verbraucherzentrale Bundesverband

26. November 2012

Mobile Commerce via Smartphones & Co.

Erwartungen des Verbraucherzentrale Bundesverbandes an eine verbraucherfreundliche Ausgestaltung des Mobile Commerce

Positionspapier

Verbraucherzentrale Bundesverband e.V. (vzbv)
Fachbereich Wirtschaft und Internationales
Markgrafenstr. 66
10969 Berlin

wirtschaft@vzbv.de
www.vzbv.de

Telefonieren war gestern. Mobiles Shoppen, Lokalisieren und Bezahlen sind neben der Nutzung Sozialer Netzwerke mittels Smartphone die Hits von heute. Die besondere Attraktivität von Smartphones und der damit erreichbaren Dienste und Anwendungen (Apps) besteht darin, diese rund um die Uhr zu jeder Zeit und überall nutzen zu können.

Ein Ende der Innovation im Bereich Mobile Commerce ist ebenso wenig absehbar wie der Kreativität beim Entwickeln weiterer Diensteangebote Grenzen gesetzt sind. Das gilt auch und gerade für das Mobile Shopping, das Mobile Payment und die Nutzung der Geo-Lokalisierung. Zwar ist auch heute schwer absehbar, was da noch alles auf die Nutzer zukommt. Trotzdem erscheint es lohnend, vor dem Hintergrund entsprechender Zukunftsprognosen frühzeitig und unabhängig von existierenden gesetzlichen Regelungen und Selbstverpflichtungen der Branche spezielle Anforderungen an eine verbraucherfreundliche Ausgestaltung des Mobile Commerce zu formulieren.

Grundsätzliche Anforderungen

- **Hoheit des Nutzers über die Verwendung seiner persönlichen Daten**: Nutzer müssen grundsätzlich darüber informiert und nach ihrer Einwilligung gefragt werden, ob und welche persönlichen Daten für welchen Zweck erhoben und verwendet und/oder an Dritte übermittelt werden dürfen. Die Einwilligung muss gesondert erfolgen und aktiv erteilt werden. Eine Koppelung von Einwilligungen zu anderen Vertragszwecken an die Nutzung bestimmter Dienste ist nicht zulässig. Eine für die Nutzer nicht erkennbare automatische Datenerhebung muss ausgeschlossen sein. Die Nutzer haben das Recht, jederzeit Auskunft in einer für sie verständlichen Weise über ihre gespeicherten Daten zu verlangen. Personenbezogene Daten müssen nach Erfüllung des Nutzungszwecks vom Anbieter unverzüglich gelöscht werden. Die Nutzer müssen die praktische Möglichkeit erhalten, das bestehende Recht auf Löschung gespeicherter Daten jederzeit selbst auszuüben beziehungsweise die Löschung veranlassen zu können sowie eine entsprechende Bestätigung zu erhalten.

- **Privacy by Design und Privacy by Default:** Hersteller von Geräten, Betreiber von App Stores und die Entwickler von Apps sollen bei der Entwicklung von Geräten, Betriebssystemen und Apps ein hohes Maß an Sicherheit und Datenschutz in die Geräte beziehungsweise Anwendungen integrieren. Standardmäßig sollen Geräte und Dienste in der Art voreingestellt sein, dass sie sich auf die Verwendung der für den Dienst unbedingt erforderlichen Daten beschränken. Dieses muss auch bei der Nutzung transparent werden.

- **Einheitliche Richtlinien für App-Entwickler und Informationen über Zugriffsrechte:** Die Betreiber von App Stores sollen verbindliche Vorgaben in datenschutz- und verbraucherschutzrechtlicher Hinsicht

für die Entwicklung von Apps aufstellen. Die Betreiber sollten Apps mit offensichtlich bestehenden Sicherheitsmängeln nicht in ihren App Stores anbieten. Des Weiteren müssen den Nutzern vor dem Herunterladen einer App alle datenschutzrelevanten Informationen gegeben werden, so zum Beispiel welche Zugriffsrechte sie einer App bei deren Nutzung erteilen.

- **Systemimmanente IT-Sicherheit auf hohem Niveau:** Die zunehmende Integration von sicherheitsrelevanten Alltagsfunktionen (Mobile Shopping, Mobile Banking) auf einem mobilen Endgerät erfordert Sicherheitssysteme auf hohem Niveau unter Gewährleistung der Nutzbarkeit (usability) der betreffenden mobilen Anwendungen. Im Fall von Datenlecks müssen die Nutzer unmittelbar informiert werden. Sicherheitslücken müssen unverzüglich geschlossen werden, und zwar vom Betriebssystemhersteller und/oder Anbieter der fraglichen sicherheitsrelevanten App (zum Beispiel für Mobile Payment). Andernfalls haften die Anbieter verschuldensunabhängig für den Schaden, der dem Nutzer entstanden ist.

- **Wesentliche Informationen dem Medium oder Endgerät angemessen gestalten:** Die wesentlichen Informationen für die Nutzer und/oder Einwilligungserklärungen müssen so gestaltet sein, dass sie dem Medium beziehungsweise den Endgeräten angemessen zur Kenntnis genommen werden können. Hersteller von Geräten, Betreiber von App Stores und die Entwickler von Apps müssen im Rahmen der Nutzung ihrer Produkte beziehungsweise ihrer Dienste stets für transparente und verständliche Informationen sowie für eine umfassende Aufklärung über die Rechte der Nutzer sorgen.

- **Wettbewerbsregeln und deren Durchsetzung an technische Entwicklung anpassen:** Gesetzgeber und Aufsichtsbehörden müssen der fortschreitenden Verbreitung von *Lock.in*- Geschäftsmodellen und der Möglichkeit, Inhalte von Drittanbietern zu blockieren, wirksam entgegentreten.

- **Gesetzeskonforme Umsetzung und Marktbeobachtung sicherstellen:** Umsetzungsdefizite und Veränderungen des Marktes müssen schnell aufgedeckt und beseitigt werden. Hier ist zu prüfen, ob die vorhandenen Instrumente wie zum Beispiel die kollektive Rechtsdurchsetzung ausreichen oder zusätzliche, zum Beispiel ein Marktwächter, gebraucht werden.

- **Verbraucherbildung stärken:** Der Bedarf an Orientierung und Informationen für die Verbraucher im Bereich des Mobile Commerce ist sowohl durch die schnellen technischen Entwicklungen als auch die sich laufend verändernden Geschäftsmodelle sehr groß. Der Verbraucherzentrale Bundesverband wird daher das Thema auch im Rahmen seines Einsatzes für eine umfassende Verbraucherbildung noch stär-

ker berücksichtigen. Alle Akteure (Bund, Länder, Schulen, Verbraucherzentralen und Wirtschaft) müssen dazu einen Beitrag leisten.

Zusätzliche Anforderungen an Geo-Lokalisierung

- **Eindeutige Anzeige eines jeden Lokalisierungsvorgangs auf dem Gerät:** Eine für den Nutzer nicht erkennbare automatische Datenerhebung oder und/oder Ortung muss ausgeschlossen werden.

Zusätzliche Anforderungen an Mobile Shopping

- **Wissen, was man tatsächlich erwirbt:** Anbieter sollten Möglichkeiten entwickeln, dem Nutzer vor seiner Kaufentscheidung eine „virtuelle Anprobe“ einzurichten.

Zusätzliche Anforderungen an Mobile Payment

- **Besondere Sicherheitsanforderungen beim Bezahlen via Smartphone:** Die heute schon verschärften Sicherheitsstandards beim Online-Banking und bei Online-Zahlungen dürfen beim Mobile Payment keinesfalls unterschritten werden (Zwei-Wege-Autorisierung). Auch beim kontaktlosen Bezahlen muss der Nutzer Herr seines Portemonnaies bleiben. Welcher Betrag mit welchem Mittel bezahlt wird, muss vom Nutzer aktiv zu bestätigen sein.

- **Kein Abwälzen des Haftungsrisikos auf den Nutzer:** Das Haftungsrisiko zum Beispiel infolge von Missbrauch, Prozessfehlern beziehungsweise Fehlfunktionen oder Funktionsausfällen darf nicht auf den Nutzer abgewälzt werden. Das geltende Zahlungsverkehrsrecht ist einzuhalten. Für den Nutzer nicht erkennbare Systemmängel oder -lücken dürfen ihm nicht zugerechnet werden.

- **Standards für neue Bezahlformen:** Neue Bezahlformen sollten auf standardisierten Verfahren aufsetzen, die dem Nutzer ermöglichen, seinen Zahlungsdienstleister frei zu wählen, der gegebenenfalls unabhängig von dem des Händlers sein kann. Nur so kann dauerhaft ein funktionierender Preis- und Leistungswettbewerb ermöglicht werden.

- **Funktionierenden Wettbewerb bei neuen mobilen Zahlungssystemen sichern:** Mobile Payment und mobiles Bezahlen brauchen einen zukunftsfähigen und funktionierenden Wettbewerb. Sicherheitsanforderungen dürfen kein Wettbewerbshindernis schaffen. Wettbewerb darf keinen Anlass bieten, Umgehungen zu programmieren, mit denen günstigere Zahlungen vom Nutzer auf Kosten der Sicherheit und des Datenschutzes des Nutzers gestaltet werden.