müssen, sondern im Hinblick auf den Schutz der Freiheitsrechte der Bürger auch nicht ausführen *dürfen*. Daher ist diese Spezialfallregelung abzulehnen, jedenfalls solange, als nicht mit einer zufriedenstellenden BÜPF-Revision eine Grundlage geschaffen wird, welche den Rahmen der Behördenpraxis klar vorgibt.

Zu Art. 17 vgl. zudem die Anmerkungen im Technischen Annex, S. 12 f.

Zu Art. 18

Auf die Unverhältnismässigkeit der Anforderung von Art. 18 Abs. 3 (permanente Erreichbarkeit) wurde bereits unter Ziff. 1.6 hingewiesen.

Die Änderungen, v.a. in den Absätzen 7 und 8, betreffen Spezialwünsche des ÜPF. Eine Gratisnutzung der Fernmeldedienste der FDA durch den ÜPF ist abzulehnen, zumal eine solche Nutzung in keiner Weise eingegrenzt wäre.

Auch die begehrten Unterstützungsleistungen hinsichtlich der Frage, ob tatsächlich die richtige Person überwacht werde, sind fragwürdig, da diese Begehren des ÜPF daher rühren, dass er in letzter Zeit bewährte Überwachungsmethoden durch billigere und unzuverlässige Methoden ersetzt hat. Abs. 8 lässt zudem völlig offen, welche technischen und organisatorischen Vorkehrungen ein Provider treffen muss, um die entsprechende Unterstützung leisten zu können.

Vgl. auch zu Art. 18 die weiter gehenden Anmerkungen im Technischen Annex, S. 13 f.

Zu Art. 19a der *bestehenden* Verordnung

Art. 19a der bestehenden VÜPF bleibt nach dem Entwurf unverändert. Die Norm bestimmt, dass die FDA sicherstellen müssen, dass beim Verkauf von Prepaid-SIM-Karten die Personalien der Kundinnen und Kunden anhand eines *für den Grenzübertritt in die Schweiz zulässigen Reisedokumentes* erfasst werden. Nach Auffassung der asut wäre hier jedoch eine Änderung vorzunehmen.

Nimmt man die geltende Bestimmung beim Wort, können Asylbewerber mit Asylbewerberausweis (Ausländerausweis F, N und S) keine Prepaid-Karten beziehen, weil dieser Ausweis nicht zum Grenzübertritt berechtigt (vgl. Hansjakob, Kommentar, N 3 zu Art. 19a VÜPF). Nach Auffassung der asut ist das Kriterium der Eignung zum Grenzübertritt jedoch unsachlich, ist doch nur die Eignung zur Identifikation, nicht aber die Möglichkeit zum Grenzübertritt für den Zweck von Art. 19a VÜPF relevant.

Das Migrationsamt schiebt für das Verbot der Verwendung von F-, N- und S-Ausweisen sodann die Begründung nach (http://www.uvek.admin.ch/themen/kommunikation/00950/00951/index.html?lang=de, Frage 16), dass die entsprechenden Ausweise oftmals auf falsche Namen ausgestellt würden, weil sie nur auf den Angaben der Asylbewerber basieren und nicht auf amtlichen Dokumenten von deren Heimatland. Aus Sicht der asut ist es jedoch unverhältnismässig, die Verwendung von Ausweisen F, N und S bloss aufgrund eines möglichen Fehlverhaltens einzelner Ausweisträger zu beschränken. Abgesehen davon wäre die Identifikationseignung eines F-, N- oder S-Ausweises selbst dann nicht in Frage gestellt, wenn der Ausweis auf falschen Angaben des Asylbewerbers basierte, ist doch der Asylbewerber auch unter dem entsprechenden (falschen) Namen registerlich erfasst, sodass er gerade auch anhand des falschen Namens zweifelsfrei ausfindig gemacht werden könnte.

Diese Situation ist immer noch besser als jene, dass Asylbewerber für die Nutzung von Mobiltelefonie gezwungen wären, einen Strohmann vorzuschicken, denn in diesem Fall wäre die Identifikation gar nicht mehr gewährleistet.

Träger der Ausweise F, N und S haben zudem in der Regel nicht die Möglichkeit, die für Postpaid-Angebote von Ausländern aus Sicherheitsgründen geforderten Depotzahlungen zu leisten. Ein Verbot, Prepaid-Karten zu beziehen, läuft damit auf eine unverhältnismässige Verletzung Kommunikationsfreiheit der entsprechenden Individuen hinaus. Entsprechend wäre bei einer Verordnungsrevision der in Art. 19a verwendete Ausweisbegriff um Ausweise F, N und S zu erweitern.

2.3 6. Abschnitt: Überwachung des Internets

Zunächst bleibt unklar, wofür der Ausdruck „Internet" verwendet (dazu die Anmerkungen im Technischen Annex, S. 16 f.) wird.

Zu Art. 23

Der Inhalt der Norm ist bezüglich Inhalt und Beschreibungstiefe mit Art.15 Abs. 1 abzugleichen (vgl. den Technischen Annex, S. 17).

Erneut ist darauf hinzuweisen, dass eine Datenherausgabe betreffend sämtlicher Netzparameter (Bst. g), welche nicht überwachungsrelevant sind und welche reine Netzdaten der betreffenden FDA bilden, nicht akzeptabel ist (dazu vorne 2.2)

Zu Art. 24

Art. 24 sieht eine massive Ausdehnung des Katalogs der Überwachungsarten vor. Die asut ist der Auffassung, dass eine derartige Ausdehnung keine genügende Rechtsgrundlage in Art. 15 BÜPF findet, zumal die meisten der entsprechenden Überwachungsarten zum Zeitpunkt der Verabschiedung von Art. 15 BÜPF noch nicht im Fokus des Gesetzgebers waren. Dementsprechend ist die geplante Ausweitung des Katalogs der Überwachungsarten durch die Delegationsnorm in Art. 15 Abs. 6 BÜPF nicht gedeckt. Die asut ist der Auffassung, eine Erweiterung des Katalogs der Überwachungsarten sei ausschliesslich auf Grund eines Gesetzes im formellen Sinn zulässig.

Eine Überwachung von VPN (Art. 24 Bst. f) wäre in jedem Fall explizit auf Anbieter zu beschränken, die VPN selber anbieten, und nicht auf die Access Provider, die VPN-Datenströme bloss von ihren Endkunden zu VPN-Anbietern im Internet weiterleiten. Dies bereits daher, weil VPN-Daten verschlüsselt und damit für eine Ausleitung ungeeignet sind.

Art. 24 Abs. 2 sieht zudem neu auch Überwachungen auf der Anwendungsebene des Internets vor (für VoIP, Instant Messaging, Multimediadienste, etc.). Die bisherige Praxis wie auch die Literatur gehen klar davon aus, dass das BÜPF auf Access Provider anwendbar ist, nicht aber auf Service Provider (Anwendungsanbieter; vgl. Hansjakob, Kommentar, N 24 zu Art. 1 BÜPF). Auch diese Norm sprengt den durch Art. 15 BÜPF vorgesehenen Rahmen daher klar, selbst die Definition der Internetanbieter nach Ziff. 1 des Anhangs der Verordnung umfasst derartige Anwendungsanbieter nicht.

Die Belastung von Anwendungsanbietern führte im internationalen Vergleich zu einer erheblichen Wettbewerbsverzerrung und vor allem zu einer Beeinträchtigung der Innovation im Bereich der Internetanwendungen, weil die Entwickler mit (im Vergleich zu den allgemein niedrigen Entwicklungskosten für die Anwendungen) ganz erhebliche Mehrkosten für die Entwicklung von Überwachungsschnittstellen einplanen müssten. Die Innovation von Anwendungen des Internets, gerade auch im Mobilfunk (Smartphones), geht heute sehr rasch voran, und entsprechend profitiert die Gesellschaft vom Internet als einem wahren Motor des Fortschritts. Diese Dynamik soll nicht durch eine übertriebene Überwachungspflicht gehemmt werden.

Im Weiteren lässt der Entwurf – und hier liegt ein weiterer schwerwiegender Kritikpunkt – völlig offen, wer für die Überwachung von Anwendungen wie VoIP, Instant Messaging oder Multimediadienste verantwortlich wäre. Angesichts dessen, dass die Access Provider bisher keinerlei technische Möglichkeiten zur Filterung von Inhalten (Deep Packet Inspection) haben, und angesichts dessen, dass eine solche Filterung in der Regel Know-How über Kommunikationsprotokolle höherer Schichten als jener des Access und allfällige Verschlüsselungsmechanismen voraussetzt, das nur der Anbieter der Anwendung selber besitzt, scheint die Vorstellung, dass die Access Provider für eine Ausleitung von aus dem Datenstrom eines Kunden ausgefilterter Anwendungsdaten verantwortlich sein sollen, nicht haltbar. Wollte man Anwendungen doch in die VÜPF aufnehmen, so müsste daher zumindest klargestellt werden, dass für die Ausleitung entweder die Anwendungsanbieter oder dann der ÜPF, nicht aber die Access Provider verantwortlich sein können. Der ÜPF muss auch dann die Filterung übernehmen, wenn die Anwendungsanbieter vom Ausland aus tätig sind und dementsprechend nicht selber dem BÜPF unterstehen (dazu Hansjakob, Kommentar, N 26 zu Art. 1 BÜPF). Technisch gesprochen darf die Überwachungspflicht der Access Provider daher nur die IP-Adresselemente, aber nicht in der IP-Payload gespeicherte Adresselemente enthalten.

Vgl. zu Art. 24 auch den Technischen Annex, S. 18 f.

Zu Art. 24a Überwachungstypen (Echtzeit)

Die Artikel 24a und 24b enthalten einen umfassenden, schwerwiegenden Ausbau an Datenlieferungspflichten, welcher für die FDA einschneidende Folgen hätte. Gemäss BÜPF/StPO ist an sich nur vorgesehen, dass die FDA den gesamten Fernmeldeverkehr von bestimmten Anschlüssen zuleiten müssen.

Die Bestimmung enthält (wie Art. 24b auch) einige Anforderungen, wonach für die Überwachung und Beweisführung im Strafverfahren überhaupt nicht relevante Daten herauszugeben wären, was teils sogar die Netzintegrität der FDA tangieren würde (wie IMSI, reale Cell ID, usw.)

Unklar bleibt ferner der Inhalt von Art. 24a Bst. b Ziff. 3, der von „Anmeldungsdaten" spricht. Die Norm wäre dahin zu präzisieren, dass, falls überhaupt, ausschliesslich Login-Daten für die Anmeldung im Netz des Access Providers, nicht aber Login-Daten für die Anwendungsebene des Internet (http, etwa für E-Banking, E-Mail-Accounts etc.) unverschlüsselt ausgeleitet werden. Login-Daten (Username plus Password) sind Credentials (Berechtigungsnachweise) und von ihrer Eigenschaft her nicht geeignet, eine Straftat zu begehen. Jede Dritte Entität, die über die Credentials einer Entität verfügt, kann in ihrem Namen, d.h. mit ihren Identitäten kommunizieren. Damit gehören Login-Daten in dieselbe Kategorie wie die IMSI. Die Ausleitung von Login-Daten der Anwendungsebene hätte erstens zur Bedingung, dass die Provider zu einer detaillierten Filterung des Internetverkehrs (Deep Packet Inspection) gezwungen würden, was hohen Investitionsbedarf mit sich brächte, und würde zweitens den Zweck der Fernmeldeüberwachung, nämlich die Inhalte von Kommunikation zu Tage zu fördern, überdehnen. Denn damit würde es den Strafverfolgern auch möglich, leicht etwa Banktransaktionen von Verdächtigen nachzuvollziehen. Abgesehen davon, sind Login-Daten einer Client zu Server Beziehung auf Anwendungsebene verschlüsselt und können durch den Access Provider nicht offengelegt werden. Für solche Aufgaben ist die Fernmeldeüberwachung aber nicht gedacht, geschweige denn fände sie im gegenwärtig geltenden BÜPF eine genügende gesetzliche Grundlage.

Unklar bleibt im Weiteren die Bestimmung in Art. 24a Bst. b Ziff. 4 hinsichtlich des Begriffs der Adressierungselemente: Ist die Bestimmung auf Adressierungselemente der IP-Ebene beschränkt, oder will die Bestimmung etwa auch eine Ausleitung für die Anwendungsebene (http) einführen? Einmal mehr kann nach Auffassung der asut nur die IP-Ebene gemeint sein, nicht aber Adresselemente, die in der IP-Payload enthalten sind.

Art. 24b Überwachungstypen (rückwirkend)

In Art. 24b (betreffend rückwirkende Überwachung) wird ebenfalls ein systematischer Ausbau vorgenommen, sodass diese Datenlieferungspflicht mit der früheren Lieferung von schlichten Verkehrs- und Rechnungsdaten nichts mehr gemein hat.

Es wird auf die bereits bei Art. 24a geäusserte Kritik zur Echtzeitüberwachung von Anmeldungsdaten verwiesen. Sie gilt für die rückwirkende Speicherung der Daten erst recht, weil ausserhalb des Zugriffsbereichs des Endkunden gespeicherte Anmeldedaten ein lohnenswertes Ziel für Hackerangriffe bilden (die Erfahrung gerade der letzten Wochen und Monate zeigt, dass auch Behörden niemals für absolute Sicherheit der von ihnen gespeicherten Daten sorgen können). Eine Pflicht zur Speicherung solcher Daten würde damit Anwendungen wie E-Banking deutlich unsicherer machen, wenn nicht gar das Vertrauen des Publikums in sie zerstören.

Unklar bleibt im Weiteren analog zum bereits zu Art. 24a Gesagten in Art. 24b Bst. a Ziff. 4 der Begriff der Adressierungselemente: Ist die Bestimmung auf Adressierungselemente der IP-Ebene auf Seiten des Endkunden beschränkt, oder will die Bestimmung auch eine rückwirkende Herausgabe für die Anwendungsebene und der vom Endkunden besuchten IP-Adressen oder URLs einführen? Letzteres liefe auf eine Vorratsdatenspeicherung für das Internet hinaus (rückwirkende Herausgabe sämtlicher besuchter Websites etc.), die den Delegationsrahmen von Art. 15 BÜPF klar sprengen würde und als höchst problematischer politischer Entscheid klar in die Hände des Gesetzgebers gehört, und die – nebenbei gesagt – aus der aktuellen Vorlage für eine Revision des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit BWIS eben erst wieder entfernt wurde. Eine Einführung einer Vorratsdatenspeicherung auf dem Verordnungsweg steht damit nach Auffassung der asut völlig ausser Frage.

Ferner ist der Begriff der periodischen Übermittlung unklar und näher zu umschreiben. Vgl. zu Art. 24 zudem auch den Technischen Annex, S. 19 ff.

Zu Art. 24c

Auch Art. 24c geht klar weiter als eine einfache Nachführung. Die Bestimmung will die FDA zu einer Art „Kopfschaltung" im Internetbereich zwingen. Die Argumente zur Kopfschaltung wurden bereits dargelegt. Auch im Internetbereich kann es nicht angehen, ohne die vom BÜPF geforderte konkrete Verdachtsgrundlage mit einer Kopfschaltung „Fallen" zu stellen, in die die Nutzer dann hereintappen. Vgl. dazu auch den Technischen Annex, S. 22 f.

Zu Art. 25-27

Vgl. zu diesen Artikeln ebenfalls die Anmerkungen im Technischen Annex (S. 23 ff.).

2.4 Definitionen

Die Definition der Internet-Anbieterin in Ziff. 1 des Anhangs der Verordnung, die allein auf die Verwendung von IP-Adressen abstellt (besser wäre ohnehin: das Internet Protocol IP), ist zu weit. Es gibt eine Reihe von Produkten, die mit IP arbeiten, aber keinen Zugang zum Internet vermitteln, denn IP ist eine universelle in Computernetzen verwendete Technologie, deren Einsatz – entgegen ihrer Bezeichnung – nicht auf das Internet beschränkt ist.

Dementsprechend wäre die Definition durch die Einführung eines Elements des Zugangs zum Internet enger zu fassen. Vgl. dazu auch den Technischen Annex, S. 2.

Gemäss Ziff. 8 des Anhangs besteht folgende Definition: Adressierungselemente: Kommunikationsparameter sowie Nummerierungselemente, wie Kennzahlen, Rufnummern und Kurznummern (Art. 3 Bst. f des Fernmeldegesetzes vom 30. April 1997 9 - FMG). Die Target Identity ist beschränkt auf ein Nummerierungselement. „Adressierungselement" in Art. 16b Abs. 2 ist damit zu ersetzen durch „Nummerierungselement".

Gemäss Ziff. 9 des Anhangs wird der Begriff der Kommunikationsparameter definiert als die Elemente zur Identifikation von Personen, Computerprozessen, Maschinen, Geräten oder Fernmeldeanlagen, die an einem fernmeldetechnischen Kommunikationsvorgang beteiligt sind (Art. 3 Bst. g FMG). Gemäss dieser Definition sind SIM-Nummer, IMSI, MSISDN Parameter, die mit dem Kunden assoziiert sind und der Identifikation der Person dienen und damit auch „Parameter zur Teilnehmeridentifikation". Die IMEI ist mit einem Mobiledevice assoziiert und ist ein „Kommunikationsparameter des Endgerätes der Mobiltelefonie". Der Begriff der SIM-Nummer ist zudem auch in ETSI TS 102 657 nicht definiert und damit unklar; in jedem Fall erlauben die durch ETSI definierten Datenformate nicht, eine SIM-Nummer auszuliefern.

Zu Ziff. 14 vgl. sodann den Technischen Annex, S. 32.

2.5 Kosten

Die gleichzeitig mit der VÜPF in Revision befindliche Verordnung über Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs sieht für eine Reihe von Überwachungsarten einen Wechsel von stundenbasierter Aufwandsentschädigung hin zu Entschädigungspauschalen vor. Dies droht zu einer signifikanten Reduktion der Entschädigungen zu führen. Angesichts dessen, dass den FDA nach offiziellen Studien nur gut 30% der Überwachungskosten entschädigt werden, lehnt die asut eine weitere Reduktion strikte ab. Immerhin werden andere Unternehmen, die den Untersuchungsbehörden bei der Polizeiarbeit behilflich sind – etwa private Bewachungsunternehmen – auch nicht nur zu 30% entschädigt.

Wie bereits erwähnt, bilden die Entschädigungen zudem einen wesentlichen Streitpunkt auch in der gegenwärtigen Revision des BÜPF. Als eminent politische Materie sind sie zumindest in den Grundzügen auf dem Weg der Gesetzgebung festzulegen und nicht durch eine Verordnungsrevision.

Sodann wären auch auf Verordnungsebene klare Kriterien vorzusehen, in welchen Fällen eine pauschalisierte Entschädigung zulässig ist und wann eine Entschädigung nach Aufwand zu bezahlen ist. Keinesfalls kann eine derartige Entscheidung an den ÜPF delegiert werden, wie dies der neue Art. 4a der Gebührenverordnung offenbar will.

Auf die Auswirkungen der Erweiterung des Katalogs der Überwachungsarten auf die Entschädigungen für die FDA wurde bereits vorne unter 1.2 hingewiesen.

In Art. 4a der Gebührenverordnung ist ferner zunächst die Rede von CHF 160.- pro Stunde, dabei sollen die Entschädigungen gemäss Absatz 4 bloss 80% des Zeit- und Sachaufwandes decken. Dies ist widersprüchlich oder zumindest unklar.

The information delivery platform for European business

colt

Eidgenössisches Justiz- und Polizeidepartement
Informatik Service Center ISC-EJPD
Dienst Überwachung Post- und Fernmeldeverkehr
Bereich Recht und Controlling
Herrn Patrick Schöpf
Fellerstraße 15
CH-3003 Bern

COLT Telecom Services AG
Mürtschenstrasse 27
CH-8048 Zürich
Switzerland
Christian Weber
Tel: + 49 (0) 69 / 5 66 06 - 6591
Fax: + 49 (0) 69 / 5 66 06 - 1200
www.colt.net

Vorab per e-mail: patrick.schoepf@isc-ejpd.admin.ch

27. Juli 2010

Anhörung anlässlich der geplanten Änderungen der *„Verordnung über die Überwachung des Post- und Fernmeldeverkehrs" (VÜPF)* sowie der *„Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs"*

Stellungnahme COLT Telecom Services AG

Sehr geehrter Herr Schöpf,

als Mitgliedsunternehmen der *asut* erlaubt sich die COLT Telecom Services AG nachfolgend individuell Stellung zur vorgenannten, mit Schreiben vom 8. Juni 2011 unterbreiteten Anhörung zu den geplanten Änderungen der vorgenannten Verordnungen zu nehmen, da diese unmittelbare Auswirkungen auf den Geschäftsbetrieb der COLT Telecom Services AG haben werden.

Colt ist Europas Information Delivery Platform und ermöglicht Unternehmen die Weitergabe, Verarbeitung und Speicherung ihrer entscheidenden Geschäftsdaten. Colt bietet großen und mittelständischen Unternehmen, Organisationen und Wholesale-Kunden ein leistungsstarkes Portfolio, das eine Kombination aus Netzwerk- und IT-Infrastruktur mit der Expertise in den Bereichen IT-Managed Services, Netzwerk- und Kommunikationslösungen darstellt.

In der Schweiz ist die COLT Telecom Services AG als Anbieterin von Fernmeldediensten tätig und erbringt vor allem festnetzbasierte Sprach- und Datendienste für Geschäftskunden.

(1) Zielsetzungen

Der „Dienst Überwachung Post- und Fernmeldeverkehr" (*nachfolgend „Dienst ÜPF"*) verfolgt mit der geplanten Teilrevision nach eigener Aussage die folgenden Ziele:

- Anpassung der Verordnungen an den Stand der Technik und die gelebte Praxis
- Klarere und transparentere Formulierung des Katalogs der Überwachungsmaßnahmen
- Schaffung der nötigen Bestimmtheit und Rechtssicherheit für alle Beteiligten

Die vom Dienst ÜPF erklärten, oben dargestellten Zielsetzungen sind als solche dem Grunde nach zunächst nicht zu beanstanden. Colt sieht ebenfalls die Notwendigkeit, den Strafverfolgungsbehörden ein geeignetes Instrumentarium zur Kriminalitätsbekämpfung zur Verfügung zu stellen.

Eine Einzel- und Detailbetrachtung der vorgesehenen Änderungen zeigt jedoch, dass der Grundsatz der Verhältnismäßigkeit nicht durchgehend beachtet und die von der Verordnung betroffenen Parteien teilweise in unzumutbarer Weise belastet. Da die Überwachung des Post- und Fernmeldeverkehrs zum einen einen erheblichen Eingriff in die verfassungsmäßigen Rechte der Bürger bedeutet und zum anderen die Anbieter von Fernmeldediensten sowohl finanziell als auch personell belastet, sind an die Einhaltung der Verhältnismäßigkeit besonders strenge Maßstäbe anzulegen.

(2) Subsidiarität der Verordnungen gegenüber höherrangigem Recht

Der Dienst ÜPF bezeichnet die Teilrevisionen als bloße „Nachführung", welche die Transparenz und die Rechtssicherheit erhöhe. Dem ist jedoch nicht beizupflichten, wie der Umfang und die Art der vorgesehenen Änderungen zeigen. Vielmehr handelt es sich um eine Ausdehnung der Überwachung im Verwaltungswege, der erhebliche rechtsstaatliche Bedenken entgegenstehen. Der Dienst begründet das Unterbleibender vorgezogenen Anpassung des BÜPF damit, dass die Revision der gesetzlichen Grundlagen derzeit ebenfalls weiterlaufe, aber der gesetzgeberische Prozess noch einige Zeit in Anspruch nehmen werde und man nach der Totalrevision des BÜPF die beiden Verordnungen ebenfalls einer Totalrevision unterziehen werde (s. FAQ 3. zu VÜPF- und Gebührenverordnungsteilrevision, http://www.ejpd.admin.ch/content/ejpd/de/home/themen/sicherheit/ueberwachung_des_post-/faq_vuepf.faq_2.html#a_faq_2). Somit ist das Vorgehen nicht nur rechtsstaatlich bedenklich, sondern zusätzlich auch noch ineffizient, da nach Erlass der BÜPF ein erneutes Verwaltungsverfahren durchgeführt werden müsste. Zudem ist nicht nachvollziehbar, weshalb der Abschluss der BÜPF-Revision nicht nach nunmehr zehn änderungsfreien Jahren noch wenige Monate abgewartet werden kann, ohne dass die Telekommunikationsüberwachung dabei Schaden nähme.

Abschließend tritt noch erschwerend hinzu, dass Bestandteile von Regelungen, die im BÜPF zu regeln sind, bereits in den gegenständlichen niederrangigen Verordnungen geregelt würden, so etwa die Neudefinition von Internetdienstleistern und ihren Verpflichtungen im 6. Abschnitt des VÜPF-Entwurfs. Dies stellt unseres Erachtens einen Verstoß gegen das in Art. 5a der Bundesverfassung der Schweizerischen Eidgenossenschaft normierte Subsidiaritätsprinzip dar.

Die vorstehend geschilderte Situation erfordert es aus unserer Sicht, zwischen den verschiedenen Gruppen von Anbietern von Fernmeldediensten eine enge Kooperation und Abstimmung erfolgen, um an der VÜPF bereits im Vorfeld gestaltend mitwirken und einen Marktkonsens der verpflichteten Unternehmen erzielen zu können. Hieran beteiligen wir uns gern.

(3) Überwachung des Internets

Im 6. Abschnitt wird mit der Internetüberwachung ein komplett neuer Regelungskomplex eingeführt. Auch wenn bereits heute Internetdaten zur Strafverfolgung von Zugangsanbietern überwacht und ausgewertet werden, bietet das BÜPF keine hinreichende formalgesetzliche Grundlage für die Schaffung einer aktiven Überwachungspflicht hinsichtlich des gesamten Internetverkehrs (*s. dazu oben (2), 2. Abs.*) inklusive der Übertragung in Echtzeit zum Dienst ÜPF.

Die Durchführung von Überwachungsmaßnahmen unterliegt auch hinsichtlich des Internets dem insoweit abschließenden Straftatenkatalog des Art. 269 StPO und steht gemäß Art. 272 Abs. 1 StPO unter dem Vorbehalt der vorherigen Genehmigung durch das Zwangsmassnahmengericht. Dies ist in der VÜPF zwingend zu verankern, mindestens jedoch muss eine gerichtliche Überprüfungsmöglichkeit hinsichtlich der Rechtmäßigkeit einer Überwachungsanordnung geschaffen werden.

Aufs Strengste abzulehnen ist auch die sog. „rückwirkende Überwachung", die letztlich eine verdachtsunabhängige Massenüberwachung aller Internetnutzer darstellt und als Eingriff in Grundrechte ebenfalls einer gesetzlichen Regelung in der BÜPF statt der VÜPF als bloßer Verordnung bedarf (vgl. *dazu oben (2), 1. Abs.*).

Die Verdoppelung der Speicherungsfrist von 6 auf 12 Monate ist bereits in Anbetracht dieser schweren rechtsstaatlichen Mängel, aber auch grundsätzlich abzulehnen.

Darüber hinaus wird mit dem Terminus „Internet-Anbieterin" eine neue Begrifflichkeit für Verpflichtete eingeführt, die nicht definiert ist und somit weder bestimmbar noch abgrenzbar von der "Anbieterin von Post- und Fernmeldediensten". Hier ist eine eindeutige Definition vorzunehmen.

(4) Gebühren und Entschädigungen

Wie oben unter (1) bereits dargestellt, ist eines der mit der Teilrevision verfolgten Ziele die *„Anpassung der Verordnungen an den Stand der Technik und die gelebte Praxis"*. Insoweit verwundert es, dass nicht ebenfalls die Höhe der Gebühren und Entschädigungen in der Gebührenverordnung nach oben angepasst wird. Der Dienst begründet dies damit, dass *„Die Höhe der Gebühren und Entschädigungen sich an der bestehenden Gebühren- und Entschädigungsstruktur [...]"* orientiert. (s. FAQ Nr. 4 zu VÜPF- und Gebührenverordnungsteilrevision, http://www.ejpd.admin.ch/content/ejpd/de/home/themen/sicherheit/ueberwachung_des_post-/faq_vuepf.faq_2.html#a_faq_2). Diese In-sich-Begründung trägt jedoch nicht, da gemäß den vom Bundesamt für Statistik veröffentlichten Werten die Gehälter und damit die Personalkosten gestiegen sind, ebenso die jahresdurchschnittliche Teuerung (mit Ausnahme von 2009, s. dazu http://www.bfs.admin.ch/bfs/portal/de/index/themen/05/02/blank/key/jahresdurchschnitte.html). Somit fallen die Mehrkosten einseitig den zur Überwachung verpflichteten Unternehmen zur Last. Es ist daher eine entsprechende Regelung zur angemessenen Entschädigung für anfallende Überwachungskosten aufzunehmen.

(5) Statistik und Auswertung

Die vom Dienst ÜPF veröffentlichte Statistik ist verbesserungsbedürftig, da sie derzeit nur in begrenztem Maße aussagekräftig ist, da lediglich die Anzahl der Überwachungen in Echtzeit, der rückwirkenden Überwachungen sowie der technisch-administrativen Auskünfte erfasst wird (s. http://www.ejpd.admin.ch/content/ejpd/de/home/themen/sicherheit/ueberwachung_des_post-/statistik.html). Aus dem direkten Vergleich mit der Situation in Deutschland, wo wir über langjährige Regulierungserfahrung verfügen, ergibt sich unseres Erachtens, dass eine weiterführende Untersuchung, wie sie die Bundesregierung im Jahr 2003 beim Freiburger Max-Planck-Institutes für ausländisches und internationales Strafrecht in Auftrag gab, zur Erreichung des unter (1) aufgeführten Zieles der Schaffung der nötigen Bestimmtheit und Rechtssicherheit für alle Beteiligten in besonderem Maße beizutragen in der Lage ist („*Rechtswirklichkeit und Effizienz der Überwachung der Telekomjunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen*", s. http://beck-aktuell.beck.de/sites/default/files/rsw/upload/Beck_Aktuell/Abschlussbericht_1_1.pdf).

Die Untersuchung beleuchtet eine Vielzahl weiterer wichtiger Aspekte im Zusammenhang mit Überwachungsmaßnahmen, beispielhaft seien nur genannt die Unterscheidung zwischen Maßnahmen im Festnetz oder Mobilfunk, Maßnahmen der Inlands- oder Auslandskopfüberwachung sowie Angaben zur Dauer der Maßnahmen, zur Anzahl eventueller Verlängerungen etc.

(6) Fazit

Wie unsere Ausführungen gezeigt haben sollten, bedarf es noch etlicher Anpassungen an den teilzurevidierenden Verordnungen. Sollte hierzu von Ihrer Seite weiterer Erläuterungs- oder Konkretisierungsbedarf bestehen, lassen Sie uns dies bitte wissen. Gerne besprechen wir mit Ihnen telefonisch oder auch persönlich die sich insbesondere aus Sicht eines Geschäftskundenanbieters erbietenden Schwierigkeiten bei der Umsetzung der gegenständlichen Verordnungen.

Mit freundlichen Grüßen
COLT Telecom Services AG

ppa. Sabine Hennig
Rechtsanwältin
Director Regulatory Affairs
Germany, Austria, Switzerland

i. V. Christian Weber
Rechtsanwalt
Senior Advisor Regulatory Affairs
Germany, Austria, Switzerland

finecom
BROADBAND ACCESS

Finecom
Telecommunications AG
www.finecom.ch
Robert-Walser-Platz 7
Postfach, CH-2501 Biel
Tel. +41 (0)32 559 99 99
Fax +41 (0)32 559 99 90

stay connected

EINSCHREIBEN

Informatik Service Center ISC-EJPD
Dienst Überwachung Post- und
Fernmeldeverkehr
Bereich Recht und Controlling
Patrick Schöpf
3003 Bern

Biel/Bienne, 28. Juli 2011

Stellungnahme zu Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) sowie der Verordnung über Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs

Sehr geehrter Damen und Herren
Wir danken Ihnen für die gemäss Schreiben von Frau Bundesrätin Simonetta Sommaruga vom 8. Juni 2011 eingeräumte Möglichkeit, sich zur VÜPF – Teilrevision anhören zu lassen. Wir möchten mit unserer Stellungnahme die wichtigsten Punkte noch einmal hervorheben und verweisen für weitere Einzelheiten auf die ausführlichere Stellungnahme der asut, welche Finecom vollumfänglich unterstützt.

Speziell möchten wir die aus Sicht Finecom wichtigen Punkte nochmals explizit hervorheben:

1. Entgegen der Darstellung im Begleitbrief würde die vorgeschlagene Revision nicht nur eine Nachführung der bereits bestehenden Praxis darstellen, sondern eine **massive Ausweitung der staatlichen Überwachung** des Bürgers mit sich bringen, insbesondere eine Vorratsdatenspeicherung des Internetverkehrs. Es handelt sich um einen eigentlichen **Etikettenschwindel,** der im geltenden Bundesgesetz über die Überwachung des Post und Fernmeldeverkehrs BÜPF zudem **keine genügende gesetzliche Grundlage** findet und kaum auf statistischen Entscheidgrundlagen basiert.
2. Sodann bringt die Vorlage, anders als in den Erläuterungen dargestellt, **keine Verbesserung der Rechtssicherheit.** Entgegen der Regelung in der geltenden VÜPF soll der Katalog der Überwachungspflichten in der neuen VÜPF nicht mehr abschliessend sein, sondern die Behörden sollen explizit die Kompetenz erhalten, ohne Verordnungsgrundlage neue Überwachungspflichten einzuführen. Anders als unter der geltenden Verordnung haben die Telekom-Unternehmen wie auch die Bürger damit genau *keine* Rechtssicherheit mehr; sie werden nicht mehr wissen, mit welchen Überwachungsmassnahmen sie zu rechnen haben.
3. Die Vorlage soll für die Behörden eine **Kostensenkung** bringen, diese würde allerdings genau gesehen **ausschliesslich zu Lasten der Telekom-Unternehmen** gehen. Schon heute werden die Kosten der Telekom-Unternehmen für die Kommunikationsüberwachung nur zu einem Drittel vom Staat entschädigt. Wir können nicht nachvollziehen, warum dieser Betrag jetzt auf dem Buckel der Telekom-Unternehmen und ihrer Kunden noch

weiter gesenkt werden soll. Mit der Kostensenkung für die Behörden droht den Telekom-Unternehmen zudem eine massive Steigerung der Zahl von Überwachungsaufträgen, für die sie dann wiederum die Mehrheit der Kosten zu tragen hätten.

4. Die Vorlage **ignoriert das Verhältnismässigkeitsprinzip**: Die Telekom-Unternehmen sollen nicht verpflichtet werden können, teure Überwachungsanlagen zu beschaffen, die sie ohnehin nur in sehr unwahrscheinlichen Fällen überhaupt brauchen werden.

Aus diesen Gründen steht Finecom der aktuellen Revision der VÜPF ablehnend gegenüber. Vor allem die geplante Ausweitung der Überwachungsmassnahmen darf nur mit einem demokratisch legitimierten Entscheid und damit nur durch Bundesgesetz erfolgen. **Entsprechend ist mit einer Revision der VÜPF bis zur Verabschiedung des BÜPF zuzuwarten.**

Finecom geht es mit ihrer Opposition gegen die Vorlage keineswegs darum, den Sinn der Telekom-Überwachung zum Zweck der Verbrechensbekämpfung in Frage zu stellen. **Finecom hat schon immer konstruktiv mit den Behörden zusammengearbeitet, um die gesetzlich vorgesehenen Überwachungsmassnahmen umzusetzen.** Finecom wehrt sich allerdings gegen die neuesten Reformpläne, weil derart schwerwiegende Eingriffe in die Privatsphäre des Bürgers und in die Wirtschaftsfreiheit und Eigentumsgarantie der Telekom-Unternehmen nicht durch die Hintertür einer Verordnungsrevision eingeführt werden dürfen.

Freundliche Grüsse

Michel Renfer
CTO

Marc Loosli
Responsible LI

ImproWare Technologie und Know How im Dienste der Kommunikation
Es ist Ihre Zukunft

Informatik Service Center ISC-EJPD
Dienst Überwachung Post- und
Fernmeldeverkehr
Bereich Recht und Controlling
Patrick Schöpf
3003 Bern

Pratteln, 27.07.2011

VÜPF Änderungsvorlage vom 8. Juni 2011: Stellungnahme

Sehr geehrte Damen und Herren

Mit grosser Sorge und gemischten Gefühlen haben wir seit geraumer Zeit die Fortschritte in dieser Sache verfolgt und sind deshalb froh, uns an dieser Stelle äussern zu dürfen.

Eine Anmerkung zu Ihrer Darstellung der Ausgangslage. Sie bemühen das Abkommen mit dem Europarat über die Cyberkriminalität (nachzulesen unter http://www.coe.int/t/dlapil/codexter/0_Accueil/09_Adopted_Texts_Conventions_en.asp unter ETS No. 185)
als ein Grund für die Ausweitung der Überwachungsmassnahmen. Da drin steht jedoch lediglich unter :

Article 20 - Real-time collection of traffic data:

b) compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,traffic data, in real-time, associated with specified communications in
its territory transmitted by means of a computer system.

man beachte das "within existing technical capability"!

ImproWare AG – Es ist Ihre Zukunft!
Zurlindenstrasse 29, CH-4133 Pratteln
Telefon 061/826 93 00 Fax 061/826 93 01 E-Mail info@imp.ch

Wir möchten auch darauf hinweisen, dass die Revision, so wie sie von Ihnen skizziert wurde, aus Providersicht schon aus dem Grund problematisch ist, da für diese nahezu alle Informationen, die Kunden betreffen, sofern sie nicht für den Betrieb und die Verrechnung vonnöten sind, für alle anderen Nutzungen verboten sind, sofern deren Sammlung und Vorhaltung nicht ausdrücklich durch Gesetze erzwungen ist, da praktisch immer das persönliche Recht auf Privatsphäre tangiert ist. Eine nicht abschliessende Liste der Überwachungsarten ist daher gleichermassen für den Provider wie für den Nutzer absolut unakzeptabel.

Auch ist aus Sicherheitsgründen eine Vorhaltung von Personenbezogenen Daten auf das absolute Minimum zu beschränken, da, sobald klar ist, dass jeder Provider diese Daten irgendwo hat, diese auch ein tendenziell einfacheres Angriffsziel darstellen.

Des Weiteren möchten wir ebenfalls unsere Zweifel an der Verfassungsmässigkeit des Vorgehens dieser Kommission Ausdruck geben und insbesondere dahingehend auf die nachstehend zitierte Stellungsnahme der ASUT, deren Mitglied wir sind, verweisen.

Freundliche Grüsse

Patrick Guelat
Leiter Technik/Mitglied des Verwaltungsrates

Daniel Müller
Head of Software Development

ImproWare AG

ImproWare AG – Es ist Ihre Zukunft!
Zurlindenstrasse 29, CH-4133 Pratteln
Telefon 061/826 93 00 Fax 061/826 93 01 E-Mail info@imp.ch

VÜPF Änderungsvorlage vom 8. Juni 2011: Stellungnahme der asut

Management Summary

Mit Schreiben vom 8. Juni 2011 eröffnete Bundesrätin Simonetta Sommaruga eine Anhörung zur Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF sowie der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs. Mit dem vorliegenden Papier nimmt der schweizerische Verband der Telekommunikation asut zu den vorgeschlagenen Änderungen kritisch Stellung.

Die folgenden Punkte stehen dabei im Zentrum:

1. Entgegen der Darstellung im Begleitbrief würde die vorgeschlagene Revision nicht nur eine Nachführung der bereits bestehenden Praxis darstellen, sondern eine **massive Ausweitung der staatlichen Überwachung** des Bürgers mit sich bringen, insbesondere eine Vorratsdatenspeicherung des Internetverkehrs. Es handelt sich um einen eigentlichen **Etikettenschwindel,** der im geltenden Bundesgesetz über die Überwachung des Post und Fernmeldeverkehrs BÜPF zudem gar **keine genügende gesetzliche Grundlage** findet und kaum auf statistischen Entscheidgrundlagen basiert.
2. Sodann bringt die Vorlage, anders als in den Erläuterungen dargestellt, **keine Verbesserung der Rechtssicherheit.** Entgegen der Regelung in der geltenden VÜPF soll nämlich der Katalog der Überwachungspflichten in der neuen VÜPF nicht mehr abschliessend sein, sondern die Behörden sollen explizit auch die Kompetenz erhalten, ohne Verordnungsgrundlage neue Überwachungspflichten einzuführen. Anders als unter der geltenden Verordnung haben die Telekom-Unternehmen wie auch die Bürger damit genau *keine* Rechtssicherheit mehr; sie werden nicht mehr wissen, mit welchen Überwachungsmassnahmen sie zu rechnen haben.
3. Die Vorlage soll für die Behörden eine **Kostensenkung** bringen, diese würde allerdings genau besehen **ausschliesslich zu Lasten der Telekom-Unternehmen** gehen. Schon heute werden die Kosten der Telekom-Unternehmen für die Kommunikationsüberwachung nur zu einem Drittel vom Staat entschädigt. Die asut kann nicht nachvollziehen, warum dieser Betrag jetzt zu Lasten der Telekom-Unternehmen und ihrer Kunden noch weiter gesenkt werden soll. Mit der Kostensenkung für die Behörden droht den Telekom-Unternehmen zudem eine massive Steigerung der Zahl von Überwachungsaufträgen, für die sie dann wiederum die Mehrheit der Kosten zu tragen hätten.
4. Die Vorlage **ignoriert das Verhältnismässigkeitsprinzip**: Die Telekom-Unternehmen sollen nicht verpflichtet werden können, teure Überwachungsanlagen zu beschaffen, die sie ohnehin nur in sehr unwahrscheinlichen Fällen überhaupt brauchen werden.

Aus diesen Gründen steht die asut der aktuellen Revision der VÜPF ablehnend gegenüber. Vor allem die geplante Ausweitung der Überwachungsmassnahmen darf nur mit einem demokratisch legitimierten Entscheid und damit nur durch Bundesgesetz erfolgen. **Entsprechend ist mit einer Revision der VÜPF bis zur Verabschiedung des BÜPF zuzuwarten.**

Der asut geht es mit ihrer Opposition gegen die Vorlage keineswegs darum, den Sinn der Telekom-Überwachung zum Zweck der Verbrechensbekämpfung in Frage zu stellen. **Die asut und ihre Mitglieder haben vielmehr schon immer konstruktiv mit den Behörden zusammengearbeitet, um die gesetzlich vorgesehenen Überwachungsmassnahmen umzusetzen.** Die asut wehrt sich allerdings gegen die neuesten Reformpläne, weil derart schwerwiegende Eingriffe in die Privatsphäre des Bürgers und in die Wirtschaftsfreiheit und Eigentumsgarantie der Telekom-Unternehmen nicht durch die Hintertür einer Verordnungsrevision eingeführt werden dürfen.

ImproWare AG – Es ist Ihre Zukunft!
Zurlindenstrasse 29, CH-4133 Pratteln
Telefon 061/826 93 00 Fax 061/826 93 01 E-Mail info@imp.ch

1 Allgemein

1.1 Teilrevision?

Gemäss dem Begleitbrief vom 8. Juni 2011 zur Vorlage, unterzeichnet durch Frau Bundesrätin Simonetta Sommaruga, soll es bei vorliegender Teilrevision der VÜPF lediglich um eine „Nachführung" gehen, welche für alle Beteiligten „die nötige Bestimmtheit und Rechtssicherheit" schaffe. Dies trifft jedoch nicht zu:

- Zunächst wird mit der Vorlage keineswegs nur die bestehende Praxis nachgeführt, sondern es werden auch diverse neue Überwachungsmassnahmen verankert, wie z.B. eine umfassende Überwachung des Internetverkehrs, zudem sollen internationale Kopfschaltungen analog zur Sprachtelefonie neu auch für SMS- und Internetüberwachungen gemacht werden. Bisher wurden als Folge eines Entscheids des Bundesverwaltungsgerichts internationale Kopfschaltungen lediglich hinsichtlich der Gesprächstelefonie eingesetzt.
- Sodann sollen mit der Revision nicht nur zweifelhafte Massnahmen wie die Kopfschaltungen in den Katalog aufgenommen werden, sondern neu auch eine Massnahme, welche unseres Erachtens illegal ist, nämlich die Antennensuchläufe. Bei solchen Massnahmen existieren keine Verdachtsmomente gegen bestimmte Personen oder Anschlüsse, wie dies von StPO und BÜPF eindeutig gefordert würde, sondern es wird ein Gebiet unspezifisch nach strafrechtlich Verwertbarem abgesucht.
- In den Erläuterungen wird zudem dargelegt, die Revision senke die Kosten: Aus Sicht der Überwachungsbehörden mag dies zwar zutreffen. Denn dadurch dass gewisse nicht vorgesehene Massnahmen in der Verordnung neu typisiert würden, gäbe es für deren Umsetzung für die Fernmeldediensteanbieter (FDA) nur noch eine geringe Pauschalentschädigung gemäss Gebührenverordnung und keine Aufwandsentschädigung gemäss bisherigem Art. 4 der Gebührenverordnung mehr. Eine solche „Kostensenkung" erfolgt aber auf dem Buckel der FDA und entspricht, zumindest nach offizieller Lesart, nicht die Meinung der Revision.
- Weiter ist der verwendete Begriff „Teilrevision" irreführend. Gemäss den Erläuterungen handelt es sich offenbar nur dann um eine Totalrevision der VÜPF, wenn sie im Nachgang einer BÜPF-Revision geschieht. Vom materiellen Gehalt her haben wir es aber bereits vorliegend mit einer Totalrevision der VÜPF zu tun, welche Entscheidungen vorwegnehmen soll, welche eigentlich in den Rahmen der BÜPF-Revision gehören.

1.2 Kein Plus an Rechtssicherheit

Die Vorlage bringt kein Plus an Rechtssicherheit, wie dies in Begleitbrief und Erläuterungen behauptet wird.

Die neueste Praxis des Bundesverwaltungsgerichts vom 21. resp. 23. Juni 2011 bestätigte die Auffassung zweier Mitglieder der asut, dass der Katalog der in der VÜPF geregelten Überwachungsarten abschliessend sei. Art. 17 Abs. 5 und Art. 25 Abs. 5 des Revisionsentwurfs widersprechen diesem Anspruch an die Rechtssicherheit im Sinne der Vorhersehbarkeit, indem sie explizit eine Kompetenz des Dienstes zur Überwachung des Post- und Fernmeldeverkehrs ÜPF zur Einführung weiterer Überwachungsmassnahmen vorsehen.

Aber selbst dann, wenn man der Auffassung ist, der Katalog sei entgegen der Auffassung des Bundesverwaltungsgerichts nicht abschliessend, bringt eine offene Formulierung des Katalogs nichts, da Fernmeldedienstanbieter und Bürger jederzeit damit rechnen müssen, dass entweder die Praxis den Katalog nicht als abschliessend betrachtet oder dass bei Bedarf einfach der Katalog wieder beliebig erweitert wird.

Dass die FDA überdies kein Rechtsmittel besitzen, um sich gegen solche von Gesetz und Verordnung nicht gedeckten Überwachungsmassnahmen zu wehren und ihre verfassungsmässigen Rechte zu wahren, hat die asut bereits in der Vernehmlassung zum VE-BÜPF heftig kritisiert. Sie sieht darin einen wesentlichen konzeptionellen Mangel des BÜPF, der weder durch den VE-BÜPF, geschweige denn durch die nun geplante Verordnungsrevision behoben wird.

Die Erklärung, dass den rechtsstaatlichen Mängeln des BÜPF mit einer VÜPF-Revision nicht beizukommen ist, findet sich im Prinzip in den Erläuterungen zur Vorlage selbst, S. 1 unten:

Nach Ansicht der anordnenden Strafverfolgungsbehörden und der die Überwachungsmassnahmen genehmigenden Zwangsmassnahmengerichte ist die Liste der Überwachungsmassnahmen in der VÜPF nicht abschliessend zu betrachten. Der Dienst und die FDA sind nach dieser Auffassung daher auch verpflichtet, angeordnete und genehmigte

Überwachungsmassnahmen durchzuführen, die nicht explizit in der VÜPF aufgeführt sind. Diese Situation führt zu einer grossen Rechtsunsicherheit und dazu, dass sowohl auf Seiten des Dienstes als auch auf Seiten der FDA bei der Durchführung von nicht explizit in der VÜPF aufgeführten Überwachungsmassnahmen erhebliche Kosten entstehen.

Die Problematik, dass aufgrund fehlender Rechtsbehelfe der Provider theoretisch alles durchgeführt werden muss, was Zwangsmassnahmengerichte, welche über kein genügendes technisches Verständnis verfügen, genehmigen, lässt sich mit einer Erweiterung des Massnahmenkatalogs sicher nicht beseitigen, solange dieser derart offen formuliert bleibt.

Damit würde nur erreicht, dass damit insgesamt den FDA die Entschädigungen gekürzt würden, weil die Aufwandsentschädigung gemäss bisherigem Art. 4 der Gebührenverordnung durch pauschal festgelegte Teilentschädigungen ersetzt würde. Weiter würde der neue Art. 1 Abs. 2 bis bewirken, dass pro überwachte Rufnummer unter einem Auftrag sämtliche möglichen Erhebungen verlangt werden könnten und dies nur unter Entschädigung der Basisleistung. Die FDA lehnen dies selbstverständlich ab. Es ist in den Erläuterungen nirgends die Rede davon, dass eine Kürzung der Entschädigungen für die FDA die Absicht wäre. In finanzieller Hinsicht ist in den Erläuterungen auf S. 2 vielmehr die Rede davon, dass es darum gehe, den FDA Investitionssicherheit zu verschaffen.

1.3 Übernahme von bisheriger Rechtssprechung und Praxis:

Oft soll mit Gesetzesrevisionen die in der Zwischenzeit aufgelaufene, „bewährte" Rechtssprechung ins neue Gesetz einfliessen, so auch hier. In diesem Fall ist aber Skepsis angebracht. Einerseits gibt es keine gefestigte Rechtssprechung, sondern nur einige wenige Einzelentscheide, und diese sind meistens nicht hilfreich. Aufgrund der konzeptionellen Fehler im BÜPF, welche zur Folge haben, dass hinsichtlich der Frage, was die Gerichte auf Beschwerde einer FDA hin nun zu prüfen haben, Konfusion herrscht, konnte sich keine Gerichtspraxis entwickeln, welche sich eignen würde, ins Gesetz aufgenommen zu werden.

An dieser Stelle kann nicht auf die Gesamtheit der Unstimmigkeiten und Widersprüchlichkeiten der aufgelaufenen Gerichtsentscheide eingegangen werden, nur soviel: Mit seinen zwei neusten Entscheiden hiess das Bundesverwaltungsgericht zwei Beschwerden von FDA gut, mit der Begründung, die FDA seien in der angefochtenen Verfügung zu Überwachungsmassnahmen verpflichtet worden, welche im Katalog der Überwachungsmassnahmen gemäss VÜPF gar nicht vorhanden sind. Da die Aufzählung der Überwachungsmassnahmen in der VÜPF abschliessend zu verstehen sei, sei eine Verpflichtung der FDA zu Massnahmen ausserhalb des Katalogs nicht zulässig. Gemäss Art. 13 Abs. 1 Bst. a BÜPF darf jedoch der ÜPF eine von Zwangsmassnahmengerichten genehmigte Überwachung nur darauf hin überprüfen, ob die angeordnete Massnahme von einer zuständigen Behörde aus erfolgt ist und ob es um ein Delikt gemäss des Deliktskatalogs des BÜPF geht. Das BVGer hat nun aber darüber hinaus geprüft, ob die angeordneten Massnahmen im Katalog der VÜPF aufgeführt seien. Den FDA ist es zwar durchaus recht, wenn das Bundesverwaltungsgericht in Ausübung einer rechtspolitischen Lückenfüllung über Art. 13. Abs. 1 Bst. a BÜPF hinaus prüft. Es erscheint aber unschlüssig, wenn sich das Gericht einerseits nicht an Art. 13 Abs. 1 Bst. a BÜPF hält und andererseits die von der Beschwerdeführerin angeführten, in diesem Papier auch schon erwähnten, konzeptionellen Fehler des BÜPF in Abrede stellt (A-8267/2010, Erw. 3.2).

Mit dem einzigen höchstrichterlichen Entscheid im Bereich Zulässigkeit von Überwachungsmassnahmen im Fernmeldebereich (BGE 130 II 249ff) wurde überdies eine Überwachungsmassnahme, welche ebenfalls nicht dem VÜPF Katalog angehört (Antennensuchläufe), nicht verhindert. Das Bundesgericht stellte sich dabei auf den Standpunkt, es dürfe die Rechtmässigkeit von Antennensuchläufen gar nicht prüfen. Wenn also in den Erläuterungen behauptet wird, Antennensuchläufe seien von der Gerichtspraxis als zulässig bestätigt worden, so stimmt das schlicht nicht, denn das Bundesgericht hat die Zulässigkeit von Antennensuchläufen gar keiner Prüfung unterzogen. Es wäre daher nicht gerechtfertigt, den Überwachungstypenkatalog der VÜPF unter Hinweis auf die Bundesgerichtspraxis zu ergänzen.

1.4 VÜPF-Revision im jetzigen Zeitpunkt ist abzulehnen

Aus den diversen oben genannten Gründen, ist diese VÜPF-Teilrevision abzulehnen. Wie dargelegt, ist es nicht möglich, mit dieser Vorlage Rechtssicherheit zu schaffen. Es besteht hingegen die Befürchtung, dass mit dieser VÜPF-Revision im etwas kleineren Kreis und ohne die nötige demokratische Legitimation Forderungen durchgedrückt werden sollen, welche in einer Revision des Gesetzes im formellen Sinn keine Chance hätten. Weiter muss die Befürchtung bestehen, dass mit dieser Verordnungsrevision, welche im Prinzip eine Wunschliste des ÜPF enthält, die längst fällige BÜPF-Revision auf die lange Bank geschoben werden soll.

ImproWare AG – Es ist Ihre Zukunft!
Zurlindenstrasse 29, CH-4133 Pratteln
Telefon 061/826 93 00 Fax 061/826 93 01 E-Mail info@imp.ch

1.5 BÜPF-Revision abwarten

Die meisten relevanten Änderungen in dieser VÜPF-Revisionsvorlage betreffen Punkte, welche gerade in der parallel laufenden BÜPF-Revision umstritten sind:

- Änderungen, welche die Kosten/Entschädigungen betreffen
- Nicht nur Ausleitung des gesamten Fernmeldeverkehrs von bestimmten Breitbandanschlüssen, sondern auch Überwachungspflichten der Zugangsanbieterinnen auf der Dienste-/Anwendungsebene (allfällige Filterungspflichten der FDA)
- Überwachungsmassnahmen gegen einen unbestimmten Personenkreis (z.B. Antennensuchläufe).

Man kann sich daher des Eindrucks nicht erwehren, der Verordnungsgeber wolle nun die Punkte, die im Rahmen der Vernehmlassung zum BÜPF ins Schussfeld der Kritik geraten sind, am Gesetzgeber vorbei in die VÜPF bringen. Damit würde der von Verfassung und Gesetz vorgesehene Stufenbau (Gesetz – Verordnung – Richtlinien) umgangen, was dem Prinzip der Rechtsstaatlichkeit widerspricht. Es geht nicht an, dass die relevanten Entscheidungen auf einer unteren Normenstufe gefällt werden und sich dann später das Gesetz im formellen Sinn danach richten soll.

Dies gilt insbesondere auch deshalb, weil der Verordnungsgeber die ihm durch Art. 15 (insbes. Abs. 6) BÜPF verliehene Rechtsetzungskompetenz in verschiedener Hinsicht eindeutig überschreitet: So regelt das BÜPF beispielsweise an keiner Stelle die Überwachung von Anwendungen wie VoIP, Instant Messaging oder Multimediadienste, die nicht von Fernmeldediensteanbietern oder Internet-Access-Providern, sondern von Internet-Anwendungsanbietern (Service Provider) angeboten werden (vgl. Hansjakob, Kommentar, N 24 zu Art. 1 BÜPF). Auch hatte der historische Gesetzgeber vor elf Jahren keine Vorstellung, welche neuen Dienstleistungen auf dem Internet zur Verfügung stehen würden, und entsprechend ist der Verordnungsgeber erst durch ein formelles Gesetz zu ermächtigen, Überwachungsarten einzuführen, die zum Zeitpunkt des Erlasses des BÜPF nicht vorstellbar waren (etwa Zugänge über VPN oder „Instant Messaging"). Dies gilt erst recht für eine Vorratsdatenspeicherung für WWW-Internetverkehr (http), die bei einer weiten Auslegung der Verordnung ebenfalls möglich wäre, und die einen schwerwiegenden Eingriff in die Privatsphäre von Bürgern beinhaltete. Ein solcher schwerwiegender Eingriff würde zwingend eine Regelung in einem formellen Gesetz voraussetzen (mehr dazu unten bei den Ausführungen zu Art. 24b des Entwurfs).

Hinzu kommt, dass die Verordnung, wie im Folgenden zu zeigen sein wird, auf technischer Ebene mehr Fragen aufwirft, als sie beantwortet. Anstatt die Verordnung an den Informationsbedürfnissen der Strafverfolgung zu orientieren, wird zudem versucht, technische Lösungen in einem bestimmten technologischen Umfeld zu beschreiben und eine Reihe von Parametern, oft in unklarem Kontext, aufzulisten (dazu den Technischen Annex dieses Dokuments, S. 1).

Da nach Auffassung der asut vor einer Revision der VÜPF der Abschluss der Revision des BÜPF mit dem normalen Durchlauf des Gesetzgebungsverfahrens nötig wäre, wird auf einen detaillierten Änderungsvorschlag verzichtet. Wegen der unklaren, bzw. inexistenten formell-gesetzlichen Grundlage müsste dieser ohnehin nur Stückwerk bleiben. Die asut hat sich bei der BÜPF-Revision schon bisher sehr kooperativ gezeigt und hat mit konstruktiven Vorschlägen an dieser mitgewirkt. Sie wird dies selbstverständlich auch künftig tun und zu einer erfolgreichen Umsetzung jenes Projekts Hand bieten.

1.6 Fehlende Berücksichtigung des Verhältnismässigkeitsprinzips in der Verordnung

Es wäre zu berücksichtigen, dass bei Anbietern mit geringer Kundenzahl, bei Anbietern mit überwiegendem Anteil an Business-Kunden oder aber bei seltenen Überwachungsarten im Hinblick auf die in diesen Fällen nur kleine Zahl von zu erwartenden Überwachungsvorgängen eine Installation von Überwachungsanlagen unverhältnismässig und nicht zumutbar scheint. Die neuen Richtlinien TR TS müssten in diesem Sinne neben den Handover Interfaces (HI), entsprechende Schnittstellen (in ETSI Terminologie Internal Network Interface, INI) spezifizieren, dass der ÜPF in vergleichbaren Fällen ad hoc Ausrüstung installieren kann. In solchen Fällen dürfen die FDA allenfalls verpflichtet werden, die für die Installation der Ausrüstung nötigen Schnittstellen zur Verfügung zu stellen, nicht aber, die Anlagen als solche „auf Vorrat" zu beschaffen.

Ebenfalls eine klare Verletzung des Verhältnismässigkeitsprinzips liegt in der Anforderung von Art. 18 Abs. 3 vor, eine 24x7-Erreichbarkeit sicherzustellen. Viele kleine Provider beschäftigen nur wenige Angestellte und wären durch eine derartige Anforderung überfordert.

1.7 Fehlende Entscheidgrundlage für eine Ausweitung der Überwachungspflichten

Abschliessend ist darauf hinzuweisen, dass die Ausweitung des Anwendungsbereichs der VÜPF offenbar erfolgt, ohne dass über die Wirksamkeit der bisherigen Überwachungsmassnahmen Statistiken erhoben worden wären. Schon die Wirksamkeit der bisherigen Methoden bleibt vielmehr völlig im Unklaren, und erst recht ist nicht gesichert, ob von der geforderten Ausweitung der Überwachungsarten überhaupt die erwünschte Wirkung zu erwarten sei. Umgekehrt betrachtet bleibt also völlig offen, ob für die mit der Vorlage neu eingeführten schweren Eingriffe in die Privatsphäre der Bürger eine sachliche Grundlage besteht.

Auch dies spricht deutlich für die Forderung der asut, die Verordnungsrevision aufzuschieben, bis einerseits die Revision des zu Grunde liegenden Gesetzes erfolgt ist, und andererseits gestützt auf zuverlässiges Datenmaterial über weitere Überwachungsmassnahmen zu entscheiden wäre.

2 Zu einer Auswahl an einzelnen Bestimmungen

2.1 2. Abschnitt: Bearbeitung von Personendaten (...)

Zu Art. 9 Abs. 2: "Übergabepunkt"

Die Frage der Bestimmung der Übergabepunkte ist nach wie vor ungelöst. Damit ist offen, für welchen Abschnitt die Provider genau verantwortlich gemacht werden sollen. Ausserdem ist unklar, welche Aspekte unter Datensicherheit fallen sollen (Confidentiality, Authentication, Availability (DoS), Integrity, Non-repudiation). Zu beiden Punkten vgl. auch den Technischen Annex, S. 4 f.

2.2 4. Abschnitt: Überwachung der „Telefondienste"

Die Abgrenzung des Fernmeldeverkehrs vom Internetverkehr bleibt unklar. Internet-Technologie (damit ist eine Protokollarchitektur gemeint) kann ausserhalb des Internet eingesetzt werden beispielsweise in einem Carrier Class IP Netz (z.B. für VoIP). Vgl. dazu die Anmerkung im Technischen Annex, S. 8.

Zu Art. 16:

In der bisherigen Verordnung wurde unterschieden zwischen „Überwachung des Fernmeldeverkehr mit Ausnahme von Internet" und „Überwachung der Internetzugänge". Neu heisst es nun im 4. Abschnitt nur noch „Überwachung der *Telefondienste*" und später im 6. Abschnitt „Überwachung des Internets".

Die genaue Terminologie müsste nochmals überprüft werden, wird doch im weiteren Verlauf des 4. Abschnitts nicht mehr von „Telefondiensten", sondern wieder von „Fernmeldeverkehr" gesprochen.

Sodann sollten keine Erhebungen gemacht werden über netzinterne Parameter wie IMSI, reale Cell IDs, usw. Solche Erhebungen sind für die Strafverfolgungsbehörden und die Gerichte nicht beweisrelevant. Die Parameter werden nur netzintern verwendet und dienen der Kundensicherheit sowie zur Sicherstellung der Netzintegrität. Bei einigen solcher Daten, wie z.B. den realen Cell IDs, handelt es sich zudem um geschäftsrelevante Daten, welche die FDA nicht herausgeben können, ohne Geschäftsgeheimnisse zu verletzen.

Im Weiteren ist darauf hinzuweisen, dass viele der für die Erhebung vorgesehenen Parameter genau besehen kaum jene Beweissicherheit bieten, die sich der Verordnungsgeber offenbar vorstellt. Vielfach sind die Parameter nämlich durch die Endkunden einfach änderbar (z.B. die MAC-Adresse), sodass sie, weil sehr schwierig verifizierbar, gar keine zuverlässige Beweisführung erlauben. Entsprechend ist deren Erhebung für die Strafverfolgungsbehörden und Gerichte nicht von Nutzen und damit auch unverhältnismässig. Die Erhebung sehr schwierig verifizierbarer Parameter führt im besten Fall zu Beweislosigkeit, im schlechteren Fall zu nicht gerechtfertigten Anschuldigungen oder gar Festnahmen. Entsprechend ist zu fordern, dass Richtlinien zur Verifizierbarkeit von Parametern bestehen und die diesbezügliche Verantwortung einzelner FDA klar umschrieben wird, basierend auf ETSI TR 187 012 clause 5.2 und Draft ETSI TS 187 017 clause 4.

SIM-Nummern sind sodann keine auf dem Netz verfügbaren Parameter, welche zu den Fernmeldeverkehrsdaten gehören. Die Information der SIM-Nummern gehört zu den Auskünften über Fernmeldeanschlüsse und wird heute schon durch eine

ImproWare AG – Es ist Ihre Zukunft!
Zurlindenstrasse 29, CH-4133 Pratteln
Telefon 061/826 93 00 Fax 061/826 93 01 E-Mail info@imp.ch

Anfrage über das CCIS angefragt und die Auskunft durch die FDA erteilt.

In Art. 16 Bst. d Ziff. 2 ist im Weiteren keine klare Zuteilung der Parameter in Klassen gegeben. Zudem erzeugt die Formulierung „(wie die SIM-Nummer, die IMSI-Nummer und die IMEI-Nummer)" Rechtsunsicherheit, da nicht festgelegt ist, welche weiteren Angaben unter dieser Bestimmung herausverlangt werden könnten.

Zu Art. 16 lit. e: Antennensuchlauf:

Diese Ergänzung darf an dieser Stelle keinesfalls gemacht werden, wenn schon müsste die Durchführbarkeit von Antennensuchläufen im Gesetz im formellen Sinn vorgesehen werden, da diese Massnahme klar gegen die geltende Strafprozessordnung verstösst, wonach Fernmeldeüberwachungen nicht zur Suche nach Verdachtsmomenten gegen unbestimmt viele Personen durchgeführt werden dürfen, sondern nur im Falle eines bereits vorliegenden Verdachts und nur betreffend bereits im Voraus klar bestimmter Anschlüsse (dazu schon vorne 1.3).

Darüber hinaus lässt sich sagen, dass es gar nicht möglich ist „an einem bestimmten Standort" rückwirkend „alle mobilen Kommunikationsvorgänge" zu eruieren. Es liesse sich höchstens eine grössere oder kleinere Zahl an Funkzellen ermitteln, welche „einen bestimmten Standort" mit einer gewissen Wahrscheinlichkeit versorgen, und anschliessend die Kommunikationen über diese Funkzellen in einem definierten Zeitraum ermitteln. Ob sich aber die gesuchte Kommunikation darunter befindet, ist nicht gewährleistet.

Zu Art. 16 und 16a vgl. zudem die Anmerkungen im Technischen Annex, S. 9f.

Zu Art. 16b Überwachungsmassnahmen mit Auslandsbezug

Mit der Einfügung dieser Norm sollen die sog. internationalen „Kopfschaltungen" verankert werden, das heisst, die FDA sollen dazu verpflichtet werden, ausländische Rufnummern, respektive schweizerische Rufnummern im Ausland (outbound Roamer) überwachen zu können, wenn diese mit ihren Kunden kommunizieren. Diese Bestimmung ist abzulehnen, obschon das Bundesverwaltungsgericht vor rund zwei Jahren entschieden hat, eine solche Massnahme sei rechtmässig. Das Bundesverwaltungsgericht (A-2335/2008) stellte sich auf den Standpunkt, dies sei im Prinzip das Gleiche wie die Überwachung einer inländischen Nummer, jedenfalls sei ja die überwachte Nummer klar bestimmt. Allerdings übersah das Bundesverwaltungsgericht die Tatsache, dass es sich

- entweder um eine Überwachung einer Person im Ausland handelt, welche nach Abschluss des Verfahrens nicht, wie von der Gesetzgebung vorgesehen, über die Vornahme der Überwachung informiert werden kann, und die darüber hinaus gegen das Territorialitätsprinzip verstösst,
- im Prinzip auch um eine Überwachung von unbestimmt vielen Personen im Inland handelt, welche Kommunikationen mit der genannten Nummer im Ausland haben. Auch die Kopfschaltung widerspricht damit dem Grundkonzept des BÜPF, wonach Fernmeldeüberwachungen nicht zur Suche nach Verdachtsmomenten gegen unbestimmt viele Personen durchgeführt werden dürfen (Rasterfahndung), sondern nur im Falle eines bereits vorliegenden Verdachts und nur betreffend bereits im Voraus klar bestimmter Anschlüsse. Auch hier ist zudem offensichtlich, dass die unbestimmte Anzahl an Personen im Inland nach Abschluss des Verfahrens nicht über die Überwachung informiert werden kann.

Entgegen der Ansicht des Bundesverwaltungsgerichts gibt es also doch starke Anzeichen dafür, dass Kopfschaltungen nicht ins Konzept des aktuellen BÜPF passen, weshalb auch die Entscheidung über die Zulässigkeit von Kopfschaltungen dem Gesetz im formellen Sinn anheimgestellt werden sollte und nicht im Rahmen einer Revision der VÜPF erfolgen darf.

Zu Art. 16b vgl. zudem die Anmerkungen im Technischen Annex, S. 11 f.

Zu Art. 17 Abs. 4

Es ist unklar was alles mit „Zuleitung" gemeint ist. ETSI spezifiziert die Auslieferungsformate an einem Übergabeinterface (Handover Interface, HI), spezifiziert jedoch die Ausleitungsnetze (Delivery Networks) aus der Infrastruktur des Providers (IIF/MD) zur Infrastruktur von ÜPF (LEMF) nur oberflächlich. Wenn „die Spezifikationen dieser Zuleitung" bedeuten würde, dass ÜPF Delivery Networks spezifiziert, würde dies einen erheblichen Eingriff in die Netzhoheit der Provider

bedeuten.

Zu Art. 17 Abs. 5 und Art. 25 Abs. 5

Obschon der Verordnungsgeber (wie auch das Bundesverwaltungsgericht) davon ausgehen will, dass der Überwachungstypenkatalog der VÜPF abschliessend sei, soll diese Bestimmung nun vorsehen, dass auch nicht explizit in der Verordnung aufgeführte Fälle von Überwachungen möglich seien. Damit wird der Katalog der Überwachungstypen offengehalten, und es besteht keine Rechtssicherheit, was vom ÜPF an Überwachungen zu erwarten ist. Dies betrifft die Betreiber im Rahmen der in diesem Zusammenhang zu erwartenden Investitionen und den Normalbürger insofern, als er nicht weiss, wie er vom Staat überwacht werden kann. Gemäss Legalitätsprinzip müsste wenigstens ein Rahmen an zulässigen Überwachungen im Gesetz im formellen Sinn definiert werden. Was darüber hinaus geht, sollen die FDA nicht nur nicht ausführen müssen, sondern im Hinblick auf den Schutz der Freiheitsrechte der Bürger auch nicht ausführen *dürfen*. Daher ist diese Spezialfallregelung abzulehnen, jedenfalls solange, als nicht mit einer zufriedenstellenden BÜPF-Revision eine Grundlage geschaffen wird, welche den Rahmen der Behördenpraxis klar vorgibt.

Zu Art. 17 vgl. zudem die Anmerkungen im Technischen Annex, S. 12 f.

Zu Art. 18

Auf die Unverhältnismässigkeit der Anforderung von Art. 18 Abs. 3 (permanente Erreichbarkeit) wurde bereits unter Ziff. 1.6 hingewiesen.

Die Änderungen, v.a. in den Absätzen 7 und 8, betreffen Spezialwünsche des ÜPF. Eine Gratisnutzung der Fernmeldedienste der FDA durch den ÜPF ist abzulehnen, zumal eine solche Nutzung in keiner Weise eingegrenzt wäre.

Auch die begehrten Unterstützungsleistungen hinsichtlich der Frage, ob tatsächlich die richtige Person überwacht werde, sind fragwürdig, da diese Begehren des ÜPF daher rühren, dass er in letzter Zeit bewährte Überwachungsmethoden durch billigere und unzuverlässige Methoden ersetzt hat. Abs. 8 lässt zudem völlig offen, welche technischen und organisatorischen Vorkehrungen ein Provider treffen muss, um die entsprechende Unterstützung leisten zu können.

Vgl. auch zu Art. 18 die weiter gehenden Anmerkungen im Technischen Annex, S. 13 f.

Zu Art. 19a der *bestehenden* Verordnung

Art. 19a der bestehenden VÜPF bleibt nach dem Entwurf unverändert. Die Norm bestimmt, dass die FDA sicherstellen müssen, dass beim Verkauf von Prepaid-SIM-Karten die Personalien der Kundinnen und Kunden anhand eines *für den Grenzübertritt in die Schweiz zulässigen Reisedokumentes* erfasst werden. Nach Auffassung der asut wäre hier jedoch eine Änderung vorzunehmen.

Nimmt man die geltende Bestimmung beim Wort, können Asylbewerber mit Asylbewerberausweis (Ausländerausweis F, N und S) keine Prepaid-Karten beziehen, weil dieser Ausweis nicht zum Grenzübertritt berechtigt (vgl. Hansjakob, Kommentar, N 3 zu Art. 19a VÜPF). Nach Auffassung der asut ist das Kriterium der Eignung zum Grenzübertritt jedoch unsachlich, ist doch nur die Eignung zur Identifikation, nicht aber die Möglichkeit zum Grenzübertritt für den Zweck von Art. 19a VÜPF relevant.

Das Migrationsamt schiebt für das Verbot der Verwendung von F-, N- und S-Ausweisen sodann die Begründung nach (http://www.uvek.admin.ch/themen/kommunikation/00950/00951/index.html?lang=de, Frage 16), dass die entsprechenden Ausweise oftmals auf falsche Namen ausgestellt würden, weil sie nur auf den Angaben der Asylbewerber basieren und nicht auf amtlichen Dokumenten von deren Heimatland. Aus Sicht der asut ist es jedoch unverhältnismässig, die Verwendung von Ausweisen F, N und S bloss aufgrund eines möglichen Fehlverhaltens einzelner Ausweisträger zu beschränken. Abgesehen davon wäre die Identifikationseignung eines F-, N- oder S-Ausweises selbst dann nicht in Frage gestellt, wenn der Ausweis auf falschen Angaben des Asylbewerbers basierte, ist doch der Asylbewerber auch unter dem entsprechenden (falschen) Namen registerlich erfasst, sodass er gerade auch anhand des falschen Namens zweifelsfrei ausfindig gemacht werden könnte.

Diese Situation ist immer noch besser als jene, dass Asylbewerber für die Nutzung von Mobiltelefonie gezwungen wären,

ImproWare AG – Es ist Ihre Zukunft!
Zurlindenstrasse 29, CH-4133 Pratteln
Telefon 061/826 93 00 Fax 061/826 93 01 E-Mail info@imp.ch

einen Strohmann vorzuschicken, denn in diesem Fall wäre die Identifikation gar nicht mehr gewährleistet.

Träger der Ausweise F, N und S haben zudem in der Regel nicht die Möglichkeit, die für Postpaid-Angebote von Ausländern aus Sicherheitsgründen geforderten Depotzahlungen zu leisten. Ein Verbot, Prepaid-Karten zu beziehen, läuft damit auf eine unverhältnismässige Verletzung Kommunikationsfreiheit der entsprechenden Individuen hinaus. Entsprechend wäre bei einer Verordnungsrevision der in Art. 19a verwendete Ausweisbegriff um Ausweise F, N und S zu erweitern.

2.3 6. Abschnitt: Überwachung des Internets

Zunächst bleibt unklar, wofür der Ausdruck „Internet" verwendet (dazu die Anmerkungen im Technischen Annex, S. 16 f.) wird.

Zu Art. 23

Der Inhalt der Norm ist bezüglich Inhalt und Beschreibungstiefe mit Art.15 Abs. 1 abzugleichen (vgl. den Technischen Annex, S. 17).

Erneut ist darauf hinzuweisen, dass eine Datenherausgabe betreffend sämtlicher Netzparameter (Bst. g), welche nicht überwachungsrelevant sind und welche reine Netzdaten der betreffenden FDA bilden, nicht akzeptabel ist (dazu vorne 2.2)

Zu Art. 24

Art. 24 sieht eine massive Ausdehnung des Katalogs der Überwachungsarten vor. Die asut ist der Auffassung, dass eine derartige Ausdehnung keine genügende Rechtsgrundlage in Art. 15 BÜPF findet, zumal die meisten der entsprechenden Überwachungsarten zum Zeitpunkt der Verabschiedung von Art. 15 BÜPF noch nicht im Fokus des Gesetzgebers waren. Dementsprechend ist die geplante Ausweitung des Katalogs der Überwachungsarten durch die Delegationsnorm in Art. 15 Abs. 6 BÜPF nicht gedeckt. Die asut ist der Auffassung, eine Erweiterung des Katalogs der Überwachungsarten sei ausschliesslich auf Grund eines Gesetzes im formellen Sinn zulässig.

Eine Überwachung von VPN (Art. 24 Bst. f) wäre in jedem Fall explizit auf Anbieter zu beschränken, die VPN selber anbieten, und nicht auf die Access Provider, die VPN-Datenströme bloss von ihren Endkunden zu VPN-Anbietern im Internet weiterleiten. Dies bereits daher, weil VPN-Daten verschlüsselt und damit für eine Ausleitung ungeeignet sind.

Art. 24 Abs. 2 sieht zudem neu auch Überwachungen auf der Anwendungsebene des Internets vor (für VoIP, Instant Messaging, Multimediadienste, etc.). Die bisherige Praxis wie auch die Literatur gehen klar davon aus, dass das BÜPF auf Access Provider anwendbar ist, nicht aber auf Service Provider (Anwendungsanbieter; vgl. Hansjakob, Kommentar, N 24 zu Art. 1 BÜPF). Auch diese Norm sprengt den durch Art. 15 BÜPF vorgesehenen Rahmen daher klar, selbst die Definition der Internetanbieter nach Ziff. 1 des Anhangs der Verordnung umfasst derartige Anwendungsanbieter nicht.

Die Belastung von Anwendungsanbietern führte im internationalen Vergleich zu einer erheblichen Wettbewerbsverzerrung und vor allem zu einer Beeinträchtigung der Innovation im Bereich der Internetanwendungen, weil die Entwickler mit (im Vergleich zu den allgemein niedrigen Entwicklungskosten für die Anwendungen) ganz erhebliche Mehrkosten für die Entwicklung von Überwachungsschnittstellen einplanen müssten. Die Innovation von Anwendungen des Internets, gerade auch im Mobilfunk (Smartphones), geht heute sehr rasch voran, und entsprechend profitiert die Gesellschaft vom Internet als einem wahren Motor des Fortschritts. Diese Dynamik soll nicht durch eine übertriebene Überwachungspflicht gehemmt werden.

Im Weiteren lässt der Entwurf – und hier liegt ein weiterer schwerwiegender Kritikpunkt – völlig offen, wer für die Überwachung von Anwendungen wie VoIP, Instant Messaging oder Multimediadienste verantwortlich wäre. Angesichts dessen, dass die Access Provider bisher keinerlei technische Möglichkeiten zur Filterung von Inhalten (Deep Packet Inspection) haben, und angesichts dessen, dass eine solche Filterung in der Regel Know-How über Kommunikationsprotokolle höherer Schichten als jener des Access und allfällige Verschlüsselungsmechanismen voraussetzt, das nur der Anbieter der Anwendung selber besitzt, scheint die Vorstellung, dass die Access Provider für eine Ausleitung von aus dem Datenstrom eines Kunden ausgefilterter Anwendungsdaten verantwortlich sein sollen, nicht haltbar. Wollte man Anwendungen doch in die VÜPF aufnehmen, so müsste daher zumindest klargestellt werden, dass für

die Ausleitung entweder die Anwendungsanbieter oder dann der ÜPF, nicht aber die Access Provider verantwortlich sein können. Der ÜPF muss auch dann die Filterung übernehmen, wenn die Anwendungsanbieter vom Ausland aus tätig sind und dementsprechend nicht selber dem BÜPF unterstehen (dazu Hansjakob, Kommentar, N 26 zu Art. 1 BÜPF). Technisch gesprochen darf die Überwachungspflicht der Access Provider daher nur die IP-Adresselemente, aber nicht in der IP-Payload gespeicherte Adresselemente enthalten.

Vgl. zu Art. 24 auch den Technischen Annex, S. 18 f.

Zu Art. 24a Überwachungstypen (Echtzeit)

Die Artikel 24a und 24b enthalten einen umfassenden, schwerwiegenden Ausbau an Datenlieferungspflichten, welcher für die FDA einschneidende Folgen hätte. Gemäss BÜPF/StPO ist an sich nur vorgesehen, dass die FDA den gesamten Fernmeldeverkehr von bestimmten Anschlüssen zuleiten müssen.

Die Bestimmung enthält (wie Art. 24b auch) einige Anforderungen, wonach für die Überwachung und Beweisführung im Strafverfahren überhaupt nicht relevante Daten herauszugeben wären, was teils sogar die Netzintegrität der FDA tangieren würde (wie IMSI, reale Cell ID, usw.)

Unklar bleibt ferner der Inhalt von Art. 24a Bst. b Ziff. 3, der von „Anmeldungsdaten" spricht. Die Norm wäre dahin zu präzisieren, dass, falls überhaupt, ausschliesslich Login-Daten für die Anmeldung im Netz des Access Providers, nicht aber Login-Daten für die Anwendungsebene des Internet (http, etwa für E-Banking, E-Mail-Accounts etc.) unverschlüsselt ausgeleitet werden. Login-Daten (Username plus Password) sind Credentials (Berechtigungsnachweise) und von ihrer Eigenschaft her nicht geeignet, eine Straftat zu begehen. Jede Dritte Entität, die über die Credentials einer Entität verfügt, kann in ihrem Namen, d.h. mit ihren Identitäten kommunizieren. Damit gehören Login-Daten in dieselbe Kategorie wie die IMSI. Die Ausleitung von Login-Daten der Anwendungsebene hätte erstens zur Bedingung, dass die Provider zu einer detaillierten Filterung des Internetverkehrs (Deep Packet Inspection) gezwungen würden, was hohen Investitionsbedarf mit sich brächte, und würde zweitens den Zweck der Fernmeldeüberwachung, nämlich die Inhalte von Kommunikation zu Tage zu fördern, überdehnen. Denn damit würde es den Strafverfolgern auch möglich, leicht etwa Banktransaktionen von Verdächtigen nachzuvollziehen. Abgesehen davon, sind Login-Daten einer Client zu Server Beziehung auf Anwendungsebene verschlüsselt und können durch den Access Provider nicht offengelegt werden. Für solche Aufgaben ist die Fernmeldeüberwachung aber nicht gedacht, geschweige denn fände sie im gegenwärtig geltenden BÜPF eine genügende gesetzliche Grundlage.

Unklar bleibt im Weiteren die Bestimmung in Art. 24a Bst. b Ziff. 4 hinsichtlich des Begriffs der Adressierungselemente: Ist die Bestimmung auf Adressierungselemente der IP-Ebene beschränkt, oder will die Bestimmung etwa auch eine Ausleitung für die Anwendungsebene (http) einführen? Einmal mehr kann nach Auffassung der asut nur die IP-Ebene gemeint sein, nicht aber Adresselemente, die in der IP-Payload enthalten sind.

Art. 24b Überwachungstypen (rückwirkend)

In Art. 24b (betreffend rückwirkende Überwachung) wird ebenfalls ein systematischer Ausbau vorgenommen, sodass diese Datenlieferungspflicht mit der früheren Lieferung von schlichten Verkehrs- und Rechnungsdaten nichts mehr gemein hat.

Es wird auf die bereits bei Art. 24a geäusserte Kritik zur Echtzeitüberwachung von Anmeldungsdaten verwiesen. Sie gilt für die rückwirkende Speicherung der Daten erst recht, weil ausserhalb des Zugriffsbereichs des Endkunden gespeicherte Anmeldedaten ein lohnenswertes Ziel für Hackerangriffe bilden (die Erfahrung gerade der letzten Wochen und Monate zeigt, dass auch Behörden niemals für absolute Sicherheit der von ihnen gespeicherten Daten sorgen können). Eine Pflicht zur Speicherung solcher Daten würde damit Anwendungen wie E-Banking deutlich unsicherer machen, wenn nicht gar das Vertrauen des Publikums in sie zerstören.

Unklar bleibt im Weiteren analog zum bereits zu Art. 24a Gesagten in Art. 24b Bst. a Ziff. 4 der Begriff der Adressierungselemente: Ist die Bestimmung auf Adressierungselemente der IP-Ebene auf Seiten des Endkunden beschränkt, oder will die Bestimmung auch eine rückwirkende Herausgabe für die Anwendungsebene und der vom Endkunden besuchten IP-Adressen oder URLs einführen? Letzteres liefe auf eine Vorratsdatenspeicherung für das Internet hinaus (rückwirkende Herausgabe sämtlicher besuchter Websites etc.), die den Delegationsrahmen von Art. 15 BÜPF klar sprengen würde und als höchst problematischer politischer Entscheid klar in die Hände des Gesetzgebers gehört, und die –

nebenbei gesagt – aus der aktuellen Vorlage für eine Revision des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit BWIS eben erst wieder entfernt wurde. Eine Einführung einer Vorratsdatenspeicherung auf dem Verordnungsweg steht damit nach Auffassung der asut völlig ausser Frage.

Ferner ist der Begriff der periodischen Übermittlung unklar und näher zu umschreiben. Vgl. zu Art. 24 zudem auch den Technischen Annex, S. 19 ff.

Zu Art. 24c

Auch Art. 24c geht klar weiter als eine einfache Nachführung. Die Bestimmung will die FDA zu einer Art „Kopfschaltung" im Internetbereich zwingen. Die Argumente zur Kopfschaltung wurden bereits dargelegt. Auch im Internetbereich kann es nicht angehen, ohne die vom BÜPF geforderte konkrete Verdachtsgrundlage mit einer Kopfschaltung „Fallen" zu stellen, in die die Nutzer dann hereintappen. Vgl. dazu auch den Technischen Annex, S. 22 f.

Zu Art. 25-27

Vgl. zu diesen Artikeln ebenfalls die Anmerkungen im Technischen Annex (S. 23 ff.).

2.4 Definitionen

Die Definition der Internet-Anbieterin in Ziff. 1 des Anhangs der Verordnung, die allein auf die Verwendung von IP-Adressen abstellt (besser wäre ohnehin: das Internet Protocol IP), ist zu weit. Es gibt eine Reihe von Produkten, die mit IP arbeiten, aber keinen Zugang zum Internet vermitteln, denn IP ist eine universelle in Computernetzen verwendete Technologie, deren Einsatz – entgegen ihrer Bezeichnung – nicht auf das Internet beschränkt ist.

Dementsprechend wäre die Definition durch die Einführung eines Elements des Zugangs zum Internet enger zu fassen. Vgl. dazu auch den Technischen Annex, S. 2.

Gemäss Ziff. 8 des Anhangs besteht folgende Definition: Adressierungselemente: Kommunikationsparameter sowie Nummerierungselemente, wie Kennzahlen, Rufnummern und Kurznummern (Art. 3 Bst. f des Fernmeldegesetzes vom 30. April 1997 9 - FMG). Die Target Identity ist beschränkt auf ein Nummerierungselement. „Adressierungselement" in Art. 16b Abs. 2 ist damit zu ersetzen durch „Nummerierungselement".

Gemäss Ziff. 9 des Anhangs wird der Begriff der Kommunikationsparameter definiert als die Elemente zur Identifikation von Personen, Computerprozessen, Maschinen, Geräten oder Fernmeldeanlagen, die an einem fernmeldetechnischen Kommunikationsvorgang beteiligt sind (Art. 3 Bst. g FMG). Gemäss dieser Definition sind SIM-Nummer, IMSI, MSISDN Parameter, die mit dem Kunden assoziiert sind und der Identifikation der Person dienen und damit auch „Parameter zur Teilnehmeridentifikation". Die IMEI ist mit einem Mobiledevice assoziiert und ist ein „Kommunikationsparameter des Endgerätes der Mobiltelefonie". Der Begriff der SIM-Nummer ist zudem auch in ETSI TS 102 657 nicht definiert und damit unklar; in jedem Fall erlauben die durch ETSI definierten Datenformate nicht, eine SIM-Nummer auszuliefern.

Zu Ziff. 14 vgl. sodann den Technischen Annex, S. 32.

2.5 Kosten

Die gleichzeitig mit der VÜPF in Revision befindliche Verordnung über Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs sieht für eine Reihe von Überwachungsarten einen Wechsel von stundenbasierter Aufwandsentschädigung hin zu Entschädigungspauschalen vor. Dies droht zu einer signifikanten Reduktion der Entschädigungen zu führen. Angesichts dessen, dass den FDA nach offiziellen Studien nur gut 30% der Überwachungskosten entschädigt werden, lehnt die asut eine weitere Reduktion strikte ab. Immerhin werden andere Unternehmen, die den Untersuchungsbehörden bei der Polizeiarbeit behilflich sind – etwa private Bewachungsunternehmen – auch nicht nur zu 30% entschädigt.

Wie bereits erwähnt, bilden die Entschädigungen zudem einen wesentlichen Streitpunkt auch in der gegenwärtigen Revision des BÜPF. Als eminent politische Materie sind sie zumindest in den Grundzügen auf dem Weg der Gesetzgebung

festzulegen und nicht durch eine Verordnungsrevision.

Sodann wären auch auf Verordnungsebene klare Kriterien vorzusehen, in welchen Fällen eine pauschalisierte Entschädigung zulässig ist und wann eine Entschädigung nach Aufwand zu bezahlen ist. Keinesfalls kann eine derartige Entscheidung an den ÜPF delegiert werden, wie dies der neue Art. 4a der Gebührenverordnung offenbar will.

Auf die Auswirkungen der Erweiterung des Katalogs der Überwachungsarten auf die Entschädigungen für die FDA wurde bereits vorne unter 1.2 hingewiesen.

In Art. 4a der Gebührenverordnung ist ferner zunächst die Rede von CHF 160.- pro Stunde, dabei sollen die Entschädigungen gemäss Absatz 4 bloss 80% des Zeit- und Sachaufwandes decken. Dies ist widersprüchlich oder zumindest unklar.

ImproWare AG – Es ist Ihre Zukunft!
Zurlindenstrasse 29, CH-4133 Pratteln
Telefon 061/826 93 00 Fax 061/826 93 01 E-Mail info@imp.ch

INIT SEVEN AG
ELIAS CANETTI-STRASSE 7 CH-8050 ZÜRICH
TELEFON: +41 44 315 44 00 FAX: +41 44 315 44 01
E-MAIL: INFO@INIT7.NET INTERNET: WWW.INIT7.NET

Zürich, 25. Juli 2011

Einschreiben
Informatik Service Center ISC-EJPD
Dienst Überwachung Post- und
Fernmeldeverkehr
Bereich Recht und Controlling
Herr Patrick Schöpf
CH-3003 Bern

VÜPF Änderungsvorlage vom 8. Juni 2011 – Stellungsnahme der asut

Sehr geehrter Herr Schöpf

In der Beilage überlasse ich Ihnen unsere Stellungnahme zur VÜPF Änderungsvorlage vom 8. Juno 2011.

Bitte lassen Sie mich wissen falls Sie dazu weitere Informationen oder/und Unterlagen benötigen. Sie erreichen mich unter Tel. +41 44 315 44 00.

Freundliche Grüsse
Init Seven AG

INIT SEVEN AG
Elias Canetti-Strasse 7
CH-8050 Zürich
http://www.init7.net

Emanuel Kleindienst

INIT SEVENAG
ELIAS CANETTI-STRASSE 7 CH-8050 ZÜRICH
TELEFON: +41 44 315 44 00 FAX: +41 44 315 44 01
E-MAIL: INFO@INIT7.NET INTERNET: WWW.INIT7.NET

VÜPF Änderungsvorlage vom 8. Juni 2011: Stellungnahme der asut

Management Summary

Mit Schreiben vom 8. Juni 2011 eröffnete Bundesrätin Simonetta Sommaruga eine Anhörung zur Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF sowie der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs. Mit dem vorliegenden Papier nimmt der schweizerische Verband der Telekommunikation asut zu den vorgeschlagenen Änderungen kritisch Stellung.

Die folgenden Punkte stehen dabei im Zentrum:

1. Entgegen der Darstellung im Begleitbrief würde die vorgeschlagene Revision nicht nur eine Nachführung der bereits bestehenden Praxis darstellen, sondern eine **massive Ausweitung der staatlichen Überwachung** des Bürgers mit sich bringen, insbesondere eine Vorratsdatenspeicherung des Internetverkehrs. Es handelt sich um einen eigentlichen **Etikettenschwindel,** der im geltenden Bundesgesetz über die Überwachung des Post und Fernmeldeverkehrs BÜPF zudem gar **keine genügende gesetzliche Grundlage** findet und kaum auf statistischen Entscheidgrundlagen basiert.
2. Sodann bringt die Vorlage, anders als in den Erläuterungen dargestellt, **keine Verbesserung der Rechtssicherheit.** Entgegen der Regelung in der geltenden VÜPF soll nämlich der Katalog der Überwachungspflichten in der neuen VÜPF nicht mehr abschliessend sein, sondern die Behörden sollen explizit auch die Kompetenz erhalten, ohne Verordnungsgrundlage neue Überwachungspflichten einzuführen. Anders als unter der geltenden Verordnung haben die Telekom-Unternehmen wie auch die Bürger damit genau *keine* Rechtssicherheit mehr; sie werden nicht mehr wissen, mit welchen Überwachungsmassnahmen sie zu rechnen haben.
3. Die Vorlage soll für die Behörden eine **Kostensenkung** bringen, diese würde allerdings genau besehen **ausschliesslich zu Lasten der Telekom-Unternehmen** gehen. Schon heute werden die Kosten der Telekom-Unternehmen für die Kommunikationsüberwachung nur zu einem Drittel vom Staat entschädigt. Die asut kann nicht nachvollziehen, warum dieser Betrag jetzt zu Lasten der Telekom-Unternehmen und ihrer Kunden noch weiter gesenkt werden soll. Mit der Kostensenkung für die Behörden droht den Telekom-Unternehmen zudem eine massive Steigerung der Zahl von Überwachungsaufträgen, für die sie dann wiederum die Mehrheit der Kosten zu tragen hätten.
4. Die Vorlage **ignoriert das Verhältnismässigkeitsprinzip**: Die Telekom-Unternehmen sollen nicht verpflichtet werden können, teure Überwachungsanlagen zu beschaffen, die sie ohnehin nur in sehr unwahrscheinlichen Fällen überhaupt brauchen werden.

Aus diesen Gründen steht die asut der aktuellen Revision der VÜPF ablehnend gegenüber. Vor allem die geplante Ausweitung der Überwachungsmassnahmen darf nur mit einem demokratisch legitimierten Entscheid und damit nur durch Bundesgesetz erfolgen. **Entsprechend ist mit einer Revision der VÜPF bis zur Verabschiedung des BÜPF zuzuwarten.**

Der asut geht es mit ihrer Opposition gegen die Vorlage keineswegs darum, den Sinn der Telekom-Überwachung zum Zweck der Verbrechensbekämpfung in Frage zu stellen. **Die asut und ihre Mitglieder haben vielmehr schon immer konstruktiv mit den Behörden zusammengearbeitet, um die gesetzlich vorgesehenen Überwachungsmassnahmen umzusetzen.** Die asut wehrt sich allerdings gegen die neuesten Reformpläne, weil derart schwerwiegende Eingriffe in die Privatsphäre des Bürgers und in die Wirtschaftsfreiheit und Eigentumsgarantie der Telekom-Unternehmen nicht durch die Hintertür einer Verordnungsrevision eingeführt werden dürfen.

1 Allgemein

1.1 Teilrevision?

Gemäss dem Begleitbrief vom 8. Juni 2011 zur Vorlage, unterzeichnet durch Frau Bundesrätin Simonetta Sommaruga, soll es bei vorliegender Teilrevision der VÜPF lediglich um eine „Nachführung" gehen, welche für alle Beteiligten „die nötige Bestimmtheit und Rechtssicherheit" schaffe. Dies trifft jedoch nicht zu:

- Zunächst wird mit der Vorlage keineswegs nur die bestehende Praxis nachgeführt, sondern es werden auch diverse neue Überwachungsmassnahmen verankert, wie z.B. eine umfassende Überwachung des Internetverkehrs, zudem sollen internationale Kopfschaltungen analog zur Sprachtelefonie neu auch für SMS- und Internetüberwachungen gemacht werden. Bisher wurden als Folge eines Entscheids des Bundesverwaltungsgerichts internationale Kopfschaltungen lediglich hinsichtlich der Gesprächstelefonie eingesetzt.

- Sodann sollen mit der Revision nicht nur zweifelhafte Massnahmen wie die Kopfschaltungen in den Katalog aufgenommen werden, sondern neu auch eine Massnahme, welche unseres Erachtens illegal ist, nämlich die Antennensuchläufe. Bei solchen Massnahmen existieren keine Verdachtsmomente gegen bestimmte Personen oder Anschlüsse, wie dies von StPO und BÜPF eindeutig gefordert würde, sondern es wird ein Gebiet unspezifisch nach strafrechtlich Verwertbarem abgesucht.

- In den Erläuterungen wird zudem dargelegt, die Revision senke die Kosten: Aus Sicht der Überwachungsbehörden mag dies zwar zutreffen. Denn dadurch dass gewisse nicht vorgesehene Massnahmen in der Verordnung neu typisiert würden, gäbe es für deren Umsetzung für die Fernmeldediensteanbieter (FDA) nur noch eine geringe Pauschalentschädigung gemäss Gebührenverordnung und keine Aufwandsentschädigung gemäss bisherigem Art. 4 der Gebührenverordnung mehr. Eine solche „Kostensenkung" erfolgt aber auf dem Buckel der FDA und entspricht, zumindest nach offizieller Lesart, nicht die Meinung der Revision.

- Weiter ist der verwendete Begriff „Teilrevision" irreführend. Gemäss den Erläuterungen handelt es sich offenbar nur dann um eine Totalrevision der VÜPF, wenn sie im Nachgang einer BÜPF-Revision geschieht. Vom materiellen Gehalt her haben wir es aber bereits vorliegend mit einer Totalrevision der VÜPF zu tun, welche Entscheidungen vorwegnehmen soll, welche eigentlich in den Rahmen der BÜPF-Revision gehören.

1.2 Kein Plus an Rechtssicherheit

Die Vorlage bringt kein Plus an Rechtssicherheit, wie dies in Begleitbrief und Erläuterungen behauptet wird.

Die neueste Praxis des Bundesverwaltungsgerichts vom 21. resp. 23. Juni 2011 bestätigte die Auffassung zweier Mitglieder der asut, dass der Katalog der in der VÜPF geregelten Überwachungsarten abschliessend sei. Art. 17 Abs. 5 und Art. 25 Abs. 5 des Revisionsentwurfs widersprechen diesem Anspruch an die Rechtssicherheit im Sinne der Vorhersehbarkeit, indem sie explizit eine Kompetenz des Dienstes zur Überwachung des Post- und Fernmeldeverkehrs ÜPF zur Einführung weiterer Überwachungsmassnahmen vorsehen.

Aber selbst dann, wenn man der Auffassung ist, der Katalog sei entgegen der Auffassung des Bundesverwaltungsgerichts nicht abschliessend, bringt eine offene Formulierung des Katalogs nichts, da Fernmeldedienstanbieter und Bürger jederzeit damit rechnen müssen, dass entweder die Praxis den Katalog nicht als abschliessend betrachtet oder dass bei Bedarf einfach der Katalog wieder beliebig erweitert wird.

Dass die FDA überdies kein Rechtsmittel besitzen, um sich gegen solche von Gesetz und Verordnung nicht gedeckten Überwachungsmassnahmen zu wehren und ihre verfassungsmässigen Rechte zu wahren, hat die asut bereits in der Vernehmlassung zum VE-BÜPF heftig kritisiert. Sie sieht darin einen wesentlichen konzeptionellen

INIT SEVEN AG
ELIAS CANETTI-STRASSE 7 CH-8050 ZÜRICH
TELEFON: +41 44 315 44 00 FAX: +41 44 315 44 01
E-MAIL: INFO@INIT7.NET INTERNET: WWW.INIT7.NET

Mangel des BÜPF, der weder durch den VE-BÜPF, geschweige denn durch die nun geplante Verordnungsrevision behoben wird.

Die Erklärung, dass den rechtsstaatlichen Mängeln des BÜPF mit einer VÜPF-Revision nicht beizukommen ist, findet sich im Prinzip in den Erläuterungen zur Vorlage selbst, S. 1 unten:

Nach Ansicht der anordnenden Strafverfolgungsbehörden und der die Überwachungsmassnahmen genehmigenden Zwangsmassnahmengerichte ist die Liste der Überwachungsmassnahmen in der VÜPF nicht abschliessend zu betrachten. Der Dienst und die FDA sind nach dieser Auffassung daher auch verpflichtet, angeordnete und genehmigte Überwachungsmassnahmen durchzuführen, die nicht explizit in der VÜPF aufgeführt sind. Diese Situation führt zu einer grossen Rechtsunsicherheit und dazu, dass sowohl auf Seiten des Dienstes als auch auf Seiten der FDA bei der Durchführung von nicht explizit in der VÜPF aufgeführten Überwachungsmassnahmen erhebliche Kosten entstehen.

Die Problematik, dass aufgrund fehlender Rechtsbehelfe der Provider theoretisch alles durchgeführt werden muss, was Zwangsmassnahmengerichte, welche über kein genügendes technisches Verständnis verfügen, genehmigen, lässt sich mit einer Erweiterung des Massnahmenkatalogs sicher nicht beseitigen, solange dieser derart offen formuliert bleibt.

Damit würde nur erreicht, dass damit insgesamt den FDA die Entschädigungen gekürzt würden, weil die Aufwandsentschädigung gemäss bisherigem Art. 4 der Gebührenverordnung durch pauschal festgelegte Teilentschädigungen ersetzt würde. Weiter würde der neue Art. 1 Abs. 2 bis bewirken, dass pro überwachte Rufnummer unter einem Auftrag sämtliche möglichen Erhebungen verlangt werden könnten und dies nur unter Entschädigung der Basisleistung. Die FDA lehnen dies selbstverständlich ab. Es ist in den Erläuterungen nirgends die Rede davon, dass eine Kürzung der Entschädigungen für die FDA die Absicht wäre. In finanzieller Hinsicht ist in den Erläuterungen auf S. 2 vielmehr die Rede davon, dass es darum gehe, den FDA Investitionssicherheit zu verschaffen.

1.3 Übernahme von bisheriger Rechtssprechung und Praxis:

Oft soll mit Gesetzesrevisionen die in der Zwischenzeit aufgelaufene, „bewährte" Rechtssprechung ins neue Gesetz einfliessen, so auch hier. In diesem Fall ist aber Skepsis angebracht. Einerseits gibt es keine gefestigte Rechtssprechung, sondern nur einige wenige Einzelentscheide, und diese sind meistens nicht hilfreich. Aufgrund der konzeptionellen Fehler im BÜPF, welche zur Folge haben, dass hinsichtlich der Frage, was die Gerichte auf Beschwerde einer FDA hin nun zu prüfen haben, Konfusion herrscht, konnte sich keine Gerichtspraxis entwickeln, welche sich eignen würde, ins Gesetz aufgenommen zu werden.

An dieser Stelle kann nicht auf die Gesamtheit der Unstimmigkeiten und Widersprüchlichkeiten der aufgelaufenen Gerichtsentscheide eingegangen werden, nur soviel: Mit seinen zwei neusten Entscheiden hiess das Bundesverwaltungsgericht zwei Beschwerden von FDA gut, mit der Begründung, die FDA seien in der angefochtenen Verfügung zu Überwachungsmassnahmen verpflichtet worden, welche im Katalog der Überwachungsmassnahmen gemäss VÜPF gar nicht vorhanden sind. Da die Aufzählung der Überwachungsmassnahmen in der VÜPF abschliessend zu verstehen sei, sei eine Verpflichtung der FDA zu Massnahmen ausserhalb des Katalogs nicht zulässig. Gemäss Art. 13 Abs. 1 Bst. a BÜPF darf jedoch der ÜPF eine von Zwangsmassnahmengerichten genehmigte Überwachung nur darauf hin überprüfen, ob die angeordnete Massnahme von einer zuständigen Behörde aus erfolgt ist und ob es um ein Delikt gemäss des Deliktskatalogs des BÜPF geht. Das BVGer hat nun aber darüber hinaus geprüft, ob die angeordneten Massnahmen im Katalog der VÜPF aufgeführt seien. Den FDA ist es zwar durchaus recht, wenn das Bundesverwaltungsgericht in Ausübung einer rechtspolitischen Lückenfüllung über Art. 13. Abs. 1 Bst. a BÜPF hinaus prüft. Es erscheint aber unschlüssig, wenn sich das Gericht einerseits nicht an Art. 13 Abs. 1 Bst. a BÜPF hält und andererseits die von der Beschwerdeführerin angeführten, in diesem Papier auch schon erwähnten, konzeptionellen Fehler des BÜPF in Abrede stellt (A-8267/2010, Erw. 3.2).

Mit dem einzigen höchstrichterlichen Entscheid im Bereich Zulässigkeit von Überwachungsmassnahmen im Fernmeldebereich (BGE 130 II 249ff) wurde überdies eine Überwachungsmassnahme, welche ebenfalls nicht dem VÜPF Katalog angehört (Antennensuchläufe), nicht verhindert. Das Bundesgericht stellte sich dabei auf den Standpunkt, es dürfe die Rechtmässigkeit von Antennensuchläufen gar nicht prüfen. Wenn also in den Erläuterungen behauptet wird, Antennensuchläufe seien von der Gerichtspraxis als zulässig bestätigt worden, so stimmt das schlicht nicht, denn das Bundesgericht hat die Zulässigkeit von Antennensuchläufen gar keiner Prüfung unterzogen. Es wäre daher nicht gerechtfertigt, den Überwachungstypenkatalog der VÜPF unter Hinweis auf die Bundesgerichtspraxis zu ergänzen.

1.4 VÜPF-Revision im jetzigen Zeitpunkt ist abzulehnen

Aus den diversen oben genannten Gründen, ist diese VÜPF-Teilrevision abzulehnen. Wie dargelegt, ist es nicht möglich, mit dieser Vorlage Rechtssicherheit zu schaffen. Es besteht hingegen die Befürchtung, dass mit dieser VÜPF-Revision im etwas kleineren Kreis und ohne die nötige demokratische Legitimation Forderungen durchgedrückt werden sollen, welche in einer Revision des Gesetzes im formellen Sinn keine Chance hätten. Weiter muss die Befürchtung bestehen, dass mit dieser Verordnungsrevision, welche im Prinzip eine Wunschliste des ÜPF enthält, die längst fällige BÜPF-Revision auf die lange Bank geschoben werden soll.

1.5 BÜPF-Revision abwarten

Die meisten relevanten Änderungen in dieser VÜPF-Revisionsvorlage betreffen Punkte, welche gerade in der parallel laufenden BÜPF-Revision umstritten sind:

- Änderungen, welche die Kosten/Entschädigungen betreffen
- Nicht nur Ausleitung des gesamten Fernmeldeverkehrs von bestimmten Breitbandanschlüssen, sondern auch Überwachungspflichten der Zugangsanbieterinnen auf der Dienste-/Anwendungsebene (allfällige Filterungspflichten der FDA)
- Überwachungsmassnahmen gegen einen unbestimmten Personenkreis (z.B. Antennensuchläufe).

Man kann sich daher des Eindrucks nicht erwehren, der Verordnungsgeber wolle nun die Punkte, die im Rahmen der Vernehmlassung zum BÜPF ins Schussfeld der Kritik geraten sind, am Gesetzgeber vorbei in die VÜPF bringen. Damit würde der von Verfassung und Gesetz vorgesehene Stufenbau (Gesetz – Verordnung – Richtlinien) umgangen, was dem Prinzip der Rechtsstaatlichkeit widerspricht. Es geht nicht an, dass die relevanten Entscheidungen auf einer unteren Normenstufe gefällt werden und sich dann später das Gesetz im formellen Sinn danach richten soll.

Dies gilt insbesondere auch deshalb, weil der Verordnungsgeber die ihm durch Art. 15 (insbes. Abs. 6) BÜPF verliehene Rechtsetzungskompetenz in verschiedener Hinsicht eindeutig überschreitet: So regelt das BÜPF beispielsweise an keiner Stelle die Überwachung von Anwendungen wie VoIP, Instant Messaging oder Multimediadienste, die nicht von Fernmeldediensteanbietern oder Internet-Access-Providern, sondern von Internet-Anwendungsanbietern (Service Provider) angeboten werden (vgl. Hansjakob, Kommentar, N 24 zu Art. 1 BÜPF). Auch hatte der historische Gesetzgeber vor elf Jahren keine Vorstellung, welche neuen Dienstleistungen auf dem Internet zur Verfügung stehen würden, und entsprechend ist der Verordnungsgeber erst durch ein formelles Gesetz zu ermächtigen, Überwachungsarten einzuführen, die zum Zeitpunkt des Erlasses des BÜPF nicht vorstellbar waren (etwa Zugänge über VPN oder „Instant Messaging"). Dies gilt erst recht für eine Vorratsdatenspeicherung für WWW-Internetverkehr (http), die bei einer weiten Auslegung der Verordnung ebenfalls möglich wäre, und die einen schwerwiegenden Eingriff in die Privatsphäre von Bürgern beinhaltete. Ein solcher schwerwiegender Eingriff würde zwingend eine Regelung in einem formellen Gesetz voraussetzen (mehr dazu unten bei den Ausführungen zu Art. 24b des Entwurfs).

Hinzu kommt, dass die Verordnung, wie im Folgenden zu zeigen sein wird, auf technischer Ebene mehr Fragen aufwirft, als sie beantwortet. Anstatt die Verordnung an den Informationsbedürfnissen der Strafverfolgung zu

INIT SEVEN AG
ELIAS CANETTI-STRASSE 7 CH-8050 ZÜRICH
TELEFON: +41 44 315 44 00 FAX: +41 44 315 44 01
E-MAIL: INFO@INIT7.NET INTERNET: WWW.INIT7.NET

orientieren, wird zudem versucht, technische Lösungen in einem bestimmten technologischen Umfeld zu beschreiben und eine Reihe von Parametern, oft in unklarem Kontext, aufzulisten (dazu den Technischen Annex dieses Dokuments, S. 1).

Da nach Auffassung der asut vor einer Revision der VÜPF der Abschluss der Revision des BÜPF mit dem normalen Durchlauf des Gesetzgebungsverfahrens nötig wäre, wird auf einen detaillierten Änderungsvorschlag verzichtet. Wegen der unklaren, bzw. inexistenten formell-gesetzlichen Grundlage müsste dieser ohnehin nur Stückwerk bleiben. Die asut hat sich bei der BÜPF-Revision schon bisher sehr kooperativ gezeigt und hat mit konstruktiven Vorschlägen an dieser mitgewirkt. Sie wird dies selbstverständlich auch künftig tun und zu einer erfolgreichen Umsetzung jenes Projekts Hand bieten.

1.6 Fehlende Berücksichtigung des Verhältnismässigkeitsprinzips in der Verordnung

Es wäre zu berücksichtigen, dass bei Anbietern mit geringer Kundenzahl, bei Anbietern mit überwiegendem Anteil an Business-Kunden oder aber bei seltenen Überwachungsarten im Hinblick auf die in diesen Fällen nur kleine Zahl von zu erwartenden Überwachungsvorgängen eine Installation von Überwachungsanlagen unverhältnismässig und nicht zumutbar scheint. Die neuen Richtlinien TR TS müssten in diesem Sinne neben den Handover Interfaces (HI), entsprechende Schnittstellen (in ETSI Terminologie Internal Network Interface, INI) spezifizieren, dass der ÜPF in vergleichbaren Fällen ad hoc Ausrüstung installieren kann. In solchen Fällen dürfen die FDA allenfalls verpflichtet werden, die für die Installation der Ausrüstung nötigen Schnittstellen zur Verfügung zu stellen, nicht aber, die Anlagen als solche „auf Vorrat" zu beschaffen.

Ebenfalls eine klare Verletzung des Verhältnismässigkeitsprinzips liegt in der Anforderung von Art. 18 Abs. 3 vor, eine 24x7-Erreichbarkeit sicherzustellen. Viele kleine Provider beschäftigen nur wenige Angestellte und wären durch eine derartige Anforderung überfordert.

1.7 Fehlende Entscheidgrundlage für eine Ausweitung der Überwachungspflichten

Abschliessend ist darauf hinzuweisen, dass die Ausweitung des Anwendungsbereichs der VÜPF offenbar erfolgt, ohne dass über die Wirksamkeit der bisherigen Überwachungsmassnahmen Statistiken erhoben worden wären. Schon die Wirksamkeit der bisherigen Methoden bleibt vielmehr völlig im Unklaren, und erst recht ist nicht gesichert, ob von der geforderten Ausweitung der Überwachungsarten überhaupt die erwünschte Wirkung zu erwarten sei. Umgekehrt betrachtet bleibt also völlig offen, ob für die mit der Vorlage neu eingeführten schweren Eingriffe in die Privatsphäre der Bürger eine sachliche Grundlage besteht.

Auch dies spricht deutlich für die Forderung der asut, die Verordnungsrevision aufzuschieben, bis einerseits die Revision des zu Grunde liegenden Gesetzes erfolgt ist, und andererseits gestützt auf zuverlässiges Datenmaterial über weitere Überwachungsmassnahmen zu entscheiden wäre.

2 Zu einer Auswahl an einzelnen Bestimmungen

2.1 2. Abschnitt: Bearbeitung von Personendaten (...)

Zu Art. 9 Abs. 2: "Übergabepunkt"

Die Frage der Bestimmung der Übergabepunkte ist nach wie vor ungelöst. Damit ist offen, für welchen Abschnitt die Provider genau verantwortlich gemacht werden sollen. Ausserdem ist unklar, welche Aspekte unter Datensicherheit fallen sollen (Confidentiality, Authentication, Availability (DoS), Integrity, Non-repudiation). Zu beiden Punkten vgl. auch den Technischen Annex, S. 4 f.

2.2 4. Abschnitt: Überwachung der „Telefondienste"

Die Abgrenzung des Fernmeldeverkehrs vom Internetverkehr bleibt unklar. Internet-Technologie (damit ist eine Protokollarchitektur gemeint) kann ausserhalb des Internet eingesetzt werden beispielsweise in einem Carrier Class IP Netz (z.B. für VoIP). Vgl. dazu die Anmerkung im Technischen Annex, S. 8.

Zu Art. 16:

In der bisherigen Verordnung wurde unterschieden zwischen „Überwachung des Fernmeldeverkehr mit Ausnahme von Internet" und „Überwachung der Internetzugänge". Neu heisst es nun im 4. Abschnitt nur noch „Überwachung der *Telefondienste*" und später im 6. Abschnitt „Überwachung des Internets".

Die genaue Terminologie müsste nochmals überprüft werden, wird doch im weiteren Verlauf des 4. Abschnitts nicht mehr von „Telefondiensten", sondern wieder von „Fernmeldeverkehr" gesprochen.

Sodann sollten keine Erhebungen gemacht werden über netzinterne Parameter wie IMSI, reale Cell IDs, usw. Solche Erhebungen sind für die Strafverfolgungsbehörden und die Gerichte nicht beweisrelevant. Die Parameter werden nur netzintern verwendet und dienen der Kundensicherheit sowie zur Sicherstellung der Netzintegrität. Bei einigen solcher Daten, wie z.B. den realen Cell IDs, handelt es sich zudem um geschäftsrelevante Daten, welche die FDA nicht herausgeben können, ohne Geschäftsgeheimnisse zu verletzen.

Im Weiteren ist darauf hinzuweisen, dass viele der für die Erhebung vorgesehenen Parameter genau besehen kaum jene Beweissicherheit bieten, die sich der Verordnungsgeber offenbar vorstellt. Vielfach sind die Parameter nämlich durch die Endkunden einfach änderbar (z.B. die MAC-Adresse), sodass sie, weil sehr schwierig verifizierbar, gar keine zuverlässige Beweisführung erlauben. Entsprechend ist deren Erhebung für die Strafverfolgungsbehörden und Gerichte nicht von Nutzen und damit auch unverhältnismässig. Die Erhebung sehr schwierig verifizierbarer Parameter führt im besten Fall zu Beweislosigkeit, im schlechteren Fall zu nicht gerechtfertigten Anschuldigungen oder gar Festnahmen. Entsprechend ist zu fordern, dass Richtlinien zur Verifizierbarkeit von Parametern bestehen und die diesbezügliche Verantwortung einzelner FDA klar umschrieben wird, basierend auf ETSI TR 187 012 clause 5.2 und Draft ETSI TS 187 017 clause 4.

SIM-Nummern sind sodann keine auf dem Netz verfügbaren Parameter, welche zu den Fernmeldeverkehrsdaten gehören. Die Information der SIM-Nummern gehört zu den Auskünften über Fernmeldeanschlüsse und wird heute schon durch eine Anfrage über das CCIS angefragt und die Auskunft durch die FDA erteilt.

In Art. 16 Bst. d Ziff. 2 ist im Weiteren keine klare Zuteilung der Parameter in Klassen gegeben. Zudem erzeugt die Formulierung „(wie die SIM-Nummer, die IMSI-Nummer und die IMEI-Nummer)" Rechtsunsicherheit, da nicht festgelegt ist, welche weiteren Angaben unter dieser Bestimmung herausverlangt werden könnten.

Zu Art. 16 lit. e: Antennensuchlauf:

Diese Ergänzung darf an dieser Stelle keinesfalls gemacht werden, wenn schon müsste die Durchführbarkeit von Antennensuchläufen im Gesetz im formellen Sinn vorgesehen werden, da diese Massnahme klar gegen die geltende Strafprozessordnung verstösst, wonach Fernmeldeüberwachungen nicht zur Suche nach Verdachtsmomenten gegen unbestimmt viele Personen durchgeführt werden dürfen, sondern nur im Falle eines bereits vorliegenden Verdachts und nur betreffend bereits im Voraus klar bestimmter Anschlüsse (dazu schon vorne 1.3).

Darüber hinaus lässt sich sagen, dass es gar nicht möglich ist „an einem bestimmten Standort" rückwirkend „alle mobilen Kommunikationsvorgänge" zu eruieren. Es liesse sich höchstens eine grössere oder kleinere Zahl an Funkzellen ermitteln, welche „einen bestimmten Standort" mit einer gewissen Wahrscheinlichkeit versorgen, und anschliessend die Kommunikationen über diese Funkzellen in einem definierten Zeitraum ermitteln. Ob sich aber die gesuchte Kommunikation darunter befindet, ist nicht gewährleistet.

INIT SEVEN AG
ELIAS CANETTI-STRASSE 7 CH-8050 ZÜRICH
TELEFON: +41 44 315 44 00 FAX: +41 44 315 44 01
E-MAIL: INFO@INIT7.NET INTERNET: WWW.INIT7.NET

Zu Art. 16 und 16a vgl. zudem die Anmerkungen im Technischen Annex, S. 9f.

Zu Art. 16b Überwachungsmassnahmen mit Auslandsbezug

Mit der Einfügung dieser Norm sollen die sog. internationalen „Kopfschaltungen" verankert werden, das heisst, die FDA sollen dazu verpflichtet werden, ausländische Rufnummern, respektive schweizerische Rufnummern im Ausland (outbound Roamer) überwachen zu können, wenn diese mit ihren Kunden kommunizieren. Diese Bestimmung ist abzulehnen, obschon das Bundesverwaltungsgericht vor rund zwei Jahren entschieden hat, eine solche Massnahme sei rechtmässig. Das Bundesverwaltungsgericht (A-2335/2008) stellte sich auf den Standpunkt, dies sei im Prinzip das Gleiche wie die Überwachung einer inländischen Nummer, jedenfalls sei ja die überwachte Nummer klar bestimmt. Allerdings übersah das Bundesverwaltungsgericht die Tatsache, dass es sich

- entweder um eine Überwachung einer Person im Ausland handelt, welche nach Abschluss des Verfahrens nicht, wie von der Gesetzgebung vorgesehen, über die Vornahme der Überwachung informiert werden kann, und die darüber hinaus gegen das Territorialitätsprinzip verstösst,
- im Prinzip auch um eine Überwachung von unbestimmt vielen Personen im Inland handelt, welche Kommunikationen mit der genannten Nummer im Ausland haben. Auch die Kopfschaltung widerspricht damit dem Grundkonzept des BÜPF, wonach Fernmeldeüberwachungen nicht zur Suche nach Verdachtsmomenten gegen unbestimmt viele Personen durchgeführt werden dürfen (Rasterfahndung), sondern nur im Falle eines bereits vorliegenden Verdachts und nur betreffend bereits im Voraus klar bestimmter Anschlüsse. Auch hier ist zudem offensichtlich, dass die unbestimmte Anzahl an Personen im Inland nach Abschluss des Verfahrens nicht über die Überwachung informiert werden kann.

Entgegen der Ansicht des Bundesverwaltungsgerichts gibt es also doch starke Anzeichen dafür, dass Kopfschaltungen nicht ins Konzept des aktuellen BÜPF passen, weshalb auch die Entscheidung über die Zulässigkeit von Kopfschaltungen dem Gesetz im formellen Sinn anheimgestellt werden sollte und nicht im Rahmen einer Revision der VÜPF erfolgen darf.

Zu Art. 16b vgl. zudem die Anmerkungen im Technischen Annex, S. 11 f.

Zu Art. 17 Abs. 4

Es ist unklar was alles mit „Zuleitung" gemeint ist. ETSI spezifiziert die Auslieferungsformate an einem Übergabeinterface (Handover Interface, HI), spezifiziert jedoch die Ausleitungsnetze (Delivery Networks) aus der Infrastruktur des Providers (IIF/MD) zur Infrastruktur von ÜPF (LEMF) nur oberflächlich. Wenn „die Spezifikationen dieser Zuleitung" bedeuten würde, dass ÜPF Delivery Networks spezifiziert, würde dies einen erheblichen Eingriff in die Netzhoheit der Provider bedeuten.

Zu Art. 17 Abs. 5 und Art. 25 Abs. 5

Obschon der Verordnungsgeber (wie auch das Bundesverwaltungsgericht) davon ausgehen will, dass der Überwachungstypenkatalog der VÜPF abschliessend sei, soll diese Bestimmung nun vorsehen, dass auch nicht explizit in der Verordnung aufgeführte Fälle von Überwachungen möglich seien. Damit wird der Katalog der Überwachungstypen offengehalten, und es besteht keine Rechtssicherheit, was vom ÜPF an Überwachungen zu erwarten ist. Dies betrifft die Betreiber im Rahmen der in diesem Zusammenhang zu erwartenden Investitionen und den Normalbürger insofern, als er nicht weiss, wie er vom Staat überwacht werden kann. Gemäss Legalitätsprinzip müsste wenigstens ein Rahmen an zulässigen Überwachungen im Gesetz im formellen Sinn definiert werden. Was darüber hinaus geht, sollen die FDA nicht nur nicht ausführen müssen, sondern im Hinblick auf den Schutz der Freiheitsrechte der Bürger auch nicht ausführen *dürfen*. Daher ist diese Spezialfallregelung

abzulehnen, jedenfalls solange, als nicht mit einer zufriedenstellenden BÜPF-Revision eine Grundlage geschaffen wird, welche den Rahmen der Behördenpraxis klar vorgibt.

Zu Art. 17 vgl. zudem die Anmerkungen im Technischen Annex, S. 12 f.

Zu Art. 18

Auf die Unverhältnismässigkeit der Anforderung von Art. 18 Abs. 3 (permanente Erreichbarkeit) wurde bereits unter Ziff. 1.6 hingewiesen.

Die Änderungen, v.a. in den Absätzen 7 und 8, betreffen Spezialwünsche des ÜPF. Eine Gratisnutzung der Fernmeldedienste der FDA durch den ÜPF ist abzulehnen, zumal eine solche Nutzung in keiner Weise eingegrenzt wäre.

Auch die begehrten Unterstützungsleistungen hinsichtlich der Frage, ob tatsächlich die richtige Person überwacht werde, sind fragwürdig, da diese Begehren des ÜPF daher rühren, dass er in letzter Zeit bewährte Überwachungsmethoden durch billigere und unzuverlässige Methoden ersetzt hat. Abs. 8 lässt zudem völlig offen, welche technischen und organisatorischen Vorkehrungen ein Provider treffen muss, um die entsprechende Unterstützung leisten zu können.

Vgl. auch zu Art. 18 die weiter gehenden Anmerkungen im Technischen Annex, S. 13 f.

Zu Art. 19a der *bestehenden* Verordnung

Art. 19a der bestehenden VÜPF bleibt nach dem Entwurf unverändert. Die Norm bestimmt, dass die FDA sicherstellen müssen, dass beim Verkauf von Prepaid-SIM-Karten die Personalien der Kundinnen und Kunden anhand eines *für den Grenzübertritt in die Schweiz zulässigen Reisedokumentes* erfasst werden. Nach Auffassung der asut wäre hier jedoch eine Änderung vorzunehmen.

Nimmt man die geltende Bestimmung beim Wort, können Asylbewerber mit Asylbewerberausweis (Ausländerausweis F, N und S) keine Prepaid-Karten beziehen, weil dieser Ausweis nicht zum Grenzübertritt berechtigt (vgl. Hansjakob, Kommentar, N 3 zu Art. 19a VÜPF). Nach Auffassung der asut ist das Kriterium der Eignung zum Grenzübertritt jedoch unsachlich, ist doch nur die Eignung zur Identifikation, nicht aber die Möglichkeit zum Grenzübertritt für den Zweck von Art. 19a VÜPF relevant.

Das Migrationsamt schiebt für das Verbot der Verwendung von F-, N- und S-Ausweisen sodann die Begründung nach (http://www.uvek.admin.ch/themen/kommunikation/00950/00951/index.html?lang=de, Frage 16), dass die entsprechenden Ausweise oftmals auf falsche Namen ausgestellt würden, weil sie nur auf den Angaben der Asylbewerber basieren und nicht auf amtlichen Dokumenten von deren Heimatland. Aus Sicht der asut ist es jedoch unverhältnismässig, die Verwendung von Ausweisen F, N und S bloss aufgrund eines möglichen Fehlverhaltens einzelner Ausweisträger zu beschränken. Abgesehen davon wäre die Identifikationseignung eines F-, N- oder S-Ausweises selbst dann nicht in Frage gestellt, wenn der Ausweis auf falschen Angaben des Asylbewerbers basierte, ist doch der Asylbewerber auch unter dem entsprechenden (falschen) Namen registerlich erfasst, sodass er gerade auch anhand des falschen Namens zweifelsfrei ausfindig gemacht werden könnte.

Diese Situation ist immer noch besser als jene, dass Asylbewerber für die Nutzung von Mobiltelefonie gezwungen wären, einen Strohmann vorzuschicken, denn in diesem Fall wäre die Identifikation gar nicht mehr gewährleistet.

Träger der Ausweise F, N und S haben zudem in der Regel nicht die Möglichkeit, die für Postpaid-Angebote von Ausländern aus Sicherheitsgründen geforderten Depotzahlungen zu leisten. Ein Verbot, Prepaid-Karten zu beziehen, läuft damit auf eine unverhältnismässige Verletzung Kommunikationsfreiheit der entsprechenden Individuen hinaus. Entsprechend wäre bei einer Verordnungsrevision der in Art. 19a verwendete Ausweisbegriff um Ausweise F, N und S zu erweitern.

INIT SEVEN AG
ELIAS CANETTI-STRASSE 7 CH-8050 ZÜRICH
TELEFON: +41 44 315 44 00 FAX: +41 44 315 44 01
E-MAIL: INFO@INIT7.NET INTERNET: WWW.INIT7.NET

2.3 6. Abschnitt: Überwachung des Internets

Zunächst bleibt unklar, wofür der Ausdruck „Internet" verwendet (dazu die Anmerkungen im Technischen Annex, S. 16 f.) wird.

Zu Art. 23

Der Inhalt der Norm ist bezüglich Inhalt und Beschreibungstiefe mit Art.15 Abs. 1 abzugleichen (vgl. den Technischen Annex, S. 17).

Erneut ist darauf hinzuweisen, dass eine Datenherausgabe betreffend sämtlicher Netzparameter (Bst. g), welche nicht überwachungsrelevant sind und welche reine Netzdaten der betreffenden FDA bilden, nicht akzeptabel ist (dazu vorne 2.2)

Zu Art. 24

Art. 24 sieht eine massive Ausdehnung des Katalogs der Überwachungsarten vor. Die asut ist der Auffassung, dass eine derartige Ausdehnung keine genügende Rechtsgrundlage in Art. 15 BÜPF findet, zumal die meisten der entsprechenden Überwachungsarten zum Zeitpunkt der Verabschiedung von Art. 15 BÜPF noch nicht im Fokus des Gesetzgebers waren. Dementsprechend ist die geplante Ausweitung des Katalogs der Überwachungsarten durch die Delegationsnorm in Art. 15 Abs. 6 BÜPF nicht gedeckt. Die asut ist der Auffassung, eine Erweiterung des Katalogs der Überwachungsarten sei ausschliesslich auf Grund eines Gesetzes im formellen Sinn zulässig.

Eine Überwachung von VPN (Art. 24 Bst. f) wäre in jedem Fall explizit auf Anbieter zu beschränken, die VPN selber anbieten, und nicht auf die Access Provider, die VPN-Datenströme bloss von ihren Endkunden zu VPN-Anbietern im Internet weiterleiten. Dies bereits daher, weil VPN-Daten verschlüsselt und damit für eine Ausleitung ungeeignet sind.

Art. 24 Abs. 2 sieht zudem neu auch Überwachungen auf der Anwendungsebene des Internets vor (für VoIP, Instant Messaging, Multimediadienste, etc.). Die bisherige Praxis wie auch die Literatur gehen klar davon aus, dass das BÜPF auf Access Provider anwendbar ist, nicht aber auf Service Provider (Anwendungsanbieter; vgl. Hansjakob, Kommentar, N 24 zu Art. 1 BÜPF). Auch diese Norm sprengt den durch Art. 15 BÜPF vorgesehenen Rahmen daher klar, selbst die Definition der Internetanbieter nach Ziff. 1 des Anhangs der Verordnung umfasst derartige Anwendungsanbieter nicht.

Die Belastung von Anwendungsanbietern führte im internationalen Vergleich zu einer erheblichen Wettbewerbsverzerrung und vor allem zu einer Beeinträchtigung der Innovation im Bereich der Internetanwendungen, weil die Entwickler mit (im Vergleich zu den allgemein niedrigen Entwicklungskosten für die Anwendungen) ganz erhebliche Mehrkosten für die Entwicklung von Überwachungsschnittstellen einplanen müssten. Die Innovation von Anwendungen des Internets, gerade auch im Mobilfunk (Smartphones), geht heute sehr rasch voran, und entsprechend profitiert die Gesellschaft vom Internet als einem wahren Motor des Fortschritts. Diese Dynamik soll nicht durch eine übertriebene Überwachungspflicht gehemmt werden.

Im Weiteren lässt der Entwurf – und hier liegt ein weiterer schwerwiegender Kritikpunkt – völlig offen, wer für die Überwachung von Anwendungen wie VoIP, Instant Messaging oder Multimediadienste verantwortlich wäre. Angesichts dessen, dass die Access Provider bisher keinerlei technische Möglichkeiten zur Filterung von Inhalten (Deep Packet Inspection) haben, und angesichts dessen, dass eine solche Filterung in der Regel Know-How über Kommunikationsprotokolle höherer Schichten als jener des Access und allfällige Verschlüsselungsmechanismen voraussetzt, das nur der Anbieter der Anwendung selber besitzt, scheint die Vorstellung, dass die Access Provider für eine Ausleitung von aus dem Datenstrom eines Kunden ausgefilterter Anwendungsdaten verantwortlich sein sollen, nicht haltbar. Wollte man Anwendungen doch in die VÜPF aufnehmen, so müsste daher zumindest klargestellt werden, dass für die Ausleitung entweder die Anwendungsanbieter oder dann der ÜPF, nicht aber die Access Provider verantwortlich sein können. Der ÜPF muss auch dann die Filterung übernehmen, wenn die

Anwendungsanbieter vom Ausland aus tätig sind und dementsprechend nicht selber dem BÜPF unterstehen (dazu Hansjakob, Kommentar, N 26 zu Art. 1 BÜPF). Technisch gesprochen darf die Überwachungspflicht der Access Provider daher nur die IP-Adresselemente, aber nicht in der IP-Payload gespeicherte Adresselemente enthalten.

Vgl. zu Art. 24 auch den Technischen Annex, S. 18 f.

Zu Art. 24a Überwachungstypen (Echtzeit)

Die Artikel 24a und 24b enthalten einen umfassenden, schwerwiegenden Ausbau an Datenlieferungspflichten, welcher für die FDA einschneidende Folgen hätte. Gemäss BÜPF/StPO ist an sich nur vorgesehen, dass die FDA den gesamten Fernmeldeverkehr von bestimmten Anschlüssen zuleiten müssen.

Die Bestimmung enthält (wie Art. 24b auch) einige Anforderungen, wonach für die Überwachung und Beweisführung im Strafverfahren überhaupt nicht relevante Daten herauszugeben wären, was teils sogar die Netzintegrität der FDA tangieren würde (wie IMSI, reale Cell ID, usw.)

Unklar bleibt ferner der Inhalt von Art. 24a Bst. b Ziff. 3, der von „Anmeldungsdaten" spricht. Die Norm wäre dahin zu präzisieren, dass, falls überhaupt, ausschliesslich Login-Daten für die Anmeldung im Netz des Access Providers, nicht aber Login-Daten für die Anwendungsebene des Internet (http, etwa für E-Banking, E-Mail-Accounts etc.) unverschlüsselt ausgeleitet werden. Login-Daten (Username plus Password) sind Credentials (Berechtigungsnachweise) und von ihrer Eigenschaft her nicht geeignet, eine Straftat zu begehen. Jede Dritte Entität, die über die Credentials einer Entität verfügt, kann in ihrem Namen, d.h. mit ihren Identitäten kommunizieren. Damit gehören Login-Daten in dieselbe Kategorie wie die IMSI. Die Ausleitung von Login-Daten der Anwendungsebene hätte erstens zur Bedingung, dass die Provider zu einer detaillierten Filterung des Internetverkehrs (Deep Packet Inspection) gezwungen würden, was hohen Investitionsbedarf mit sich brächte, und würde zweitens den Zweck der Fernmeldeüberwachung, nämlich die Inhalte von Kommunikation zu Tage zu fördern, überdehnen. Denn damit würde es den Strafverfolgern auch möglich, leicht etwa Banktransaktionen von Verdächtigen nachzuvollziehen. Abgesehen davon, sind Login-Daten einer Client zu Server Beziehung auf Anwendungsebene verschlüsselt und können durch den Access Provider nicht offengelegt werden. Für solche Aufgaben ist die Fernmeldeüberwachung aber nicht gedacht, geschweige denn fände sie im gegenwärtig geltenden BÜPF eine genügende gesetzliche Grundlage.

Unklar bleibt im Weiteren die Bestimmung in Art. 24a Bst. b Ziff. 4 hinsichtlich des Begriffs der Adressierungselemente: Ist die Bestimmung auf Adressierungselemente der IP-Ebene beschränkt, oder will die Bestimmung etwa auch eine Ausleitung für die Anwendungsebene (http) einführen? Einmal mehr kann nach Auffassung der asut nur die IP-Ebene gemeint sein, nicht aber Adresselemente, die in der IP-Payload enthalten sind.

Art. 24b Überwachungstypen (rückwirkend)

In Art. 24b (betreffend rückwirkende Überwachung) wird ebenfalls ein systematischer Ausbau vorgenommen, sodass diese Datenlieferungspflicht mit der früheren Lieferung von schlichten Verkehrs- und Rechnungsdaten nichts mehr gemein hat.

Es wird auf die bereits bei Art. 24a geäusserte Kritik zur Echtzeitüberwachung von Anmeldungsdaten verwiesen. Sie gilt für die rückwirkende Speicherung der Daten erst recht, weil ausserhalb des Zugriffsbereichs des Endkunden gespeicherte Anmeldedaten ein lohnenswertes Ziel für Hackerangriffe bilden (die Erfahrung gerade der letzten Wochen und Monate zeigt, dass auch Behörden niemals für absolute Sicherheit der von ihnen gespeicherten Daten sorgen können). Eine Pflicht zur Speicherung solcher Daten würde damit Anwendungen wie E-Banking deutlich unsicherer machen, wenn nicht gar das Vertrauen des Publikums in sie zerstören.

Unklar bleibt im Weiteren analog zum bereits zu Art. 24a Gesagten in Art. 24b Bst. a Ziff. 4 der Begriff der Adressierungselemente: Ist die Bestimmung auf Adressierungselemente der IP-Ebene auf Seiten des Endkunden

INIT SEVEN AG
ELIAS CANETTI-STRASSE 7 CH-8050 ZÜRICH
TELEFON: +41 44 315 44 00 FAX: +41 44 315 44 01
E-MAIL: INFO@INIT7.NET INTERNET: WWW.INIT7.NET

beschränkt, oder will die Bestimmung auch eine rückwirkende Herausgabe für die Anwendungsebene und der vom Endkunden besuchten IP-Adressen oder URLs einführen? Letzteres liefe auf eine Vorratsdatenspeicherung für das Internet hinaus (rückwirkende Herausgabe sämtlicher besuchter Websites etc.), die den Delegationsrahmen von Art. 15 BÜPF klar sprengen würde und als höchst problematischer politischer Entscheid klar in die Hände des Gesetzgebers gehört, und die – nebenbei gesagt – aus der aktuellen Vorlage für eine Revision des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit BWIS eben erst wieder entfernt wurde. Eine Einführung einer Vorratsdatenspeicherung auf dem Verordnungsweg steht damit nach Auffassung der asut völlig ausser Frage.

Ferner ist der Begriff der periodischen Übermittlung unklar und näher zu umschreiben. Vgl. zu Art. 24 zudem auch den Technischen Annex, S. 19 ff.

Zu Art. 24c

Auch Art. 24c geht klar weiter als eine einfache Nachführung. Die Bestimmung will die FDA zu einer Art „Kopfschaltung" im Internetbereich zwingen. Die Argumente zur Kopfschaltung wurden bereits dargelegt. Auch im Internetbereich kann es nicht angehen, ohne die vom BÜPF geforderte konkrete Verdachtsgrundlage mit einer Kopfschaltung „Fallen" zu stellen, in die die Nutzer dann hereintappen. Vgl. dazu auch den Technischen Annex, S. 22 f.

Zu Art. 25-27

Vgl. zu diesen Artikeln ebenfalls die Anmerkungen im Technischen Annex (S. 23 ff.).

2.4 Definitionen

Die Definition der Internet-Anbieterin in Ziff. 1 des Anhangs der Verordnung, die allein auf die Verwendung von IP-Adressen abstellt (besser wäre ohnehin: das Internet Protocol IP), ist zu weit. Es gibt eine Reihe von Produkten, die mit IP arbeiten, aber keinen Zugang zum Internet vermitteln, denn IP ist eine universelle in Computernetzen verwendete Technologie, deren Einsatz – entgegen ihrer Bezeichnung – nicht auf das Internet beschränkt ist.

Dementsprechend wäre die Definition durch die Einführung eines Elements des Zugangs zum Internet enger zu fassen. Vgl. dazu auch den Technischen Annex, S. 2.

Gemäss Ziff. 8 des Anhangs besteht folgende Definition: Adressierungselemente: Kommunikationsparameter sowie Nummerierungselemente, wie Kennzahlen, Rufnummern und Kurznummern (Art. 3 Bst. f des Fernmeldegesetzes vom 30. April 1997 9 - FMG). Die Target Identity ist beschränkt auf ein Nummerierungselement. „Adressierungselement" in Art. 16b Abs. 2 ist damit zu ersetzen durch „Nummerierungselement".

Gemäss Ziff. 9 des Anhangs wird der Begriff der Kommunikationsparameter definiert als die Elemente zur Identifikation von Personen, Computerprozessen, Maschinen, Geräten oder Fernmeldeanlagen, die an einem fernmeldetechnischen Kommunikationsvorgang beteiligt sind (Art. 3 Bst. g FMG). Gemäss dieser Definition sind SIM-Nummer, IMSI, MSISDN Parameter, die mit dem Kunden assoziiert sind und der Identifikation der Person dienen und damit auch „Parameter zur Teilnehmeridentifikation". Die IMEI ist mit einem Mobiledevice assoziiert und ist ein „Kommunikationsparameter des Endgerätes der Mobiltelefonie". Der Begriff der SIM-Nummer ist zudem auch in ETSI TS 102 657 nicht definiert und damit unklar; in jedem Fall erlauben die durch ETSI definierten Datenformate nicht, eine SIM-Nummer auszuliefern.

Zu Ziff. 14 vgl. sodann den Technischen Annex, S. 32.

2.5 Kosten

Die gleichzeitig mit der VÜPF in Revision befindliche Verordnung über Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs sieht für eine Reihe von Überwachungsarten einen Wechsel von stundenbasierter Aufwandsentschädigung hin zu Entschädigungspauschalen vor. Dies droht zu einer signifikanten Reduktion der Entschädigungen zu führen. Angesichts dessen, dass den FDA nach offiziellen Studien nur gut 30% der Überwachungskosten entschädigt werden, lehnt die asut eine weitere Reduktion strikte ab. Immerhin werden andere Unternehmen, die den Untersuchungsbehörden bei der Polizeiarbeit behilflich sind – etwa private Bewachungsunternehmen – auch nicht nur zu 30% entschädigt.

Wie bereits erwähnt, bilden die Entschädigungen zudem einen wesentlichen Streitpunkt auch in der gegenwärtigen Revision des BÜPF. Als eminent politische Materie sind sie zumindest in den Grundzügen auf dem Weg der Gesetzgebung festzulegen und nicht durch eine Verordnungsrevision.

Sodann wären auch auf Verordnungsebene klare Kriterien vorzusehen, in welchen Fällen eine pauschalisierte Entschädigung zulässig ist und wann eine Entschädigung nach Aufwand zu bezahlen ist. Keinesfalls kann eine derartige Entscheidung an den ÜPF delegiert werden, wie dies der neue Art. 4a der Gebührenverordnung offenbar will.

Auf die Auswirkungen der Erweiterung des Katalogs der Überwachungsarten auf die Entschädigungen für die FDA wurde bereits vorne unter 1.2 hingewiesen.

In Art. 4a der Gebührenverordnung ist ferner zunächst die Rede von CHF 160.- pro Stunde, dabei sollen die Entschädigungen gemäss Absatz 4 bloss 80% des Zeit- und Sachaufwandes decken. Dies ist widersprüchlich oder zumindest unklar.

Init Seven AG

INIT SEVEN AG
Elias Canetti-Strasse 7
CH-8050 Zürich
http://www.init7.net

Ihnen dienen

Zürich, 25.7.2011

NETSTREAM AG
NEUGUTSTRASSE 66
8600 DÜBENDORF

TEL 0848 000 527
FAX 0848 000 528

WWW.NETSTREAM.CH
INFO@NETSTREAM.CH

EINGESCHRIEBEN
Informatik Service Center ISC-EJPD
Dienst Überwachung Post- und Fernmeldeverkehr
Bereich Recht und Controlling
Patrick Schöpf
3003 Bern

Datum	29. Juli 2011
Ihr Kontakt	Alexis Caceda, Chief Executive Officer
Betreff	VÜPF Änderungsvorlage vom 8. Juni 2011: Stellungnahme der Netstream AG

Mit Schreiben vom 8. Juni 2011 eröffnete Bundesrätin Simonetta Sommaruga eine Anhörung zur Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF sowie der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs. Mit dem vorliegenden Papier nimmt die Netstream AG zu den vorgeschlagenen Änderungen kritisch Stellung.

Die folgenden Punkte stehen dabei im Zentrum:

1. Entgegen der Darstellung im **Begleitbrief** würde die vorgeschlagene Revision nicht nur eine Nachführung der bereits bestehenden Praxis darstellen, sondern eine **massive Ausweitung der staatlichen Überwachung** des Bürgers mit sich bringen, insbesondere eine Vorratsdatenspeicherung des Internetverkehrs. Es handelt sich um einen eigentlichen **Etikettenschwindel**, der im geltenden Bundesgesetz über die Überwachung des Post und Fernmeldeverkehrs BÜPF zudem gar **keine genügende gesetzliche Grundlage** findet und kaum auf statistischen Entscheidungsgrundlagen basiert.

2. Sodann bringt die Vorlage, anders als in den Erläuterungen dargestellt, **keine Verbesserung der Rechtssicherheit.** Entgegen der Regelung in der geltenden VÜPF soll nämlich der Katalog der Überwachungspflichten in der neuen VÜPF nicht mehr abschliessend sein, sondern die Behörden sollen explizit auch die Kompetenz erhalten, ohne Verordnungsgrundlage neue Überwachungspflichten einzuführen. Anders als unter der geltenden Verordnung haben die Telekom-Unternehmen wie auch die Bürger damit genau *keine* Rechtssicherheit mehr; sie werden nicht mehr wissen, mit welchen Überwachungsmassnahmen sie zu rechnen haben.

3. Die Vorlage soll für die Behörden eine **Kostensenkung** bringen, diese würde allerdings genau besehen **ausschliesslich zu Lasten der Telekom-Unternehmen** gehen. Schon heute werden die Kosten der Telekom-Unternehmen für die Kommunikationsüberwachung nur zu einem Drittel vom Staat entschädigt. Die Netstream AG kann nicht nachvollziehen, warum dieser Betrag jetzt zu Lasten der Telekom-Unternehmen und ihrer Kunden noch weiter gesenkt werden soll. Mit der Kostensenkung für die Behörden droht den Telekom-Unternehmen zudem eine massive Steigerung der Zahl von Überwachungsaufträgen, für die sie dann wiederum die Mehrheit der Kosten zu tragen hätten.

4. Die Vorlage **ignoriert das Verhältnismässigkeitsprinzip**: Die Telekom-Unternehmen sollen nicht verpflichtet werden können, teure Überwachungsanlagen zu beschaffen, die sie ohnehin nur in sehr wahrscheinlichen Fällen überhaupt brauchen werden.

Aus diesen Gründen steht die Netstream AG der aktuellen Revision der VÜPF ablehnend gegenüber. Vor allem die geplante Ausweitung der Überwachungsmassnahmen darf nur mit einem demokratisch legitimierten Entscheid und damit nur durch Bundesgesetz erfolgen. **Entsprechend ist mit einer Revision der VÜPF bis zur Verabschiedung des BÜPF zuzuwarten.**

Der Netstream AG geht es mit ihrer Opposition gegen die Vorlage keineswegs darum, den Sinn der Telekom-Überwachung zum Zweck der Verbrechensbekämpfung in Frage zu stellen. Die Netstream AG wehrt sich gegen die neuesten Reformpläne, weil derart schwerwiegende Eingriffe in die Privatsphäre des Bürgers und in die Wirtschaftsfreiheit und Eigentumsgarantie der Telekom-Unternehmen nicht durch die Hintertür einer Verordnungsrevision eingeführt werden dürfen.

NETSTREAM AG
NEUGUTSTRASSE 66
8600 DÜBENDORF

TEL 0848 000 527
FAX 0848 000 528

WWW.NETSTREAM.CH
INFO@NETSTREAM.CH

Aus den diversen oben genannten Gründen, ist diese VÜPF-Teilrevision abzulehnen. Wie dargelegt, ist es nicht möglich, mit dieser Vorlage Rechtssicherheit zu schaffen. Es besteht hingegen die Befürchtung, dass mit dieser VÜPF-Revision im etwas kleineren Kreis und ohne die nötige demokratische Legitimation Forderungen durchgedrückt werden sollen, welche in einer Revision des Gesetzes im formellen Sinn keine Chance hätten. Weiter muss die Befürchtung bestehen, dass mit dieser Verordnungsrevision, welche im Prinzip eine Wunschliste des ÜPF enthält, die längst fällige BÜPF-Revision auf die lange Bank geschoben werden soll.

Freundliche Grüsse
Netstream AG

Alexis Caceda
Chief Executive Officer