12. März 2014

Untersuchung von Apps

Zugriffsberechtigung, Kontaktmöglichkeiten, Verbraucherinformationen und In-App-Käufe

Eine Untersuchung des Projekts „Verbraucherrechte in der digitalen Welt“ des Verbraucherzentrale Bundesverbandes (vzbv)

Verbraucherzentrale Bundesverband e.V.
Projekt „Verbraucherrechte in der digitalen Welt“
Markgrafenstr. 66
10969 Berlin
www.surfer-haben-rechte.de
surfer-haben-rechte@vzbv.de
Twitter: @surferrechte

Gefördert durch:
Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Inhaltsverzeichnis

Zusammenfassung

Eine Untersuchung des vom Bundesverbraucherministerium finanziell geförderten Projekts „Verbraucherrechte in der digitalen Welt“ des Bundesverbandes Verbraucherzentrale (vzbv) hat ergeben, dass sich die Zugriffsberechtigungen von Apps, denen der Verbraucher vor dem Herunterladen einer App zustimmen muss, nicht immer auf das für die Nutzung der App erforderliche Maß beschränken. Oft bleiben die Verbraucher im Dunkeln, weshalb Apps bestimmte Berechtigungen einfordern. Entsprechende Anfragen bei den Anbietern werden überwiegend gar nicht oder völlig unzureichend beantwortet. Die meisten App-Anbieter haben ihren Firmensitz auch im außereuropäischen Ausland. Das kann ein Grund sein, dass die Firmenstrukturen wenig nachvollziehbar und die verantwortlichen Anbieter nur mit unverhältnismäßig großen Aufwand zu ermitteln sind. Vereinzelt überprüfte Apps haben darüber hinaus gezeigt, dass In-App-Käufe auch im zweistelligen hochpreisigen Eurobereich angeboten werden und darüber hinaus auch vollwertige Shopfunktionen integriert sind, in denen reale Produkte gekauft werden können.

I. Einleitung und Problembeschreibung

Die Nutzung von internetfähigen Handys steigt rasant. Im Oktober 2013 haben 37 Millionen Deutsche ein Smartphone genutzt.[1] Einher mit dieser Entwicklung geht der App-Markt. Apps (Applikationen) sind mobile Anwendungsprogramme mittels derer der Nutzer spezielle Dienste wie beispielsweise Nachrichten, Wetterinformationen oder Unterhaltung auf sein Smartphone herunterladen kann.

In Deutschland nutzen 83 Prozent der Smartphone-Besitzer Apps. Im Jahr 2012 wurden in Deutschland 1,7 Milliarden Apps heruntergeladen.[2] Weltweit werden es mehr als 1,8 Millionen Apps angeboten. Wie Apple kürzlich bekannt gab, haben Apple-Nutzer im „App Store“ im Jahr 2013 insgesamt mehr als zehn Milliarden US-Dollar ausgegeben. Google soll bei seinen App-Downloads zahlenmäßig sogar noch vor Apple liegen und seinen Marktanteil weiter ausgebaut haben.[3] Das zeigt, dass Apps ein nicht zu unterschätzender Wirtschaftsfaktor sind. Die Europäische Kommission spricht in ihrem aktuellen Bericht sogar von einem „App-Boom“: Fast 5 Millionen neue Arbeitsplätze und 63 Milliarden Euro Umsatz sind im europäischen App-Sektor bis zum Jahr 2018 zu erwarten.[4]

Apps werden nicht nur zum Freizeitvertreib in Form von Spielen, Sport und Unterhaltung genutzt. Sie bieten Verbrauchern eine große Chance, den Alltag unabhängig von Zeit und Raum zu begleiten und zu erleichtern. Das Auffinden der nächsten Tankstelle, der Abruf des aktuellen Fahrplans der Bahn, das Einloggen ins E-Mail-Postfach von unterwegs oder das Bezahlen des Parktickets sind nur einige wenige Beispiele hierfür.

Entwickler, die ihre Apps kostenlos oder niedrigpreisig zur Verfügung stellen, suchen Refinanzierungsquellen, in dem sie Werbung während der Nutzung einer App einblenden oder auch sogenannte In-App-Käufe, das heißt kostenpflichtige Käufe innerhalb der App, anbieten. Vielfach zahlen die Nutzer auch mit ihren Daten, mal mehr, mal weniger freiwillig.

---

[1] Statista, Anzahl der Smartphone-Nutzer in Deutschland in den Jahren 2009 bis 2013 (in Millionen): http://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/

[2] Presseinformation des Bitkom vom 26.03.2013, Rekord bei App-Downloads: http://www.bitkom.org/de/themen/64026_75628.aspx

[3] Stuttgarter Zeitung vom 08.01.2014, Apple verbucht Download-Rekord: http://www.stuttgarter-zeitung.de/inhalt.app-store-apple-verbucht-download-rekord.710b7928-9941-4cfc-a34f-156d4120053d.html

[4] Pressemitteilung der Europäischen Kommission vom 13.02.2013, App-Boom, Laut EU-Bericht fast 5 Millionen neue Arbeitsplätze und 63 Mrd. EUR. Umsatz im europäischen App-Sektor bis 2018: http://europa.eu/rapid/press-release_IP-14-145_de.htm

Nicht ungewöhnlich sind Zugriffe der Apps zum Beispiel auf Adress- und Standortdaten der Nutzer, den Browserverlauf oder die Identifikationsnummer des Gerätes. Der Zugriff eines Messenger-Dienstes auf die Telefonkontakte oder die Erhebung von Standortdaten bei einer Navigationsapp ist soweit noch nachvollziehbar. Aber ob eine Spiele-App tatsächlich einen dauerhaften Internetzugang für das Betreiben des Spiels benötigt oder doch nur, um Werbung auf die App einzuspielen, bleibt für viele Nutzer unklar.

Ob die Daten für eigene Werbung oder Marketing des App-Anbieters genutzt werden, mit anderen Daten zusammen geführt oder gar an Werbenetzwerke weiter gegeben werden sollen, entzieht sich also oftmals der Kenntnis der Verbraucher. Hinzu kommt, dass die meisten Verbraucher eine Vielzahl an unterschiedlichen Apps auf Ihren Endgeräten installiert haben. Hier ein Standortdatum, dort das Alter und das Gewicht des Verbrauchers, ein kleiner Blick der App auf die Kontaktliste des Nutzers, Einsichtnahme in die Seriennummer des Endgeräts: Alles in allem handelt es sich zwar „nur“ um einzelne Daten, aber diese einzelnen Daten an irgendeiner Stelle von irgendwen zusammengeführt und verknüpft, ergeben am Ende ein umfassendes Profil einer Person, deren Lebensgewohnheiten, Verhalten, Bewegungsmuster und Wohnort genauestens analysiert und für andere Zwecke ohne ihr Wissen und Einverständnis genutzt werden können. Aus dem X-Unbekannt wird sodann ein X-Sehrbekannt.

Daher ist es wichtig, dass Verbraucher in die Lage versetzt werden, zu beurteilen, wann und welche ihrer Daten für die Nutzung einer App erforderlich sind und in welchen Fällen womöglich andere Interessen des Anbieters dahinter stecken könnten. Die für den Verbraucher nötige Beurteilungsgrundlage kann nur durch eine vollständige und für den Verbraucher verständliche Information durch den App-Anbieter gebildet werden.

II. Untersuchungsgegenstand und Methode

Das Projekt des Verbraucherzentrale Bundesverbandes (vzbv) hat die Zugriffsberechtigungen von insgesamt 50 Apps für Smartphones untersucht. Die Untersuchung beschränkte sich in erste Linie auf Berechtigungen der Apps, denen der Nutzer vor dem Herunterladen zustimmen muss. Die einzelnen Berechtigungen umfassten unter anderem Zugriffe auf Kontaktlisten und Kalender, aber auch Standortdaten. Als Kriterium für die Auswahl der Apps dienten die „Top Charts“ des Google Play Stores, die in dem Zeitraum vom 24.02.2014 bis zum 05.03.2014 zum Herunterladen zur Verfügung standen. Die Auswahl war hierbei relativ identisch mit den häufig im iTunes Store von Apple

heruntergeladenen Apps. Bei der Auswahl handelte es sich, mit Ausnahme von 10 Apps aus anderen Kategorien, überwiegend um kostenlose und kostenpflichtige Spiele-Apps. Gegenstand dieser Untersuchung war hingegen nicht, ob und welche Apps außerhalb der vom Nutzer erteilten Berechtigungen die Daten tatsächlich auch anderweitig nutzen.

Ferner legte das Projekt auch ein besonderes Augenmerk darauf, ob und welche Kontaktmöglichkeiten Verbrauchern angeboten wurden, um sich mit Fragen zur App, aber auch zu den Berechtigungen, an den Anbieter der App zu wenden. Im weiteren Fokus standen auch die Reaktionen auf die Anfragen und ob die Fragestellungen zumindest zufriedenstellend beantwortet wurden.

Darüber hinaus prüfte das Projekt exemplarisch einzelne Apps auf geeignete Verbraucherinformationen im Hinblick auf die wesentlichen Inhalte der App, einschließlich etwaiger In-App-Kaufangebote, sowie die textlichen Länge von Allgemeinen Geschäftsbedingungen (AGB).

Da im Apples iTunes Store vor dem Herunterladen und der Installation die Berechtigungen nicht dargestellt werden, beschränkte sich die Überprüfung auf 13 Apps für das Betriebssystem iOS im Hinblick auf etwaige im Nachhinein zu erteilende Berechtigungen sowie Kontakt- und Verbraucherinformationen.

Die Einzelheiten sind der Anlage 2 dieses Dokuments zu entnehmen.

Bereits im August 2013 hatte das Projekt 32 Kinder-Apps überprüft. Der Untersuchungsbericht und das Forderungspapier stehen auf der Seite www.surfer-haben-rechte.de zur Verfügung.[5]

III. Untersuchungsfelder im Einzelnen

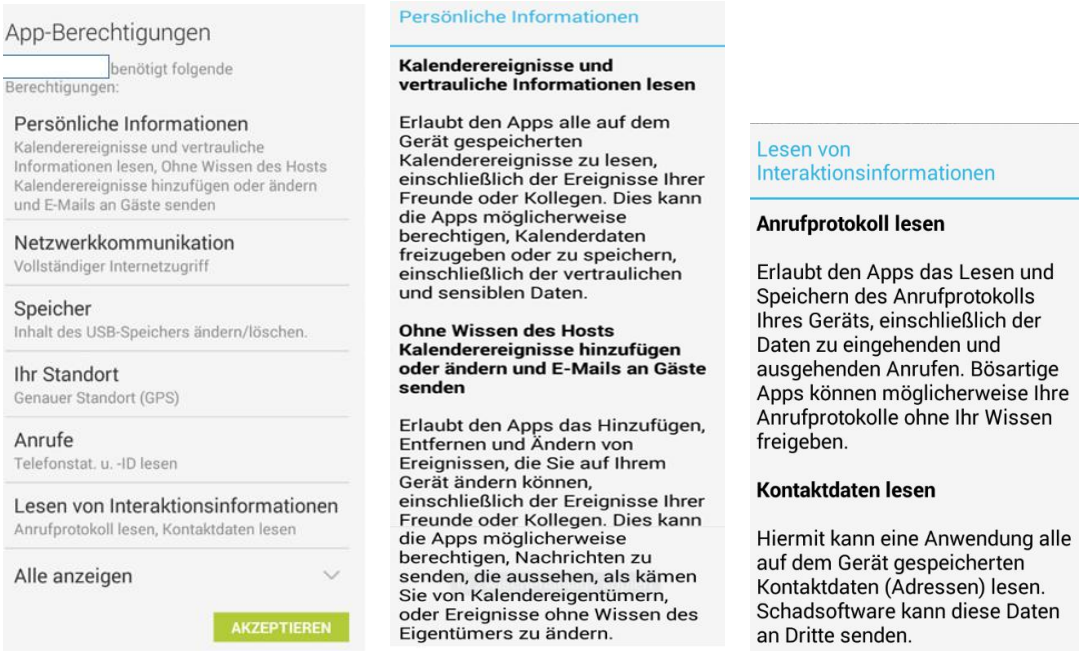
1. Zugriffsberechtigungen von Apps

Apps im Google Play Store

Untersuchungsgegenstand waren in erster Linie die Zugriffsberechtigungen der Apps, denen der Verbraucher vor dem Herunterladen und der Installation der Apps auf sein Endgerät

[5] Vzbv, Untersuchungsbericht zu Kinder-Apps: http://www.surfer-haben-rechte.de/cps/rde/xbcr/digitalrechte/Untersuchungsbericht_Kinder-Apps_final.pdf
Anforderungen an Kinder-Apps: http://www.surfer-haben-rechte.de/cps/rde/xbcr/digitalrechte/Positionspapier_Kinder-Apps_final.pdf

zustimmen muss. Nach der Auswahl einer App im Google Play Store und dem Betätigen des Installationsbuttons öffnet sich ein separates Fenster, das im Einzelnen die Berechtigungen einer App auflistet. Beim Anklicken einer der Berechtigungen erfolgt eine weitere dort hinterlegte Erklärung:

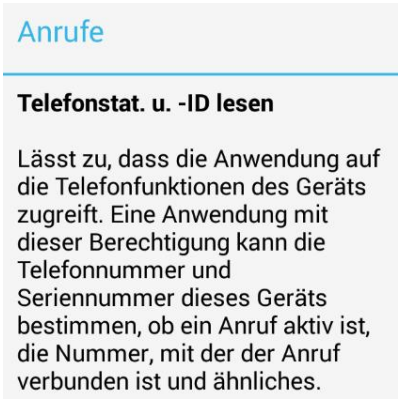


Sofern der Verbraucher den Button „Akzeptieren“ betätigt und damit sein Einverständnis in die genannten Zugriffsrechte der App erklärt, wird die App auf das Endgerät des Nutzers heruntergeladen und installiert.

Der Berechtigungsumfang einzelner Apps ist sehr unterschiedlich und variiert auch nach Art und Umfang einer App. Wenige Apps benötigen gar keine bis nur 2-3 Berechtigungen, andere verlangen bis zu 12 Berechtigungen. Bei Messenger-Diensten, die in erster Linie zum Beispiel auch Telefonate und das Versenden von Fotos ermöglichen, kann ein Zugriff auf die Kontaktdaten sinnvoll sein. Wenn sich darüber auch Termine verwalten lassen, dann ist auch ein Zugriff auf den Kalender des Nutzers berechtigt.

Nach Auffassung des Projekts ist auffällig, dass sich diese Zugriffberechtigungen oft nicht auf das für die Nutzung der App erforderliche Maß beschränken. So ist zum Beispiel nicht nachvollziehbar, weshalb eine Spiele-App auf Standortdaten zugreifen oder Audioaufnahmen aufzeichnen will und der Spielbeschreibung dazu keine Erklärung zu entnehmen ist.

Für fragwürdig hält das Projekt auch die nachfolgende Berechtigung, den Telefonstatus und zugleich die Telefon–ID lesen zu dürfen.



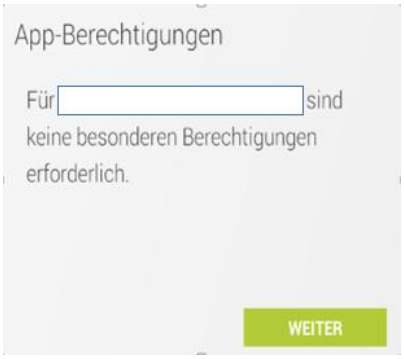
Auf der einen Seite mag es bei bestimmten Apps gerechtfertigt sein, auf die Telefonfunktionen des Endgeräts zuzugreifen. Denn wird der Verbraucher bei der Nutzung einer App zum Beispiel angerufen, so erkennt die App diesen Anruf, pausiert und speichert die Inhalte ab. Demgegenüber lässt sich meistens nicht nachvollziehen, weshalb dieses Zugriffsrecht auch das Auslesen sensibler Mobiltelefon-Identifikatoren wie IMEI[6] und IMSI[7] ermöglicht. Immerhin können anhand dieser eindeutigen Daten Rückschlüsse auf den Teilnehmer und das Mobilfunkendgerät gezogen werden. Fast alle überprüften Apps erfordern diese gekoppelte Berechtigung und verlangen undifferenziert das Einverständnis der Nutzer.

Das Problem an dieser zwangsgekoppelten Berechtigung (Telefonstatus und –ID lesen) ist, dass weder der Nutzer, noch der App-Entwickler eine Differenzierung vornehmen könnte. Denn bislang gibt Google den Entwicklern die Art und Kategorien der einzelnen Berechtigungen vor. Sofern der Entwickler für die störungsfreie Nutzung seiner App auf den Telefonstatus zugreifen muss, meldet er diese Berechtigung gegenüber Google an. Da diese Berechtigung zugleich auch das Lesen der Telefon-ID beinhaltet, wird ihm diesbezüglich auch dieses Zugriffsrecht eingeräumt. Insofern würde die Trennung dieser beiden Berechtigungen, die aus Sicht des Projekts nicht zwingend miteinander verbunden sein müssen, zu einer Entschärfung des Problems führen.

Untersuchungsgegenstand war nicht, ob und welche konkreten Zugriffe auf bestimmte Informationen und Daten des Mobilfunkgeräts genommen wurden. Aber allein die Tatsache, dass sich App-Anbieter teils nicht nachvollziehbare Berechtigungen einräumen lassen und wenn auch nur theoretische Zugriffsrechte auf bestimmte Daten der Nutzer haben, trägt nicht zur Transparenz bei und gibt einen faden Beigeschmack. Bei derart weitreichenden Zugriffsrechten auf teils hoch sensible Daten der Nutzer, könnten durchaus Begehrlichkeiten nicht nur bei den Anbietern, sondern auch bei Dritten wie Werbenetzwerken und –

[6] Bundesamt für Sicherheit in der Informationstechnik, Kommunikation in GSM-Mobilfunknetzen: https://www.bsi.bund.de/DE/Publikationen/Studien/anonym/kommunikationgsm.html:
IMEI (International Mobile Equipment Identity): Geräteidentifizierung anhand einer 15-stelligen Seriennummer
https://www.bsi.bund.de/DE/Publikationen/Studien/anonym/kommunikationgsm.html:
IMSI (International Mobile Subscriber Identity): Identifizierung des Teilnehmers

vermarktern entstehen. Schließlich finanzieren sich viele Apps auch durch Werbung, das heißt je passgenauer sie auf der Grundlage der von ihnen erhobenen Daten Werbung auf den Endgeräten der Nutzer ausliefern können, desto größer ist der wirtschaftliche Vorteil.



Demgegenüber hat die Überprüfung auch gezeigt, dass es Apps gibt, die sich wenige bis hin gar keine Berechtigungen einräumen lassen. Doch das ist der Einzelfall. Fast alle Apps lassen sich von den Nutzern Zugriffsrechte einräumen. Doch in den wenigsten Fällen ist für den Nutzer nachvollziehbar, wozu einzelne Berechtigungen erforderlich sind. Teils machen Berechtigungen Sinn, wie die Erhebung von Standortdaten bei Navigationsapps, bei Spielen weniger.

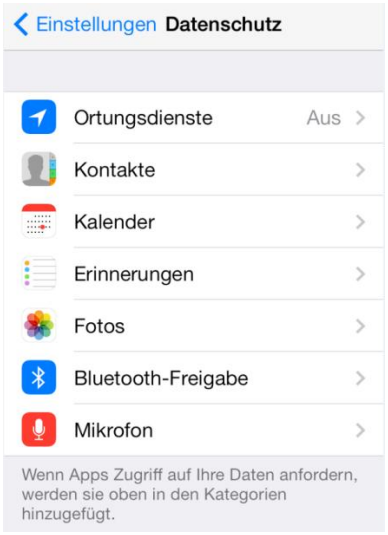
Oft ist es nicht eine einzelne Berechtigung, die kritisch zu werten ist. Problematisch kann es dann werden, wenn innerhalb einer App unterschiedliche Berechtigungen eingeräumt werden oder die Daten wie Informationen über Anruferlisten, Mobilfunkgeräte-Identifikatoren und Standortdaten aus unterschiedlichen Quellen zusammengeführt werden. Dies ist besonders dann der Fall, wenn ein Werbenetzwerk die Anzeigen in verschiedenen Apps ausliefert und gleichzeitig über diese verschiedenen Apps die Daten des Nutzers sammelt. Hierin besteht die Gefahr, dass ein aussagekräftiges Profil des Nutzers entsteht. Letztlich kann sich der Nutzer dieser Datensammelei nur mit hohem technischen Wissen und Aufwand entziehen, es sei denn, er entscheidet sich gegen die Installation der App. Denn eine Einzelauswahl oder „Abwahl“ einzelner Berechtigungen, die für die Nutzung der App entbehrlich sind, ist derzeit bei einer Standardinstallation von Android nicht möglich. Entweder der Nutzer akzeptiert die vorgegebenen Berechtigungen im vollen Umfang oder er lässt die Finger davon.

Apps in Apples iTunes Store

Nutzer des Apples iTunes Stores werden vor dem Download von Apps nicht vorab über etwaige Zugriffsrechte einer App auf das System des Endgeräts oder die Daten der Nutzer informiert, geschweige denn, dass sie vorab den Zugriffsrechten zustimmen.

Andererseits ist das Betriebssystem iOS auf dem Endgerät des Nutzers standardmäßig datenschutzfreundlicher voreingestellt (sogenanntes privacy by default). Das heißt, dass der App per se einige Zugriffsrechte wie Standortdaten, Kontakte, Kalender, Fotos und Mikrofon entzogen sind. Der Nutzer hat sodann die Möglichkeit, jeder einzelnen App die gewünschte

Berechtigung zu erteilen (sogenannte opt-in-Lösung). Auf der anderen Seite lässt sich über das Betriebssystem auch nachprüfen, ob und welche Berechtigungen für einzelne Apps vorgesehen sind. Zum Beispiel sind beim Aufruf der Unterkategorie „Ortungsdienste“ zunächst alle Apps aufgeführt, die diese Daten erheben wollen. Dennoch ist diese Funktion zunächst deaktiviert, das heißt, der Nutzer muss generell den Zugriff auf Ortungsdienste freigeben und darüber hinaus jeder einzelnen App ein Zugriffsrecht einräumen.



2. Kontaktmöglichkeiten

Ein besonderes Augenmerk dieser Untersuchung lag auch auf den Kontaktmöglichkeiten zum Anbieter einer App. Hierbei wurde kontrolliert, ob dem Verbraucher einfache zugängliche Anlaufstellen zur Verfügung stehen, um sich mit seinem Anliegen oder beispielsweise seinen Fragen zu den Berechtigungen, In-App-Kaufangeboten oder den

Datenschutz an den Anbieter einer App zu wenden. Außerdem wurde ausgewertet, ob auf Anfragen eine Reaktion erfolgte und die Anfragen ausreichend beantwortet wurden.

Auf der Seite des Google Play Stores waren für die einzelnen Apps Kontaktmöglichkeiten angegeben. Überwiegend konnte hierfür eine verlinkte E-Mail-Adresse genutzt werden, und zwar sowohl bei der Nutzung des Stores über eine Internetseite am PC, als auch über das Smartphone. Von den 43 über den Link auf Google Play genutzten Kontakt-E-Mail-Adressen erfolgte von 25 Anbietern keine Reaktion, beziehungsweise wurde in vier Fällen in einem Autoreply darüber informiert, dass noch eine Antwort folge. Bei den restlichen Anfragen waren lediglich vier Anbieter imstande, halbwegs bis sehr gut die Nachfragen zu den App-Berechtigungen zu beantworten. Bei den übrigen Anbietern ging eine automatisierte zumeist englischsprachige Antwortmail ein, in denen der Sachverhalt absolut nicht aufgriffen wurde oder die Antworten schlichtweg falsch waren. In den meisten Fällen allerdings wurde auf teilweise unbrauchbare Hilfebereiche oder Kontaktformulare auf den Internetseiten der Anbieter verwiesen, die wenig mit der Fragestellung zu tun hatten.

Im Apple iTunes Store konnten vor dem Herunterladen einer App keine direkten Kontaktmöglichkeiten für Verbraucher gefunden werden. Dort wird lediglich der Anbieter namentlich benannt.

3. Weitere Überprüfungen

a) Verbraucherinformationen

Auf den Seiten der einzelnen Apps im Google Play Store stehen neben der App-Beschreibung auch weitere Informationen zur Verfügung. Damit sich der Verbraucher vor dem Herunterladen und der Installation einer App über den App-Anbieter, also seinen Vertragspartner, informieren kann, ist neben Verlinkungen zur Datenschutzerklärung und zur Webseite, wie bereits aufgeführt, auch ein E-Mail-Kontakt angegeben.

Die auf den Seiten der angebotenen Apps dargestellten - nicht immer deutschsprachigen - Verbraucherinformationen im Hinblick auf Spielinhalt und –ablauf, waren vom Umfang und Informationsgehalt unterschiedlich gestaltet. Häufig verwiesen die App-Anbieter auf ihre englischsprachigen Nutzungsbedingungen und Datenschutzbestimmungen, die sich teilweise über mehrere Seiten erstreckten, in einem Fall über 35 DIN A4-Seiten. Das Lesen solcher umfänglichen AGB stellt sich schon am PC als eine Herausforderung dar, erst recht auf einem Smartphone.

Bei dem Versuch, den Verantwortlichen einer App, sowie dessen ladungsfähigen Anschrift zu ermitteln, stieß das Projekt schnell an seine Grenzen. Wie bereits beschrieben, war die Kontaktaufnahme über den Link „E-Mail an Anbieter senden“ selten von Erfolg gekrönt. Aber auch Verlinkungen zur Webseite der Anbieter führten oft ins digitale Nirvana, teils waren die Seiten gar nicht aufrufbar oder sie befanden sich noch „im Aufbau“ oder es wurde auf andere Webseiten, teils auch auf Kontaktformulare weitergeleitet. Die vermutlichen App-Verantwortlichen konnten – wenn überhaupt - oft nur durch eine längere Recherchearbeit und oft nur durch das vollständige Lesen der AGB und Datenschutzbestimmungen ermittelt werden. Von den 43 App-Angeboten konnten in 13 Fällen kein Firmensitz ermittelt werden. Ob die, der Übersicht zu entnehmenden, recherchierten Firmensitze der Anbieter tatsächlich korrekt sind, kann seitens des Projekts nicht mit 100-prozentiger Sicherheit bestätigt werden. In nur 5 Fällen haben die Anbieter ihren Sitz in Deutschland, das heißt alle anderen überprüften Anbieter sitzen überwiegend im –teils auch außereuropäischen– Ausland.

Insgesamt waren die Darstellungen der Informationen im Google Play Store über das Smartphone-Display relativ identisch mit denen über die Internetseite am PC. Lediglich der Hinweis auf die für die Nutzung der App erforderliche Android-Version fehlte bei der Darstellung über das Smartphone-Display.

b) In-App-Käufe

In-App-Käufe werden nicht ausschließlich bei kostenlosen Apps angeboten, auch kostenpflichtige Apps bieten die Käufe innerhalb der App an. 29 kostenlose und kostenpflichtige der 50 gesichteten Apps bieten laut Beschreibung der Anbieter auch In-App-Käufe an. Im Google Play Store wird auf der Webseite am PC direkt unterhalb des Installationsbuttons einer App darauf verwiesen, in der Darstellung auf dem Smartphone in der Nähe des Buttons.

Bei iTunes erfolgt die Information unterhalb des App-Titels und am Ende der App-Beschreibung. Dort lassen sich direkt die einzelnen Kaufangebote nach virtuellem Gegenstand oder virtueller Währung mit dem jeweiligen Kaufpreis einzeln anzeigen.

Für den Kauf virtueller Güter werden unterschiedliche Bezahlmöglichkeiten angeboten, angefangen bei der Kreditkarte über Paypal bis hin zur Abrechnung über die Telefonrechnung beziehungsweise über die Prepaid-Karte eines Smartphones. Dementsprechend unterschiedlich hoch sind die Hürden vor allem für Kinder, kostenpflichtige Apps herunterzuladen oder In-App-Käufe zu bezahlen.

Bei der inhaltlichen Überprüfung einiger weniger Apps ist aufgefallen, dass sich In-App-Kaufangebote nicht nur darauf beschränken, das mit echtem Geld innerhalb einer App virtuelle Güter oder virtuelle Währung erworben werden können. Vielmehr können in Apps vollwertige Shopfunktionen integriert sein, in denen Nutzer gegen Geld reale Produkte wie Baseballkappen, Schlüsselanhänger, Tassen oder Handyhüllen erwerben können. Zumindest in den getesteten Apps konnten die Käufe nur mittels Kreditkarte oder anderen – vor allem für Kinder - nicht einfach zugänglichen Bezahlsystemen realisiert werden. Auffällig war in einem Fall auch, dass der Warenkorb bereits auf eine Stückzahl von „8 Stück“ für ein gegen echtes Geld zu erwerbendendes Produkt voreingestellt war. Generell können durch die in Apps integrierten Shopfunktionen die geschäftliche Unerfahrenheit von Kindern ausgenutzt werden. Nach Auffassung des Projekts besteht besonders bei Spiele-Apps, die in ihrem Spiel auch In-App-Kauffunktionen integriert haben, die Gefahr, dass insbesondere Kinder nicht richtig zwischen In-App-Käufen gegen echtes Geld (virtuelles Schwert für 3,00 Euro) und virtuellen Käufen (virtuelle Währung gegen virtuelles Schwert) unterscheiden können, das heißt die reale Bezahlung verschwimmt mit der virtuellen Bezahlung.

Unabhängig davon, dass in Apps gerne Social-Media-Tools wie Facebook oder Twitter integriert sind, werden diese Dienste mitunter auch dafür genutzt, dem Nutzer als Belohnung für das Verbinden oder Teilen mit dem jeweiligen Dienst virtuelle Güter oder virtuelles Geld zu übertragen.

Bei In-App-Kaufangeboten sind die Preise nicht immer korrekt in Euro, sondern auch zum Beispiel in US-Dollar oder gar ohne Währung angegeben. Die Höhe der Preise selbst bewegt sich immer wieder auch im oberen zweistelligen Eurobereich.

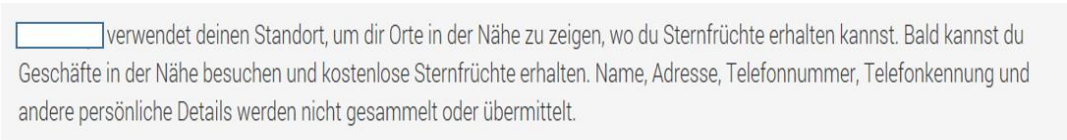
Positiv hervorzuheben ist, dass einige App-Anbieter im Google Play Store darauf hinweisen, dass In-App-Käufe zwar nicht direkt innerhalb der App, aber zumindest über die Geräteeinstellungen deaktiviert werden können.


Diese App bietet In-App-Käufe an. Diese können über die Geräteeinstellungen deaktiviert werden. Vor einem In-App-Kauf bitte Rücksprache mit der für die Zahlung verantwortlichen Person halten. Eltern finden unter https://support.google.com/googleplay/answer/1626831?hl=en&ref_topic=2803018 Hinweise zur Einrichtung von Einkaufspasswörtern.

Genau genommen lassen sich beim Android Betriebssystem die In-App-Käufe nicht deaktivieren, allerdings kann sich der Verbraucher einen Passwortschutz über den Google Play Store einrichten, so dass mobile Käufe nur nach Eingabe eines Passwortes möglich sind.
Bei iOS-Geräten lassen sich In-App-Käufe komplett über das Endgerät deaktivieren.

c) Lockangebote

Grotesk schien in einer App der Hinweis, dass Standortdaten verwendet werden würden, damit der Nutzer kostenlos Sternfrüchte erhalten könne - Daten gegen Obst:


verwendet deinen Standort, um dir Orte in der Nähe zu zeigen, wo du Sternfrüchte erhalten kannst. Bald kannst du Geschäfte in der Nähe besuchen und kostenlose Sternfrüchte erhalten. Name, Adresse, Telefonnummer, Telefonkennung und andere persönliche Details werden nicht gesammelt oder übermittelt.

Beliebt ist vor allem bei Spiele-Apps das plötzliche Einblenden von Werbung für ein anderes Spiel, das „nur heute“ kostenlos genutzt werden könne. Vor allem Kinder sind für solche Art der Werbung besonders empfänglich. An dieser Stelle werden der Spieltrieb und die geschäftliche Unerfahrenheit der Kinder ausgenutzt. Denn oft lassen sich solche Spiele nur wenige Minuten kostenfrei spielen und sollen den Nutzer kurze Zeit später veranlassen, In-App-Käufe zu tätigen.

IV. Zusammenfassendes Untersuchungsergebnis und Bewertung

Nach Einschätzung des Projekts sind bestimmte **Zugriffsberechtigungen** für die Nutzung einer App nicht immer erforderlich. Vor allem ist es für Verbraucher schwierig zu ermessen, ob und welche Berechtigungen tatsächlich für die Nutzung eines Dienstes erforderlich sind. Zu beanstanden am Android Betriebssystem ist, dass der Nutzer keine Möglichkeit hat, einzelne Zugriffsberechtigungen zu verweigern. Der Nutzer ist gezwungen den vom Anbieter dargestellten Berechtigungen im vollen Umfang zuzustimmen oder von der Installation einer App Abstand zu nehmen. Demgegenüber wird beim Herunterladen einer App aus dem Apple-Store der Nutzer zwar zuvor nicht über die einzelnen Berechtigungen informiert. Andererseits sind einige Berechtigungen wie der Zugriff auf Standortdaten und Kontakte deaktiviert, die der Nutzer erst im Nachhinein freigeben muss.

Scharf zu kritisieren ist die mangelnde Bereitschaft vieler App-Anbieter, auf Anfragen zu den Berechtigungen adäquat, beziehungsweise überhaupt zu reagieren. Die angebotenen **Kontaktmöglichkeiten** für Verbraucher laufen meist faktisch ins Leere. Diese von sehr vielen App-Anbietern gelebte Praxis verdeutlicht, dass interessierte Verbraucher keine Chance haben, sich vor dem Herunterladen einer App weitere Informationen, zum Beispiel zu Fragen des Datenschutzes oder über die Zugriffsrechte, zu verschaffen.

Die Ermittlung **ladungsfähiger Anschriften der App-Anbieter** war ebenso ein mühseliges Unterfangen und erforderte nicht selten eine zeitintensive Recherche durch Einsichtnahme der AGB und Datenschutzbestimmungen, die teilweise englischsprachig waren und eine Länge von mehreren DIN A4-Seiten hatten. Das kann zur Folge haben, dass Verbraucher von der Verfolgung und Durchsetzung rechtlicher Ansprüche, beispielsweise wegen unberechtigter Abbuchungen aus vermeintlichen In-App-Käufen, wegen des erhöhten Prozesskostenrisikos abgehalten werden. Aus diesem Grunde müssen Verbraucher vor dem

Herunterladen und der Installation einer App wissen, mit welchem Anbieter sie ein Rechtsverhältnis eingehen und ob sie das Risiko im Falle einer streitigen Auseinandersetzung bereit sind zu tragen. Insofern ist es auch wichtig, dass App-Vertriebsplattformen den Nutzern ebenfalls leicht auffindbare Kontaktmöglichkeiten und Unterstützung anbieten, wenn es Auseinandersetzungen mit App-Anbietern gibt.

Die für die Nutzung einer App erforderlichen Informationen über die Systemanforderungen, aber auch die App-Beschreibungen und der Hinweis auf In-App-Kaufangebote sind nach derzeitigem Kenntnisstand größtenteils gelungen. Allerdings wird von App-Anbietern nicht immer beachtet, dass diese Informationen, einschließlich der Regelungen in Allgemeinen Geschäftsbedingungen und Datenschutzbestimmungen in deutscher Sprache verfasst sein müssen. App-Anbieter, die ihre Dienste global anbieten und diese über Vertriebsplattformen vertreiben, die sich an Verbraucher richten, müssen die jeweilige Landesprache berücksichtigen.

Bei den **In-App-Kaufangeboten** ist positiv hervor zu heben, dass im Apple-Store vor dem Herunterladen einer App, angebotene In-App-Käufe einzeln aufgelistet werden, so dass sich der Verbraucher vorab darüber informieren kann, was und welche Preisstruktur ihn dort erwartet. Dieses ist vor allem für Eltern von jüngeren Kindern von besonderem Interesse, zumal die Preise für angebotene In-App-Käufe teilweise exorbitant bis zu 100,00 Euro teuer sind. Daher ist es unerlässlich, Verbrauchern, vor allem Eltern, Instrumente der Kostenkontrolle anzubieten wie die Einrichtung von Kostenobergrenzen oder gänzlich die Deaktivierung der Bezahlfunktionen. Nur so können sie sich und ihre Kinder vor ungewollten In-App-Käufen zu schützen. Denkbar wären auch nach Nutzern differenzierte Profile auf einem Endgerät mit unterschiedlichen Zugriffsrechten, Befugnissen und Datenschutzeinstellungen zu ermöglichen.

Wie Verbraucherschutz bei Apps aussehen sollte, ist der Anlage 1 dieses Berichts zu entnehmen.

Anlage 1: Verbraucherschutz bei Apps sollte so aussehen

Zugriffberechtigungen

- Apps sollten generell nur in dem Umfang Zugriffsberechtigungen haben, wie diese für die Nutzung der App erforderlich ist. Zwingende Zugriffsberechtigungen sind optisch hervorzuheben. Es muss dabei nicht nur die Information aufgeführt werden, welche Berechtigungen benötigt werden, sondern auch zu welchem konkreten Zweck sie notwendig sind.
- Bei darüber hinaus gehenden Zugriffsberechtigungen muss der Nutzer die Möglichkeit haben, einzelne Berechtigungen zu verweigern, bzw. diese zu deaktivieren.
- Stärkung des Datenschutzes durch Privacy by Design und Privacy by Default

Kontaktmöglichkeiten

- App-Anbieter müssen nicht nur in der App ein vollständiges Impressum mit Namen, Anschrift, Kontakt- und E-Mail-Adresse zur Verfügung stellen, sondern auch bereits auf der jeweiligen App-Vertriebsplattform, so dass sich der Nutzer vor dem Herunterladen über seinen Vertragspartner informieren kann.
- App-Anbieter müssen eine für Verbraucher einfach auffindbare und zugängliche Kontaktadresse zur Verfügung stellen, an die sie sich mit Fragen des Datenschutzes, Zugriffsberechtigungen, sonstigen Fragen/Streitigkeiten etc. wenden können
- Anfragen von Verbrauchern sind zeitnah und auf die Fragestellung abzielend zu beantworten
- App-Vertriebsplattformen sollten Verbrauchern ebenfalls eine unmittelbar leicht erreichbare Kontaktmöglichkeiten bieten, an die sie sich mit Fragen auch für den Fall, dass es Probleme mit einem App-Anbieter gibt, wenden können

Zwingende Verbraucherinformationen

- Bei App-Angeboten, die sich an deutsche Verbraucher richten, müssen die Verbraucherinformationen, Allgemeine Geschäftsbedingungen und Datenschutzbestimmungen in deutscher Sprache verfasst sein. Dasselbe gilt für die Beantwortung von Verbraucheranfragen.

AGB und Datenschutzbestimmungen

- Die AGB und Datenschutzbestimmungen müssen sich auf die für das betreffende App-Angebot relevanten Inhalte beschränken und sich sprachlich und gestalterisch an den Bedürfnissen und Fähigkeiten der Zielgruppe orientieren.
- App-Anbieter sollten darüber informieren, wie sich der Dienst finanziert (App-Kauf, Werbung, Datenabfragen, In-App-Käufe etc.)

In-App-Kaufangebote

- Vor der Installation einer App sollte detailliert über In-App-Kaufangebote in Bezug auf die „Kaufgegenstände“ und die Höhe des Kaufpreises informiert werden.
- Die Bezahlfunktion sollte insgesamt oder auch nur in Bezug auf einzelne Apps deaktivierbar sein. App-Anbieter sollten auf die Deaktivierungsfunktionen für den In-App-Kaufbereich hinweisen.
- Bei In-App-Kauffunktionen dürfen die dort eingebundenen Warenkörbe nicht voreingestellt sein.
- Verbrauchern sollten auch nach Nutzern differenzierte Profile auf einem Endgerät mit unterschiedlichen Zugriffsrechten, Befugnissen und Datenschutzeinstellungen ermöglicht werden.

Speziell für Kinder

- Kinder dürfen bei der Nutzung von Kinder-Apps zum Beispiel nach kurzer Spielzeit oder durch eine überproportional lange Wartezeit nicht „gezwungen“ werden, für die Wiederaufnahme des Spiels In-App-Käufe zu tätigen
- Die Kosten pro In-App-Kauf müssen sich an der spielenden Zielgruppe orientieren und vom durchschnittlich üblichen Taschengeld des Kindes zu bestreiten sein. Anderenfalls muss die Einwilligung der Eltern für den Kauf sichergestellt werden. Außerdem sollte Eltern bzw. Erziehungsberechtigten die Möglichkeit eingeräumt werden, jedwede In-App-Käufe zu deaktivieren
- Anbieter von Kinder-Apps sollten Eltern bzw. Erziehungsberechtigte ein Instrument zur Kostenkontrolle zur Verfügung stellen, mittels dem sie eine Höchstgrenze für alle innerhalb einer App getätigten Käufe pro Monat vorgeben können
- Shopfunktionen sollten nicht in Apps integriert sein, wenn sich das Angebot auch an Kinder richtet
- Externe Social-Media-Tools wie Facebook und Twitter dürfen nicht in Kinder-Apps eingebunden sein

Anlage 2: Übersicht Überprüfung von Apps

Überprüfung von Apps

SURFER HABEN RECHTE

Eine Untersuchung des vzbv-Projekts "Verbraucherrechte in der digitalen Welt" (Untersuchungszeitraum 24.02.-05.03.2014)

Stand: 10.03.2014

App	Anbieter	Firmensitz	Kostenpfl.	Google	Apple	unklare Berechtigungen	unauffällig	In-App-Kauf	Anmerkungen
94 Grad		Frankreich		x			x	ja	keine Nachfrage
Age of Warring	Silent Ocean	?	nein	x	x	Standortdaten Telefonstatus u. -ID lesen		ja	keine Antwort
Angry Bird	Rovio Entertainment ltd.	Finnland	nein	x	x	Telefonstatus u. -ID lesen Standortdaten Kalendertermine und Mails an Gäste		ja	Antwort ++
Anti Virus	AVG Technologies CZ s.r.o.	Tschechische Republik	nein	x		Telefonstatus u. -ID lesen Standortdaten Kalendertermine und Mails an Gäste		ja	Antwort +, Verweis auf Webseite, Kontaktformular (umständlich)
Barcode Scanner	ZXing Team	evtl. San Francisco (Firma github)	nein	x		Kontaktdaten lesen Standortdaten		nein	Antwort +, lediglich Verweis auf Store-Infos (unzureichend)
Blitzer.de PLUS	Efrig Media GmbH	Hamburg	4,99	x		Telefonstatus u. -ID lesen (Standortdaten)		nein	Antwort +++, sehr ausführlich
Candy Crush	King.com	Malta	nein	x	x	Zugriff auf bekannte Konten		ja	keine Antwort
Castle Clash	IGG.COM	Singapur (China, USA, Kanada, Philippinen)	nein	x		Telefonstatus u. -ID lesen		ja	keine Antwort
Clash of Clans	Supercell	Finnland	nein	x	x	Telefonstatus u. -ID lesen		ja	Antwort Autoreply: Antwort soll noch folgen
Crazy Doctor	CanadaDroid	?	nein	x			x	ja	keine Nachfrage
die Simpsons™ Springfield	EA Swiss Sarl	Schweiz	nein		x	Telefonstatus u. -ID lesen		ja	Antwort +, Autoreply und Verweis auf Webseite, bzw. Kontaktformular
Empire for Kindom	Goodgame Studios	Hamburg	nein	x	x	Telefonstatus u. -ID lesen Zugriff auf bekannte Konten		ja	keine Antwort
Facebook	Facebook Ireland Limited	Irland	nein	x		diverse, u.a. Hinzufügen von Kalenderterminen Versand von E-Mails an Gäste Anruf von Telefonnummern		nein	keine Antwort
Farm Heroes Saga	King.com Limited	Malta (Stockholm, Barcelona, Bukarest, Malmö, London, San Francisco)	nein	x			x	ja	keine Nachfrage
Fifa	EA Swiss Sarl	Schweiz	nein	x	x	Telefonstatus u. -ID lesen		ja	Antwort +, Autoreply und Verweis auf Webseite, bzw. Kontaktformular
Flappy Bird	Floppy Bird Fly!	?	nein	x	nicht im Store	Audioaufnahmen Standortdaten Telefonstatus u. -ID lesen		nein	Antwort von Floppy Bird + (völlig unzureichend)
Floppy Bird/Silly Bird	Bird World	?			nicht im Store	Audioaufnahmen Standortdaten Telefonstatus u. -ID lesen		nein	keine Antwort, da Antwort von Floppy Bird für Flappy Bird (?)
Gangstar Vegas	Gameloft	Kalifornien/Frankreich?	0,89	x		Telefonstatus u. -ID lesen		ja	Antwort +, Verweis auf Webseite, nur allg. Support
Gewicht Assistent	Kevin Tung	?	nein	x		Telefonstatus u. -ID lesen		nein	keine Antwort
Hay Day	Supercell	Finnland	nein	x		Telefonstatus u. -ID lesen		ja	Autoreply, Antwort soll noch folgen
Hi Frog	DIE KAPITÄNE Media GmbH	Dresden	nein	x	x	Standortdaten erheben Abruf ausgeführter Anwendungen Telefonstatus u. -ID lesen		ja	Antwort +++ sehr ausführlich
Hobbit	Kabam	San Francisco	nein	x	x	Telefonstatus u. -ID lesen		ja	Antwort +, Autoreply und Verweis auf Link innerhalb des Spiels
Instagram	Instagram	USA	nein	x	x	Standortdaten erheben Profil- u. Kontaktdaten lesen Profildaten versenden		nein	keine Antwort
Iphone 5s Keyboard	Better Keyboards Inc	evtl. San Francisco, London, Peking, Seoul (Firma swift key)	nein	x	nicht im Store	Standortdaten erheben Telefonstatus u. -ID lesen		nein	keine Antwort
Jet Ski	Studio 3wg	Luxemburg	nein	x		Abruf ausgeführter Anwendungen Telefonstatus u. -ID lesen		nein	keine Antwort
Kleine Hautarzt	6677g.com	?	nein	x		Telefonstatus u. -ID lesen		nein	keine Antwort
Lazors	Pyrosphere	?	nein	x			x	ja	keine Nachfrage - Keine besonderen Berechtigungen erforderlich
Mad Skills	Turbonilla	Schweden	nein	x		Telefonstatus u. -ID lesen		ja	keine Antwort
Minecraft	Mojang	Schweden	5,49	x			x	nein	keine Anfrage
Modern Combat 4: Zero Hour	Gameloft	Frankreich	5,99			Telefonstatus u. -ID lesen		ja	Antwort +, Verweis auf Webseite, nur allg. Support
Moorhuhn Deluxe	Doyodo	Düsseldorf	0,89	x		Telefonstatus u. -ID lesen		nein	Anwort ++
Nike+ Running	Nike, Inc	USA, Niederlande	nein	x	x	Telefonstatus u. -ID lesen Zugriff auf Anrufprotokolle, pers. Infos, Kalender Versenden von Mails + hinzufügen von Ereignissen		nein	Antwort +, Autoreply, danach weitere Antwortmail (völlig unzureichend)
Pet Shop Story	TeamLava Games	Kalifornien	nein	x		Telefonstatus u. -ID lesen		ja	Antwort +, Autoreply
Plants vs. Zombies	EA Swiss Sarl	Schweiz	0,89	x		Telefonstatus u. -ID lesen		ja	Antwort +, Autoreply und Verweis auf Webseite, bzw. Kontaktformular
Plumpen Vogel	Candy Mobile	?	nein	x			x	ja	keine Nachfrage
Pou	Zakeh	?	nein	x		Audioaufnahmen		ja	Antwort +, Autoreply, link zur Webseite
Quizduell/Qizduell Premium	FEO Media AB	Schweden	nein/2,69	x		Telefonstatus u. -ID lesen		nein	keine Antwort
Rise of an Empire	Warner Bros. International Enterprises	Kalifornien	nein	x		Telefonstatus u. -ID lesen		nein	Antwort +, es werden noch weitere Informationen benötigt (Vol-Nachname,
Runtastic	runtastic GmbH	Österreich	4,99	x		Telefonstatus u. -ID lesen Zugriff auf geschützten Speicher Abruf ausgeführter Anwendungen (Standortdaten)		ja	Antwort +, Autoreply und Link auf Hilfebereich der Webseite und Help-Team
Schlag den Raab	Raab TV Produktion GmbH	Deutschland	2,69	x		Telefonstatus u. -ID lesen		ja	keine Antwort
Smart Tools - Werkzeugkasten	Smart Tools co	?	1,99	x		Standortdaten erheben		nein	keine Antwort,
Stadt-Land-Fluss	byte-werk Andreas Lochmann	Singen	nein	x			x	nein	Keine besonderen Berechtigungen erforderlich
Swift Key Tastatur		San Francisco, London, Peking, Seoul			nicht im Store	Telefonstatus u. -ID lesen SMS lesen		nein	keine Antwort (Anfrage über Kontaktformular)
Toca Lab	Toca Boca AB	San Francisco	0,78	x		Telefonstatus u. -ID lesen		nein	Antwort +, Autoreply, Antwort soll folgen
Smart Tools - Werkzeugkasten	Smart Tools co	?	1,99	x		Standortdaten erheben		nein	keine Antwort,
Top Eleven Fußballmanager	Nordeus Ltd	Irland	nein	x	x	Abruf ausgeführter Anwendungen Telefonstatus u. -ID lesen		ja	Antwort + Autoreply, Antwort soll noch folgen
Unroll me	Turbo Chilli	?	nein	x	x	Abruf ausgeführter Anwendungen Telefonstatus u. -ID lesen		ja	keine Antwort
Virtual Tattoo	Super DEC Games	?	nein	x		Telefonstatus u. -ID lesen		nein	keine Antwort
WhatsApp	WhatsApp Inc.	Kalifornien	nein	x		Nachfrage, ob 1. Daten auch für and. Zwecke genutzt, 2. Datenaustausch mit Facebook und 3. Löschungsfristen		ja	Antwort + (passt nicht auf Fragestellungen)
Wo ist mein Wasser?	Disney	USA	1,49	x		Telefonstatus u. -ID lesen		ja	keine Antwort