



Bundesamt für Justiz
 Frau BRin Simonetta Sommaruga
Per Adresse
 Informatik Service Center ISC-EJPD
 Dienst Überwachung Post- und
 Fernmeldeverkehr
 Bereich Recht und Controlling
 Patrick Schöpf
 CH-3003 Bern

Zürich, 27.07.2011

VÜPF Änderungsvorlage vom 8. Juni 2011: Stellungnahme der Open Systems AG (basierend auf der Stellungnahme des 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 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 Kommunikations-

überwachung 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 einer demokratisch legitimierten Entscheidung 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 Fernmeldediensteanbieter 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 Fernmelde-diensteanbietern 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 beinhaltet. 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 Entscheidungsgrundlage 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 Fernmeldeverkehrs 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

Seite 9/15

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 Vorname 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 Auslieferungsnetze (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.

Seite 10/15

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.

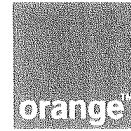
Auch die begehrten Unterstützungsleistungen hinsichtlich der Frage, ob tatsächlich die richtige Person überwacht werde, sind fragwürdig, da diese Begehren des ÜPF daher rühren, dass er in letzter Zeit bewährte Überwachungsmethoden durch billigere und unzuverlässige Methoden ersetzt hat. Abs. 8 lässt 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.



Orange Communications SA
Hardturmstrasse 161
8005 Zürich

Email: amadeus.klein@orange.ch
Phone: +41 78 787 35 65

LSI

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

Zürich, 27. Juli 2011

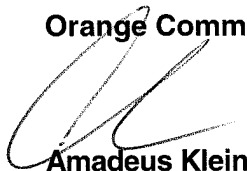
Stellungnahme Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und die dazugehörige Gebührenverordnung

Sehr geehrter Herr Schöpf

Gerne lasse ich Ihnen anbei die Stellungnahme der Orange Communications SA in obgenannter Sache zukommen. Hinsichtlich des technischen Anhangs verweisen wir auf die Stellungnahme des Branchenverbandes asut.

Mit freundlichen Grüßen

Orange Communications SA



Amadeus Klein
Senior Legal Counsel



Markus Hungerbühler
Senior Political Affairs Specialist

VÜPF Änderungsvorlage vom 8. Juni 2011: Stellungnahme Orange Communications SA

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.

Übersicht:

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 eine Anpassung grundlegender Aspekte, die im geltenden Bundesgesetz über die Überwachung des Post und Fernmeldeverkehrs BÜPF 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 **keine Rechtssicherheit** mehr; sie werden nicht mehr wissen, auf welche Überwachungsmassnahmen sie sich vorzubereiten bzw. mit welchen Überwachungsarten 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.
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 Orange 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 Orange geht es mit ihrer Opposition gegen die Vorlage keineswegs darum, den Sinn der Telekom-Überwachung zum Zweck der Verbrechensbekämpfung in Frage zu stellen. Orange hat vielmehr schon immer konstruktiv mit den Behörden zusammengearbeitet, um die gesetzlich vorgesehenen Überwachungsmassnahmen umzusetzen. Orange 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. Dem wird Folgendes entgegengehalten:

- 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 verfügt werden können. Bisher wurden als Folge eines Entscheids des Bundesverwaltungsgerichts internationale Kopfschaltungen lediglich für 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 Kosten 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 insbesondere 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 Fernmeldedienstanbieter, 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.

Eine offene Formulierung des Katalogs, wie jene im Entwurf VÜPF, führt dazu, dass Fernmeldedienstanbieter und Bürger jederzeit damit rechnen müssen, dass bei Bedarf einfach der Katalog 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 Orange bereits in der Vernehmlassung zum VE-BÜPF bereits 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 meistens über kein genügendes technisches Verständnis verfügen, genehmigen, lässt sich mit einer Erweiterung des Massnahmenkatalogs keineswegs beseitigen, solange dieser derart offen formuliert bleibt.

1.3 Übernahme von bisheriger Rechtsprechung und Praxis:

Bei Gesetzesrevisionen soll die in der Zwischenzeit aufgelaufene, gefestigte Rechtsprechung ins neue Gesetz einfließen, so auch hier. Vorliegend ist aber Skepsis angebracht. Einerseits gibt es keine gefestigte Rechtsprechung, sondern nur einige wenige Einzelentscheide, und diese sind nicht hilfreich. Die konzeptionellen Fehler im BÜPF haben zur Folge, dass hinsichtlich der Frage, was die Gerichte auf Beschwerde einer FDA hin nun zu prüfen haben, Konfusion herrscht. Daher 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 FDAs gut, mit der Begründung, die FDAs seien in der angefochtenen Verfügung zu Überwachungsmassnahmen verpflichtet worden, welche im Katalog der Überwachungsmassnahmen gemäss VÜPF gar nicht vorhanden seien. Da die Aufzählung der Überwachungsmassnahmen in der VÜPF abschliessend zu verstehen sei, sei eine Verpflichtung der FDAs 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 BVerwGer hat nun darüber hinaus geprüft, ob die angeordneten Massnahmen im Katalog der VÜPF aufgeführt seien und korrigierend eingegriffen. Den FDAs 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 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 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, damit 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 Fernmeldeverkehrs, sondern auch Überwachungspflichten 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 ermächtigt, 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 beinhaltet. 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 Orange 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. Orange hat sich bei der BÜPF-Revision schon bisher 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 ist. Die neuen Richtlinien TR TS sehen denn in diesem Sinne auch schon vor, dass der ÜPF in vergleichbaren Fällen ad hoc Ausrüstung installiert. 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, eine 24x7-Erreichbarkeit sicherzustellen. Viele kleine Provider beschäftigen nur wenige Angestellte und wären durch eine derartige Anforderung überfordert.

1.7 Fehlende Entscheidungsgrundlage 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, 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 da nochmals überprüft werden, wird doch im weiteren Verlauf des 4. Abschnitts nicht mehr von „Telefondiensten“, sondern doch wieder von „Fernmeldeverkehr“ gesprochen.

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 gar keine zuverlässige Beweisführung erlauben. Entsprechend ist deren Erhebung für die Strafverfolgungsbehörden und Gerichte nicht von Nutzen und damit auch unverhältnismässig. Die Erhebung solcher Parameter führt im besten Fall zu Beweislosigkeit, im schlechteren Fall zu nicht gerechtfertigten Anschuldigungen oder gar Festnahmen. Entsprechend ist zu fordern, dass nur Parameter, die auch klar verifizierbar sind, überhaupt erhoben werden dürfen.

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 erzeugen Formulierung „(wie die SIM-Nummer, die IMSI-Nummer und die IMEI-Nummer)“ Rechtsunsicherheit, da nicht festgelegt ist, welche weiteren Angaben unter dieser Bestimmung heraus verlangt werden könnten.

Zu Art. 16 lit. e: Antennensuchlauf:

Diese Ergänzung darf keinesfalls auf Verordnungsstufe 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 bestimmte 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 überwachen zu können. 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 bestimmte 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 hinausgeht, 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 Orange 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 Orange 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 Orange 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 Strohmännchen 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 Ordnungsrevision 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. Orange 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. Orange 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 (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 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 ausgefilterten 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.

Unklar bleibt ferner der Inhalt von Art. 24a Bst. b Ziff. 3, der von „Anmeldungsdaten“ spricht. Die Norm wäre dahin zu präzisieren, dass ausschliesslich Login-Daten für die Anmeldung im Netz des Access Providers, nicht aber Logindaten für die Anwendungsebene des Internet (http, etwa für E-Banking, E-Mail-Accounts etc.) ausgeleitet werden. Letzteres 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. 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 Orange 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 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 Mobiltelefon 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.

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 Orange 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.

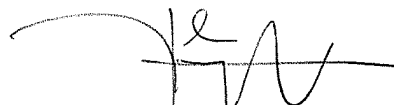
In Art. 4a der Gebührenverordnung ist ferner zunächst die Rede von 160.- Franken pro Stunde, dabei sollen die Entschädigungen gemäss Absatz 4 bloss 80% des Zeit- und Sachaufwandes decken. Dies ist widersprüchlich oder zumindest unklar.

Orange Communications SA



Amadeus Klein

Senior Legal Counsel



Markus Hungerbühler

Senior Political Affairs Specialist

Q-X GmbH, Postfach 61, CH-8308 Illnau

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

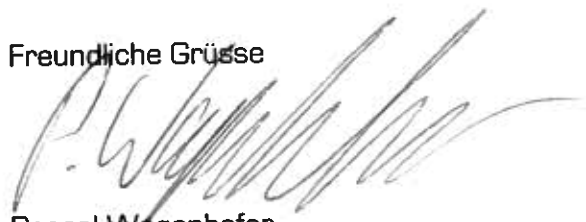
Illnau, 26.07.2011

Stellungnahme der Q-X GmbH bezüglich der VÜPF Änderungsvorlage vom 8. Juni 2011

Sehr geehrte Damen und Herren

Hiermit teilen wir Ihnen mit, dass wir uns dem Schreiben der asut (beigelegt) anschliessen.

Freundliche Grüsse



Pascal Wagenhofer
Head of Technical Services Q-X GmbH



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 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 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 Revisionsrevision eingeführt werden dürfen.

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 Rechtsprechung und Praxis

Oft soll mit Gesetzesrevisionen die in der Zwischenzeit aufgelaufene, „bewährte“ Rechtsprechung ins neue Gesetz einfließen, so auch hier. In diesem Fall ist aber Skepsis angebracht. Einerseits gibt es keine gefestigte Rechtsprechung, 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).

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 Entscheidungsgrundlage 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.

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

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

Einschreiben

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

Zürich, 28. Juli 2011

Sunrise-Stellungnahme zur 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

Sehr geehrter Herr Schöpf

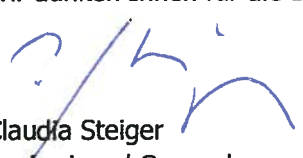
Wir beziehen uns auf die Anhörung zur Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF sowie der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs.

Sunrise war an der Erarbeitung der Stellungnahme der asut, welche sämtliche Interessen von Sunrise abdeckt, massgeblich beteiligt. Wir verzichten deshalb auf die Eingabe einer separaten Stellungnahme und verweisen für die Anliegen von Sunrise auf die Stellungnahme der asut.

Die asut-Stellungnahme setzt sich aus folgenden Dokumenten zusammen:

- Stellungnahme asut VÜPF
- Stellungnahme asut VÜPF – Technischer Anhang

Wir danken Ihnen für die Berücksichtigung der Interessen von Sunrise.


Claudia Steiger
Senior Legal Counsel


Andreas Meier
Senior Regulatory Specialist

Beilage



Schweizerischer Verband der Telekommunikation
Association Suisse des Télécommunications
Swiss Telecommunications Association

asut-Stellungnahme zur 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

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 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 asut kann 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 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 Fernmeldediensteanbieter 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 Ordnungsrevision 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 Rechtsprechung und Praxis:

Oft soll mit Gesetzesrevisionen die in der Zwischenzeit aufgelaufene, „bewährte“ Rechtsprechung ins neue Gesetz einfließen, so auch hier. In diesem Fall ist aber Skepsis angebracht. Einerseits gibt es keine gefestigte Rechtsprechung, 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 höchststrichterlichen 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 beinhaltet. 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 Entscheidungsgrundlage 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.

Leider ist es in der Vorlage nicht gelungen, eine genügende Rechtssicherheit hinsichtlich dem *persönlichen und sachlichen Anwendungsbereich* wie den Rechtsunterworfenen und den Überwachungsmassnahmen bzw. -typen zu erreichen, da gewisse Bestimmungen zu offen formuliert worden sind bzw. die Definitionen nicht hinreichend klar sind.

So hatte bereits VE BÜPF in Art. 1 hinsichtlich des *sachlichen Anwendungsbereiches* den Mangel, dass der Begriff des *Internetverkehrs* - als Teilmenge des Fernmeldeverkehrs - *namentlich* Mail und Internettelefonie - nicht hinreichend klar definiert war und z.B. offen lies, ob weitere auf TCP/IP basierender Dienste wie HTTP, FTP, Telnet etc. resp. Software, welche auf diesen Diensten aufbaut (z.B. Webbrowser, Newsreader, FTP-Client etc.) zum Internetverkehr im Sinne des Gesetzes zählen werden oder nicht.

Genauso unklar ist der Begriff des *Internets* bzw. der Begriff der *Anwendungen* im vorliegenden Entwurf zum VÜPF. Art. 24 Abs. 2 lit a und b E VÜPF nehmen Postdienste und Multimediadienste in einer nicht abgeschlossenen Aufzählung auf. Damit wird auf Verordnungsstufe der sachliche Anwendungsbereich erweitert, was aber einer gesetzlichen Grundlage bedürfte und somit im BÜPF zu regeln wäre. Zudem ist im Rahmen der Rechtssicherheit eine abschliessende Liste zu definieren; *eine Aufzählung mit usw. ist nicht hinreichend für die Legitimation des Eingriffes in Grundrechte*.

Betreffend dem persönlichen Anwendungsbereichs hinsichtlich Internet ist die Begriffsdefinition „*Internet-Anbieterin*“ bei den Begriffen und Abkürzungen relevant. *Aufgrund der derzeitigen Formulierung wären Dienste innerhalb einer Closed-User-Gruppe deshalb nicht erfasst, was vor dem Gesagten auch richtig erscheint*.

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 Ordnungsgeber 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 bestimmte 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 bestimmte 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 billige 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 Strohmännchen 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.

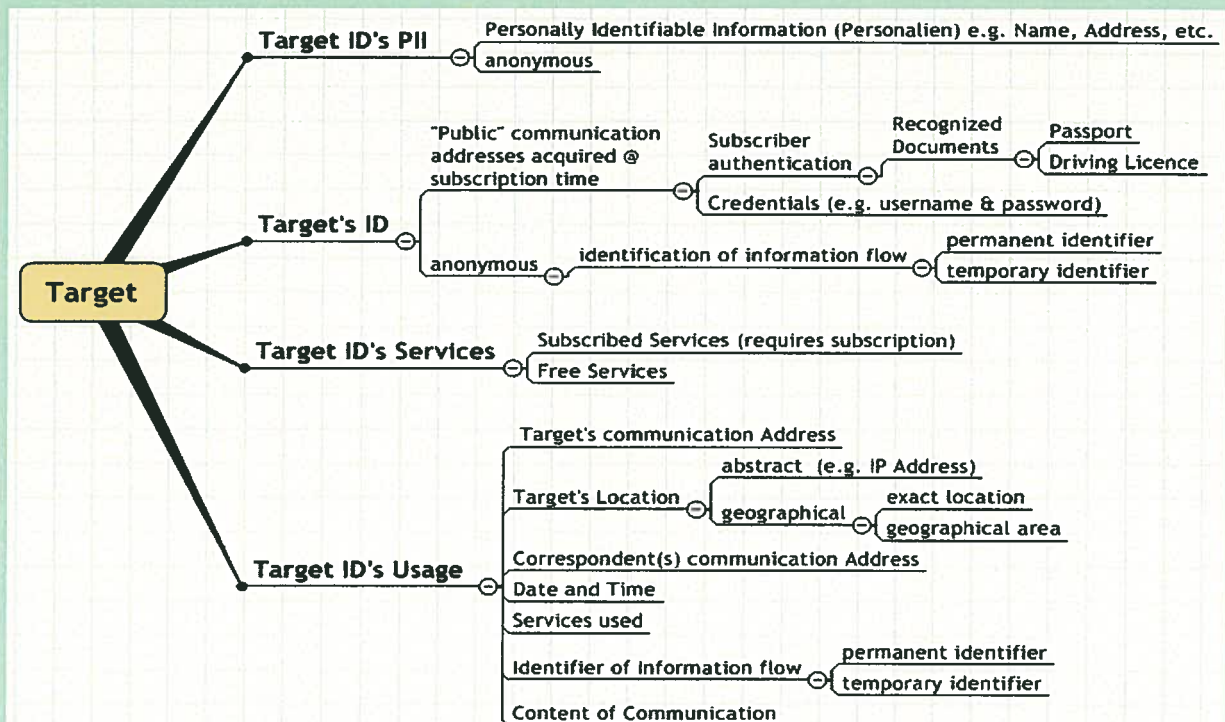
Sodann wären auch auf Verordnungsebene klare Kriterien vorzusehen, in welchen Fällen eine pauschalisierte Entschädigung zulässig ist und wann eine Entschädigung nach Aufwand zu bezahlen ist. Keinesfalls kann eine derartige Entscheidung an den ÜPF delegiert werden, wie dies der neue Art. 4a der Gebührenverordnung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

asut-Stellungnahme zur 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

Technik-asut: Zusammenfassend wird festgestellt, dass VÜPF keine klaren Strukturen hat um darzulegen, was Strafbehörden von Providern wissen wollen, wie dies beispielsweise in der unterstehenden Darstellung ausgedrückt wird (dazu kommen noch die Rechnungsdaten).



Anstatt in der Verordnung an Informationsbedürfnissen der Strafverfolgung zu orientieren, wird versucht, technische Lösungen in einem bestimmten technologischen Umfeld zu beschreiben und eine Reihe von Parametern, oft in unklarem Kontext, aufzulisten. Für die technische Umsetzung sind die Technischen Richtlinien einzusetzen, die durch starke Anlehnung an ETSI den verpflichteten Providern gestatten, Weltmarktprodukte ihrer Lieferanten einzusetzen und damit das Gesetz mit kostengünstigen Lösungen zu erfüllen.

Die VÜPF wurde im Jahr 2001 geschrieben vor den Hintergrund des traditionellen Telefondienstes, ergänzt mit E-mail; durch die punktuellen Anpassungen kann der rasanten Entwicklung der Technologie und der neuen Rollenteilung der verschiedenen Provider nicht Rechnung getragen werden.

vom 31. Oktober 2001 (Stand am 1. September 2007)
Änderung vom ...2011

Der Schweizerische Bundesrat, gestützt auf Artikel 17 des Bundesgesetzes vom 6. Oktober 2000¹ betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), verordnet:

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Geltungsbereich

1 Diese Verordnung regelt die Organisation und das Verfahren zur Überwachung des Post- oder Fernmeldeverkehrs sowie die Erteilung von Auskünften über die Fernmeldeanschlüsse.

2 Sie gilt für:

- a. den Dienst für die Überwachung des Post- und Fernmeldeverkehrs (Dienst);
- b. die anordnenden Behörden;
- c. die Genehmigungsbehörden;
- d. die Anbieterinnen von Postdiensten;
- e. die Anbieterinnen von Fernmeldediensten, einschliesslich die Internet- Anbieterinnen;
- f. die Betreiberinnen von internen Fernmeldenetzen oder Hauszentralen.

Art. 2 Begriffe und Abkürzungen

Die in dieser Verordnung verwendeten Begriffe und Abkürzungen sind im Anhang definiert.

Art. 3 Dienst

1 Der Dienst ist dem Eidgenössischen Justiz- und Polizeidepartement (Departement) administrativ zugewiesen.⁴

2 Er ergreift die notwendigen Massnahmen, um, innerhalb und ausserhalb der Dienstzeit, die Überwachungsanordnungen empfangen und die Prüfung nach Artikel

11 Absatz 1 Buchstabe a und Artikel 13 Absatz 1 Buchstabe a BÜPF durchführen zu können.

Art. 4 Meldung der Namen der zuständigen Behörden

Die Kantone und die zuständigen Bundesämter melden dem Dienst den Namen:

- a. der Behörden, die zur Anordnung einer Überwachung zuständig sind;
- b. der Genehmigungsbehörde;
- c. der Behörden nach Artikel 14 Absatz 2 Buchstaben b und c BÜPF, die Auskünfte über Fernmeldeanschlüsse verlangen können.

Art. 5 Einreichung der Überwachungsanordnung beim Dienst

1 Die anordnende Behörde kann die Überwachungsanordnung beim Dienst einreichen:

- a. per Post, per Telefax oder mit einem anderen durch das Departement zugelassenen sicheren Übertragungsmittel;
- b. mündlich, in dringlichen Fällen.

2 Wenn sie die Überwachung mündlich anordnet, erhält sie die Nutzinformationen, die Verkehrs- und Rechnungsdaten sowie weitere Auskünfte über den Post- oder Fernmeldeverkehr einer Person erst, nachdem sie die Überwachungsanordnung mit einem Übertragungsmittel nach Absatz 1 Buchstabe a bestätigt hat.

3 Die anordnende Behörde reicht ebenfalls jede Abänderung oder jede Verlängerung der Überwachungsanordnung sowie jede gemachte Ergänzung mit einem Übertragungsmittel nach Absatz 1 Buchstabe a beim Dienst ein.

Art. 6 Mitteilung des Entscheids der Genehmigungsbehörde

Die Genehmigungsbehörde teilt dem Dienst ihren Entscheid mit den allfälligen zusätzlichen Vorkehren zum Schutz der Persönlichkeit umgehend, schriftlich mit.

2. Abschnitt: Bearbeitung von Personendaten im Rahmen der Überwachung des Post- oder Fernmeldeverkehrs

Art. 7 Kontrolle der Ausführung der Überwachungsanordnungen

1 Die Behörden, die Überwachungen anordnen oder genehmigen, sowie die Anbieter von Post- oder Fernmeldediensten können diejenigen Personendaten bearbeiten, die sie für die Kontrolle der Ausführung der Überwachungsanordnungen benötigen.

2 Der Dienst führt eine Geschäftskontrolle über:

- a. die Durchführung der Überwachungen von Post- oder

- Fernmeldediensten;
b. die Gebühren und Entschädigungen.

Art. 8 Verarbeitungszentrum

1 Der Dienst errichtet und betreibt ein Verarbeitungszentrum für die Daten aus der Überwachung des Fernmeldeverkehrs- und der Kommunikation im Internet.

Technik-asut: Es ist unklar, wofür Ausdruck Internet verwendet wird, d.h. für:

- a) "The Internet" wobei man behaupten könnte, dass jeder der als "Vernetzer" und/oder "Hoster" auftritt, Mitglied der "Internet Community" ist;
- b) Ein Netz in IP-Technologie, dessen Kommunikation nie in "The Internet" verlaufen muss, aber bei Nomadisierung in "ferne Länder" kann.

SIEHE KOMMENTAR ZU ABSCHNITT 6

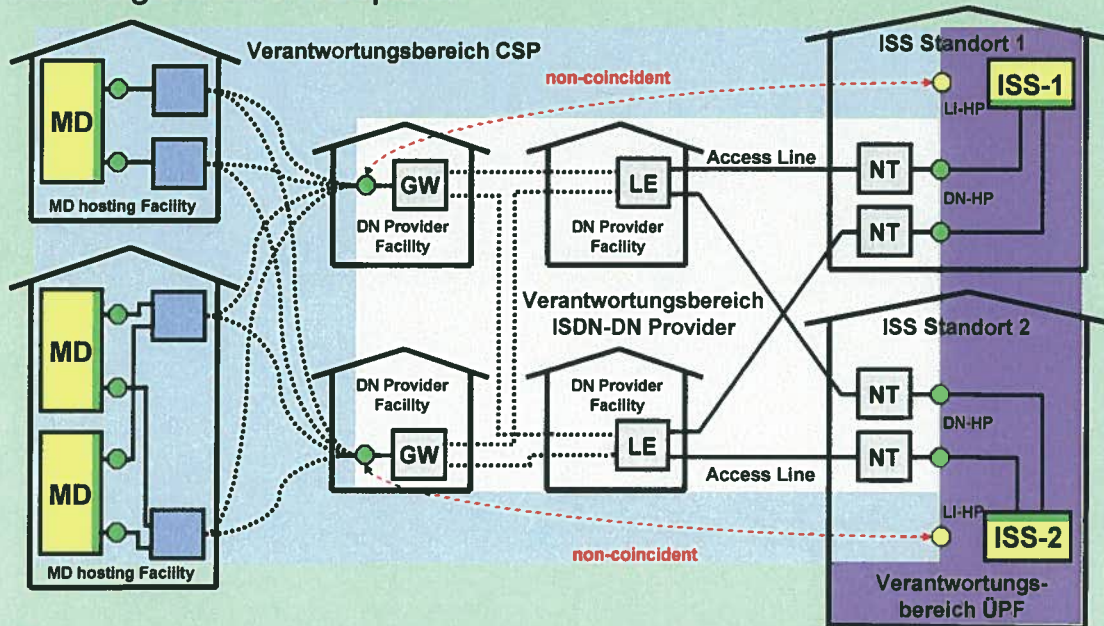
- 2 Das Verarbeitungszentrum muss rund um die Uhr einsatzfähig sein, um:
- a. die durch die Anbieterinnen von Fernmeldediensten gelieferten Daten aus der Überwachung des Fernmeldeverkehrs entgegenzunehmen und in einem Informationssystem aufzuzeichnen;
 - b. die Daten für die betroffene Strafverfolgungsbehörde bereitzustellen.
- 3 Der Dienst macht die Daten der Überwachung der Behörde zugänglich, die als Empfängerin der Überwachungsdaten vorgesehen ist.
- 4 Der Dienst kann dieser Behörde die Daten auch in einer anderen Form übermitteln.

Art. 9 Datensicherheit

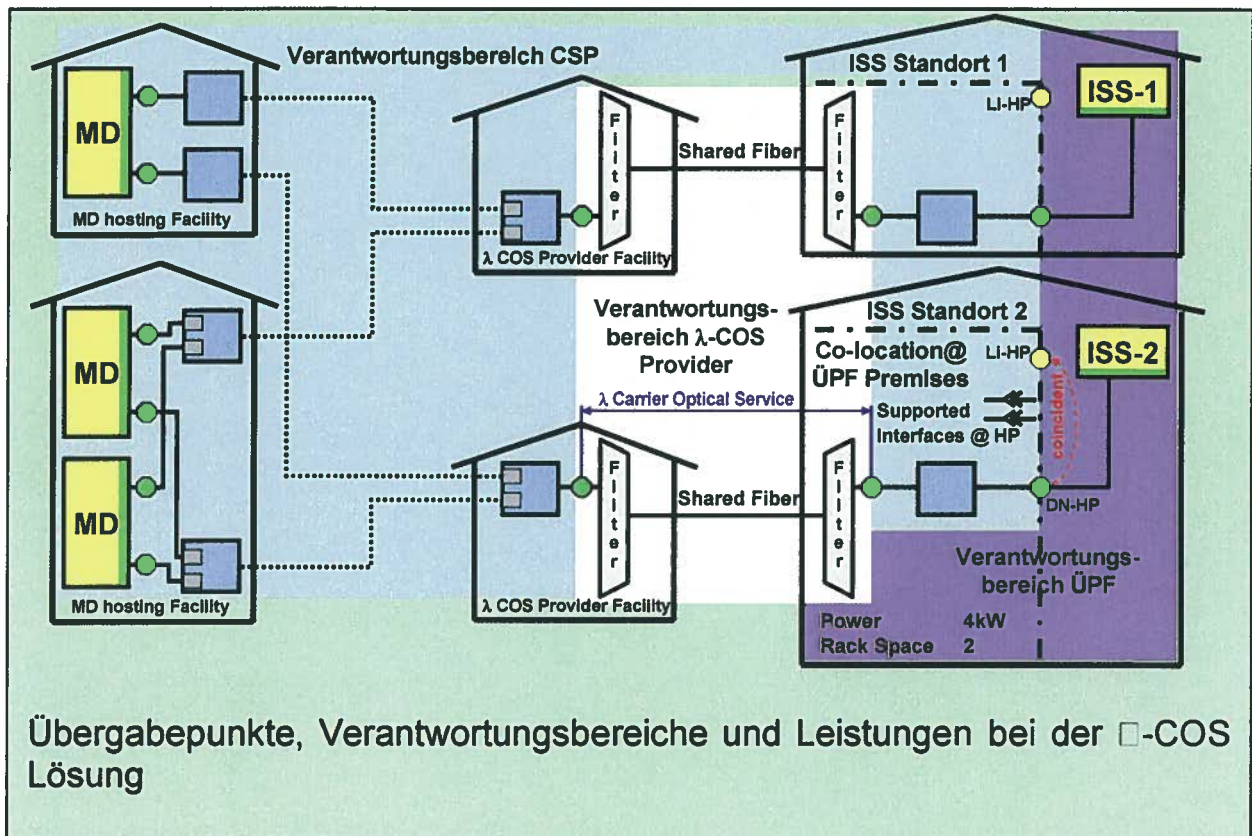
- 1 Für die Gewährleistung der Datensicherheit gelten die Verordnung vom 14. Juni 1993⁵ zum Bundesgesetz über den Datenschutz und die Artikel 14 und 15 der Verordnung vom 23. Februar 2000⁶ über die Informatik und Telekommunikation in der Bundesverwaltung.
- 2 Die Anbieterinnen von Post- oder Fernmeldediensten folgen den Anweisungen des Dienstes für die Datensicherheit bezüglich der Übertragung der Überwachungsdaten. Sie sind für die Datensicherheit bis zum Übergabepunkt der Daten an den Dienst verantwortlich.

Technik-asut: Die Frage der Bestimmung der Übergabepunkte ist nach wie vor ungelöst. Damit ist offen, für welchen Abschnitt Provider verantwortlich gemacht werden sollen. Ausserdem ist unklar, welche Aspekte unter Datensicherheit fallen sollen (Confidentiality, Authentication, Availability (DoS), Integrity, Non-repudiation).

In der Publikation „Ausleitungskonzept zwischen CSP und ISS“ spricht ÜPF von einem physikalischen und logischen Übergabepunkt, ohne eine Definition zu liefern. Anlässlich der Diskussionen des Ausleitungskonzeptes (dieses soll gemäss der Aussage von ÜPF an der Sitzung des erweiterten Kernteams ISS vom 30. Juni 2011 Ende Juli 2011 erscheinen) wurde offensichtlich, dass eine Definition schwierig ist, weil es mehrere Übergabepunkte gibt und diese auf der Netzwerkebene (grün in Beispielfiguren) und der „Datenformat“-Ebene (gelb in Beispielfiguren). Nachfolgend zwei Beispiele:



Übergabepunkte und Verantwortungsbereiche im ISDN Delivery Network



Art. 10 Vernichtung der Daten

1 Der Dienst vernichtet die Überwachungsdaten, nachdem er sie den Behörden nach Artikel 8 Absätze 3 oder 4 übergeben hat, spätestens aber drei Monate nach der Einstellung der Überwachung.

2 Er vernichtet die Daten aus der Geschäftskontrolle ein Jahr nach Einstellung der Überwachung.

3 Der Artikel 962 des Obligationenrechts⁷ und die Gesetzgebung über die Archivierung bleiben vorbehalten.

3. Abschnitt: Überwachung des Postverkehrs

Art. 11 Überwachungsanordnung

Die beim Dienst eingereichte Überwachungsanordnung muss die folgenden Angaben enthalten:

- den Namen der anordnenden Behörde;
- den Namen der Strafverfolgungsbehörde, die als Empfängerin der Überwachungsdaten vorgesehen ist;
- soweit diese Daten bekannt sind: die Namen, Adressen und Berufe der tatverdächtigen Personen und der allenfalls zu

- d. im Fall von Personen, die einem Berufsgeheimnis nach Artikel 271 Absatz 1 der Strafprozessordnung² (StPO) unterstehen: einen Vermerk über diese Besonderheit;
- e. die Straftat, die mit der Überwachung aufgeklärt werden soll;
- f. den Namen der Postdienst-Anbieterin und, wenn möglich, den Namen der mitwirkenden Poststellen;
- g. die angeordneten Überwachungstypen;
- h. wenn nötig, die weiteren Auskünfte über den Postverkehr einer Person und die Anträge auf zusätzliche Vorkehren zum Schutz der Persönlichkeit;
- i. den Beginn und die Dauer der Überwachung.

Art. 12 Überwachungstypen

Folgende Überwachungstypen können angeordnet werden:

- a. das Abfangen der Postsendungen (Echtzeit-Überwachung);
- b. die Lieferung folgender Daten über den Postverkehr (Echtzeit-Überwachung), soweit diese Daten verfügbar sind:
 - 1. die Identität der Empfängerinnen und Empfänger der Postsendungen,
 - 2. die Identität der Absenderinnen und Absender der Postsendungen,
 - 3. die Art der Postsendungen,
 - 4. den Zustellungsstand der Postsendungen;
- c. die Lieferung folgender Verkehrs- und Rechnungsdaten (rückwirkende Überwachung):
 - 1. für Postsendungen mit Zustellnachweis: die Empfängerin oder den Empfänger, die Absenderin oder den Absender und die Art der Postsendung sowie, wenn die Information verfügbar ist, den Zustellungsstand der Postsendung,
 - 2. wenn die Anbieterin von Postdiensten Daten registriert und sie nach Abschluss der von einer Kundin oder eines Kunden verlangten Dienstleistung aufbewahrt: sämtliche verfügbaren Daten;
- d. die weiteren Auskünfte über den Postverkehr einer Person, die in der Überwachungsanordnung festgehalten sind.

Art. 13 Durchführung der Überwachung

¹ Der Dienst bestimmt im Einzelfall, wenn nötig nach Absprache mit der anordnen- den Behörde, die technischen und organisatorischen Massnahmen für die Durchführung der Überwachung.

² Jede Anbieterin von Postdiensten meldet dem Dienst die Ausführung der

angeordneten Massnahmen.

3 Ist eine Anbieterin von Postdiensten infolge betrieblicher Probleme vorübergehend nicht in der Lage, ihre Pflichten bei einer aktiven Überwachung oder zum Vollzug einer neuen Überwachungsanordnung wahrzunehmen, muss sie dies dem Dienst unverzüglich melden.

4 Der Dienst prüft mit der Anbieterin von Postdiensten, ob Begehren über weitere Auskünfte über den Postverkehr einer Person erfüllt werden können und ob die verlangten Verkehrs- und Rechnungsdaten vorhanden sind. Er benachrichtigt die anordnende Behörde über seine Feststellungen und berät sie, wenn nötig, über das weitere Vorgehen.

Art. 14 Pflichten der Anbieterinnen von Postdiensten

1 Jede Anbieterin von Postdiensten muss in der Lage sein, jene Überwachungstypen nach Artikel 12 auszuführen, die durch sie angebotene Dienste betreffen.

2 Jede Anbieterin von Postdiensten muss in der Lage sein, die Überwachungsanordnungen auch ausserhalb der Dienstzeit entgegenzunehmen und sie so rasch wie möglich auszuführen. Sie meldet dem Dienst den Namen der Kontaktpersonen.

4. Abschnitt: Überwachung des Fernmeldeverkehrs mit Ausnahme von Internet

Technik-asut: Die Abgrenzung des Fernmeldeverkehrs vom Internetverkehr ist nach wie vor unklar, Internet Technologie (damit ist eine Protokollarchitektur gemeint) kann ausserhalb des Internet eingesetzt werden beispielsweise in einen Carrier Class IP Netz (z.B. für VoIP). Damit kann derselbe Dienst (funktionell gesehen) angeboten werden ohne jeglichen Informationstransport über das Internet, unter breitem Einsatz des Internet, oder als Mischform. Sollten sich aus einer Deklaration „Fernmeldedienst-Anbieterin“ vs. „Internet-Anbieterin“ unterschiedlich Verpflichtungen ergeben, besteht die Gefahr von ungleichen Behandlungen verschiedener Provider.

Art. 15 Überwachungsanordnung

1 Die beim Dienst eingereichte Überwachungsanordnung muss die folgenden Angaben enthalten:

- a. den Namen der anordnenden Behörde;
- b. den Namen der Strafverfolgungsbehörde, die als Empfängerin der Überwachungsdaten vorgesehen ist;

- c. soweit diese Daten bekannt sind: die Namen, Adressen und Berufe der tat- verdächtigen Personen und der allenfalls zu überwachenden weiteren Personen;
- d. im Fall von Personen, die einem Berufsgeheimnis nach Artikel 271 Absatz 1 der Strafprozessordnung³ (StPO) unterstehen: einen Vermerk über diese Besonderheit;
- e. die Straftat, die mit der Überwachung aufgeklärt werden soll;
- f. wenn möglich, den Namen der Anbieterin von Fernmeldediensten;
- g. die angeordneten Überwachungstypen;
- h. die bekannten Adressierungselemente;
- i. wenn nötig, die Anträge:
 - 1. auf die Bewilligung einer Direktschaltung,
 - 2. auf die allgemeine Genehmigung für die Überwachung von mehreren Anschlüssen ohne Genehmigung im Einzelfall (Artikel 272 Absätze 2 und 3 StPO)⁴, und 3. auf die zusätzlichen Vorkehren zum Schutz der Persönlichkeit;
- j. den Beginn und die Dauer der Überwachung;
- k. die vom Dienst gewünschten Zusatzaufgaben gemäss Artikel 13 Absatz 2 BÜPF.

2 Wenn die Durchführung gewisser Überwachungstypen es erfordert, kann das Departement vorsehen, dass die dem Dienst eingereichte Überwachungsanordnung weitere technische Angaben enthalten soll.

Art. 16 Überwachungstypen (Echtzeit und rückwirkend)

Folgende Überwachungstypen können angeordnet werden:

- a. die Übertragung des Fernmeldeverkehrs (Echtzeit-Überwachung der Nutz-informationen);
- b. bei Mobiltelefonie: die Bestimmung und die periodische Übertragung des Zell-Identifikators (Cell ID), des Standortes und der Hauptstrahlungsrichtung der Antenne , mit der das Endgerät der überwachten Person momentan verbunden ist (Echtzeit-Überwachung);

Technik-asut: Dieser Fall bezieht sich auf einen dauernden Locationupdate, auch wenn weder eine erfolgreiche Kommunikation noch ein erfolgloser Versuch (z.B. Besetzt) zu Stande kommt.

- c. die Bereitstellung und die simultane oder periodische Übertragung folgender Angaben , selbst wenn es nicht zum Aufbau einer Kommunikation kommt, (Echtzeit-Überwachung):
 - 1. die verfügbaren Adressierungselemente (Rufnummern der

- abgehenden und ankommenden Kommunikationsvorgänge),
2. die tatsächliche bekannte Zielrufnummer und die zwischengeschalteten verfügbaren Rufnummern, falls der Anruf um- oder weitergeleitet wurde,
 3. die erzeugten Signale, einschliesslich der Zeichengabe für den Bereitschaftszustand, die Parameter der Fernmeldeanlagen (z. B. SIM-Nummer, IMSI-Nummer, IMEI-Nummer) und die erzeugten Signale für die Aktivierung von Konferenzschaltung oder Anrufumleitung,
 4. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist,
 5. das Datum, die Zeit und die Dauer der Verbindung;

Technik-asut: Bei Echtzeitüberwachung sind die Parameter gemäss 5. durch Time Stamps gegeben.

- d. die Lieferung folgender Daten, wenn es zum Aufbau einer Kommunikation gekommen ist (rückwirkende Überwachung):
 1. die verfügbaren Adressierungselemente (Rufnummern der abgehenden und eingehenden Kommunikationsvorgänge, sofern diese der Fernmeldediensteanbieterin bekannt sind),
 2. die Kommunikationsparameter des Endgerätes der Mobiltelefonie und die Parameter zur Teilnehmeridentifikation (wie die SIM-Nummer, die IMSI-Nummer und die IMEI-Nummer),

Technik-asut: Unter der Anwendung der Terminologie gemäss ETSI TS 102 657 bezieht sich Art. 16 Bst. d. auf „Verkehrsdaten“ (→ Usage), Für Telefonie sind die Parameter definiert in ETSI TS 102 657 Annex B.3, set telephonyServiceUsage.

Da die Abgrenzung Fernmeldedienst zu Internet nicht klar ist, bleibt offen, welche andern Annexes Anwendung finden.

Gemäss „Begriffe und Abkürzungen“ 9. besteht folgende Definition: Kommunikationsparameter: 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 (was ist wirklich damit gemeint; Seriennummer des SIM? In ETSI TS 102 657 ist die SIM-Nummer

nicht definiert), IMSI, MSISDN Parameter, die mit dem Kunden assoziiert sind und der Identifikation der Person dienen und sind „Parameter zur Teilnehmeridentifikation“. Die IMEI ist mit einem Mobiledevice assoziiert und ist ein „Kommunikationsparameter des Endgerätes der Mobiltelefonie“. In 2. ist keine klare Zuteilung der Parameter in Klassen gegeben; IMEI sei als „Kommunikationsparameter des Endgerätes“ und IMSI als „Parameter zur Teilnehmeridentifikation“ auszuweisen. Zudem erzeugen Formulierung „(wie die SIM-Nummer, die IMSI-Nummer und die IMEI-Nummer)“ Rechtsunsicherheit, da nicht festgelegt ist, was auch noch gemeint sein könnte.

In jedem Fall ist aus der Sicht Technik in ETSI TS 102 657 die vollständige Liste der Parameter enthalten, die unter Vorbehalt einer gesetzlichen Grundlage gefordert werden können.

Die Definition des „Kommunikationsparameter“ gemäss FMG hat eine enge Verwandtschaft zu der Definition gemäss ITU-T Recommendation Y.2091:

13.1 identifier: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects). Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties).

3. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist,
4. das Datum, die Zeit und die Dauer der Verbindung
- e. der Antennensuchlauf: zur rückwirkenden Eruierung aller an einem bestimmten Standort angefallenen mobilen Kommunikationsvorgänge während eines bestimmten Zeitraumes, wenn es zum Aufbau einer Kommunikation gekommen ist.

Art.16a Suche und Rettung vermisster Personen

Für die Suche und Rettung vermisster Personen gemäss Artikel 3 BÜPF 5 können nur die folgenden Überwachungstypen angeordnet werden

- a. die Überwachungstypen nach Artikel 16 Buchstaben b, c und d,

- b. soweit möglich die Bestimmung der letzten aktiven Position des mobilen Endgerätes der vermissten Person und die Lieferung aller zur Standortbestimmung notwendigen Angaben, wie:
1. Zell-Identifikator (Cell ID),
 2. Standort,
 3. Hauptstrahlungsrichtung und Frequenzband der Antenne der Mobiltelefonie.

Art. 16b Überwachungsmassnahmen mit Auslandsbezug

1 Ziel der Überwachungsmassnahmen nach Artikel 16 Buchstabe a, Buchstabe c Ziffern 1, 2, 3 und 5 und Buchstabe d Ziffern 1, 2 und 4 kann jedes Adressierungselement sein, unabhängig vom Standort des Endgeräts, von der Landeskennzahl der Rufnummer und von der Netzzugehörigkeit.

2 Ziel der Überwachungsmassnahmen nach Artikel 16 Buchstabe a, Buchstabe b, Buchstabe c Ziffer 4 und Buchstabe d Ziffer 3 und nach Artikel 16a kann auch ein ausländisches Adressierungselement sein, welches sich im Netzwerk einer schweizerischen Fernmeldedienstanbieterin befindet.

Technik-asut: Es muss klargestellt werden, dass bezugnehmend auf Art. 16 Bst. c. nur jene Parameter ermittelbar sind, die den Gateway in Form von Signalisierung passieren, mit einigen Vorbehalten bezüglich der Verifikation derer Richtigkeit. Der Bezug zu Artikeln aus der Überwachung eines Telefondienstes vermittelt den falschen Eindruck, bei einer Kopfschaltung liesse sich derselbe Umfang an Parametern ermitteln. Die Methode Anforderungen gemäss Art. 16 auf die Kopfschaltung zu übertragen ist ungeeignet und schafft Rechtsunsicherheit.

Technik-asut: Betreffend Anwendung von Art. 16 Bst. d. (rückwirkende Überwachung) ist zu berücksichtigen dass vom Target in der Regel, weil nicht Kunde des verpflichteten Providers (Ausnahmen sind outbound Roamer und inbound Roamer) kein Datensatz existieren kann, der mit einer Subscription assoziiert ist. Es ist nicht zumutbar, dass ein Provider eine Art „virtuelle Accounts“ kreiert und die gesamte Kommunikation von Targets mit Auslandsbezug analysiert und durch Korrelation der vielfältigen sogenannten Kommunikationsparameter einem „virtuellen Account“ zuordnen muss; dies würde eine Data Retention im Bereich „Usage“ für alle inbound und outbound Verbindungen bedingen. Auch in diem Fall ist die Methode Anforderungen gemäss Art. 16 auf die Kopfschaltung zu übertragen ungeeignet und schafft Rechtsunsicherheit.

Technik-asut: Gemäss „Begriffe und Abkürzungen“ bestehen folgende Definitionen:

8. 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“ sei zu ersetzen durch „Nummerierungselement“.

Hier besteht ein gewisses Terminologieproblem zu der Definition gemäss ITU-T Recommendation Y.2091:

13.3 address: An address is the identifier for a specific termination point and is used for routing to this termination point.

Gemäss ITU-T ist eine Address ein Identifier, der einem bestimmten Zweck dient, womit Identifier hierarchisch über der Address steht (d.h. ein Identifier kann eine Address sein, muss es jedoch nicht). Die von BAKOM im FMG niedergeschriebene Hierarchie steht zu jener von ITU-T im Widerspruch.

Art. 17 Durchführung der Überwachung

1 Der Dienst bestimmt im Einzelfall, wenn nötig nach Absprache mit der anordnenden Behörde, die technischen und organisatorischen Massnahmen für die Durchführung der Überwachung.

2 Wenn der Dienst feststellt, dass die angeordnete Überwachung den Anschluss von Trägerinnen und Trägern von Berufsgeheimnissen betrifft, ohne dass Vorkehren nach Artikel 271 Absatz 1 der Strafprozessordnung⁶ (StPO) angeordnet worden sind, so zeichnet der Dienst den Fernmeldeverkehr auf und benachrichtigt die Genehmigungsbehörde.

3 Jede Anbieterin von Fernmeldediensten meldet dem Dienst die Ausführung der angeordneten Massnahmen.

4 Sie leitet dem Dienst auf Verlangen die Daten zu. Der Dienst regelt in seinen Richtlinien nach Anhörung der Anbieterinnen die Spezifikationen dieser Zuleitung unter Berücksichtigung der Standards des Europäischen Institutes für Telekommunikationsnormen (ETSI).

Technik-asut: 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.

5 Bei Überwachungsmaßnahmen, die nicht explizit in dieser Verordnung aufgeführt sind, stellt sie dem Dienst jene Schnittstellen zur Verfügung, von denen aus der Fernmeldeverkehr der überwachten Person in Echtzeit und permanent zum Verarbeitungszentrum übertragen werden kann. Der Dienst regelt die Überwachungsmodalitäten im Einzelfall.

Technik-asut: Eine Schnittstelle ist ein Übergabepunkt zwischen Entitäten, im vorliegenden Fall zwischen Ausrüstungen der Provider und solchen von ÜPF. Damit ein Provider solche Schnittstellen zur Verfügung stellen kann, müssen diese in Technischen Richtlinien spezifiziert sein (mit Ausnahme eines passiven Arrangements zur Auskopplung von Daten, wie TAP).

Der Wortlaut „von denen aus der Fernmeldeverkehr der überwachten Person in Echtzeit und permanent zum Verarbeitungszentrum übertragen werden kann“ lässt darauf schliessen, dass ÜPF mit eigenen Ausrüstungen an Standorten der Provider ist.

Eine der Kernfragen in diesem Zusammenhang ist die Definition des Spezialfalles.

In den Erläuterungen Site 2 steht:

Der Dienst und die Fernmeldediensteanbieterinnen 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 Fernmeldediensteanbieterinnen bei der Durchführung von nicht explizit in der VÜPF aufgeführten Überwachungsmaßnahmen erhebliche Kosten entstehen. Die Durchführung von diesen Spezialmassnahmen, z. B. im Bereich der Internetüberwachung, kann Kosten für die Anschaffung von Überwachungstechnologie und Supportleistungen sowie den Beibezug von externen Spezialisten in Höhe von mehreren hunderttausend Franken pro Fall verursachen, welche bisher durch den Dienst getragen werden mussten.

Für die Kosten der Provider ist nicht massgebend, ob eine Massnahme in VÜPF definiert ist, sondern ob eine Technische Richtlinie besteht, die es einem Provider gestattet, jene technischen Vorkehrungen zu treffen, die eine kostengünstige Überwachung erlauben. Die Technische Richtlinien sind auch notwendig, damit ÜPF eigne Ausrüstungen beschaffen kann, um die Daten entgegennehmen zu können.

Damit müssten Technische Richtlinien erarbeitet werden für Massnahmen die im VÜPF nicht vorgesehen sind.

6 Ist infolge technischer oder anderer Pannen eine Anbieterin von

Fernmeldediensten vorübergehend nicht in der Lage, ihre Pflichten bei aktiven Überwachungen oder zum Vollzug neuer Überwachungsanordnungen wahrzunehmen, muss sie dies dem Dienst unverzüglich mitteilen. Die Verkehrsdaten, welche nicht dem Dienst übertragen werden konnten, sind nachzuliefern.

Technik-asut: In der Praxis hat sich gezeigt, dass hier Interpretationsspielraum in der „Schuldfrage“ besteht. Die sogenannte Panne kann verursacht werden durch Probleme im Bereich der Datenaufbereitung ein verpflichteten Provider, im Delivery Network, bei Ausrüstungen der Behörden, die den ausgeleiteten Verkehr nicht entgegennehmen können.
Die Lösung des Problems bedingt die Definition von Übergabepunkten, siehe Kommentar zu Art.9 Abs. 2

7 Die Überwachung ist so durchzuführen, dass weder die überwachte Person noch andere Teilnehmerinnen und Teilnehmer davon Kenntnis erhalten. Sie ist so zu planen, dass eine unbefugte oder unsachgemäße Verwendung der erfassten Informationen verhindert wird.

Art. 18 Pflichten der Anbieterinnen von Fernmeldediensten

1 Jede Anbieterin von Fernmeldediensten muss in der Lage sein, die Überwachungstypen nach Artikel 16 auszuführen, die durch sie angebotene Dienste betreffen.

2 Die Überwachung des Fernmeldeverkehrs ist von der Aufnahme des Kundenbetriebes eines Fernmeldedienstes an sicherzustellen.

3 Jede Anbieterin von Fernmeldediensten muss sicherstellen, dass sie die Überwachungsanordnungen ausserhalb der Dienstzeit entgegennehmen und sie so rasch wie möglich ausführen kann. Sie meldet dem Dienst schriftlich die Kontaktangaben der verantwortlichen Personen.⁴ Sie muss eine durch den Dienst im Verhältnis der Zahl ihrer Teilnehmerinnen und Teilnehmer festgelegte Anzahl Anschlüsse gleichzeitig überwachen können.

5 Sie hat zu gewährleisten, dass innerhalb des durch die Überwachungsanordnung bestimmten Zeitraumes die Überwachung des gesamten über ihre eigene Infrastruktur geführten Fernmeldeverkehrs ermöglicht wird:

- a. wenn er über den überwachten Anschluss abgewickelt wird;
- b. wenn er zu technischen Speichereinrichtungen unter Kontrolle der eigenen Infrastruktur geleitet wird; oder
- c. wenn er aus solchen abgerufen wird.

6 Der Dienst kann die Anbieterinnen von Fernmeldediensten zur Zusammenarbeit verpflichten, um die Überwachung des Fernmeldeverkehrs zu vollziehen, der zwischen verschiedenen Netzen übermittelt wird oder von verschiedenen Anbieterinnen verarbeitet wird.

7 Zur Überprüfung der Überwachungsbereitschaft haben die Anbieterinnen von Fernmeldediensten dem Dienst die Benutzung ihrer Fernmeldedienste unentgeltlich zu gewähren.

Technik-asut: Hier geht es um das sogenannte „permanent Testing Environment“, in dem permanent Testtargets angelegt auf Abbos der Behörden eingerichtet sind. Es ist nicht klar, wessen „Überwachungsbereitschaft“ überprüft werden soll; dies hat einen Einfluss auf den Umfang „permanent Testing Environment“. Es ist auch nicht klar, welche Testmethode eingesetzt werden soll (periodisch vs. bei Unregelmässigkeiten) ; dies hat einen Einfluss auf den Verkehr, den die Provider gratis abzuwickeln haben, gegebenenfalls ins Ausland.

8 Wenn nötig, unterstützen die Anbieterinnen von Fernmeldediensten den Dienst, um sicherzustellen, dass die übermittelten Überwachungsdaten tatsächlich mit dem Fernmeldeverkehr der überwachten Personen übereinstimmen .

Technik-asut: Dies könnte bedeuten, dass die Provider zwecks späterer Verifikation Kopien von abgelieferten Daten erstellen müsste. Es ist unklar, welche technischen und organisatorischen Vorkehrungen ein Provider treffen muss, um diese Unterstützung zu leisten.

5. Abschnitt: Auskünfte über Fernmeldeanschlüsse mit Ausnahme von Internet

Art. 19 System zur Vermittlung der Auskunftsgesuche über die Fernmeldeanschlüsse

1 Der Dienst erstellt und führt in Zusammenarbeit mit den Anbieterinnen von Fernmeldediensten ein System, das die Auskunftsgesuche über die Fernmeldeanschlüsse vermittelt und folgende Auskünfte gibt (Vermittlungssystem):

- a. die Adressierungselemente der Anschlüsse einer bestimmten Person;
- b. soweit verfügbar, die Identität der Personen, deren Anschlüsse mit bestimmten Adressierungselementen übereinstimmen.

Technik-asut: Hier handelt es sich um Daten, die durch das Call Center Information System (CCIS) erhoben werden. Dies entspricht in der Data Retention gemäss ETSI TS 102 657 den Formaten in Annex A.3.3 GenericSubscriberInfo sowie Annexes B.3,, C.3, D.1, E3 <service>Subscriber .

2 Das Vermittlungssystem sucht den Namen der Anbieterin von Fernmeldediensten und die Angaben nach Artikel 14 Absatz 1 BÜPF:

- a. durch den automatisierten Abruf des Verzeichnisses der Fernmeldeanschlüsse der Anbieterin von Fernmeldediensten; oder
- b. durch die Weiterleitung des Auskunftsgesuches an die Anbieterin von Fernmeldediensten.

3 Die Anbieterinnen von Fernmeldediensten müssen die Auskunftsgesuche innert der Frist beantworten, die das Departement für die betreffende Dringlichkeitsstufe festlegt.

4 Die Anbieterinnen von Fernmeldediensten müssen die Informationen nach Absatz 1 laufend nachführen. Nach Ausschalten eines Anschlusses müssen die diesbezüglichen Daten noch während sechs Monaten zur Auskunftserteilung zur Verfügung stehen.

5 Die Anbieterinnen von Fernmeldediensten übernehmen die Kosten der Infrastruktur, die sie für die Behandlung der Auskunftsgesuche brauchen; der Dienst über- nimmt die Installations- und Betriebskosten für das Vermittlungssystem.

Art. 19a⁸ Erfassung von Personendaten beim Verkauf von Prepaid-SIM-Karten

Die Anbieterinnen von Fernmeldediensten müssen sicherstellen, dass beim Verkauf von Prepaid-SIM-Karten die Personalien der Kundinnen und Kunden (Name, Vorname, Adresse, Geburtsdatum) anhand eines gültigen Reisepasses, einer Identitätskarte oder eines anderen für den Grenzübertritt in die Schweiz zulässigen Reisedokumentes erfasst werden. Ausserdem sind die Art des Ausweises und die Ausweisnummer zu erfassen.

Art. 20 Benützung des Vermittlungssystems

1 Jede in Artikel 14 Absatz 2 BÜPF erwähnte Behörde bezeichnet die Personen, die für die Benutzung des Vermittlungssystems vorgesehen sind.

2 Der Dienst erteilt die Zugriffsbewilligungen an diese Personen, wenn eine genügende Benutzungsfrequenz zu erwarten ist:

- a. zur Bestimmung der zu überwachenden Anschlüsse und Personen;
- b. für die Erfüllung von Polizeiaufgaben;
- c. zur Erledigung von Verwaltungsstrafsachen.

Art. 21 Protokollierung

- 1 Der Dienst protokolliert die Zugriffe auf das Vermittlungssystem.
- 2 Er bewahrt die Protokolle während eines Jahres auf. Die Protokolle werden so ausgestaltet, dass die abgefragten Daten festgestellt werden können. Er vernichtet sie nach Ablauf der Aufbewahrungsfrist.
- 3 Die Anbieterinnen von Fernmeldediensten dürfen die Auskunftsgesuche anonymisiert protokollieren.

Art. 22 Auskunftserteilung durch den Dienst

- 1 Die in Artikel 14 Absatz 2 BÜPF erwähnten Behörden können vom Dienst Auskunft über die Fernmeldeanschlüsse verlangen. Sie reichen ihre Auskunftsbegehren per Post, per Telefax oder mit einem anderen durch das Departement zugelassenen sicheren Übertragungsmittel ein.
- 2 Der Dienst bewahrt die Auskunftsgesuche und die erteilten Antworten während eines Jahres auf. Er vernichtet diese Daten nach Ablauf der Aufbewahrungsfrist.

6. Abschnitt: Überwachung des Internets

Technik-asut: Es ist unklar, wofür Ausdruck Internet verwendet wird, d.h. für:

- a) "The Internet" wobei man behaupten könnte, dass jeder der als "Vernetzer" und/oder Application Service Povider und/oder "Hoster" auftritt, Mitglied der "Internet Community" ist;
- b) Ein Netz in IP-Technologie, dessen Kommunikation nie in "The Internet" verlaufen muss, aber bei Nomadisierung in "ferne Länder" in "The Internet" verlaufen kann.

Mit dem Titel "Überwachung des Internet" will offenbar ÜPF "jedermann" verpflichten der IP-Technologie einsetzt, unabhängig davon, ob eine Kommunikation im "eigenen" Netz bleibt oder in "The Internet" verläuft, respektive ob er nur „Application Service Provider“ und/oder „Hoster“ ist. "The Internet" selbst ist eine „unfassbare Wolke“ die zu überwachen schwierig ist; deshalb ist der Ausdruck "Überwachung des Internet"

ungeeignet, eine bestimmte Absicht auszudrücken.

Die Definition im Anhang „Begriffe und Abkürzungen“

1. Internet-Anbieterin: Fernmeldedienstanbieterin oder der Teil einer Fernmeldedienstanbieterin, die der Öffentlichkeit fernmeldetechnische Übertragungen von Informationen auf der Basis der IP-Technologien (Netzprotokoll im Internet [Internet Protocol]) unter Verwendung von IP-Adressen anbietet;

zeigt eher auf b).

Rahmen des Internet werden folgende Dienstleistungen erbracht:

- i) Zugang zu Internet
- ii) Application Services wie E-mail
- iii) Hosting von Applikationen für Dritte

Art. 23 Überwachungsanordnung

Technik-asut: Der Inhalt ist bezüglich Inhalt und Beschreibungstiefe mit Art.15 Abs. 1 abzugleichen.

Die beim Dienst eingereichte Überwachungsanordnung muss die folgenden Angaben enthalten:

- a. den Namen der anordnenden Behörde;
- b. den Namen der Strafverfolgungsbehörde, die als Empfängerin der Überwachungsdaten vorgesehen ist;
- c. soweit diese Daten bekannt sind: die Namen, Adressen und Berufe der tatverdächtigen Personen und der allenfalls zu überwachenden weiteren Personen;
- d. im Fall von Personen, die einem Berufsgeheimnis nach Artikel 271 Absatz 1 der Strafprozessordnung⁷ (StPO) unterstehen: einen Vermerk über diese Besonderheit;
- e. die Straftat, die mit der Überwachung aufgeklärt werden soll;
- f. den Namen der Internet-Anbieterin, wenn sie bekannt ist;
- g. die angeordneten Überwachungstypen, einschliesslich :
 1. der bekannten Adressierungselemente (E-Mail-, elektronische Postfach-, Rechner- und IP-Adresse, Benutzername, MAC-Adresse, E.164-Nummer, SIP URI, IMSI-Nummer, IMEI-Nummer usw.),

Technik-asut: In Art. 15, Abs. 1, Bst. h. steht: „ die bekannten Adressierungselemente;“ ohne Liste.

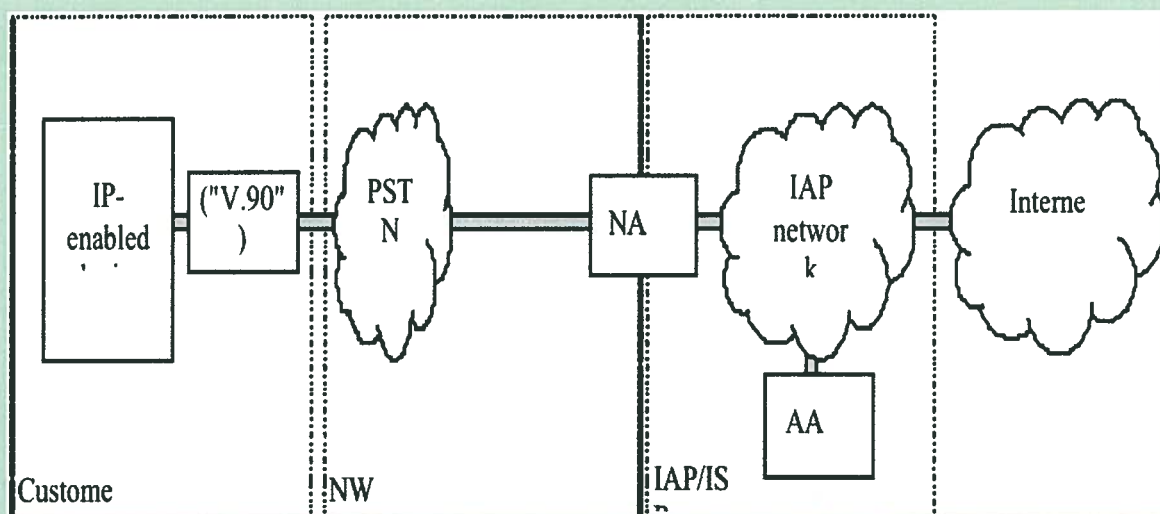
2. der bekannten Anmeldungsdaten (Log-in),
3. der Bewilligung einer Direktschaltung,
4. der Anträge von zusätzlichen Vorkehren zum Schutz nicht beteiligter Benutzerinnen und Benutzer;
- h. den Beginn und das Ende der Überwachung;
- i. die vom Dienst gewünschten Zusatzaufgaben gemäss Artikel 13 Absatz 2 BÜPF.

Art. 24 Überwachbare Internetzugänge und Anwendungen

¹ Folgende Internetzugänge können überwacht werden:

- a. Zugang über eine Telefonverbindung;

Technik-asut: Ein Zugang über eine Telefonverbindung ist ein Arrangement gemäss ETSI TS 102 232-3 § 5.1.1 Dial-up access, siehe Figur 2/TS 102 232-3



Der Accessprovider ist eigentlich der Provider des Network Access Servers (NAS), d.h. der Internet Access Provider (IAP), der auch AAA implementiert, und nicht der Provider des PSTN/ISDN. Für den PSTN/ISDN Provider handelt es sich um eine „normale“ Verbindung, die im Rahmen der „Anwendungsüberwachung“ ausgelenkt wird, allerdings zusammen mit der Kommunikation zwischen Personen. Eine Filterung ist in diesem Fall Angelegenheit der Behörden.

Es ist zu berücksichtigen, dass anstelle des PSTN/ISDN auch ein GSM oder ein VoIP Netz eingesetzt werden könnte d.h. jedes Netz, das ein

Modem mit einem Network Access Server (NAS) verbinden kann.

a. sollte geändert werden von „Zugang über eine Telefonverbindung“ auf „Zugang durch eine Wählverbindung zu einem Network Access Server“

Massgebend ist die funktionelle Architektur wie in Figur 2/TS 102 232-3 dargestellt und weniger die Technologie des Netzes für den Zugang zum NAS

- b. Breitbandzugang (xDSL, Kabelmodem usw.);
- c. Zugang über ein Mobilfunknetz (GSM, GPRS, UMTS, LTE usw.);

Technik-asut: Massgebend ist die angewendete Mobile Packet Data Technologie wie GPRS und weniger „ein Mobilfunknetz“. Mobile Circuit Switched (CS) ist durch a. abgedeckt.

c. sollte geändert werden von „Zugang über ein Mobilfunknetz (GSM, GPRS, UMTS, LTE usw.)“ auf „Zugang mittels Mobile Packet Data Technologie“

- d. kabelloser Zugang (Wi-Fi, Wimax, WLL usw.);
- e. andere Zugänge zum Netz via OSI-Schicht 2 (z.B. Ethernet über FTTH-Zugang);
- f. andere Zugänge zum Netz via OSI-Schicht 3 (z.B. VPN-Zugang).

Technik-asut: Eine Zugangsüberwachung sei beschränkt auf eine Analyse der Inhalte und deren Auslenkung bis zur höchsten Protokollschicht in der Access Architektur und enthält keine Pflicht zur Filterung und selektiven Ausleitung der Protokolle über dem „Access Layer“.

Es sei folgende Ergänzung „Bei diese Überwachung besteht keine Pflicht einer Filterung und selektiver Ausleitung von Informationsflüssen die durch Elemente über der höchsten Protokollschicht in der Access Architektur identifiziert werden.“

2 Folgende Anwendungen können überwacht werden:

- a. synchrone und asynchrone elektronische Postdienste (Instant Messaging, E-Mail usw.);
- b. Multimediadienste (VoIP, Audio- und Videoübertragungen usw.).

Art. 24a Überwachungstypen (Echtzeit)

Als Echtzeitüberwachung können folgende Überwachungstypen angeordnet werden:

- a. die Übermittlung sämtlicher Daten, die über den überwachten Zugang gesendet oder empfangen werden;

Technik-asut: Mit „sämtlichen“ Daten sind wohl Content of Communication (CC, HI3) und Intercept Related Information (IRI, HI2) im Sinne des ETSI gemeint.

- b. die Bereitstellung und die simultane oder periodische Übermittlung der folgenden Auskünfte über den Internetzugang:

Technik-asut: Der Ausdruck „Auskünfte“ hat gegeben durch BÜPF verschiedene Bedeutungen, jedoch in keinem Fall im Zusammenhang mit einer Echtzeitüberwachung:
 BÜPF Art. 5 „Auskünfte über den Post- und Fernmeldeverkehr“
 BÜPF Art. 14 „Auskünfte über Fernmeldeanschlüsse“
 Der Ausdruck „Auskünfte“ sei zu ersetzen durch „Angaben“ (in Art 24 Bst. d. wird auch der Ausdruck „Angaben“ verwendet),

1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wird,

Technik-asut: Bei Echtzeitüberwachung sind die Parameter gemäss 1. durch Time Stamps gegeben.

2. die Art der Datenverbindung oder des Anschlusses,
3. die verwendeten Anmeldungsdaten (Log-in),
4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation,
5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (MAC-Adresse, IMEI-Nummer, IMSI-Nummer usw.),

Technik-asut: Es muss eine klare Zuordnung der Parameter in Klassen „Kommunikationsparameter des Endgerätes“ → IMEI und „Parameter zur Teilnehmeridentifikation“ → IMSI geben. Siehe auch Kommentar zu Art. 16 Bst. d.

6. bei Zugang über ein Mobilfunknetz: die Bestimmung und die periodische Übertragung des Zell-Identifikators (Cell ID), des

Standortes und der Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person momentan verbunden ist,

7. die technischen Änderungen, die während der Verbindung stattfinden, und ihre Ursachen, falls bekannt;

Technik-asut: Gemäss den Erläuterungen handelt es sich bei 7. um folgende Situationen: „Diese Ziffer erwähnt die Informationen, die während einer Kommunikationsverbindung verlangt werden können. In diesem Fall hat die Strafverfolgungsbehörde die Möglichkeit, einen technischen Bericht betreffend alle Änderungen zu verlangen, die die überwachte Person oder die Fernmeldedienstanbieterin veranlasst hat. Es handelt sich etwa um Abonnementsänderungen oder um Änderungen am Netzwerk.

7. scheint Bezug zu nehmen auf Änderungen, die ein Kunde über ein Portal an seiner Subscription oder seinen Einstellungen im Netz (irreführend als „Änderungen am Netzwerk“ bezeichnet) vornimmt. Es ist jedoch nicht realistisch anzunehmen, dass eine gleichwertige Änderung durch einen Agenten des Providers (diese Aktion läuft über Managementkanäle) im Rahmen einer Echtzeitüberwachung eines Zuganges erfasst werden kann.

- c. die Übermittlung der Nutzinformationen, die über die überwachte Anwendung gesendet oder empfangen werden ;
- d. die Bereitstellung und die simultane oder periodische Übermittlung folgender Angaben über die überwachte Anwendung :
 1. das Datum und die Uhrzeit der Kommunikation (Beginn und Ende),

Technik-asut: Bei Echtzeitüberwachung sind die Parameter gemäss 1. durch Time Stamps gegeben.

2. die verfügbaren Adressierungselemente, insbesondere diejenigen des Ursprungs und des Ziels der Kommunikation ,
3. die verwendeten Anmeldungsdaten (Log-in),
4. bei der Überwachung von E-Mail-Verkehr: die Umschlaginformationen gemäss SMTP-Protokoll,
5. die anderen verfügbaren Kommunikationsparameter,
6. die technischen Änderungen während der Kommunikation und ihre Ursachen, falls bekannt.

Technik-asut: Gemäss den Erläuterungen handelt es sich bei 6. um folgende Situationen: „Diese Ziffer erwähnt die Informationen, die während einer Kommunikation über einen Internetservice verlangt werden können. In diesem Fall hat die Strafverfolgungsbehörde die Möglichkeit, einen technischen Bericht betreffend alle Änderungen zu verlangen, die die überwachte Person oder die Fernmeldediensteanbieterin veranlasst hat. Es handelt sich etwa um Abonnementständerungen oder um Änderungen am Log-in.

6. scheint Bezug zu nehmen auf Änderungen, die ein Kunde über ein Portal an seiner Subscription oder seinen Securityeinstellungen vornimmt. Es ist jedoch nicht realistisch anzunehmen, dass eine gleichwertige Änderung durch einen Agenten des Providers (diese Aktion läuft über Managementkanäle) im Rahmen einer Echtzeitüberwachung eines Anwendung erfasst werden kann.

Art. 24b Überwachungstypen (rückwirkend)

Als rückwirkende Überwachung können folgende Überwachungstypen angeordnet werden:

- a. die Übermittlung der folgenden Angaben über den überwachten Zugang:
 1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wurde,
 2. die Art der Datenverbindung oder des Anschlusses,
 3. die verwendeten Anmeldungsdaten (Log-in),
 4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation,
 5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (MAC-Adresse, IMEI-Nummer, IMSI-Nummer usw.),

Technik-asut: Es muss eine klare Zuordnung der Parameter in Klassen „Kommunikationsparameter des Endgerätes“ → IMEI und „Parameter zur Teilnehmeridentifikation“ → IMSI geben. Siehe auch Kommentar zu Art. 16 Bst. d.

6. bei Zugang über ein Mobilfunknetz: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist,

- b. die Übermittlung der folgenden Angaben bei Versand oder Empfang von Meldungen durch einen asynchronen elektronischen Postdienst :
 - 1. das Datum und die Uhrzeit des Versands oder des Empfangs von Mitteilungen bei der Internet-Anbieterin,
 - 2. bei der Überwachung von E-Mail-Verkehr: die Umschlaginformationen nach SMTP-Protokoll,
 - 3. die IP-Adressen der sendenden und empfangenden Fernmeldeanlagen der asynchronen elektronischen Postdienste ,
 - 4. die anderen verfügbaren Adressierungselemente.

Art. 24c Überwachungsmassnahmen mit Auslandsbezug

Ziel der Überwachungsmassnahmen nach Artikel 24a Buchstaben a und b und 24b Buchstabe a können auch Anschlüsse nach Artikel 24 Absatz 1 Buchstaben c und d sein, die ein ausländisches Adressierungselement haben, welches sich im Netzwerk einer schweizerischen Fernmeldedienstanbieterin befindet.

Technik-asut: Bei einer Accessüberwachung gemäss Art. 24a Bst. a. und b. sowie Art. 24b Bst. a. stellt sich die Frage, welche Parameter die auftraggebenden Behörden einem Provider bekanntgeben, um einen Informationsfluss zu überwachen, der einen Ursprung „irgendwo“ hat und von „irgendwem“ zugeteilte Indikatoren (z.B. IP-Address) verwendet. Es ist insbesondere zu berücksichtigen, dass Indikatoren des Zuganges dynamisch zugeteilt werden können und demzufolge „falsche Targets“ überwacht würden. In keinem Fall ist der verpflichtete Schweizerische Provider der Accessprovider, sondern betreibt allenfalls ein sogenanntes zwischengehaltets Transportnetz.

Bezugnehmend auf den Hinweis auf Artikel 24 Absatz 1 Buchstaben c und d sei festgestellt dass in einem Gateway, die am fernen Ende eingesetzte Access Technologie in der Regel nicht erkennen kann, wobei dies für den beabsichtigten Zweck (d.h. der Überwachung der Kommunikation eines Targets mit einem Kunden des verpflichteten Providers) nicht relevant ist.

Da solche Überwachungen in Gateways umgesetzt werden müssen, was schon durch den Ausdruck „Kopfschaltung“ offensichtlich wird, kommt nur eine Überwachung der Anwendung in Frage.

Es muss klargestellt werden, dass bei einer Echtzeit-Überwachung der Anwendung bezugnehmend auf Art. 24a Bst. c. und d. nur jene Parameter

ermittelbar sind, die den Gateway passieren, mit einigen Vorbehalten bezüglich der Verifikation derer Richtigkeit. Der Bezug zu Artikeln (d.h. Art. 24a), die aus der Überwachung eines Telefondienstes abgeleitet wurden vermittelt den falschen Eindruck, bei einer Kopfschaltung liesse sich derselbe Umfang an Parametern ermitteln. Die Methode Anforderungen gemäss Art. 24a auf die Kopfschaltung zu übertragen ist ungeeignet und schafft Rechtsunsicherheit.

Betreffend Anwendung von Art. 24b Bst. b. (rückwirkende Überwachung) ist zu berücksichtigen dass vom Target in der Regel, weil nicht Kunde des verpflichteten Providers (Ausnahmen sind outbound Roamer und inbound Roamer) kein Datensatz existieren kann, der mit einer Subscription assoziiert ist. Es ist nicht zumutbar, dass ein Provider eine Art „virtuelle Accounts“ kreiert und die gesamte Kommunikation von Targets mit Auslandsbezug analysiert und durch Korrelation der vielfältigen sogenannten Kommunikationsparameter einem „virtuellen Account“ zuordnen muss; dies würde eine Data Retention im Bereich „Usage“ für alle inbound und outbound Verbindungen bedingen.

Auch in diem Fall ist die Methode Anforderungen gemäss Art. 24b auf die Kopfschaltung zu übertragen ungeeignet und schafft Rechtsunsicherheit.

Art. 25 Durchführung der Überwachung

1 Der Dienst bestimmt im Einzelfall:

- a. die technischen und organisatorischen Massnahmen für die Durchführung der Überwachung, wenn nötig im Einvernehmen mit der anordnenden Behörde;
- b. die zu verwendenden Datenträger, die Art und Weise der Übermittlung und die zulässigen Datenformate, wenn nötig nach Anhörung der Internet-Anbieterin.

2 Wenn der Dienst feststellt, dass die angeordnete Überwachung Trägerinnen und Träger von Berufsgeheimnissen betrifft, ohne dass Vorkehren nach Artikel 271 Absatz 1 der Strafprozessordnung⁸ (StPO) angeordnet worden sind, zeichnet der Dienst die Daten auf und benachrichtigt die Genehmigungsbehörde.

3 Die Internet-Anbieterinnen melden dem Dienst die Ausführung der angeordneten Massnahmen.

4 Sie leiten dem Dienst auf Verlangen die Daten zu. Der Dienst regelt in seinen Richtlinien nach Anhörung der Anbieterinnen die Spezifikation dieser Zuleitung unter Berücksichtigung der Standards des Europäischen Institutes für Telekommunikationsnormen (ETSI).

Technik-asut: 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.

5 Bei Überwachungsmaßnahmen, die nicht explizit in dieser Verordnung aufgeführt sind, stellen sie dem Dienst jene Schnittstellen zur Verfügung, von denen aus der Fernmeldeverkehr der überwachten Person in Echtzeit und permanent zum Verarbeitungszentrum übertragen werden kann. Der Dienst regelt die Überwachungsmodalitäten im Einzelfall.

Technik-asut: Eine Schnittstelle ist ein Übergabepunkt zwischen Entitäten, im vorliegenden Fall zwischen Ausrüstungen der Provider und solchen von ÜPF. Damit ein Provider solche Schnittstellen zur Verfügung stellen kann, müssen diese in Technischen Richtlinien spezifiziert sein (mit Ausnahme eines passiven Arrangements zur Auskopplung von Daten, wie TAP).

Der Wortlaut „von denen aus der Fernmeldeverkehr der überwachten Person in Echtzeit und permanent zum Verarbeitungszentrum übertragen werden kann“ lässt darauf schliessen, dass ÜPF mit eigenen Ausrüstungen an Standorten der Provider ist.

Eine der Kernfragen in diesem Zusammenhang ist die Definition des Spezialfalles.

In den Erläuterungen Site 2 steht:

Der Dienst und die Fernmeldediensteanbieterinnen 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 Fernmeldediensteanbieterinnen bei der Durchführung von nicht explizit in der VÜPF aufgeführten Überwachungsmaßnahmen erhebliche Kosten entstehen. Die Durchführung von diesen Spezialmassnahmen, z. B. im Bereich der Internetüberwachung, kann Kosten für die Anschaffung von Überwachungstechnologie und Supportleistungen sowie den Beibezug von externen Spezialisten in Höhe von mehreren hunderttausend Franken pro Fall verursachen, welche bisher durch den Dienst getragen werden mussten.

Für die Kosten der Provider ist nicht massgebend, ob eine Massnahme in VÜPF definiert ist, sondern ob eine Technische Richtlinie besteht, die es

einem Provider gestattet, jene technischen Vorkehrungen zu treffen, die eine kostengünstige Überwachung erlauben. Die Technische Richtlinien sind auch notwendig, damit ÜPF eigne Ausrüstungen beschaffen kann, um die Daten entgegennehmen zu können.

Damit müssten Technische Richtlinien erarbeitet werden für Massnahmen die im VÜPF nicht vorgesehen sind.

6 Ist infolge technischer oder anderer Pannen eine Internet-Anbieterin vorübergehend nicht in der Lage, ihre Pflichten bei Echtzeit-Überwachungen oder zum Vollzug neuer Überwachungsanordnungen wahrzunehmen, muss sie es dem Dienst unverzüglich mitteilen. Die Verkehrsdaten, welche nicht dem Dienst übertragen werden konnten, sind nachzuliefern.

Technik-asut: In der Praxis hat sich gezeigt, dass hier Interpretationsspielraum in der „Schuldfrage“ besteht. Die sogenannte Panne kann verursacht werden durch Probleme im Bereich der Datenaufbereitung ein verpflichteten Provider, im Delivery Network, bei Ausrüstungen der Behörden, die den ausgeleiteten Verkehr nicht entgegennehmen können.

Die Lösung des Problems bedingt die Definition von Übergabeputen, siehe Kommentar zu Art.9 Abs. 2

7 Die Überwachung ist so durchzuführen, dass weder die überwachte Person noch andere Teilnehmerinnen und Teilnehmer davon Kenntnis erhalten. Sie ist so zu planen, dass eine unbefugte oder unsachgemässe Verwendung der erfassten Informationen verhindert wird.

Art. 26 Pflichten der Internet-Anbieterinnen

1 Jede Internet-Anbieterin muss in der Lage sein, die Überwachungstypen nach diesem Abschnitt auszuführen, die durch sie angebotene Dienste betreffen.

2 Die Überwachung des Fernmeldeverkehrs ist von der Aufnahme des Kundenbetriebes eines Internet-Dienstes an sicherzustellen.

3 Jede Internet-Anbieterin muss sicherstellen, dass sie die Überwachungsanordnungen auch ausserhalb ihrer Bürozeiten empfangen und so rasch wie möglich ausführen kann. Sie meldet dem Dienst schriftlich die Kontaktangaben der verantwortlichen Personen.

4 Sie hat zu gewährleisten, dass innerhalb des durch die Überwachungsanordnung bestimmten Zeitraumes die Überwachung des gesamten über ihre eigene Infrastruktur geführten und den

Überwachungen gemäss Artikel 24 - 24 unterliegenden Internetverkehrs ermöglicht wird, der von der Überwachungsanordnung erfasst ist.

5 Der Dienst kann die Internet-Anbieterinnen zur Zusammenarbeit verpflichten, um die Überwachung des Fernmeldeverkehrs zu vollziehen, der durch mehr als ein Netzwerk führt.

Technik-asut: Es wird zu einer echten Herausforderung für ÜPF werden, die beteiligten Provider zu ermitteln, Grundlage dazu wäre eine funktionelle Architektur und ein Rollenmodell.

6 Zur Überprüfung der Überwachungsbereitschaft haben die Internet-Anbieterinnen dem Dienst die Benutzung ihrer Dienste unentgeltlich zu gewähren.

Technik-asut: Hier geht es um das sogenannte „permanent Testing Environment“, in dem permanent Testtargets angelegt auf Abbos der Behörden eingerichtet sind. Es ist nicht klar, wessen „Überwachungsbereitschaft“ überprüft werden soll; dies hat einen Einfluss auf den Umfang „permanent Testing Environment“. Es ist auch nicht klar, welche Testmethode eingesetzt werden soll (periodisch vs. bei Unregelmässigkeiten) ; dies hat einen Einfluss auf den Verkehr, den die Provider gratis abzuwickeln haben, gegebenenfalls ins Ausland.

7 Wenn nötig, unterstützen die Internet-Anbieterinnen den Dienst, um sicherzustellen, dass die übermittelten Überwachungsdaten tatsächlich mit dem Fernmeldeverkehr der überwachten Personen übereinstimmen.

Technik-asut: Dies könnte bedeuten, dass die Provider zwecks späterer Verifikation Kopien von abgelieferten Daten erstellen müsste. Es ist unklar, welche technischen und organisatorischen Vorkehrungen ein Provider treffen muss, um diese Unterstützung zu leisten.

Art. 27 Auskünfte über Internet-Teilnehmerinnen und -Teilnehmer

1 Die zuständige Internet-Anbieterin meldet dem Dienst auf Anfrage folgende

Daten:

Technik-asut: Hier handelt es sich um Daten, die gegeben durch ihre Charakteristik im Prinzip durch das Call Center Information System (CCIS) erhoben werden müssten. Dies entspricht in der Data Retention gemäss ETSI TS 102 657 den Formaten in Annex A.3.3 GenericSubscriberInfo sowie Annexes C.3, D.1, E.3 <service>Subscriber .

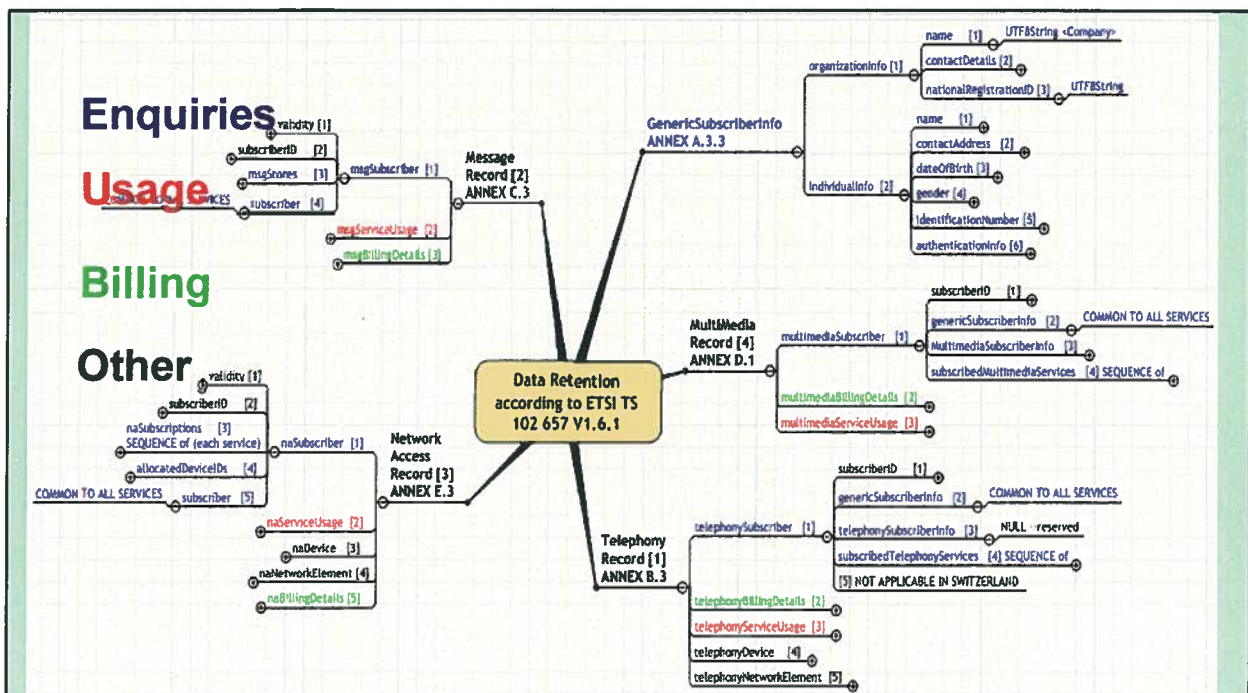
- a. bei IP-Adressen: die Art des Anschlusses, das Datum und die Uhrzeit der Zuteilung oder das Datum und die Uhrzeit des Anfanges und gegebenenfalls des Endes des Zuteilungszeitraumes , den Namen, die Adresse, die Anmeldungsdaten (Log-in) und, soweit bekannt, den Beruf der Teilnehmerin oder des Teilnehmers, sowie weitere IP-Adressen, die die Internet-Anbieterin dieser oder diesem zugeteilt hat;

Technik-asut: In diesem Fall geht es um Auskünfte im Sinn von BÜPF Art. 14 „Auskünfte über Fernmeldeanschlüsse“.

Diese Auskünfte sind beschränkt auf Personalien, respektive gleichwertige Daten von Unternehmen sowie deren „Subscriptions“ und decken niemals Parameter ab, die durch Interaktionen zwischen einem Kunden und dem Netz erworben werden, wie beispielsweise eine dynamische IP-Adresse mittels DHCP.

Da gemäss Art. 17 Abs. 4 ETSI –Standards berücksichtigt werden sollen, sollte die Klassenbildung von Parametern gemäss ESI TS 102 657 übernommen werden.

Es handelt sich dabei um die blauen Bereiche in der untenstehenden Figur:



Sollte VÜPF von der Klassenbildung gemäss ETSI abweichen, wird eine technische Umsetzung von VÜPF interpretierbar und es besteht die Gefahr von unnötigen rechtlichen Auseinandersetzungen.

BÜPF Art. 5 „Auskünfte über den Post- und Fernmeldeverkehr“ bezieht sich in Abs. 1 auf „Usage“ und „Billing“. Die bezüglich „Usage“ zu erfüllenden Anforderungen sind bereits in Art. 24b definiert.

Die Erweiterung auf alle IP-Adressen und log-in sei zurückzunehmen.

- b. bei EDV-Systemen: sofern verfügbar, zusätzlich die Domainnamen und weitere Adressierungselemente unter denen diese der Internet-Anbieterin bekannt sind;
- c. bei elektronischen Postdiensten, sofern sie von den Internet-Anbieterinnen zur Nutzung durch Kunden eingerichtet sind: soweit bekannt, den Namen, die Adresse und den Beruf der Teilnehmerin oder des Teilnehmers.

2 Der Dienst sucht über die öffentlich zugänglichen Datenbanken die zuständige Internet-Anbieterin für Auskunftsgesuche und Überwachungen der Internet- Zugänge.

3 Er bewahrt die Auskunftsgesuche und die erteilten Antworten während eines Jahres auf. Er vernichtet diese Daten nach Ablauf der Aufbewahrungsfrist.

7. Abschnitt: Überwachung des Verkehrs innerhalb von internen Fernmeldenetzen oder Hauszentralen

Art. 28 Vorbereitung der Überwachung

Wenn die Überwachungsanordnung eine Überwachung des Verkehrs innerhalb eines internen Fernmeldenetzes oder einer Hauszentrale vorsieht, bestimmt der Dienst im Einvernehmen mit der Betreiberin dieses Netzes oder dieser Zentrale und wenn nötig mit der anordnenden Behörde, wie die Überwachung durchzuführen ist.

Art. 29 Durchführung der Überwachung

1 Der Dienst richtet die Überwachung selber ein oder beauftragt damit auf eigene Kosten die Betreiberin des internen Fernmeldenetzes oder der Hauszentrale, wenn diese einverstanden ist und über die angemessenen Einrichtungen verfügt.

2 Wenn die Betreiberin mit der Überwachung beauftragt ist, müssen die Auflagen für die Datensicherheit im Auftrag enthalten sein.

8. Abschnitt: Gebühren und Rechtsschutz

Art. 30 Gebühren und Entschädigungen

1–2 ...9

3 Die anordnende Behörde kann vom Dienst verlangen, dass er ihr die zu erwarten- den Kosten für eine bestimmte Überwachung mitteilt.

Art. 31 Rechnungsstellung

1 Der Dienst stellt den anordnenden Behörden nach Abschluss der Überwachung

Rechnung für die gesamten erbrachten Dienstleistungen.

2 Die Anbieterinnen von Post- oder Fernmeldediensten übermitteln dem Dienst ihre

Abrechnungen spätestens zwei Monate nach Abschluss der Überwachung.

Art. 32¹⁰ Rechtsschutz

Gegen Verfügungen des Dienstes über den Vollzug dieser Verordnung kann nach den allgemeinen Bestimmungen über die Bundesrechtspflege Beschwerde geführt werden.

9. Abschnitt: Schlussbestimmungen

Art. 33 Vollzug

¹ Das Departement regelt:

- a. die zugelassenen Übertragungsmittel zur Einreichung der Überwachungsanordnungen nach Artikel 5 Absatz 1 Buchstabe a;
- b. die Fristen für die Beantwortung der Auskunftsgesuche nach Artikel 19 Absatz 3 in Funktion der verschiedenen Dringlichkeitsstufen;
- c. die Anforderungen an die Auskunftsgesuche nach den Artikeln 22 und 27;
- d. wenn nötig, die technischen ergänzenden Angaben, die in Artikel 15 Absatz 2 erwähnt sind;
- e. ...¹¹

^{1bis} Der Dienst regelt durch Richtlinien die technischen und administrativen Einzelheiten der einzelnen Überwachungstypen.¹²

⁹ Aufgehoben durch Art. 7 der V vom 7. April 2004 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (SR 780.115.1).

¹⁰ Fassung gemäss Ziff. II 77 der V vom 8. Nov. 2006 über die Anpassung von Bundesratsverordnungen an die Totalrevision der Bundesrechtspflege, in Kraft seit 1. Jan. 2007 (AS 2006 4705).

¹¹ Aufgehoben durch Ziff. I der V vom 12. März 2004 (AS 2004 1431).

¹² Eingefügt durch Ziff. I der V vom 12. März 2004 (AS 2004 1431).

² Er legt Form und Inhalt folgender Formulare fest:

- a. die durch die anordnende Behörde zu verwendenden Formulare, um die Überwachungsanordnung beim Dienst einzureichen;
- b. die durch den Dienst zu verwendenden Formulare, um die Anbieterinnen von Post- oder Fernmeldediensten mit der Durchführung der Überwachungsanordnung zu beauftragen;
- c. die durch die Behörden nach Artikel 14 Absatz 2 BÜPF zu verwendenden Formulare, um vom Dienst die Auskünfte nach den Artikeln 22 und 27 einzuholen.

³ Das Departement räumt den Anbieterinnen von Post- und Fernmeldediensten beim Erlass von technischen Vorschriften

angemessene Übergangsfristen für die Umsetzung ein.

Art. 34 Aufhebung bisherigen Rechts

Die Verordnung vom 1. Dezember 1997¹³ über den Dienst für die Überwachung des Post- und Fernmeldeverkehrs wird aufgehoben.

Art. 35 Änderung bisherigen Rechts

Die Verordnung vom 6. Oktober 1997¹⁴ über Fernmeldedienste wird wie folgt geändert:

Art. 50 Abs. 1

...

Art. 36 Übergangsbestimmungen

1 Während maximal drei Monaten nach Inkrafttreten dieser Verordnung vollzieht der Dienst die Überwachungsanordnungen, die nach dem alten Recht genehmigt worden sind.

2 Bis zur Inbetriebnahme des Verarbeitungszentrums nach Artikel 8 übertragen die Anbieterinnen von Fernmeldediensten die Daten aus der Überwachung des Fernmeldeverkehrs nach bisheriger Praxis an den Dienst. Der Dienst zeichnet den Fernmeldeverkehr auf oder überträgt ihn mit Direktschaltung an die Strafverfolgungsbehörde, die als Empfängerin der Überwachungsdaten vorgesehen ist.

3 Die Anbieterinnen von Post- oder Fernmeldediensten melden innert drei Monaten nach Inkrafttreten dieser Verordnung die Überwachungsmassnahmen innerhalb ihres Dienstleistungsangebots, die sie nicht imstande sind auszuführen. Sie treffen die notwendigen Massnahmen, um diese Überwachungstypen innerhalb der durch den Dienst im Einzelfall festgesetzten Frist ausführen zu können und melden es dem Dienst, sobald sie dazu in der Lage sind.

13 [AS 1997 3022]

14 [AS 1997 2833, 2000 1044. AS 2001 2759 Art. 83]

4 Spätestens vom 1. April 2004 an übertragen die Anbieterinnen von Fernmelde- diensten die Daten aus jeder Überwachung des Fernmeldeverkehrs gemäss den Richtlinien nach Artikel 33 Absatz 1bis. Das Departement kann den Gebührenanteil von Anbieterinnen, die diese Daten schon zwischen dem 1. April 2003 und dem 1. April 2004 nach den neuen Anforderungen übertragen, angemessen

erhöhen; die Mehrkosten werden nicht auf die anordnenden Behörden überwält. Es kann mit einer Anbieterin einen späteren Beginn der Datenübertragung vereinbaren. Dieser richtet sich nach den technischen Möglichkeiten der Anbieterin und kann spätestens auf den Zeitpunkt der Aufhebung der regionalen Dienststellen festgelegt werden.¹⁵

⁵ Die Internet-Anbieterinnen übertragen vom 1. April 2003 an die Daten aus jeder Überwachung dem Dienst. Vorher müssen sie die Auskünfte nach Artikel 14 BÜPF erteilen und vorhandene Verkehrsdaten des E-Mail-Verkehrs übermitteln.

⁶ ...¹⁶

Art. 36a¹⁷ Übergangsbestimmung zur Änderung vom 23. Juni 2004

Anbieterinnen von Fernmeldediensten müssen von ihren Kundinnen und Kunden, deren Prepaid-SIM-Karte nach dem 1. November 2002 in Betrieb genommen worden ist, bis zum 31. Oktober 2004 die Daten nach Artikel 19a erfassen. Nach Ablauf dieser Frist sind die Nummern der nicht registrierten Kundinnen und Kunden ausser Betrieb zu nehmen.

Art. 37 Inkrafttreten

Diese Verordnung tritt am 1. Januar 2002 in Kraft.

Diese Änderung tritt am ... 2011 in Kraft.

Begriffe und Abkürzungen

1. Internet-Anbieterin: Fernmeldedienstanbieterin oder der Teil einer Fernmeldedienstanbieterin, die der Öffentlichkeit fernmeldetechnische Übertragungen von Informationen auf der Basis der IP-Technologien (Netzprotokoll im Internet [Internet Protocol]) unter Verwendung von IP-Adressen anbietet;
2. Betreiberinnen von internen Fernmeldenetzen oder Hauszentralen: die Personen, die über die Beschaffung, die Erstellung und den Betrieb dieser Einrichtungen entscheiden;
3. Echtzeit-Überwachung: das Abfangen in Echtzeit und die simultane, leicht verzögerte oder periodische Übertragung der Post- oder Fernmeldeverkehrsdaten, inklusive der Nutzinformationen, durch die Anbieterinnen von Post- oder Fernmeldediensten gemäss den Angaben der Überwachungsanordnung;
4. rückwirkende Überwachung: die Herausgabe der Verkehrs- und Rechnungsdaten der zurückliegenden sechs Monate durch die Anbieterinnen von Post- oder Fernmeldediensten;
5. Direktschaltung: direkte Übertragung des Fernmeldeverkehrs der überwachten Person vom Dienst an die anordnende Behörde;
6. Nutzinformationen: der Anteil des zu überwachenden

Fernmeldeverkehrs, welcher die zwischen Benutzenden bzw. zwischen deren Endeinrichtungen ausgetauschten Informationen (z.B. Laute, Telefax, E-Mails und Daten) enthält;

7. Verkehrs- und Rechnungsdaten: die Informationen, die von der Anbieterin über den Post- oder Fernmeldeverkehr von Teilnehmerinnen und Teilnehmern aufgezeichnet werden, um die Tatsache der Postsendung oder der Kommunikation und die Rechnungsstellung zu belegen;
8. Adressierungselemente: Kommunikationsparameter sowie Nummerierungselemente, wie Kennzahlen, Rufnummern und Kurznummern (Art. 3 Bst. f des Fernmeldegesetzes vom 30. April 1997 9 - FMG);
9. Kommunikationsparameter: die Elemente zur Identifikation von Personen, Computerprozessen, Maschinen, Geräten oder Fernmeldeanlagen, die an einem fernmeldetechnischen Kommunikationsvorgang beteiligt sind (Art. 3 Bst. g FMG);
10. E.164-Nummer: Adressierungselement des Nummerierungsplans E.164 (vgl. das 2. Kapitel der Verordnung vom 6. Oktober 1997 über die Adressierungselemente im Fernmeldebereich10-AEFV);
11. IMEI-Nummer (IMEI: International Mobile Equipment Identity): internationale Nummer zur Identifizierung von Mobiltelefonie-Geräten;
12. IMSI-Nummer (IMSI: International Mobile Subscribers Identity): internationale Nummer, die zur Identifikation der Teilnehmerin oder des Teilnehmers in einem Mobilfunknetz dient;
13. IP-Adresse (Internet-Protokoll-Adresse): Adresse, die alle verbundenen Geräte in einem Informatiknetzwerk identifiziert, die das Internet-Protokoll benutzen;
14. MAC-Adresse (Media Access Control Address): Hardware-Adresse, die in einer Netzwerkkarte- oder einem Netzwerkadapter hinterlegt ist und als eindeutige Adresse auf der Ebene der Sicherungsschicht gebraucht wird (OSI-Schicht 2);

Technik-asut: Im Zusammenhang mit dem MAC-sublayer kann die Schicht 2 nur als Sicherungsschicht bezeichnet werden, wenn darüber ein Logical Link Control (LLC) Sublayer eingesetzt wird, der zur HDLC Familie gehört und in der Lage ist, Übertragungsfehler zu korrigieren.

IEEE 802.3

1.4.212 MAC frame: Consists of the Destination Address, Source Address, Length/Type field, MAC Client Data, Pad (if required), and Frame Check Sequence.

Generell muss in Frage gestellt werden, ob eine Verordnung der richtige Ort ist, die Technik von Protokollarchitekturen zu erklären.

15. URI (Uniform Resource Identifier): Identifikator einer Ressource im Internet (Webseiten, Dateien, Webservices, SIP-Adresse usw.);
16. SIM-Nummer (SIM: Subscriber Identity Module): Serien-Nummer der SIM Karte, die die Karte eindeutig identifiziert ;
17. Cell ID: unveränderter Zell-Identifikator (Cell Global Identification) der Mobiltelefonie;
18. Umschlaginformationen: Adressierungselemente, die den Datagrammen eines E-Mail angehängt werden;
19. Kopf-Informationen: Informationen, die dem Inhalt einer Meldung vorangestellt sind;
20. Dial-up: Einwahl-Internetzugang über Telefonverbindungen (Analog-Modem oder ISDN);
21. DSL (Digital Subscriber Line): Breitband-Internetzugang mittels Bitübertragungsschicht auf einer Teilnehmeranschlussleitung, der einen hohen Datenfluss erlaubt;
22. xDSL: Gruppe von Techniken, die mit der DSL-Technologie verwandt sind. Der Buchstabe «x» steht für diverse Abkürzungen, mit denen die verschiedenen DSL-Technologien bezeichnet werden;
23. FTTH (Fiber To The Home): Glasfaserleitung bis zur Wohnung des Teilnehmers;
24. Kabelmodem: Modemtyp, der es erlaubt, sich mit dem Internet über ein Kabelfernsehtz zu verbinden;
25. SIM-Karte (SIM Subscriber Identity Module): Chipkarte, die zur Identifikation der Teilnehmerin oder des Teilnehmers in einem Mobilfunknetz dient;
26. Prepaid SIM-Karte: SIM-Karte, bei welcher die Kundenbeziehung für Mobiltelefone nicht über ein Abonnementsverhältnis aufgenommen wird;
27. GPRS (General Packet Radio Service): Mobiltelefoniedienst, der die paketvermittelte Datenübertragung über GSM erlaubt;
28. GSM (Global System for Mobile Communications): Standard der zweiten Mobilfunk-Generation;
29. UMTS (Universal Mobile Telecommunications System): Standard der dritten Mobilfunk-Generation;
30. LTE (Long Term Evolution): Standard der vierten Mobilfunk-Generation;
31. OSI-Referenzmodell (Open Systems Interconnection): Modell nach ISO-Norm 7498, welches zur Beschreibung offener

- Kommunikationsarchitekturen in Computernetzen dient;
32. OSI-Schicht 2: Sicherungsschicht (engl. Data Link Layer) nach dem OSI-Referenzmodell;
 33. OSI-Schicht 3: Vermittlungsschicht (engl. Network Layer) nach dem OSI-Referenzmodell;
 34. Ethernet: Familie von Netzwerktechnologien der OSI-Schichten 1 und 2 auf der Basis der IEEE-Norm 802.3;
 35. SIP (Session Initiation Protocol): standardisiertes Signalisierungsprotokoll der IETF für die Steuerung von IP-Telefonie und Multimediakommunikation (Sprache, Audio, Video, Fax usw.);
 36. SMTP (Simple Mail Transfer Protocol): Protokoll für die Übermittlung von E-Mail in Computernetzen ;
 37. Instant Messaging (sofortige Nachrichtenübermittlung): synchrone Echtzeitkommunikation zwischen zwei oder mehr Teilnehmern. Es gibt eine Vielzahl von Instant Messaging Diensten und es werden zum Teil proprietäre Protokolle verwendet. Neben Textnachrichten können häufig auch Multi-media-Inhalte übertragen werden.
 38. VoIP (Voice over IP auch IP-Telefonie oder Internet-Telefonie): Technik, die es erlaubt, über das IP Protokoll zu telefonieren;
 39. VPN (Virtual Private Network): ein virtuelles Computernetz mit gekapselter Datenübertragung zwischen 2 oder mehr vernetzten Geräten;
 40. Wi-Fi: Standard für kabellose Netzwerke nach der IEEE-Norm 802.11;
 41. Wimax (Worldwide Interoperability for Microwave Access): Standard für kabellose Netzwerke nach der IEEE-Norm 802.16;
 42. WLL (Wireless Local Loop): drahtloser Teilnehmeranschluss, der eine Alternative zum leitungsgebundenen Anschlussnetz darstellt;
 43. IEEE (Institute of Electrical and Electronics Engineers): gemeinnützige Organisation, die die Veröffentlichung der Normen, die von den Mitgliedern der Organisation verfasst werden, sicherstellt;
 44. IETF (Internet Engineering Task Force): internationale, informelle Organisation, die die meisten Internetstandards erarbeitet;
 45. ISO (International Organization for Standardization): weltweite Organisation für die Erarbeitung und Veröffentlichung internationaler Normen;
 46. ITU (International Telecommunication Union): internationale Organisation der Vereinten Nationen, die sich dem Wachstum und der nachhaltigen Entwicklung von Telekommunikations- und Informationstechnologie widmet;
 47. ITU-T: Bereich der ITU, der Empfehlungen im Bereich der Telekommunikationsstandardisierung herausgibt.



swisscom

007937 14.JUL 2011 09:16

Swisscom (Schweiz) AG, Legal Services & Regulatory Affairs,
Alte Tiefenastrasse 6, 3050 Bern

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

Datum	8. Juli 2011
Ihr Kontakt	Andreas Heiniger / andreas.heiniger@swisscom.com
Thema	VÜPF - Teilrevision

Seite
1 von 3

Sehr geehrter Herr Schöpf

Wir danken für die gemäss Schreiben von Frau Bundesrätin Simonetta Sommaruga vom 8. Juni 2011 eingeräumte Möglichkeit, sich zur VÜPF – Teilrevision anhören zu lassen. Grundsätzlich arbeitet Swisscom auch an einer Stellungnahme des Branchenverbands asut mit. Vorab möchten wir uns mit dieser Stellungnahme summarisch vernehmen lassen und verweisen für weitere Einzelheiten auf die ausführlichere Stellungnahme der asut, welche von Swisscom ausdrücklich unterstützt wird.

Gemäss dem Schreiben von Frau Bundesrätin Sommaruga vom 8. Juni 2011 soll es bei vorliegender Teilrevision der VÜPF lediglich um eine „Nachführung“ gehen, welche für alle Beteiligten „die nötige Bestimmtheit und Rechtssicherheit“ schaffe. Dies ist jedoch gemäss unserer Ansicht nicht zutreffend respektive gar nicht möglich:

- Erstens wird nicht nur bestehende Praxis nachgeführt, sondern es werden auch neue Überwachungsmassnahmen verankert, wie z.B. die umfassende Überwachung des Internetverkehrs oder internationale Kopfschaltungen in allen denkbaren Varianten.
- Zweitens sollen mit der Revision auch rechtlich zweifelhafte Massnahmen in den Katalog aufgenommen werden, zu denken ist namentlich an die Antennensuchläufe, welche sich nicht gegen bestimmte Personen oder Anschlüsse richten, sondern gegen unbestimmt viele, was nicht im Einklang mit der StPO und dem BÜPF ist.
- Schliesslich ist es entgegen der offiziell dargelegten Absicht der Vorlage gar nicht möglich, mit einer Revision der VÜPF für mehr Rechtssicherheit zu sorgen. Das Rechtssicherheitsproblem kann einzig mit einer BÜPF – Revision gelöst werden, da das Problem im BÜPF liegt, indem die (technisch meist nicht versierten) Strafverfolgungsbehörden grundsätzlich anordnen können, was sie wollen, ohne dass dies von einer anderen Instanz überprüft werden könnte. Daran ändern auch die beiden jüngsten Bundesverwaltungsgerichtsentscheide nichts (s. dazu unten „Keine unkritische Übernahme von bisheriger Rechtsprechung und Praxis“).

Keine Revision der VÜPF zum jetzigen Zeitpunkt

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 Fernmeldeverkehrs, sondern auch Überwachungspflichten auf der Dienste-/Anwendungsebene (allfällige Filterungspflichten der FDA)
- Überwachungsmassnahmen gegen einen unbestimmten Personenkreis (z.B. Antennensuchläufe)

Der von Verfassung und Gesetz vorgesehene Stufenbau (Gesetz – Verordnung – Richtlinien) ist strikt einzuhalten. Es geht nicht an, dass im Prinzip die relevanten Entscheidungen auf einer unteren Normenstufe gefällt werden und dass sich dann später das Gesetz im formellen Sinn danach richten muss.

Da es wie dargelegt weiter nicht möglich ist, mit dieser Vorlage mehr Rechtssicherheit zu schaffen, ist eine Revision der VÜPF im jetzigen Zeitpunkt nicht angezeigt und klar abzulehnen. Vielmehr ist die BÜPF Revision abzuwarten bzw. zügig voran zu treiben, damit das Überwachungswesen im Post- und Telekommunikationsbereich auf eine saubere Grundlage gestellt werden kann.

Swisscom zeigt sich hinsichtlich Durchführung von Internetüberwachungen kooperativ, sofern die ihr auferlegten Pflichten im verhältnismässigen Rahmen bleiben. Es besteht also nicht die Absicht, nun die Behörden buchstabengetreu auf den ergangenen Bundesverwaltungsgerichtsentscheiden hinsichtlich Internetüberwachung zu behaften. Auch von daher ist eine eiligst durchgedrückte VÜPF Revision unnötig.

Keine unkritische Übernahme von bisheriger Rechtsprechung und Praxis

Oft soll mit Gesetzesrevisionen die in der Zwischenzeit aufgelaufene, „bewährte“ Rechtsprechung ins neue Gesetz einfliessen, so offiziell zum Teil auch hier. In diesem Fall ist aber Skepsis angebracht. Einerseits gibt es keine eigentliche Rechtsprechung, sondern nur ein paar Einzelentscheide und diese sind meistens nicht hilfreich. Aufgrund der konzeptionellen Fehler im BÜPF, welche zur Folge haben, dass Konfusion herrscht hinsichtlich der Frage, was die Gerichte auf Beschwerde einer FDA hin nun zu prüfen haben und was nicht, konnte sich verständlicherweise keine Gerichtspraxis entwickeln, welche es verdienen würde, in Gesetze aufgenommen zu werden. Oder anders und etwas pointierter formuliert: Es wäre fatal, wenn sich der Gesetzgeber darauf verlassen würde, dass die Gerichte unter einem schlechten Gesetz gute Entscheide fällen würden.

Gerade die neusten 2 Entscheidungen des Bundesverwaltungsgerichts haben gezeigt, dass das Gericht an sich nicht erfasst hat, was es eigentlich tut: Auf der einen Seite behauptet es kühn, das BÜPF leide nicht unter konzeptionellen Mängeln, auf der anderen Seite hält es sich nicht an den Wortlaut des BÜPF und prüft (offenbar in Ausfüllung einer unechten, sogenannten rechtspolitischen Gesetzeslücke?) Dinge die es gemäss BÜPF gar nicht prüfen dürfte, s. Art. 13. Abs. 1 lit. a. BÜPF und die Tatsache, dass das Bundesverwaltungsgericht geprüft hat, ob eine angeordnete Überwachungsmassnahme einen Überwachungstyp gemäss der VÜPF bildet.

Mit dem einzigen höchstrichterlichen Entscheid im Bereich Zulässigkeit von Überwachungsmassnahmen im Fernmeldebereich (BGE 130 II 249ff) wurde eine Überwachungsmassnahme, welche ebenfalls nicht dem VÜPF Katalog angehört (Antennensuchläufe) nicht verhindert. Das Bundesgericht hielt sich damals an Art. 13 Abs. 1 Bst. a BÜPF und stellte sich auf den Standpunkt, es dürfe die Rechtmässigkeit von Antennensuchläufen (auf Beschwerde einer Fernmeldedienstanbieterin hin) nicht prüfen. Wenn also in



den Erläuterungen behauptet wird, Antennensuchläufe seien von der Gerichtspraxis als zulässig bestätigt, so stimmt das nicht und der Überwachungstypenkatalog der VÜPF darf nicht entsprechend ergänzt werden.

Aufgrund dieser Ausführungen möchten wir Sie bitten, eine voreilige VÜPF Revision zurück zu stellen und sich stattdessen dafür einzusetzen, dass eine Revision des BÜPF vorangetrieben wird.

Mit freundlichen Grüßen

Swisscom (Schweiz) AG

Andreas Heiniger, Pürsprecher
Senior Counsel

Urs Meienberger
Business Assurance



Verizon Switzerland AG • Förrlibuckstrasse 150 • CH-8005 Zürich

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

Verizon Switzerland AG
 Förrlibuckstrasse 150
 8005 Zürich
 Switzerland
 Tel. +41 44 580 80 11
 Fax. +41 44 580 80 21

Verizon Switzerland SA
 18, Chemin de Trèfle-Blanc
 1228 Plan-les-Ouates
 Switzerland
 Tel. +41 22 580 70 11
 Fax. +41 22 580 70 21

Zürich, 14. Juli 2011

Anhörung Revision VÜPF: Stellungnahme Verizon Switzerland AG

Sehr geehrter Herr Schöpf

Wir nehmen Bezug auf das mit Schreiben vom 8. Juni 2011 eröffnete Vernehmlassungsverfahren zur Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs.

Verizon Switzerland AG ist eine in der Schweiz tätige Fernmeldediensteanbieterin (FDA) welche Ihre Dienste ausschliesslich (grösseren) Geschäftskunden erbringt. Dabei ist die Anzahl der Kunden, insbesondere im Vergleich mit den Verhältnissen im Privatkundenmarkt klein. Im Mobilfunk hat Verizon in der Schweiz keine Aktivitäten.

Verizon hat als Mitglied der asut von der Anhörung erfahren und arbeitet auch an einer Stellungnahme des Branchenverbands asut mit, welche von Verizon ausdrücklich unterstützt wird.

Obwohl nicht namentlich zur Stellungnahme eingeladen, als jedoch schon von der derzeit geltenden Rechtslage und um so mehr von den vorgeschlagenen Änderungen unmittelbar und möglicherweise einschneidend betroffenes Unternehmen erlauben wir uns, Ihnen nachfolgend unsere ergänzende Stellungnahme zu unterbreiten.

Verizon stellt die Notwendigkeit einer effizienten Strafverfolgung und die dafür notwendige Bereitstellung von Überwachungsmöglichkeiten nicht in Frage. Bedingt einerseits durch die hohen zusätzlichen Investitionskosten für Überwachungsanlagen, welche für den eigentlichen Betrieb der Telekommunikationsdienste nicht benötigt werden und andererseits möglichen Beeinträchtigungen der Netzperformance durch allzu umfängliche Eingriffe in die Netze zwecks Realisierung der Überwachungsmassnahmen ist jedoch den Fragen des Nutzens von geforderten Massnahmen, der Verhältnismässigkeit und der Rechtssicherheit genügend Aufmerksamkeit zu schenken.

Gemäss dem Schreiben von Frau Bundesrätin Sommaruga soll es bei der (Teil-) Revision der VüPF lediglich um eine „Nachführung“ gehen und zwar mit folgenden Zielen:

- Die Bestimmungen dem Stand der Technik anpassen
- Den Katalog der Überwachungsmassnahmen klarer und transparenter formulieren
- Die nötige Bestimmtheit und Rechtssicherheit schaffen.

Wir können die formulierten Ziele nachvollziehen und unterstützen, insbesondere da schon die heutige Gesetzesgrundlage zuviel Interpretationsspielraum lässt.

Die gesetzten Ziele werden verfehlt

Hingegen müssen wir feststellen, dass die Ziele aus unserer Sicht keineswegs erfüllt werden, im Gegenteil. Die schon heute bestehende Rechtsunsicherheit und Unbestimmtheit wird stark vergrößert und der Katalog der Überwachungsmaßnahmen massiv ausgedehnt, so dass die geforderten neuen Überwachungsmaßnahmen weit über das hinausgehen, was bisher angeordnet wurde.

Zudem sollen mit der Revision auch rechtlich zweifelhafte Überwachungsmaßnahmen gefordert werden, welche sich nicht auf bestimmte Personen oder Anschlüsse beziehen, sondern gegen unbestimmt viele Personen bzw. Anschlüsse, was durch BÜPF und StPO nicht gestützt wird. Beispiele dafür sind die internationale Kopfschaltung oder die Antennensuchläufe.

Im Weiteren wird der Geltungsbereich des 6. Abschnitts substantiell vergrößert indem der Titel „Internet-Zugang“ in „Internet“ geändert wird, sowie in Art. 24 Abs. 2 (VüPF neu) auch verlangt wird, dass Anwendungen überwacht werden können. Der Begriff „Anwendung“ wird dabei weder direkt, noch durch eine abschliessende Aufzählung definiert und führt zu mangelnder Klarheit und daher zu Rechtsunsicherheit.

Es ist auch unklar, auf wen die Verpflichtung, eine bestimmte Anwendung zu überwachen fallen würde. Diese Unklarheit kann daher rühren, dass die Natur des Internets ungenügend verstanden und somit nicht oder zu wenig berücksichtigt wurde, dass an der Abwicklung von Internetverkehr und an über das Internet genutzten Applikationen verschiedene unabhängige Dienstleister auf verschiedenen Protokollschichten beteiligt sind und beispielsweise ein Zugangsanbieter auf den unteren Protokollschichten reine Datenpakete transportiert, ohne in die Schichten, welche die Anwendungen enthält, überhaupt eingreifen zu müssen, bzw. zu dürfen, sei es aus Gründen des Datenschutzes, der Netzneutralität oder um die Performance des Netzes nicht negativ zu beeinflussen.

Aus obigen Gründen können diese Erweiterungen nicht als blosse „Nachführung“ betrachtet werden, Klarheit und Transparenz wird keine erreicht und es wird bezweifelt, dass das aktuelle BÜPF dafür eine genügende gesetzliche Grundlage bietet.

Umfang der Überwachung muss auf der politischen Ebene festgelegt werden

Gemäss VüPF Art. 33 ^{1bis} ist der Dienst ermächtigt, *die technischen und administrativen Einzelheiten der einzelnen Überwachungstypen* zu regeln. Darunter sind die anzuwendenden Übertragungsprotokolle sowie die administrativen Abläufe zu verstehen. Nicht in diese Zuständigkeit gehört aber die klare und unmissverständliche Definition der Überwachungstypen, dies ist eine politische Frage und muss abschliessend auf Verordnungsstufe, basierend auf einer soliden gesetzlichen Grundlage im BÜPF, geschehen. Diesbezüglich ist auch die Bedeutung von Art 17 Abs. 5 (VüPF neu) unklar, insbesondere was die Kompetenzen des Dienstes betrifft.

Es muss auch vermieden werden, dass Überwachungstypen gefordert werden, für die keine Klarheit herrscht, ob und wie die daraus gewonnenen Rohinformationen ausgewertet werden können und welche konkreten Erkenntnisse aus diesen Informationen durch die Strafverfolgungsbehörden überhaupt gewonnen werden können. Sonst besteht die Gefahr, dass auf Kosten der FDA eine „Experimentier- und Testumgebung“ erstellt wird, was unzumutbar und volkswirtschaftlich bedenklich wäre.

Eine Entschärfung dieser Problematik könnte dadurch erreicht werden, dass die Kosten von Überwachungsausrüstungen vollumfänglich vom Staat getragen werden. Dies ist ja auch ganz grundsätzlich zu fordern, da es sich bei der Strafverfolgung um eine staatliche Aufgabe handelt. Dies ist beispielsweise in Österreich für die Fernmeldeüberwachung bereits so geregelt und das nationale Gesetz,

womit die Europäische Richtlinie zur Vorratsdatenspeicherung in Österreich umgesetzt wird, sieht dies auch vor.

Im Weiteren wird angeregt, dass im Sinne der Verhältnismässigkeit, Zumutbarkeit und Kosteneffizienz Ausnahmestimmungen geschaffen werden, welche erlauben, dass FDAs für bestimmte Überwachungstypen und/oder bis zu einer gewissen Grösse (z.B. anhand der Anzahl Kunden oder der bedienten Kundensegmente) von gewissen Verpflichtungen ausgenommen werden können, bzw. im konkreten aber seltenen Fall der Beauftragung einer bestimmten Überwachungsmassnahme Dritte beziehen kann.

Keine losgelöste VüPF Revision

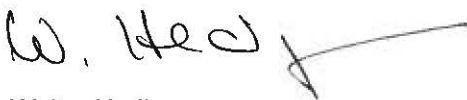
Wir sind aus den oben aufgeführten Gründen der Ansicht, dass die Problematik aus technischer wie auch aus rechtlicher Sicht einer eingehenden Diskussion Bedarf, damit die formulierten Ziele erreicht werden können. Es ist offensichtlich, dass dafür eine von der laufenden BÜPF-Revision losgelöste VüPF-Revision nicht dienlich ist.

Wir bitten Sie deshalb eindringlich, von einer überstürzten VüPF-Revision, welche mehr Probleme schaffen, als lösen würde, abzusehen und die Revision des BÜPF voranzutreiben. Allenfalls könnte sich eine „VüPF Revision light“ auf notwendige Anpassungen infolge des Inkrafttretens der StPO am 1. Januar 2011 beschränken. Im Weiteren erachten wir eine Zusammenarbeit der verschiedenen FDA-Gruppen (Festnetzanbieter Privatkunden, Mobilanbieter, Geschäftskundenanbieter), dem Dienst und den nachfragenden Untersuchungsbehörden für eine fundierte Formulierung einer revidierten VüPF als notwendig und zielführend. Verizon beteiligt sich gerne an einer solchen Zusammenarbeit.

Wir ersuchen Sie um Berücksichtigung unserer Stellungnahme und sind gerne bereit, Ihnen die Problematik der Fernmeldeüberwachung aus der Sicht eines Geschäftskundenanbieters in einem persönlichen Gespräch weiter zu erläutern.

Mit freundlichen Grüssen

Verizon Switzerland AG

A handwritten signature in black ink, appearing to read "W. Hediger", followed by a long horizontal stroke.

Walter Hediger
Regulatory Affairs Switzerland, Austria und Eastern Europe



ZAPP AG
Bahnhofstrasse 28
3076 Worb

Bernhard Schmocker
Tel: 031 / 710 34 38
Bernhard.schmocker@medianet.ch

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

26. Juli 2011

VÜPF Änderungsvorlage vom 8. Juni 2011: Stellungnahme der ZAPP AG

Sehr geehrter Herr Schöpf

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.

Es geht uns keineswegs darum, den Sinn der Telekom-Überwachung zum Zweck der Verbrechensbekämpfung in Frage zu stellen. Die aktuellen Vorkommnisse in Norwegen zeigen eindrücklich, welche Rolle heutige und künftige Kommunikationsmedien spielen können.

Auch als kleiner ISP sind wir durchaus bereit, im Rahmen unserer Möglichkeiten einen sinnvollen Beitrag zu leisten. Wir wehren uns aber 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.

Hiermit nimmt die ZAPP AG zu den vorgeschlagenen Änderungen kritisch Stellung.

Folgende Punkte stehen für uns 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 **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 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 stehen wir 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.**

Weitere Informationen finden Sie im beigelegten Arbeitspapier.

Wir danken für Ihre Kenntnisnahme

Freundliche Grüsse

ZAPP AG

A handwritten signature in black ink, appearing to read 'Schmocker', written over the printed name.

Bernhard Schmocker, Leiter Technik

VÜPF Änderungsvorlage vom 8. Juni 2011: Arbeitspapier

1 Allgemeines

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 dargestellt 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 Fernmeldediensteanbieter 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 Rechtsprechung und Praxis

Oft soll mit Gesetzesrevisionen die in der Zwischenzeit aufgelaufene, „bewährte“ Rechtsprechung ins neue Gesetz einfließen, so auch hier. In diesem Fall ist aber Skepsis angebracht. Einerseits gibt es keine gefestigte Rechtsprechung, 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 so viel: 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 daraufhin überprüfen, ob die angeordnete Massnahme von einer zuständigen Behörde aus erfolgt ist und ob es um ein Delikt gemäss des Deliktatalogs 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 Ordnungsrevision, 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 Ordnungsgeber 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 Ordnungsgeber 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. Hans Jakob, 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 Ordnungsgeber 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 unserem Verständnis 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. 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.

1.6 Fehlende Entscheidungsgrundlage 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, 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 Bemerkungen 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 Auslieferungsnetze (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. Hier wäre 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. Hans Jakob, Kommentar, N 3 zu Art. 19a VÜPF). Nach unserer Auffassung 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. Es scheint uns 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 Strohmännchen 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. Wir sind 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.

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. Hans Jakob, 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 unsere Auffassung nur die IP-Ebene gemeint sein, nicht aber Adresselemente, die in der IP-Payload enthalten sind.

Zu 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 unserem Verständnis 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.