

Spies: USA: Mehr Datenschutz für Mobile Apps – Neue Leitlinien und Empfehlungen aus Kalifornien

ZD-Aktuell 2013,  
03417

## **USA: Mehr Datenschutz für Mobile Apps – Neue Leitlinien und Empfehlungen aus Kalifornien**

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

**Am 10.1.2013 hat die kalifornische Generalstaatsanwältin (Attorney General) Kamala D. Harris, die gleichzeitig die Funktion einer bundesstaatlichen Justizministerin erfüllt, eine lesenswerte Publikation mit dem Titel "Privacy On The Go: Recommendations for the Mobile Ecosystem" herausgegeben.**

Die Veröffentlichung dieser „Empfehlungen“ geschah etwa einen Monat, nachdem die kalifornische Behörde ihre erste Durchführung von Zwangsmaßnahmen nach dem Online Privacy California Protection Act (CalOPPA) von 2003, Cal. Bus & Prof. Code § 22575 et. seq. (2004), gegen ein Unternehmen eingeleitet hatte, das mobile Anwendungen in Form von Apps bereitstellt. Die Durchsetzungsverfahren in Sachen „Privacy“ insbesondere gegen App-Anbieter dürften in Zukunft verstärkt in Kalifornien auftreten. Die Empfehlungen sind deshalb von großer faktischer Bedeutung für die Anbieter.

Nach dem kalifornischen Gesetz CalOPPA ist jeder Betreiber einer Webseite oder eines Onlinedienstes, der persönliche Informationen von in Kalifornien ansässigen Verbrauchern speichert, verpflichtet, klare und deutliche Datenschutzbestimmungen zu veröffentlichen. Attorney General *Harris* hat im Jahr 2012 mehrere Versuche unternommen, um die Anwendung und Durchsetzung dieses Gesetzes für mobile Anwendungen sicherzustellen. Im Februar 2012 vermittelte sie eine Vereinbarung, um die mit mobilen Diensten befasste Industrie in Einklang mit CalOPPA zu bringen. Im Juli 2012 setzte der Staat Kalifornien eine neue Privacy Enforcement and Protection Unit ein. Attorney General *Harris* ließ im Herbst 2012 ihre Behörde dann formelle Benachrichtigungen an Unternehmen verschicken, die mobile Apps anbieten, um diese auf mögliche Verstöße gegen CalOPPA und die Konsequenzen hinzuweisen. Im Dezember 2012 leitete die Behörde erstmalig ein Klageverfahren gegen *Delta Airlines* ein.

Da CalOPPA und andere Datenschutzgesetze zu einer Zeit verabschiedet wurden, da die mobile Technologie noch nicht so verbreitet war wie gegenwärtig, bleibt abzuwarten, wie CalOPPA von den Gerichten bei der Entscheidung von Fragen der Anwendungen auf solche Technologien ausgelegt werden wird. In der Zwischenzeit werden die genannten Empfehlungen der *Attorney General* Anwendung finden und die Schwerpunkte der Kontrolle durch die Strafverfolgungsbehörden definieren.

In der o. g. Publikation führt die *Attorney General* aus: „Wir bieten dieses Paket von

Empfehlungen für die „Privacy-Practice“ für App-Entwickler und andere zur Unterstützung an, damit der Schutz der Privatsphäre in der Entwicklung möglichst frühzeitig Berücksichtigung finden kann.“ Die Empfehlungen wurden in Absprache mit einem breiten Kreis von Interessenten (Stakeholders) entwickelt und erkennen die Bedeutung von Innovation in Form einer Balance zwischen Innovation und Privatsphäre an. Die Empfehlungen sind nicht auf App-Entwickler beschränkt, sondern gelten auch für andere Akteure im mobilen „Ökosystem“, wie Softwareentwickler, Plattform-Anbieter, Werbenetzwerke, Entwickler von Betriebssystemen und Mobilfunkbetreiber. Die Empfehlungen beinhalten u. a. konkrete Anleitungen für mobile Werbeangebote auf Smartphones, um sog. Out-of-App-Anzeigen zu vermeiden, zur Änderung von Browser-Einstellungen oder zur Platzierung von Symbolen auf dem mobilen Desktop. Ziel ist der Datenschutz und Datensparsamkeit bei der Benutzung sog. Unified Identifikatoren (UID). Vorgeschlagen werden in dem Dokument auch interne Datenschutzrichtlinien (privacy policies) für App-Entwickler und App-Anbieter zu Gunsten von Endnutzern.

Die Empfehlungen beinhalten weiterhin spezifische Leitlinien zu einigen speziellen Datenschutzfragen, die zurzeit diskutiert werden. Z. B. vertreten die Verfasser die Auffassung, dass Geräte-Identifikatoren (Unique Device Identifiers – UDI) innerhalb der Definition von personenbezogenen Daten (personally identifiable data) des Gesetzes anzusiedeln sind. Dies ist in den USA noch häufig umstritten. Nach dem CalOPPA gelten als personenbezogene Daten:

- Vor- und Zuname einer Person
- Wohnungsadresse
- E-Mail-Adresse
- Telefonnummer
- Sozialversicherungsnummer
- jedes andere Identifikationsmerkmal, das es erlaubt, die Person physisch oder online zu kontaktieren
- Informationen, die eine Website über einen Nutzer online sammelt und in persönlich identifizierbarer Form in Kombination mit den o. g. Daten bereithält oder speichert.

Abgesehen von dieser Klarstellung ist die *Generalstaatsanwaltschaft* auch der Auffassung, dass Standortdaten (Geolocation-Daten) unter die Definition von sensiblen Informationen zu subsumieren sind. Diese Rechtspositionen dürften auf andere Foren, die diese Fragen diskutieren, Einfluss haben, z. B. auf die *National Telecommunications and Information Administration* (NTIA), die an das *US-Justizministerium* angebunden ist und ebenfalls an Verhaltenskodizes für den Datenschutz auf Bundesebene arbeitet.

Die *Generalstaatsanwaltschaft* empfiehlt außerdem ein Konzept der „Überraschungsminimierung“. In diesem Zusammenhang nennt sie konkrete Schritte, um Überraschungen der Verbraucher zu vermeiden, falls eine App, die sie herunterladen, persönliche Daten speichert, die nicht notwendig sind, um die grundlegenden Funktionen der App zu gewährleisten. Zur frühzeitigen Vermeidung solcher Überraschungen empfiehlt sie besondere Maßnahmen und Hinweise in der Privacy Policy zu einem möglichst frühen Zeitpunkt und im relevanten Kontext. Die *Generalstaatsanwaltschaft* befürwortet außerdem den Einsatz von „besonderen Datenschutzerklärungen“, um dem Verbraucher überraschende Praktiken aufzuzeigen und die es den Nutzern erlauben zu überprüfen, welche Datenschutzeinstellungen er vorgenommen hat und wie er diese unkompliziert ändern kann. Sie mahnt weiterhin zu besonderer Vorsicht, wenn Unternehmen Daten von Kindern unter 13 Jahren sammeln oder verarbeiten. Diese Verarbeitung ist nur dann zulässig, wenn sie mit dem Children Online Privacy Protection Act (COPPA), der kürzlich geändert wurde, im Einklang steht.

Schließlich erkennt die *Attorney General* an, dass die genannten Empfehlungen über die bestehenden Verpflichtungen nach verschiedenen Datenschutzgesetzen hinausgehen können. Allerdings zeigt die Behörde nicht auf, welche Empfehlungen nach ihrer Ansicht auf Grund der bestehenden Gesetze zwingend sind und welche nicht. Demgemäß gibt es eine Grauzone, wann die *Generalstaatsanwaltschaft* oder andere Strafverfolgungs- und Regulierungsbehörden Rechtsverstöße bei Nichteinhaltung der Empfehlungen ahnden können und wann nicht. So kann die Umsetzung von Maßnahmen wie die genannten „besonderen Datenschutzerklärungen“ zu ungeklärten Konsequenzen bei der Anwendung des CalOPPA führen. Z. B. stellt sich die Frage, wo und wie die Erklärung platziert werden muss und wann Weblinks (z.B. eine Verlinkung zur Webseite des Unternehmens) für Privacy Policies zulässig sind. In Anbetracht dieser Entwicklungen kann nur dringend empfohlen werden, dass derjenige, der mit Apps in Kalifornien Geschäfte machen will, seine Datenschutzrichtlinien und Datenschutzpraktiken genau daraufhin überprüft, ob sie mit den Empfehlungen der *Attorney General* im Einklang stehen.

#### **Weiterführende Links**

Vgl. zum Datenschutz bei Apps ZD-Aktuell 2012, 02958; *Schütze*, ZD-Aktuell 2012, 02833; zu den neuen Datenschutz-Prinzipien – Consumer Privacy Bill of Rights *Spies*, ZD-Aktuell 2012, 02788 und *Spies*, ZD-Aktuell 2012, 02918.