In Kooperation mit:
BITKOM - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
davit im DAV - Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein
eco - Verband der Internetwirtschaft e.V.
VPRT - Verband Privater Rundfunk und Telemedien e.V.

MMR
MultiMedia und Recht
6/2016

EDITORIAL

Zwei US-Behörden für mehr Datenschutz und Datensicherheit

Lesedauer: 10 Minuten

Die *Federal Trade Commission* (*FTC*) und die *Federal Communications Commission* (*FCC*) haben am 10.5.2016 zwei getrennte Untersuchungsverfahren gegen bestimmte TK-Anbieter und Hersteller von Smartphones etc. eingeleitet. Die US-Behörden wollen wissen, wie diese Unternehmen Updates zur Datensicherheit vornehmen, wie die Kunden die Updates umsetzen und wie die Unternehmen eventuelle Schwachstellen in den Geräten in Angriff nehmen. Das wirft die allgemeine Frage auf, welche Kompetenzen beide Behörden in den Bereichen Datenschutz und Datensicherheit haben und wie sie zusammenarbeiten.

Federal Communications Commission – FCC

Die *FCC* stützt sich auf drei Vorschriften, um personenbezogene Daten im TK-Bereich zu regeln: Section 201(b), 222(a) und Section 222(c) Communications Act. Section 201(b) legt folgende allgemeine Regel fest, die auch den Bereich „Privacy" umfasst: „Alle Gebühren, Praktiken, Klassifikationen und Vorschriften für und in Verbindung mit (zwischenstaatlichen oder ausländischen) Kommunikationsdiensten (leitungsgebunden oder drahtlos) müssen gerecht und vernünftig sein; eine Gebührenerhebung, Praxis, Klassifizierung oder Verordnung, die ungerecht oder unvernünftig ist, muss für rechtswidrig erklärt werden." Section 222(a) Communications Act regelt allgemein die Pflicht der TK-Anbieter, die Vertraulichkeit der Informationen ihrer Kunden zu schützen. Section 222(c)(1) erlaubt es den TK-Anbietern, nur solche personenbezogene Daten (Customer Proprietary Network Information – CPNI) zu verarbeiten, die für die Erbringung der TK-Dienste erforderlich sind, es sei denn, das Gesetz oder die Einwilligung des Kunden erlaube etwas anderes.


Dr. Axel Spies

Die *FCC* hat diese weite Befugnis u.a. in dem Verfahren gegen *Terracom* und *YourTel* im Oktober 2014 angewandt, indem sie beiden Unternehmen getrennt behördliche Strafbefehle (Notice of Apparent Liability) i.H.v. US$ 10 Mio. zugestellt hat (vgl. *Spies*, ZD-Aktuell 2014, 04387). Beide Unternehmen hatten laut *FCC* TK-Daten entgegen den o.g. Vorschriften verarbeitet, die sie von Kunden i.R.v. sog. Lifeline-Diensten (TK-Grunddienste für finanziell Bedürftige) erhalten hatten. Hinzu kam ein Bruch der Datensicherheit. Die Unternehmen einigten sich mit der *FCC* im Juli 2015 auf eine erhebliche, rechtskräftige Geldbuße i.H.v. US$ 3,5 Mio.

Die in vieler Hinsicht wegweisende Open Internet Order der *FCC* v. 26.2.2015 (vgl. *Spies*, MMR-Aktuell 2015, 367980) enthält einen weiteren Schritt für mehr Datenschutz im TK-Bereich und weitergehender Aufsicht der *FCC*, indem sie die o.g. Vorschriften von Section 201(b) und Section 222 Communications Act auf die

Vermittler von Internet-Zugangsdiensten (Broadband Internet Access Services – BIAS) ausdehnt. Die Open Internet Order ist allerdings vor Gericht angefochten worden, auch im Hinblick auf deren Privacy-Regelungen. Mit einer Entscheidung des Berufungsgerichts ist in einigen Wochen zu rechnen.

Das derzeit noch laufende Konsultationsverfahren der *FCC* „Broadband and Data Security NPRM" v. 1.4.2016 (vgl. *Spies*, ZD-Aktuell 2016, 377151) ist ein weiterer wichtiger Meilenstein für den Ausbau des Datenschutzes im TK-Bereich. Die *FCC* will dieses Konsultationsverfahren bis zum 27.6.2016 abschließen.

Damit nähert sich die *FCC* in einigen wichtigen Bereichen, z.B. bei der Definition der PII, dem EU-Datenschutzstandard für den von ihr überwachten TK-Sektor an.

Große Bedeutung behält in den USA weiterhin all das, was der Anbieter selbst in seinen Datenschutz-Richtlinien (Privacy Policies) seinen Kunden gegenüber verspricht. Die Behörden halten den Anbieter daran fest. Nach der Vorstellung der *FCC* sollen die Privacy Policies der Anbieter zumindest folgende Informationen enthalten:

- Die erfassten Datenkategorien, die der Anbieter verwendet,
- eine vollständige Liste der Stellen, die TK-Daten vom Anbieter erhalten und zu welchem Zweck,
- die Opt-out- und/oder Opt-in-Rechte der Kunden (ohne zusätzliche Kosten) in Bezug auf die Bereitstellung von Breitband-Dienstleistungen,
- detaillierte Bestimmungen über die Einwilligungen der Kunden in einem einfachen und transparenten Verfahren sowie zu deren Rücknahme.

Bei den neuen Regeln zum Bruch der Datensicherheit in der NPRM bemüht sich die *FCC* um Vereinheitlichung der nach dem Recht von 46 Einzelstaaten bestehenden Vorgaben für den TK-Sektor (State Data Breach Notification Laws), da ein Bundesgesetz bislang fehlt.

Egal was die nahe Zukunft bringen mag, kann man feststellen, dass die *FCC* auch schon mit dem bestehenden regulatorischen Werkzeug in der Lage ist, für ihren Geschäftsbereich Datenschutzvorschriften zu erlassen und notfalls mithilfe des personell gut ausgestatteten und geschulten *Enforcement Bureau* gegenüber den TK-Anbietern durchzusetzen. Sollte die Open Internet Order in dieser Hinsicht vor dem Berufungsgericht Bestand haben (vgl. *Spies*, MMR Aktuell 2015, 374380), müssen sich auch zahlreiche Anbieter von Breitband-Internetzugang an die neuen Regeln halten und diese durch ihre Privacy Policies umsetzen.

Federal Trade Commission – FTC

Die *FTC* ist von ihrer Konzeption her eine Verbraucherschutzbehörde und keine unabhängige Datenschutzbehörde i.S.d. europäischen DS-RL. Dreh- und Angelpunkt der *FTC*-Kompetenz im Bereich „Privacy" ist Section 5 FTC Act. Die nur schwer zu übersetzende Vorschrift verbietet als Generalklausel „unfaire oder täuschende Handlungen oder Praktiken im Handel oder mit Auswirkungen auf den Handel („unfair or deceptive acts or practices in or affecting commerce"). Die Vorschrift gibt der *FTC* weitaus mehr Spielraum als die enger gefassten Regeln der *FCC*.

Ein gutes neueres Beispiel für die Nutzung der Kompetenz ist der Wyndham-Fall. Ohne hier auf die Einzelheiten des Sachverhalts eingehen zu wollen, ging es ebenfalls um einen Bruch der Datensicherheit. Die *FTC* war zur der Erkenntnis gelangt, dass das Hotel-Unternehmen *Wyndham* seinen Kunden gegenüber unrichtige oder irreführende Angaben und Zusicherungen zur Datensicherheit gemacht hatte, und dass das Unternehmen keine sinnvollen und geeigneten Maßnahmen ergriffen habe, um personenbezogene Daten der Kunden vor einem unberechtigten Zugriff zu schützen. Auf Grund dessen sei es zu betrügerischen Abbuchungen i.H.v. rd. US$ 10 Mio. durch Hacker gekommen, die einen erheblichen, vermeidbaren Schaden für die Verbraucher herbeigeführt hätten. Die Daten von mehreren 100.000 Kunden seien ungeschützt zugänglich gewesen. Dieser Schaden werde durch geldwerte Vorteile für die Verbraucher (Schadensersatz gegen Dritte etc.) nicht aufgewogen.

Wyndham und die *FTC* schlossen am 9.12.2015 eine Vereinbarung zur Erledigung des Verfahrens. Darin verpflichtet sich *Wyndham* u.a. dazu, ein detailliertes Programm zur Informationssicherheit für Karteninhaberdaten umzusetzen, einschließlich jährlicher Audits. Die vereinbarten Schutzmaßnahmen für einen Zeitraum von 20 Jahren umfassen auch den Schutz der Server der Franchisenehmer von *Wyndham*. Durch diesen Vergleich entging *Wyndham* empfindlichen Bußgeldern. Gleichwohl ist *Wyndham* weiterhin auf dem Radarschirm der *FTC*. Sollte *Wyndham* die Vereinbarung verletzen, könnte die *FTC* ein Exempel mit noch empfindlicheren Sanktionen statuieren.

Die *FTC* ist derzeit eng in die Verhandlungen der *US-Regierung* mit der EU zur Einrichtung des neuen EU/US-Privacy-Shield involviert (vgl. hierzu *Spies*, ZD-Aktuell 2016, 04992 und ZD-Aktuell 2016, 05005). Die *FCC* bleibt in diesem Fall außen vor, da der Privacy Shield derzeit nicht auf TK-Daten anwendbar ist. Sollte die *EU-Kommission* den neuen Regeln zustimmen, dürften die Unternehmen (Datenimporteure) mit einer intensiven Kontrolle der *FTC* zu rechnen haben. Die Datenimporteure müssen sich unter dem Privacy Shield selbst zertifizieren, dass sie die Daten aus der EU/EWR im Einklang mit den im Privacy Shield-Framework festgeschriebenen Regeln verarbeiten. Wenn sie die Regeln verletzen, drohen ihnen u.a. Sanktionen der *FTC*. Die *FTC* hat bereits Workshops zum neuen Privacy Shield für die US-Industrie angekündigt. Ein weiterer Schwerpunkt der Arbeit der *FTC* liegt auf der Durchsetzung der Datenschutzregeln, deren Einhaltung die Unternehmen in ihren jeweiligen Privacy Policies ihren Kunden gegenüber versprechen, den Auswirkungen des Internet of Things (IoT) und, ähnlich wie in Europa, dem Thema „Privacy by Design."

Zusammenarbeit der beiden Behörden

Die Tatsache, dass die *FCC* und die *FTC* teilweise überlappende Kompetenzen im Bereich „Privacy" haben, könnte zu rivalisierenden Maßnahmen der beiden Behörden oder, positiv ausgedrückt, zu einem Wettlauf um den besseren Datenschutz führen. Von offizieller Seite wird eine Rivalität vehement verneint. Durch ihre Fachkompetenz im bestimmten Bereichen (TK gegenüber Verbraucherschutz) ergänzen sich die Behörden jedenfalls in ihrer Arbeit. Der Informationsfluss zwischen den Mitarbeitern beider Behörden ist gut.

Die *FCC* und die *FTC* haben im November 2015 ein Memorandum of Understanding (MoU) unterzeichnet, um ihre Zusammenarbeit bei Verbraucherschutzthemen zu fördern. Das MoU, das über den Bereich Privacy hinausgeht, soll die bestehende Zusammenarbeit zwischen den Behörden formalisieren und beschreibt Methoden zur Koordination und zum Informationsaustausch. So soll nach dem MoU die *FTC* nicht gegen TK-Unternehmen vorgehen, ohne vorher die *FCC* zu konsultieren. Dies ist besonders relevant für Ermittlungen und andere Maßnahmen der *FTC* nach dem Fair Credit Reporting Act und nach dem Telephone Disclosure and Dispute Resolution Act von 1992, für die die *FTC* (und nicht die *FCC*) originäre Zuständigkeit hat. Umgekehrt ist eine Konsultationspflicht vorgesehen, wenn die *FCC* in Verbraucherschutzfragen aktiv wird. Die Behörden informieren sich gegenseitig über eingehende Verbraucherbeschwerden. Zentrale Kontaktstellen (Designated Liaison Officers) beider Behörden sollen mögliche Kompetenzkonflikte schon in einem frühen Stadium ausräumen.

Washington, im Juni 2016

Dr. Axel Spies
ist Rechtsanwalt in der Kanzlei Morgan, Lewis & Bockius LLP in Washington DC und Mitherausgeber der MMR.