International Working Group
on Data Protection
in Telecommunications

675.29.9 19. November 2004

Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten

- angenommen auf der 29. Sitzung am 15./16. Februar 2001 in Bangalore -
- überarbeitet und ergänzt auf der 36. Sitzung am 18./19. November 2004 in Berlin -

- Übersetzung -

Aufenthaltsinformationen wurden in mobilen Kommunikationsdiensten von Anfang an verarbeitet. Solange diese Informationen nur zum Aufbau und zur Aufrechterhaltung einer Verbindung zu dem mobilen Endgerät generiert und genutzt wurden, verfügten nur die Anbieter von Telekommunikationsnetzen, die in den meisten Ländern sehr strikt auf die Wahrung des Fernmeldegeheimnisses verpflichtet sind, über Aufenthaltsinformationen. Die Genauigkeit der Ortung richtete sich nach der Größe der betreffenden Funkzelle in den zellularen Netzwerken.

Teilweise veranlasst durch gesetzliche Verpflichtungen, präzisere Informationen über den Aufenthaltsort eines mobilen Endgerätes für Rettungsdienste verfügbar zu machen, haben die Betreiber von Netzwerken damit begonnen, die technische Infrastruktur ihrer Netzwerke zu verändern, um diese Verpflichtungen zu erfüllen. Dies bedeutet, dass in naher Zukunft wesentlich genauere Informationen über den Aufenthaltsort eines jeden mobilen Endgerätes verfügbar sein werden. Endgerätehersteller geben an, dass selbst heute eine Präzision von bis zu fünf Metern technisch möglich ist, wenn GPS-unterstützte Systeme benutzt werden. Gleichzeitig ist abzusehen, dass die Entwicklung des mobilen elektronischen Geschäftsverkehrs zur Schaffung einer Vielzahl neuer Dienste führen wird, die auf der Kenntnis des präzisen Aufenthaltsortes des Nutzers basieren. Diese Dienste werden aller Wahrscheinlichkeit nach nicht nur von Telekommunikationsdiensteanbietern, sondern auch von Dritten angeboten werden, die nicht an die gesetzlichen Beschränkungen des Fernmeldegeheimnisses gebunden sind.

Die verbesserte Genauigkeit von Aufenthaltsinformationen und ihrer Verfügbarkeit nicht nur für die Betreiber mobiler Telekommunikationsnetzwerke kann neue, bisher nicht da gewesene Risiken für den Datenschutz von Nutzern mobiler Endgeräte in Telekommunikationsnetzwerken zur Folge ha-

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.datenschutz-berlin.de

ben. Die Arbeitsgruppe hält es dafür für erforderlich, dass die Technologie zur Ortung mobiler Endgeräte in einer Weise entwickelt wird, die die Privatsphäre so wenig wie möglich beeinträchtigt.

Hinsichtlich des Angebotes von Mehrwertdiensten sollten die folgenden Prinzipien beachtet werden:

1. Der Entwurf und die Auswahl technischer Einrichtungen solcher Dienste sollten an dem Ziel orientiert sein, entweder überhaupt keine oder so wenig wie möglich personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen.

2. Präzise Aufenthaltsinformation sollte nicht als ein Standard-Leistungsmerkmal eines Dienstes generiert werden, sondern nur „nach Bedarf“, wenn dies notwendig ist, um einen bestimmten Dienst zu erbringen, der an den Aufenthaltsort des Nutzers geknüpft ist.

3. Der Nutzer muss die volle Kontrolle darüber behalten, ob präzise Aufenthaltsinformationen im Netzwerk entstehen. In dieser Hinsicht scheinen Endgeräte-basierte Lösungen, bei denen die Entstehung präziser Aufenthaltsinformation durch das mobile Endgerät initiiert wird, ein höheres Maß an Datenschutz zu bieten als Netzwerk-basierte Lösungen, bei denen Aufenthaltsinformationen als ein Standard-Leistungsmerkmal generiert und die Kontrolle des Nutzers sich darauf beschränkt, in welchem Umfang diese Informationen an Dritte übermittelt werden. In jedem Fall sollte der Mobilfunkteilnehmer immer in der Lage sein, sowohl die Inanspruchnahme jedes standortbezogenen Dienstes als auch spezieller standortbezogener Dienste zu kontrollieren. Der Anbieter sollte dem Teilnehmer die Möglichkeit einräumen, bei Abschluss des Teilnehmervertrags in die Nutzungsmöglichkeit jedes standortbezogenen Dienstes einzuwilligen. Der Teilnehmer darf bereits zu diesem Zeitpunkt oder später seine Zustimmung geben und darf die Inanspruchnahme sämtlicher Dienste jederzeit ablehnen. In Fällen, in denen der Mobilfunkteilnehmer eingewilligt hat, sollte der Mobilfunknutzer, der nicht mit dem Teilnehmer identisch ist, die Möglichkeit haben den Dienst zu akzeptieren oder abzulehnen.

4. Der Telekommunikationsdiensteanbieter darf nur in den Fällen Informationen an Dritte liefern, in denen der Mobilfunkteilnehmer zu der anderweitigen Nutzung der Aufenthaltsinformationen seine informierte Einwilligung erteilt hat. Nutzer sollten die Möglichkeit haben, die präzise Aufenthaltsbestimmung jederzeit abschalten zu können, ohne dafür die Verbindung ihres Endgerätes zum Netzwerk trennen zu müssen. Nutzer und Teilnehmer sollten auch die Möglichkeit haben, Aufenthaltsinformationen mit einem selbstgewählten Grad von Genauigkeit zu offenbaren (z. B. auf der Ebene eines einzelnen Gebäudes, einer Straße, einer Stadt oder eines Bundesstaates).

5. Aufenthaltsinformation sollte Anbietern von Mehrwertdiensten nur zugänglich gemacht werden, wenn der Nutzer seine informierte Einwilligung zu einer solchen Offenlegung erteilt hat. Die Einwilligung kann auf eine einzelne Transaktion oder bestimmte Anbieter von Mehrwertdiensten beschränkt sein. Der Nutzer muss in der Lage sein, auf Daten über seine Präferenzen zuzugreifen, diese zu berichtigen und zu löschen, unabhängig davon, ob dieseauf dem mobilen Endgerät oder innerhalb des Netzwerkes gespeichert sind.

6. Die Erstellung von Bewegungsprofilen durch Anbieter von Telekommunikationsdiensten und Anbieter von Mehrwertdiensten sollte durch Gesetz strikt verboten werden, außer wenn dies für die Erbringung eines bestimmten Dienstes notwendig ist und der Nutzer hierzu zweifelsfrei seine informierte Einwilligung gegeben hat.

7. Daten über den Aufenthaltsort stellen eine hoch sensible Kategorie von Informationen dar. Der Zugriff auf solche Informationen sowie deren Übermittlung und Nutzung sollten Gegenstand der gleichen oder gleichartiger Kontrollen sein wie für Inhaltsdaten, die durch das Fernmeldegeheimnis geschützt werden. Die Arbeitsgruppe weist auf ihren Gemeinsamen Standpunkt über die öffentliche Verantwortung im Hinblick auf das Abhören privater Kommunikation hin (Hong Kong, 15. April 1998; http://www.datenschutz-berlin.de/attachments/173/inter_de.pdf).

8. Wo immer dies möglich ist, sollten Betreiber von Mobilfunknetzen Aufenthaltsinformationen nicht zusammen mit personenbezogenen Informationen über den Nutzer an Anbieter von Mehrwertdiensten weiterleiten. Stattdessen sollten pseudonymisierte Informationen genutzt werden. Personenbezogene Informationen (z. B. die Kennung eines mobilen Endgerätes) sollten Anbietern von Mehrwertdiensten nur zugänglich gemacht werden, wenn der Nutzer seine informierte Einwilligung gegeben hat. Jegliche Aufenthaltsinformation sollte vom Anbieter gelöscht werden, sobald sie für die Erbringung des Dienstes nicht länger erforderlich ist.

9. Ein Anbieter darf die Nutzung eines Dienstes oder die Bedingungen für die Nutzung eines Dienstes nicht von der Einwilligung des Nutzers in die Verarbeitung personenbezogener Aufenthaltsinformationen abhängig machen, wenn diese Daten für die Erbringung des Dienstes nicht erforderlich sind.