Axel Spies EU: Standortdaten der Smartphones sind personenbezogene Daten – Einwilligung der Nutzer?

MMR-Aktuell 2011, 318376

Die *Art. 29-Arbeitsgruppe* (*Working Party – WP*) ist der Ansicht, dass Standortdaten in der Regel personenbezogene Daten sind. Die kürzlich veröffentlichte „Opinion" 185 der Gruppe ist durchaus lesenswert, auch wenn sie nicht unmittelbar für die Datenschutzbehörden in der EU verbindlich ist. Die Stellungnahme geht in die technischen Einzelheiten und stellt fest, dass in vielen Fällen eine Einwilligung der Betroffenen erforderlich ist, verbunden mit der permanenten, jederzeit widerrufbaren Möglichkeit des Opt-out durch den Nutzer. Immer mehr Anwendungen der Smartphones (oder andere sog. Smart Mobile Devices, wie ein iPad) nutzen GPS (Global Position Systems) in Verbindung mit Smart Chips, um den aktuellen Aufenthaltsort zu bestimmen. Der Aufenthaltsort kann sich auch aus der Verbindung zum nächsten WiFi-Netz über die individuelle Medium Access Control (MAC)-Adresse ergeben. Wie dem auch sei – es fallen auf jeden Fall Standortdaten an, mit denen der Nutzer bis auf wenige Meter genau lokalisiert werden kann.

Risiken für den Datenschutz

Die *WP* stellt fest, dass die meisten Menschen ihr Smartphone dicht bei sich tragen und es nur in seltenen Fällen verleihen. Mithin lasse sich aus den Standortdaten ein Bewegungsprofil des Nutzers erstellen, das die *WP* „social graph" nennt. Dieses Datenschutzrisiko werde dadurch verschärft, dass diese Daten – zumindest theoretisch – weltweit online abrufbar seien.

Rechtsrahmen

Die *WP* stellt weiter fest, dass die genannten Standortdaten der EU-DatenschutzRL (95/46/EG) und der E-PrivacyRL (2002/58/EG) – letztere für die TK-Anbieter – unterfallen. Die genannten TK-Dienste seien Dienste der Informationsgesellschaft nach der E-PrivacyRL. Es handele sich um personenbezogene Daten, auch wenn der konkrete Nutzer dem Anbieter noch persönlich bekannt sei. Das gelte gleichfalls für die MAC-Adresse in Verbindung mit den Informationen über das gerade genutzte WiFi-Netz.

Interessant wird es bei der Erörterung der Frage, wer die verantwortliche Stelle (Data Controller) ist. Dies kann der Betreiber der Datenbasis sein, in bestimmten Fällen auch der Diensteanbieter (z.B. einer Smartphone-App, die eine Wettervorhersage je nach Standort zulässt), je nachdem, wer die Daten für welche Zwecke sammelt.

Rechtfertigung der Datensammlung

Die Sammlung und Verwertung der Standortdaten ist nicht per se unzulässig. Falls der Diensteanbieter die Daten nutzen will, bedarf es der vorherigen Einwilligung. Das Einholen der Einwilligung ist in machen Fällen durchaus problematisch, z.B. bei der Überwachung von Arbeitnehmern (Kurierfahrten) und der Einwilligung von Kindern, die Smartphones nutzen.

Bei Arbeitnehmern ist die *WP* besonders streng. Für ihn müsse es möglich sein, die Lokalisierungsfunktion außerhalb der Arbeitszeiten abzuschalten. Es dürfen nicht weitere Daten durch die Funktion abgegriffen werden, z.B. zur Ermittlung einer eventuellen Geschwindigkeitsüberschreitung des angestellten Fahrers. In jedem Fall muss die Zustimmung „spezifisch" sein und den Zweck der Datenverarbeitung abdecken. Die *WP* empfiehlt, dem Nutzer eine Zustimmung je nach Messdichte des Aufenthalts zu ermöglichen (Land, Postleitzahl usw.). Durch ein Symbol auf dem Bildschirm des Smartphones solle er permanent daran erinnert werden, dass die Messung seines Standorts eingeschaltet ist.

Falls Persönlichkeitsprofile erstellt werden, müssen diese dem Nutzer auf Anfrage in einem lesbaren Format zur Verfügung gestellt werden. Das Einholen der Zustimmung allein auf Grund von AGB sei nicht erlaubt. Es müsse ein explizites Opt-out zur Verfügung stehen.

Einige offene Fragen

Die gut gegliederte Analyse der *WP* leidet – nicht zum ersten Mal – darunter, dass die Analyse bestechend ist, die Schlussfolgerungen aber recht vage sind.

Die Speicherung solcher Daten sei für begrenzte Zeiträume möglich (eine genaue Zeitvorgabe gibt die Arbeitsgruppe nicht). Danach sollten diese Daten gelöscht werden. Auch sollen die TK-Anbieter die individuelle Zustimmung nach Ablauf einer „angemessenen Zeitperiode" erneut einholen. Die Speicherung zur Sicherstellung des Betriebs, z.B. von MAC- und IDID-Adressen soll max. 24 Stunden betragen. Das wird die staatlichen Ermittlungsorgane wenig freuen, für die Standortdaten der mobilen Geräte ein wichtiges Ermittlungswerkzeug sind.

Ob das Abgeben einer Zustimmungserklärung je nach Messdichte des Standorts überhaupt technisch möglich ist, wird sich zeigen. Viele Hersteller und TK-Anbieter werden sich nicht leicht damit abfinden, dass die Grundeinstellung der Smartphones und der relevanten Anwendungen die Sammlung von Standortdaten ausschließen soll: Viele Dienste und Apps sind unter solchen Umständen kaum sinnvoll einsatzfähig.

Wie ein Opt-out des Anbieters aussehen soll, ohne dass weitere personenbezogene Daten des Nutzers gesammelt werden, ist ebenfalls unklar. Was ist z.B. mit dem Nutzer, der die Standortdaten gerne für die Anzeige bestimmter Restaurants in der Nachbarschaft preisgeben will, nicht aber für andere Zwecke? Muss für alle Zwecke eine individuelles Opt-out eingeholt werden? Eine ähnliche Problematik stellt sich bei der Bereitstellung von Onlinewerbung durch Suchmaschinen.

Ein „Schmankerl" zum Schluss: Viele Kinder und Jugendliche werden der *WP* applaudieren, dass ihre Datenschutzrechte gegenüber den eigenen Eltern gestärkt werden: Nach der *WP*-Opinion (S. 15) dürfen sie nämlich keiner „Über-Überwachung" (Over-surveillance) durch die eigenen Eltern ausgesetzt werden, die wissen wollen, wo sich die Kinder gerade befinden. Das würde die „Autonomie" der Kinder reduzieren. Viele Eltern, die ihre Kinder gerade aus diesem Grund mit teuren Smartphones ausstatten, werden davon nicht begeistert sein.

■ Vgl. zu dem Themenkomplex auch die Diskussion im Beck-Blog und MMR-Aktuell 2011, 318002 m.w.Nw.

Dr. Axel Spies
ist Rechtsanwalt in der Kanzlei Bingham McCutchen in Washington DC und Mitherausgeber der MMR.