

Antwort

des Ministeriums für Inneres, Sport und Integration auf die Frage der Abg. Grant-Hendrik Tonne, Daniela Behrens, Sigrid Leuschner, Wiard Siebels und Hans-Dieter Haase (SPD)

### **Erfassung von Netzdaten durch Dritte? – Teil 1?**

Die Abgeordneten hatten gefragt:

Der Medienberichterstattung zufolge erfassen Wirtschaftsunternehmen in Deutschland (u. a. Google) WLAN-Daten bzw. Netzdaten im Allgemeinen, sammeln und vermarkten diese.

Dabei soll laut Medienberichten nicht nur der Verschlüsselungsstatus der Geräte, sondern sollen auch Seriennummer (MAC-Adresse) und teilweise der vom Nutzer vergebene Name der Funkstation (SSID) erkannt und gespeichert werden.

Wir fragen die Landesregierung:

1. Welche Netzdaten werden nach Kenntnis der Landesregierung von WLAN-Routern oder ähnlichen Geräten gesendet, die von Dritten aufgefangen bzw. gelesen werden können?
2. Wie und wo können diese Daten von Dritten aufgefangen bzw. gelesen werden?
3. Hat die Landesregierung Kenntnis, dass Private bzw. Unternehmen solche Netzdaten Dritter sammeln, speichern und kommerziell verwerten?

Ich beantworte die Anfrage, unter Berücksichtigung der Stellungnahme des Landesbeauftragten für den Datenschutz (LfD), namens der Landesregierung wie folgt:

Zu 1:

Der Landesregierung ist bekannt, dass von WLAN-Routern die eindeutige Identifikation des Gerätes (MAC Adresse), der vom Nutzer vergebene Name der Funkstation (SSID) und der Verschlüsselungsstatus des Netzwerkes gesendet werden. Diese Daten können mit frei verfügbaren Programmen von jeder WLAN-Netzwerkkarte im Empfangsgebiet des WLAN ermittelt werden. Bei diesem Verfahren werden zwangsläufig Nutzdaten (Payload) temporär gespeichert und verarbeitet, die wiederum personenbezogene Daten enthalten können. Zusätzlich kann bei einem offenen und nicht verschlüsselten WLAN auch der gesamte Datenverkehr zwischen einem Netzwerkteilnehmer und dem WLAN-Router mit frei verfügbaren Programmen aufgezeichnet und teilweise im Klartext gelesen werden.

Der Landesbeauftragte für Datenschutz weist darauf hin, dass bei der Entwicklung von Technik, für den internationalen Markt, überwiegend keine datenschutzrechtlichen Belange berücksichtigt werden.

Aus diesen Gründen wird allgemein darauf hingewiesen, dass bei einem Einsatz von WLAN ein Mindestmaß an Sicherheitsvorkehrungen zu treffen ist. Hierzu zählen die Unterdrückung der SSID, die Verwendung einer nicht deskriptiven SSID (der Name sollte keinerlei verwertbare Informationen enthalten), der Einsatz einer im WLAN-Router konfigurierbaren Datenverschlüsselung sowie die Nutzung einer MAC-Filterung, um sicher zu stellen, dass nur bekannte Geräte sich an dem Netzwerk anmelden können.

Zu 2:

Die Daten können mit am Markt frei verfügbaren Programmen (teilweise Open Source Produkten), sogenannten WLAN-Sniffern und Netzwerk-Protokoll-Analyse-Werkzeugen, in der Reichweite des WLAN ermittelt werden. Die Reichweite von WLAN hängt grundsätzlich von verschiedenen Faktoren ab. Die wichtigsten sind die Räumlichkeiten, die direkte Umgebung, die Antenne, sowie auch die Sendeleistung des Gerätes. Als grobe Einschätzung gilt, dass Geräte mit normalen Antennen im Freien auf etwa 300 Meter, in Gebäuden mit dünnen Wänden auf etwa 40 Meter Reichweite kommen. Mit speziell gerichteten Antennen können auch Werte bis zu 20 Kilometer Entfernung erreicht werden.

Der Landesbeauftragte für Datenschutz hat darüber hinaus mitgeteilt, dass die lokalen Funknetze die folgenden Frequenzbereiche nutzen:

802.11a 5,15 - 5,725 GHz

802.11b/g 2,4 - 2,4835 GHz

802.11n = a und b/g

Er weist weiter darauf hin, dass man theoretisch mit jedem Funkempfänger, der die Möglichkeit hat, den oben dargestellten Frequenzbereich zu empfangen und der die entsprechenden Demodulations-/Demultiplex-verfahren beherrscht, entsprechende Signale empfangen und zur Weiterverarbeitung zur Verfügung stellen kann. In der Regel reicht es aber aus, eine handelsübliche mobile Datenverarbeitungsanlage wie Smartphone, Laptop, PDA oder PlayStation Portable mit frei verfügbarer Software (WLAN-Sniffer) auszustatten, um drahtlose Netzwerke aufzuspüren. Darüber hinaus gibt es mittlerweile auch eigens konzipierte, kompakte Embedded-Produkte für das Aufspüren von WLANs.

Im Übrigen verweise ich auf die Antwort zur Mündlichen Anfrage Nr. 37 des 35. Tagungsabschnittes am 27.05.2011.

Zu 3:

Die Landesregierung hat nach Presseberichten Kenntnis davon, dass die in Hamburg ansässige Firma Google bei der Aufnahme von Straßenpanoramen im Bundesgebiet gleichzeitig Nutzdaten von WLANs mit erfasst hat.

Der Landesregierung liegen in ihrem Zuständigkeitsbereich keine Erkenntnisse vor.

Der Landesbeauftragte für Datenschutz hat mitgeteilt, dass ihm ebenfalls keine Erkenntnisse zu Unternehmen mit Sitz in Niedersachsen vorliegen. Er weist weiter daraufhin, dass es im Bundesgebiet Firmen wie z.B. Apple Inc. gibt, die in ihrer Datenschutzerklärung darlegen, dass sowohl sie als auch Dritte in Echtzeit die präzise Standortdaten z.B. von Smartphones erheben, nutzen und weitergeben können. Die zuständigen Aufsichtsbehörden in Hamburg und Bayern prüfen z. Z. in wie weit dies rechtliche Konsequenzen haben kann.

Aufgrund der im Sitz der verantwortlichen Stellen begründeten Nichtzuständigkeit gegenüber den bisher bekannten Unternehmen bleibt dem Landesbeauftragten für den Datenschutz Niedersachsen nur die Information und Aufklärung der Bürger (s. Tätigkeitsbericht 2009/2010).