IMPULSE

März 2015

Die Cloud im rechtsfreien Raum

Wie regeln wir den Datenzugriff durch Sicherheitsbehörden im 21. Jahrhundert?

Jan-Peter Kleinhans
Projektmanager
Europäische Digitale Agenda

Einleitung

Beim Internet stößt das Territorialitätsprinzip an seine Grenzen. Denn die Frage, welches Recht auf welche Person wann und an welchem Ort anzuwenden ist, lässt sich gerade in einem globalen Netzwerk aus Netzwerken nicht so leicht klären. Auf der Bundespressekonferenz im Juli 2013 hatte. Bundeskanzlerin Angela Merkel versichert, dass auf „deutschem Boden deutsches Recht“ gelte.[1]

Fraglich in Bezug auf das Internet ist jedoch, wann man sich überhaupt auf „deutschem Boden“ befindet. Gerade mit Blick auf die Strafverfolgung ist diese Frage ganz entscheidend: Wann haben nationale Sicherheitsbehörden Zugriff auf bestimmte Nutzerdaten eines Service Providers? Der einfachste Fall, Sicherheitsbehörde, angefragtes Unternehmen, betroffener Nutzer und relevante Server sind alle inländisch, ist gleichzeitig der unwahrscheinlichste – zumindest außerhalb der Vereinigten Staaten.

Betrachtet man das heutige „Cloud-Ökosystem“ ist es sogar extrem unwahrscheinlich, dass sich das angefragte Unternehmen und die relevanten Server, auf denen die Nutzerdaten liegen, in derselben Jurisdiktion befinden. Einer der Gründe hierfür ist, dass „die Cloud“ in der Regel aus einem Zusammenspiel unterschiedlicher Dienste und dienstleistender Unternehmen besteht. Diese können grundsätzlich in drei Kategorien eingeteilt werden:

- **Infrastructure as a Service** (IaaS), z.B. amazon Elastic Compute Cloud. Prozessor- und Speicherkapazität als Dienstleistung.[2]
- **Platform as a Service** (PaaS), z.B. Google App Engine oder Salesforce.com. Cloud-Entwicklungsumgebungen als Dienstleistung.[3]
- **Software as a Service** (SaaS), z.B. Microsofts Office 365 oder Google Drive. Anwendersoftware als Dienstleistung.[4]

Durch das Zusammenspiel verschiedener Dienstleister können mehrere private Unternehmen bei der Verarbeitung von Nutzerdaten involviert sein. So können Facebook Apps (SaaS) z.B. mittels Heroku (PaaS) entwickelt und angeboten werden und zugleich auf Prozessor- und Speicherkapazität von amazons Web Services (IaaS) aufbauen[5]. In diesem Szenario ist es sehr schwierig genau zu bestimmen, wann und wo welche Daten eines Nutzers anfallen und letztlich abgespeichert werden.

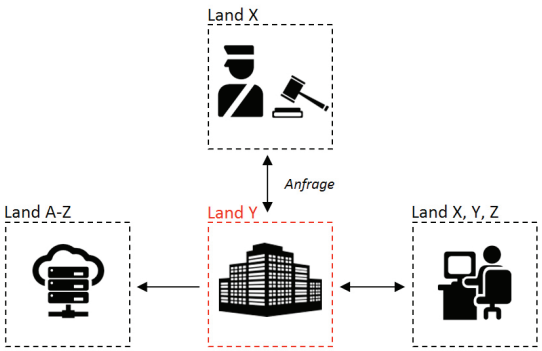
Realitäten des extraterritorialen Zugriffs

Unterliegen nun Nutzer, privates Unternehmen und anfragende Sicherheitsbehörde jeweils unterschiedlicher Jurisdiktion müsste es zur Rechtsabwägung kommen. Dies geschieht in Strafverfahren typischerweise durch Rechtshilfeabkommen. Die Abwägung, ob die anfragende Sicherheitsbehörde im Recht ist, obliegt somit nicht

nur ihrem inländischen Gericht, sondern auch dem ausländischen Gericht des betroffenen Unternehmens bzw. Nutzers. In der Praxis wird dieser Rechtsweg jedoch oft mit einer Abkürzung umgangen: Ungeachtet der Territorialität der Nutzerdaten und Nationalität des Nutzers werden Cloud-Anbieter heutzutage direkt durch ausländische Strafverfolgungsbehörden zur Herausgabe von Nutzerdaten aufgefordert. In den letzten Jahren gingen immer mehr Unternehmen dazu über, Statistiken über diese Anfragen in Form von sogenannten Transparenzberichten zu veröffentlichen.[6] Anhand dieser Berichte wird deutlich, wie groß das Missverhältnis zwischen Nutzung von Rechtshilfeabkommen und direkten Anfragen ausländischer Behörden ist:

Betrachtet man beispielhaft die Daten aus Googles Transparenzbericht[7] für das erste Halbjahr 2014, so erhielt das Unternehmen rund 12.500 Anfragen durch US amerikanische Strafverfolgungsbehörden. Ungewiss ist, wie viele dieser Anfragen im Zuge eines internationalen Rechtshilfeersuchens erfolgten. Da Deutschland, Frankreich, Großbritannien, Italien und Indien (nach den Vereinigten Staaten die fünf Länder mit den meisten Anfragen) zusammen etwa 11.700 direkte Anfragen an Google stellten, ist davon auszugehen, dass der Weg über Rechtshilfeabkommen nur selten genutzt wird.

Abbildung 1: Direkte Anfrage an Diensteanbieter durch ausländische Behörden



Bei diesem Vorgang wird durch die direkte Anfrage ausländischer Strafverfolgungsbehörden eine Entscheidung auf private Unternehmen übertragen, die eigentlich zwischen zwei Gerichten geklärt werden sollte. Das Abwägen von unterschiedlichen Rechtsverständnissen, Datenschutzgesetzen, Straf- und Persönlichkeitsrechten wird direkt dem privaten Unternehmen übertragen. Wie gewissenhaft die Prüfung der Anfrage an das Unternehmen ausfällt, ist für Außenstehende nicht nachvollziehbar. Wie *Abbildung 1* verdeutlicht, werden außerdem eventuell relevante Jurisdiktionen beim bisherigen Status Quo ignoriert: Der physische Ort der Server sowie Aufenthaltsort bzw. Lebensmittelpunkt oder Nationalität des Nutzers.

Microsoft wehrt sich zurzeit vor Gericht gegen eine solche Anfrage nach Nutzerdaten durch US-amerikanische Strafverfolgungsbehörden, die nach Microsofts Auffassung nur über ein Rechtshilfegesuch möglich ist, da die verlangten Daten sich auf einem Server im Ausland befinden.[8] Im konkreten Fall ging es darum, dass US-amerikanische Strafverfolgungsbehörden auch auf Nutzerdaten zugreifen wollen, die auf Servern in Irland liegen, welche nicht durch die US amerikanische Microsoft Corp. sondern die irische Tochtergesellschaft betrieben werden. In den bisher durchlaufenen Instanzen war die Antwort des Gerichtes recht eindeutig: US-amerikanische Strafverfolgungsbehörden haben auch direkten Zugriff auf Daten, die auf Microsofts Servern in Irland liegen.

Die Ratio der Rechtsprechung[9] des New Yorker Gerichts ist dabei folgende: Zum einen befinden sich die Nutzerdaten in Microsofts „Besitz“. Dadurch sei es irrelevant, wo genau die Server stünden, da das inländische Unternehmen den nationalen Gesetzen unterliegt. Im konkreten Fall wird diese Pflicht zur Datenherausgabe außerdem vom US amerikanischen Mutterkon-

zern (Microsoft Corporation) auf die irische Microsoft Tochter übertragen.[10] Zum anderen wird angeführt, dass die Prozesse bei Rechtshilfeabkommen wesentlich zu lange dauern, als dass sie zur Sicherung digitaler Beweise adäquat wären.[11] Ein Argument, das auch durch deutsche Strafverfolgungsbehörden als Rechtfertigung für direkte Anfragen hervorgebracht wird.[12] Einzig relevant für das New Yorker Gericht ist somit, dass der Hauptsitz des Unternehmens in den USA ist. Dadurch haben US-amerikanische Strafverfolgungsbehörden Zugriff auf jegliche Nutzerdaten des Unternehmens – ganz gleich, wo auf der Welt diese liegen.[13]

Bei dem Rechtsstreit geht es um schwerwiegende Konsequenzen. Verliert Microsoft den Prozess, hätte dies zur Folge, dass US-amerikanische Strafverfolgungsbehörden aufgrund der internationalen Vormachtstellung US-amerikanischer Cloud-Anbieter, direkten Zugriff auf die überwiegende Mehrheit der Cloud-Daten hätten. Dadurch werden zum einen nationale und europäische Datenschutzbestimmungen effektiv unterwandert. Zum anderen findet eine Art Privatisierung des Rechts statt, da nun Cloud-Anbieter bei extraterritorialen Datenanfragen die Aufgabe ausländische Gerichte übernehmen, indem sie abwägen welchen Anfragen sie Folge leisten und welchen nicht.[14]

Auch Gerichte anderer Länder sind in der Vergangenheit einer ähnlichen Ratio in Bezug auf extraterritorialen Zugriff auf Nutzerdaten gefolgt. 2011 hatte sich Yahoo! vor belgischen Gerichten gegen die Herausgabe von E-Mails gewehrt – erfolglos. Auch, wenn Yahoo! keine Niederlassung in Belgien hat, argumentierte das Gericht, dass es belgischen Bürgern Dienste anböte (Marktortprinzip) und somit den Anfragen belgischer Strafverfolgungsbehörden Folge leisten müsse.[15]

Wichtig ist hier zu beachten, dass die Nationalität der Nutzer in den erwähnten Gerichtsfällen irrelevant war. Der Dienstanbieter kann in aller Regel keine definitive Aussage über die Staatsangehörigkeit des Nutzers machen.

In den beiden erwähnten Fällen stand der Rechtsweg über Rechtshilfeabkommen offen und wurde bewusst nicht gewählt. Durch die starke Dominanz US-amerikanischer Cloud-Anbieter ist der Microsoft-Fall jedoch wesentlich kritischer zu bewerten: Unter den 10 größten IaaS-, PaaS- oder SaaS-Anbietern sind jeweils mindestens 9 US-amerikanische Unternehmen. Nach geltender Rechtsprechung haben US-amerikanische Strafverfolgungsbehörden weltweit Zugriff auf personenbezogene Nutzerdaten dieser Cloud-Anbieter. Bei Anfragen durch ausländische Strafverfolgungsbehörden liegt die Entscheidung beim US-amerikanischen Unternehmen, ob und in welchem Umfang sie kooperieren. Wie Unternehmen mit diesen Anfragen umgehen ist sehr intransparent. Das Wissen über dieses Phänomen beruht hauptsächlich auf freiwilligen Auskünften in Transparenzberichten.

Modernisierung der Prozesse

Die Entwertung der Rechtshilfeabkommen führt zu einer Vielzahl an Problemen. Ein paar Sätze zum Verlust an Legitimität wenn internationale Normen der Zusammenarbeit unterhöhlt werden.

Durch ein Umgehen von Rechtshilfeabkommen werden nicht nur Datenschutzrichtlinien unterwandert,[16] sondern langfristig wird es auch zu einem Wettlauf um Sanktionen kommen: In den Entwürfen der EU Datenschutz-Grundverordnung (DG-VO) war Artikel 42 hart umkämpft und wurde abwechselnd gestrichen und wieder eingeführt.[17] Dieser Artikel soll unterbinden, dass personenbezogene Daten von EU Bürgern an Drittländer weitergegeben werden, solange dies nicht auf Grundlage von Rechtshilfeabkommen oder gleichwertigen bilateralen Abkommen geschieht. Bei Verstoß sollen Bußgelder in Höhe von mindes-

tens 100 Mio. Euro auferlegt werden. Es ist abzusehen, dass private Unternehmen im Zweifelsfall schlicht abwägen werden, welche Verhaltensweise für sie die geringeren Sanktionen bedeutet. Für US-amerikanische Unternehmen bedeutet der direkte Zugriff heimischer Strafverfolgungsbehörden jedoch vor allem ein Vertrauensverlust und somit Umsatzeinbußen – gerade in Europa.

Wir brauchen eine Debatte, wie der extraterritoriale Zugriff auf Daten durch Strafverfolgungsbehörden wieder rechtsstaatlichen Prozessen unterworfen werden kann. Dazu müssen in einem ersten Schritt die relevanten technischen und rechtlichen Problemfelder identifiziert werden. Denn jegliche Versuche etwas am Status Quo zu ändern, müssen sich der Herausforderung stellen, die damit verbundenen Prozesse an die Realitäten des digitalen Zeitalters anzupassen. Im Folgenden werden bestimmte Problemfelder aufgezeigt:

Schon heute fällt es schwer die Jurisdiktion der angefragten Daten und den Serverstandort genau zu benennen. Dies wird in Zukunft nahezu unmöglich werden, da ein einziger Infrastrukturanbieter Serverstandorte in 50 und mehr Ländern betreiben kann und die Daten je nach Nachfrage voll-automatisiert und in nahezu Echtzeit über verschiedenste Server verteilt. Ein starrer Fokus auf den „tatsächlichen“ Speicherort der angefragten Daten scheint wenig zielführend, da es schon jetzt nicht einen einzigen sondern etliche gleichzeitige Speicherorte geben kann. Auch im Microsoft-Irland Fall lag ein Teil der angefragten Nutzerdaten in den Vereinigten Staaten und ein weiterer in Irland.

Gleichzeitig sollte die sinkende Relevanz der physischen Lokalität der Daten nicht dazu führen, dass lediglich der Hauptsitz des Unternehmens ausschlaggebend ist. Genau gegen diese Ratio klagt Microsoft zu Recht in den Vereinigten Staaten. Auch aus Perspektive der Verbraucher wäre es unzumutbar, Hauptsitz und Gerichtsbarkeit des Dienstanbieters kennen zu müssen, um somit Rückschlüsse auf die geltenden Datenschutzgesetze zu ziehen. So unterliegen Google, Twitter und LinkedIn ausschließlich der Gerichtsbarkeit Kaliforniens. Microsoft, Yahoo! und Apple hingegen besitzen in verschiedenen Regionen der Welt rechtliche Entitäten. Dieser Unterschied in der Gerichtsbarkeit kann potenziell weitreichende Konsequenzen für die Nutzer haben.

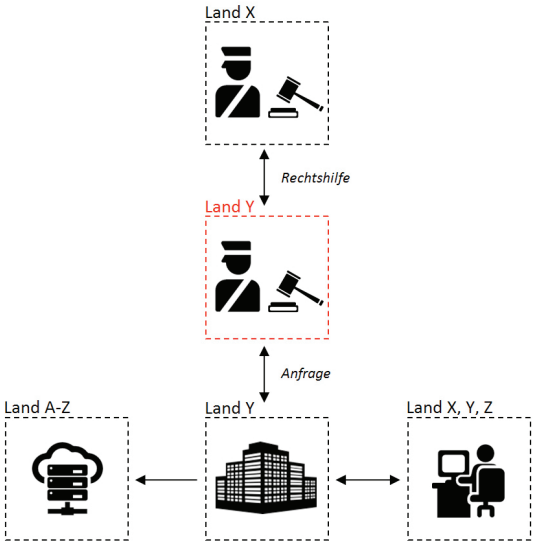
Neben dem Serverstandort und der Jurisdiktion des Unternehmens ist eine weitere relevante Größe der Lebensmittelpunkt des Nutzers. Im Gegensatz zur Nationalität können Diensteanbieter u.a. aufgrund der IP-Adresse häufig Aussagen über den wahrscheinlichen Lebensmittelpunkt des Nutzers treffen.

Letztlich sind natürlich auch die Gesetze der ermittelnden, ausländischen Strafverfolgungsbehörde relevant. Wie zuvor erwähnt, sind somit leicht drei bis vier unterschiedliche Jurisdiktionen involviert. Die Notwendigkeit einer Abwägung zwischen diesen potenziell kollidieren Rechtsverständnissen scheint daher zwingend notwendig.

Besteht ein Rechtshilfeabkommen zumindest zwischen Land X (ermittelnde Strafverfolgungsbehörde) und Land Y (Sitz des Unternehmens) sollte hier grundsätzlich der Weg über die Rechtshilfe genommen werden, da sich dann ein Teil der Verantwortung vom Unternehmen zur Strafverfolgungsbehörde des eigenen Landes (Y) verschiebt. (*Siehe Abbildung 2*) Genau dieser Prozess des Ersuchens der Rechtshilfe muss beschleunigt werden. Im Falle der Vereinigten Staaten (Kalifornien) besteht dieser aus 14 formalen Schritten.[18] Auch wenn im Idealfall eine Bearbeitungszeit von 45 Minuten bis zur Beweisübergabe möglich ist[19],

vergehen in der Regel 6-18 Monate. Daher ist es wenig verwunderlich, dass Strafverfolgungsbehörden andere Wege suchen, um an die Informationen zu gelangen.[20]

Abbildung 2: Einbeziehung weiterer Strafverfolgungsbehörde durch Rechtshilfeersuchen



Von zentraler Bedeutung ist hier, dass beim Ersuchen der Rechtshilfe die Informationsflüsse beschleunigt werden, so viel wie möglich automatisiert abläuft und der gesamte Prozess transparenter gestaltet wird. Denn zurzeit ist eines der Hauptprobleme, dass es erst ganz am Ende des Prozesses Feedback an die anfragende Behörde gibt – für diese ist das Rechtshilfeersuchen daher eine Black-Box.[21] Langfristig muss das Ziel sein, dass private Unternehmen, im Gegensatz zur jetzigen Situation statt einer bewertenden eine vermittelnde Rolle einnehmen. Nur wenn es kein Rechtshilfeabkommen zwischen dem anfragenden Land und dem Land des Unternehmenssitzes gibt, sollten Diensteanbieter direkte Anfragen selbst bearbeiten. In dieser Situation kann sich z.B. am Vorschlag der *Necessary and Proportionate-Prinzipien* orientiert werden: Im Zweifelsfall sollte sich nach dem Datenschutzgesetz gerichtet werden, das die Persönlichkeitsrechte des Nutzers am besten schützt.[22]

> *„…where the laws of more than one state could apply to Communications Surveillance, the available standard with the higher level of protection for individuals is applied.“*

Da das (Neu)Verhandeln von Rechtshilfeabkommen sehr langwierig ist, sollte im ersten Schritt die Praxis modernisiert werden. So wurden in jüngster Vergangenheit in den Vereinigten Staaten einige Initiativen zur Verbesserung der Rechtssicherheit zum (extraterritorialen) Zugriff auf Nutzerdaten durch Strafverfolgungsbehörden initiiert:

- Digital Due Process[23] ist eine Initiative dutzender US amerikanischer IT-Unternehmen, Cloud-Anbieter und Bürgerrechtsorganisationen, um den Electronic Communications Privacy Act (ECPA) von 1986 zu modernisieren.

- Laut Antrag[24] soll das US amerikanische Justizministerium 2015 zusätzlich 24.1 Mio USD zur Modernisierung der Prozesse bei Rechtshilfeabkommen erhalten. Neben der Einführung von Online-Formularen und der engeren Kooperation mit Unternehmen sollen vor allem zusätzliche Mitarbeiter eingestellt und geschult werden. Ziel ist es die Beantwortungszeit bis Ende 2015 zu halbieren.

- Drei US Senatoren (in Kooperation mit verschiedenen Bürgerrechtsorganisationen) haben den Law Enforcement Access to Data Stored Abroad Act (LEADS Act)[25] vorgestellt, der zumindest bewirken würde, dass Strafverfolgungsbehörden nicht mehr direkt auf extraterritoriale Nutzerdaten zugreifen können. Ausgenommen wären jedoch Nutzerdaten von US-Bürgern auf ausländischen Servern.

Auch auf europäischer Ebene wird sich mit dem extraterritorialen Zugriff bzw. der Weitergabe personenbezogener Daten durch private Unternehmen an Drittländer beschäftigt. So hat sich der irische Minister für Europaangelegenheiten und Datenschutz, Dara Murphy, bzgl. des Microsoft-Falls an die Europäische Kommission gewandt.[26] Auch auf internationaler Ebene wurde erkannt, dass eine Modernisierung der Rechtshilfeabkommen dringend notwendig ist, um den extraterritorialen Zugriff auf digitale Daten durch Strafverfolgungsbehörden zu legitimieren. Unter anderem hatte die internationale Handelskammer (ICC) hierzu 2012 konkrete Reformvorschläge veröffentlicht.[27]

Schlussfolgerungen

Private und berufliche Kommunikation findet immer mehr über das Internet statt. Diese digitalen Daten liegen nicht mehr nur auf dem eigenen Computer sondern zunehmend „in der Cloud“. Sicherheitsbehörden haben ein starkes Interesse daran, bei Ermittlungen möglichst zügig und unkompliziert auf jene Cloud zugreifen zu können – ganz gleich, wo genau sich die entsprechenden Daten physisch befinden. Es ist nachvollziehbar, dass Strafermittler nicht Monate, teils Jahre, auf die Sicherstellung von Beweisen warten können. Gleichzeitig darf diese Notwendigkeit nicht dazu führen, dass Datenschutzrichtlinien umgangen werden und internationale Abkommen aufgrund von pragmatischen Überlegungen ignoriert werden. Dies untergräbt langfristig das Vertrauen in den Rechtsstaat und die Integrität Informationstechnischer Systeme und fördert letztlich auch den Protektionismus einzelner Staaten. Die einzig gute Antwort auf dieses Problem ist es, die Prozesse der Rechtshilfe an das 21. Jahrhundert anzupassen. Die derzeitige Praxis mit ihrem Mangel an rechtsstaatlich legitimierten Prozessen ist für alle involvierten Parteien – Strafverfolgung, Unternehmen und Nutzer bzw. Kunden – unbefriedigend.

Globalisierung von Kommunikation und Datenströmen darf nicht zu einer Schwächung von rechtsstaatlichen Normen und Prozessen führen. Ziel muss es daher sein, den Zugriff auf Cloud-Daten rechtsstaatlich und transparent zu regeln und zu legitimieren. Rechtshilfeabkommen sind hierfür ein wichtiges Mittel. Jeglicher Datenzugriff durch Sicherheitsbehörden sollte erst nach einer Abwägung der entsprechenden nationalen Rechtsrahmen bzgl. Datenschutz, Persönlichkeitsrechte und dem Strafverfolgungsinteresse stattfinden. Diese Abwägungen können und sollten nicht durch private Unternehmen getroffen werden, sondern müssen von rechtsstaatlich legitimierten Institutionen vorgenommen werden.

Endnoten

1 Vitzthum, Thomas Sebastian. 2013. „Auf deutschem Boden gilt deutsches Recht". Die Welt. http://www.welt.de/politik/deutschland/article118207603/Auf-deutschem-Boden-gilt-deutsches-Recht.html

2 http://www.clouds360.com/iaas.php

3 The Top 20 Platform as a Service (PaaS) Vendors. http://www.clouds360.com/paas.php

4 Services and SaaS trends. PwC. http://www.pwc.com/gx/en/technology/publications/global-software-100-leaders/saas-trends.jhtml

5 Walden, Ian, Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent (November 14, 2011). Queen Mary School of Law Legal Studies Research Paper No. 74/2011. http://ssrn.com/abstract=1781067

6 Transparency Reporting Index. 2015. Access Now. https://www.accessnow.org/pages/transparency-reporting-index

7 Google Transparency Report. 2014. http://www.google.com/transparencyreport/userdatarequests/countries/

8 Mason Hayes & Curran. 2014. „Can US law enforcement access information on Irish servers? – the Microsoft saga". http://www.lexology.com/library/detail.aspx?g=5e75da37-60c5-4409-91a3-e47407958459

9 United States District Court Southern District Of New York. 2014. „In The Matter Of A Warrant To Search A Certain E-Mail Account Controlled And Maintained By Microsoft Corporation". http://www.nysd.uscourts.gov/cases/show.php?db=special&id=398

10 Kai-Uwe Plath. 2014. „Datenherausgabepflicht für Cloud-Anbieter nach US-Recht vs. EU-Datenschutzrecht". CR-Online. http://www.cr-online.de/blog/2014/05/13/datenherausgabepflicht-fuer-cloud-anbieter-nach-us-recht-vs-eu-datenschutzrecht/

11 PayPal White Paper. 2011. „Combating Cybercrime – Principles, Policies and Programs"
https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf

12 Philip Banse. 2012. „Online-Überprüfung potenzieller Straftäter". Deutschlandfunk http://www.deutschlandfunk.de/online-ueberpruefung-potenzieller-straftaeter.862.de.html?dram:article_id=227768

13 Greg Nojeim. 2014. „Microsoft Ireland Case: Can a US Warrant Compel A US Provider to Disclose Data Stored Abroad?". https://cdt.org/insight/microsoft-ireland-case-can-a-us-warrant-compel-a-us-provider-to-disclose-data-stored-abroad/

14 Google Transparenzbericht Deutschland. 2014. http://www.google.com/transparencyreport/userdatarequests/?hl=de

15 BNA International. „The Belgian Yahoo! Case: Supreme Court Provides Broad Interpretation Of Concept Of 'Electronic Communication Service Provider'". World Data Protection Report, Volume 11 Number 4. https://www.huntonprivacyblog.com/uploads/file/Belgian_Yahoo_Case.pdf

16 Irish Government News Service. 2014. „European Commission agrees to consider request on Microsoft case – Murphy". http://www.merrionstreet.ie/en/News-Room/Releases/European_Commission_agrees_to_consider_request_on_Microsoft_case_–_Murphy_.html

17 „LIBE-Ausschuss bestätigt Gesetzentwurf zur EU-Datenschutz-Grundverordnung". 2013. https://www.datenschutzbeauftragter-info.de/libe-ausschuss-bestaetigt-gesetzentwurf-zur-eu-datenschutz-grundverordnung/

18 Kate Westmoreland und Gail Kent. 2015. „International Law Enforcement Access to User Date: A Survival Guide and Call for Action". Working Paper. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2547289

19 Luisa Seeling und Varinia Bernau. 2015. „Warum Microsoft für Landesgrenzen im Netz kämpft". Süddeutsche.de. http://www.sueddeutsche.de/digital/ueberwachung-warum-microsoft-fuer-landesgrenzen-im-netz-kaempft-1.2314365

20 Siehe Endnote 7

21 Acces Now. 2014. „MLAT: A four-letter-word in need of reform, Access Now". https://www.accessnow.org/blog/2014/01/09/mlat-a-four-letter-word-in-need-of-reform

22 Necessary and Proportionate: Principle 12: Safeguards For International Cooperation https://en.necessaryandproportionate.org/text#principle_12

23 Digital Due Process – Modernizing Surveillance Laws for the Internet Age. http://www.digitaldueprocess.org/

24 Letter to US Congress Urging Increase to MLAT Funding. https://cdt.org/insight/letter-to-us-congress-urging-increase-to-mlat-funding/

25 Greg Nojeim. 2014. „LEADS Act Extends Important Privacy Protections, Raises Concerns". Center for Democracy and Technology. https://cdt.org/blog/leads-act-extends-important-privacy-protections-raises-concerns/

26 Irish Government News Service. 2014. „Minister for European Affairs and Data Protection requests legal brief by European Commission in Microsoft case". http://merrionstreet.ie/en/News-Room/Releases/Minister_for_European_Affairs_and_Data_Protection_requests_legal_brief_by_European_Commission_in_Microsoft_case.html

27 International Chamber of Commerce. 2012. „ICC policy statement on Using Mutual Legal Assistance Treaties (MLATs) To Improve Cross-Border Lawful Intercept Procedures". http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2012/mlat/

Über die Stiftung

Die stiftung neue verantwortung ist ein unabhängiger, gemeinnütziger und überparteilicher Think Tank mit Sitz in Berlin. Sie fördert kreatives, interdisziplinäres und sektor-übergreifendes Denken zu den wichtigsten gesellschaftspolitischen Themen und Herausforderungen des 21. Jahrhunderts. Durch ihr Fellow- und Associateprogramm ermöglicht sie den intensiven Austausch junger Experten, Praktiker und Vordenker aus Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft.

Danksagung

Der Autor bedankt sich besonders bei den Teilnehmerinnen und Teilnehmern des Workshops *IT-Sicherheit und Zugriff auf extra-territoriale Daten: Technische und rechtliche Lösungsansätze* vom 12. Dezember 2014 in Kooperation mit dem Hasso-Plattner-Institut und bei Eric H. Loeb.

Impressum

stiftung neue verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin
T. +49 30 81 45 03 78 80
F. +49 30 81 45 03 78 97
www.stiftung-nv.de
info@stiftung-nv.de

Gestaltung:
Pentagram Design, Berlin

Schlusslektorat:
Franziska Wiese

Kostenloser Download:
www.stiftung-nv.de