Bezirksgericht Southern District of New York (SDNY): US-Beschlagnahmebeschluss kann auch Cloud-Daten im Ausland umfassen

18 U.S.C. §§ 2701 – 2712
Entscheidung (Richter James C. Francis IV, US Magistrate Judge) vom 25.4.2014 – 13 Mag. 2814

Leitsatz der Redaktion

Eine von einem US-Richter gegen einen Internet Service Provider erlassene strafrechtliche Beschlagnahmeanordnung für E-Mail-Verkehr (SCA-Warrant) kann auch in der EU belegene Daten umfassen.

Anm. d. Red.: Vgl. hierzu auch *EuGH* ZD 2014, 350 m. Anm. *Karg* – in diesem Heft = *EuGH* MMR 7/2014 m. Anm. *Sörup* und *Voigt*, MMR 2014, 158.

E-Mail-Daten
Cloud Computing
Speicherort
Auskunftsersuchen
Internet Service Provider

Sachverhalt

Microsoft Corp. (*Microsoft*) moves to quash a search warrant to the extent that it directs *Microsoft* to produce the contents of one of its customer's e-mails where that information is stored on a server located in Dublin, Ireland. *Microsoft* has long owned and operated a web-based e-mail service that has existed at various times under different internet domain names, including Hotmail.com, MSN.com, and Outlook.com. Users of a *Microsoft* e-mail account can, with a user name and a password, send and receive email messages as well as store messages in personalized folders. E-mail message data include both content information (the message and subject line) and non-content information (such as the sender address, the recipient address, and the date and time of transmission). *Microsoft* stores e-mail messages sent and received by its users in its datacenters. Those datacenters exist at various locations both in the United States and abroad, and where a particular user's information is stored depends in part on a phenomenon known as "network latency"; because the quality of service decreases the farther a user is from the datacenter where his account is hosted, efforts are made to assign each account to the closest datacenter. Accordingly, based on the "country code" that the customer enters at registration, *Microsoft* may migrate the account to the datacenter in Dublin. When this is done, all content and most non-content information associated with the account is deleted from servers in the United States. The non-content information that remains in the United States when an account is migrated abroad falls into three categories.

First, certain non-content information is retained in a data warehouse in the United States for testing and quality control purposes. Second, *Microsoft* retains "address book" information relating to certain web-based e-mail accounts in an "address book clearing house." Finally, certain basic non-content information about all accounts, such as the user's name and country, is maintained in a database in the United States.

On December 4, 2013, in response to an application by the United States, I issued the search warrant that is the subject of the instant motion. That warrant authorizes the search and seizure of information associated with a specified web-based e-mail account that is "stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at One Microsoft Way, Redmond, WA." The information to be disclosed by *Microsoft* pursuant to the warrant consists of:

- The contents of all e-mails stored in the account, including copies of e-mails sent from the account;
- All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and sources of payment (including any credit or bank account number);
- All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
- All records pertaining to communications between MSN ... and any person regarding the account, including contacts with support services and records of actions taken.

It is the responsibility of Microsoft's Global Criminal Compliance (GCC) team to respond to a search warrant seeking stored electronic information. Working from offices in California and Washington, the GCC team uses a database program or "tool" to collect the data. Initially, a GCC team member uses the tool to determine where the data for the target account is stored and then collects the information remotely from the server where the data is located, whether in the United States or elsewhere. In this case, *Microsoft* complied with the search warrant to the extent of producing the non-content information stored on servers in the United States. However, after it determined that the target account was hosted in Dublin and the content information stored there, it filed the instant motion seeking to quash the warrant to the extent that it directs the production of information stored abroad.

Aus den Gründen

The obligation of an Internet Service Provider (ISP) like *Microsoft* to disclose to the Government customer information or records is governed by the Stored Communications Act (SCA), passed as part of the Electronic Communications Privacy Act of 1986 (ECPA) and codified at 18 U.S.C. §§ 2701–2712. That statute authorizes the Government to seek information by way of subpoena, court order, or warrant. The instrument law enforcement agents utilize dictates both the showing that must be made to obtain it and the type of records that must be disclosed in response.

First, the *Government* may proceed upon an "administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena", 18 U.S.C. § 2703(b)(1)(B)(i). In response, the service provider must produce (1) basic customer information, such as the customer's name, address, Internet Protocol connection records, and means of payment for the account, 18 U.S.C. § 2703(c)(2); unopened e-mails that are more than 180 days old, 18 U.S.C. § 2703(a); and any opened e-mails, regardless of age, 18 U.S.C. §§ 2703(b)(1)(B)(i). ... The usual

standards for issuance of compulsory process apply, and the SCA does not impose any additional requirements of probable cause or reasonable suspicion. However, the *Government* may obtain by subpoena the content of e-mail only if prior notice is given to the customer, 18 U.S.C. § 2703(b)(1)(B)(i). If the *Government* secures a court order pursuant to 18 U.S.C. § 2703(d), it is entitled to all of the information subject to production under a subpoena and also "record(s) or other information pertaining to a subscriber (...) or customer," such as historical logs showing the e-mail addresses with which the customer had communicated, 18 U.S.C. § 2703(c)(1). In order to obtain such an order, the *Government* must provide the court with "specific and articulable facts showing that there are reasonable grounds to believe that the content of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation", 18 U.S.C. 2703(d).

Finally, if the *Government* obtains a warrant under section 2703(a) (SCA Warrant), it can compel a service provider to disclose everything that would be produced in response to a section 2703(d) order or a subpoena as well as unopened e-mails stored by the provider for less than 180 days. In order to obtain an SCA Warrant, the *Government* must "us(e) the procedures described in the Federal Rules of Criminal Procedure" and demonstrate probable cause (18 U.S.C. § 2703(a); see Fed. R. Crim. P. 41(d)(1) – requiring probable cause for warrants).

Microsoft's argument is simple, perhaps deceptively so. It notes that, consistent with the SCA and Rule 41 of the Federal Rules of Criminal Procedure, the Government sought information here by means of a warrant. Federal courts are without authority to issue warrants for the search and seizure of property outside the territorial limits of the United States. Therefore, *Microsoft* concludes, to the extent that the warrant here requires acquisition of information from Dublin, it is unauthorized and must be quashed. That analysis, while not inconsistent with the statutory language, is undermined by the structure of the SCA, by its legislative history, and by the practical consequences that would flow from adopting it.

A. Statutory Language: ... This language is ambiguous in at least one critical respect. The words "using the procedures described in the Federal Rules of Criminal Procedure" could be construed to mean, as *Microsoft* argues, that all aspects of Rule 41 are incorporated by reference in Sec. 2703(a), including limitations on the territorial reach of a warrant issued under that rule. But, equally plausibly, the statutory language could be read to mean that while procedural aspects of the application process are to be drawn from Rule 41 (for example, the presentation of the application based on sworn testimony to a magistrate judge), more substantive rules are derived from other sources. ...

B. Structure of the SCA: The SCA was enacted at least in part in response to a recognition that the Fourth Amendment protections that apply in the physical world, and especially to one's home, might not apply to information communicated through the internet. ... In particular, the SCA authorizes the *Government* to procure a warrant requiring a provider of electronic communication service to disclose e-mail content in the provider's electronic storage.

Although Sec. 2703(a) uses the term "warrant" and refers to the use of warrant procedures, the resulting order is not a conventional warrant; rather, the order is a hybrid: part search warrant and part subpoena. It is obtained like a search warrant when an application is made to a neutral magistrate who issues the order only upon a showing of probable cause. On the other hand, it is executed like a subpoena in that it is served on the ISP in possession of the information and does not involve government agents entering the premises of the ISP to search its servers and seize the e-mail account in question. This unique structure supports the *Government's* view that the SCA does not implicate principles of extraterritoriality. It has long been the law that a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information (see Marc Rich & Co., A.G. v. United States, 707 F.2d 663, 667 (2d Cir. 1983); "Neither may the witness resist the production of documents on the ground that the documents are located abroad. The test for production of documents is control, not location" (citations omitted; Tiffany (NJ) LLC v. Qi Andrew, 276 F.R.D. 143, 147-48 (S.D.N.Y. 2011); "If the party subpoenaed has the practical ability to obtain the documents, the actual physical location of the documents – even if overseas – is immaterial."; in re NTL, Inc. Securities Litigation, 244 F.R.D. 179, 195 (S.D.N.Y. 2007); United States v. Chase Manhattan Bank, N.A., 584 F. Supp. 1080, 1085 (S.D.N.Y. 1984)). ... This approach is also consistent with the view that, in the context of digital information, "a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer" (Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 551 (2005)). In this case, no such exposure takes place until the information is reviewed in the United States, and consequently no extraterritorial search has occurred. ...

C. Legislative History: Although scant, the legislative history also provides support for the Government's position. When the SCA was enacted as part of the ECPA, the Senate report, although it did not address the specific issue of extraterritoriality, reflected an understanding that information was being maintained remotely by third-party entities. ... *Congress* thus appears to have anticipated that an ISP located in the United States would be obligated to respond to a warrant issued pursuant to section 2703(a) by producing information within its control, regardless of where that information was stored. ...

D. Practical Considerations: If the territorial restrictions on conventional warrants applied to warrants issued under section 2703(a), the burden on the *Government* would be substantial, and law enforcement efforts would be seriously impeded. If this were merely a policy argument, it would be appropriately addressed to *Congress*. But it also provides context for understanding congressional intent at the outset, for it is difficult to believe that, in light of the practical consequences that would follow, *Congress* intended to limit the reach of SCA Warrants to data stored in the United States. First, a service provider is under no obligation to verify the information provided by a customer at the time an e-mail account is opened. Thus, a party intending to engage in criminal activity could evade an SCA Warrant by the simple expedient of giving false residence information, thereby causing the ISP to assign his account to a server outside the United States.

Second, if an SCA Warrant were treated like a conventional search warrant, it could only be executed abroad pursuant to a Mutual Legal Assistance Treaty (MLAT). As one commentator has observed, "This process generally remains slow and laborious, as it requires the cooperation of two governments and one of those governments may not prioritize the case as highly as the other" (Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Penn. L. Rev. 373, 409 (2014)). Moreover, nations that enter into MLATs nevertheless generally retain the discretion to decline a request for assistance. For example, the MLAT between the United States and Canada provides that "(t)he Requested State may deny assistance to the extent that ... execution of the request is contrary to its public interest as determined by its Central Authority" (Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Can., March 18, 1985, 24 I.L.M.

1092 (U.S.-Can. MLAT), Art. V(1)). Similarly, the MLAT between the United States and the United Kingdom allows the Requested State to deny assistance if it deems that the request would be "contrary to important public policy" or involves "an offense of a political character" (Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-U.K., Jan. 6, 1994, S. Treaty Doc. No. 104-2 (U.S.-U.K. MLAT), Art. 3(1)(a) & (c)(i)). Indeed, an exchange of diplomatic notes construes the term "important public policy" to include "a Requested Party's policy of opposing the exercise of jurisdiction which is in its view extraterritorial and objectionable" (Letters dated January 6, 1994 between *Warren M. Christopher*, Secretary of State of the United States, and *Robin W. Renwick*, Ambassador of the United Kingdom of Great Britain and Northern Ireland, attached to U.S.-U.K. MLAT).

Finally, in the case of a search and seizure, the MLAT in both of these examples provides that any search must be executed in accordance with the laws of the Requested Party (U.S.-Can. MLAT, Art. XVI(1); U.S.-U.K. MLAT, Art. 14(1), (2)). This raises the possibility that foreign law enforcement authorities would be required to oversee or even to conduct the acquisition of information from a server abroad. Finally, as burdensome and uncertain as the MLAT process is, it is entirely unavailable where no treaty is in place. ... Thus, under *Microsoft's* understanding, certain information within the control of an American service provider would be completely unavailable to American law enforcement under the SCA. ... The practical implications thus make it unlikely that *Congress* intended to treat a Sec. 2703(a) order as a warrant for the search of premises located where the data is stored.

E. Principles of Extraterrioriality: ... But the concerns that animate the presumption against extraterritoriality are simply not present here: an SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored. At least in this instance, it places obligations only on the service provider to act within the United States. ... Thus, the nationality principle, one of the well-recognized grounds for extension of American criminal law outside the nation's borders (see Marc Rich, 707 F.2d at 666, citing Introductory Comment to Research on International Law, Part II, Draft Convention on Jurisdiction With Respect to Crime, 29 Am. J. Int'l Law 435, 445 (Supp. 1935)), supports the legal requirement that an entity subject to jurisdiction in the United States, like *Microsoft*, may be required to obtain evidence from abroad in connection with a criminal investigation. ... But this language, too, does not advance *Microsoft's* cause. The fact that protections against "interceptions and disclosures" may not apply where those activities take place abroad hardly indicates that *Congress* intended to limit the ability of law enforcement agents to obtain account information from domestic service providers who happen to store that information overseas.

Conclusion: Even when applied to information that is stored in servers abroad, an SCA Warrant does not violate the presumption against extraterritorial application of American law. Accordingly, *Microsoft's* motion to quash in part the warrant at issue is denied. ...

Anmerkung

RA Dr. Christian Schröder, BDO Legal, Düsseldorf / RA Dr. Axel Spies, Bingham McCutchen, Washington DC

Die hier in Auszügen abgedruckte Entscheidung des *Bezirksgerichts Southern District of New York* (*SDNY*) gegen *Microsoft* hat in der Cloud Computing-Szene zu Unruhe geführt. Das *Gericht* hat am 4.12.2013 auf Antrag der Vereinigten Staaten (die beantragende Behörde wurde nicht genannt) einen Durchsuchungs- und Beschlagnahmebeschluss (Warrant) erlassen. Die Ermächtigung für diesen Warrant liegt, wie aus den Entscheidungsgründen ersichtlich, in 18 U.S.C. § 2703(a), der aus dem Stored Communications Act (SCA) folgt und Teil des Electronic Communications Privacy Act von 1986 (ECPA) ist. Der vom *SDNY* erlassene Warrant verpflichtet *Microsoft* zur Herausgabe von Informationen in Bezug auf einen E-Mail-Account, unabhängig vom Speicherungsort der belegenen Daten. *Microsoft* gab hierauf abgefragte Informationen heraus, die *Microsoft* auf einem in den USA belegenen Server gespeichert hatte. *Microsoft* verweigerte jedoch die Herausgabe von Informationen, die auf einem in Dublin, Irland, belegenen Server gespeichert waren und legte insofern Beschwerde zur *Kammer* (*Trial Judge*) ein. *Microsoft* war und ist der Auffassung, dass ein US-Bundesgericht nicht zuständig ist für den Erlass von SCA-Warrants, die außerhalb des Territoriums der USA belegene Informationen erfassen. Der mit der Beweisaufnahme befasste Einzelrichter des Bezirksgerichts SDNY, *Richter Francis* (Magistrate Judge), lehnte in dem ausführlichen Urteil (s.o.) diese Auffassung ab. *Microsoft* hat das Urteil unmittelbar danach angefochten und sieht sich und andere am Beginn einer längeren rechtlichen Auseinandersetzung. Die *Kammer* hat über den Warrant v. 4.12.2013 bei Redaktionsschluss noch nicht entschieden. Die Prozessakten sind der Öffentlichkeit nicht zugänglich.

In der Cloud Computing-Szene wird die Entscheidung des *Bezirksgericht SDNY* teilweise mit Sorge gesehen. Setzte sich die Auffassung des Einzelrichters *Francis* durch, würden grds. selbst dann keine bei US-Unternehmen gespeicherten Daten vor dem Zugriff von US-Behörden „sicher" sein, wenn sie auf Servern außerhalb der USA gespeichert sind. Damit würde die Strategie verschiedener US-Dienstleister, insb. EU-Datenschutzsorgen wegen aus europäischer Sicht exzessiver Zugriffe auf EU-Daten u.a. auf Grund des US Patriot Act durch Verlagerung ihrer Server ins Ausland zu begegnen, durchkreuzt. Die von US-Internet Service Providern (ISPs) auf EU-Servern gespeicherten Daten auch z.B. europäischer Bürger wären demnach nicht „absolut" sicher gegen Zugriffe von US-Behörden. Dies könnte leicht dazu führen, dass EU-Anbieter mit angeblich vor US-Zugriff sicheren Servern für ihre Produkte und Dienstleistungen und somit mit der Angst der EU-Bürger für ihre Dienste werben. Verlöre hingegen die *US-Regierung* den Prozess rechtskräftig, wäre möglicherweise zeitnah mit einer Korrektur des ECPA durch den *Kongress* zu rechnen, da dieser die Strafverfolgung vermutlich nicht auf lediglich in den USA belegene Informationen beschränkt sehen will.

Bei genauerer Bewertung der noch nicht rechtskräftigen Entscheidung des *US District Court* wird jedoch deutlich, dass ein Zugriff nach dem SCA keine für die Privatsphäre vergleichbare Bedrohung darstellt wie die Zugriffe nach dem US Patriot Act oder PRISM etc. Insofern stellt sich hier auch kein bzw. kein so starker Konflikt mit dem europäischen Datenschutzrecht. Darüber hinaus muss angesichts eines im Regelfall sehr breiten Jurisdiktionsverständnisses in den USA auch eine Behauptung über eine angebliche Sicherheit von Daten vor US-Zugriffen im Einzelfall hinterfragt werden. Immerhin kann bereits eine Zweigniederlassung oder Repräsentanz eines EU-Cloud-Diensteanbieters in den USA genügend Anknüpfungspunkte für die Anwendung von US-Recht bieten.

1. Auskunftsersuchen und Voraussetzungen für einen Warrant

Um die wichtigsten Punkte gleich vorwegzunehmen: Dem Warrant liegt offenbar kein Auskunftsersuchen der *NSA* zu Grunde. Die *NSA* erhält ihre Informationen entweder direkt durch eigene Ermittlungsmaßnahmen oder durch einen National Security Letter (NSL; vgl. *Spies*, ZD-Aktuell 2012, 03062). Wäre die Behörde

durch einen NSL vorgegangen, wäre die Entscheidung wahrscheinlich gar nicht der Öffentlichkeit bekannt geworden. Im Fall des vom *SDNY* erlassenen Warrant liegen die Dinge anders: Ein nach dem SCA erlassener Warrant wird von einem ordentlichen US-Gericht auf Grund eines auf Herausgabe bestimmter Informationen beschränkten Antrags erlassen und muss der Aufklärung in einem bereits eingeleiteten Strafverfahren dienen. Diese Voraussetzungen muss die Behörde dem Gericht vor Erlass des beantragten Warrant glaubhaft darlegen. Hierfür sind im Regelfall eidesstattliche Erklärungen erforderlich – vgl. Regel 18 U.S.C. § 2703(d) sowie o.g. Entscheidung: „In order to obtain such an order, the Government must provide the court with 'specific and articulable facts showing that there are reasonable grounds to believe that the content of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.'"

Diese für den Erlass eines Warrant zu nehmende Hürde ist daher relativ hoch. Wie sich auch insb. aus der Reaktion von *Microsoft* zeigt, kann das betroffene Unternehmen den Beschluss zudem rechtlich angreifen. Hierüber wird in einem ordentlichen Verfahren vor der *Kammer* entschieden. Eine solche Vorgehensweise ist der Beantragung eines Beschlagnahmebeschlusses nach deutschem Strafprozessrecht ähnlich und ist i.Ü. als Mittel strafrechtlicher Aufklärung allgemein in Rechtsstaaten anerkannt. Selbst die EU-Kommissarin *Reding*, die sich 2013 in einem an die USA gerichteten Brief gegen die extensiven Zugriffe von US-Geheimdiensten gewandt hat (Schreiben v. 10.6.2013, abrufbar unter: http://www.statewatch.org/news/2013/jun/eu-usa-reding-ag.letter.pdf), hat ausdrücklich Zugriffe zur Aufklärung bei spezifischen Verdachtslagen von ihrer Kritik ausgenommen.

Berücksichtigt man das konkrete Strafverfolgungsinteresse, sind auch die Ausführungen des Einzelrichters *Francis* zum Anwendungsbereich des Warrant durchaus verständlich. Seine Überlegungen, wonach Unternehmen den Zugriff von Strafverfolgungsbehörden nicht durch Wahl des Serverorts verhindern können sollen, sind auch aus europäischer Sicht nachvollziehbar, auch beim Cloud Computing, bei dem sich Speicherorte ggf. in Sekundenbruchteilen ändern. Warum sollte sich ein Rechtsstaat insofern i.R.e. Strafverfolgung auf Informationen beschränken, die in seinem Staatsgebiet gespeichert sind? Dies würde, worauf auch Richter *Francis* hinweist, Kriminellen Tür und Tor für ein Ausweichen in „zugriffsfeste" Jurisdiktionen öffnen. Kriminelle sollen sich nicht in der Cloud dem Zugriff verbergen können. Der *Einzelrichter* nimmt ausdrücklich Bezug auf Überlegungen, sich durch Offshore-Server dem Zugriff von jeglichen staatlichen Behörden zu entziehen, um seine Maßnahme zu rechtfertigen. Insofern stellt sich – zu Recht – die an dieser Stelle nicht zu vertiefende Frage, ob das Territorialprinzip beim Datenschutz in Zeiten des Cloud Computing ausgedient hat. Bislang beruhen die meisten Datenschutzgesetze jedoch auf diesem Prinzip (ausf. dazu *Spies*, AICGS Report (April 2014), German/U.S. Data Transfers Crucial for Both Economies, Difficult to Regain Trust, abrufbar unter: http://www.aicgs.org/site/wp-content/uploads/2014/04/IB-46-ERP-Data-Privacy-FINAL.pdf).

2. Beachtung des europäischen Datenschutzrechts?

Obwohl die Daten in Irland liegen und demnach zumindest beschränkt europäisches Datenschutzrecht Anwendung finden dürfte, finden sich in dem Urteil des *US-District Court* keine Ausführungen zur Lösung dieses potenziellen Rechtskonflikts. Ob *Microsoft* sich hierauf überhaupt berufen hat, ist nicht bekannt. Allerdings dürfte auch das Ergebnis einer solchen Berufung keineswegs klar vorhersehbar sein.

So stellt sich hier zunächst die Frage, in welchem Umfang europäisches Datenschutzrecht überhaupt auf die Speicherung von Daten auf einem in Europa belegenen Server Anwendung findet. Handelte es sich z.B. um eine reine Auftragsdatenverarbeitung für *Microsoft* in den USA, wäre durchaus fraglich, ob über die Einhaltung von technischen oder organisatorischen Anforderungen zur Datensicherung hinaus weitergehendes materielles Recht Anwendung fände (s. Fallgruppen F ff. der „Fallgruppen zur internationalen Auftragsdatenverarbeitung", Handreichung des *Düsseldorfer Kreises* zur rechtlichen Bewertung, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/HandreichungApril2007.html?nn=409242).

Unterstellt man eine umfassende Anwendung des materiellen Rechts, wäre hingegen für *Microsoft* ein Rechtskonflikt durchaus denkbar. So sieht das europäische Datenschutzrecht grds. keine Öffnung für den Zugriff fremder staatlicher Organe auf Daten vor, sofern dieser Zugriff nicht zugleich auch dem öffentlichen Interesse aus autonomer europäischer Sicht entspricht. In der Stellungnahme 10/2006 der *Art. 29-Datenschutzgruppe* zur Verarbeitung von personenbezogenen Daten durch die *Society for Worldwide Interbank Financial Telecommunication (SWIFT)* heißt es dementsprechend zur Datenübermittlung nach Art. 26 Abs. 1 lit. d der DS-RL: „Bei diesem Punkt der Richtlinie hatten die Verfasser ganz klare Vorstellungen, dass in diesem Zusammenhang nur wichtige öffentliche Interessen darunter fallen, die von der nationalen Gesetzgebung, die auf die in der EU niedergelassenen für die Verarbeitung von Daten Verantwortlichen Anwendung findet, auch als solche bezeichnet sind. Jede andere Auslegung würde es einer ausländischen Behörde leicht machen, das in der Richtlinie festgelegte Erfordernis eines angemessenen Schutzes im Empfängerland zu umgehen." (S. 31. abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_de.pdf).

Allerdings muss vorliegend berücksichtigt werden, dass der Zugriff des *US-Gerichts* offenbar der Strafverfolgung dient und in einem auch aus europäischer Sicht nachvollziehbaren rechtsstaatlichen Verfahren geregelt wird. Insofern spricht viel dafür, ein öffentliches Interesse an der Förderung eines strafrechtlichen Ermittlungsverfahrens auch aus autonomer europäischer Sicht zu bejahen. Sofern es sich bei den Daten jedoch um Daten eines deutschen Kunden von *Microsoft* handelt, dürften seine Daten nicht nur vom allgemeinen Datenschutzrecht, sondern auch vom Fernmeldegeheimnis geschützt sein. Ohne Einschaltung deutscher Behörden dürfte dann ein Zugriff auf solche vom Fernmeldegeheimnis geschützten Daten nicht zulässig sein.

3. Sind europäische Clouds „sicher"?

Vor dem Hintergrund der o.g. Überlegungen erscheinen folglich erste Reaktionen in der deutschen Presse, wonach das Urteil zu einer weiteren Stärkung einer „Festung Europa" führen könnte, deutlich überzogen. „Die Welt" v. 30.4.2014 interpretiert das nicht rechtskräftige Urteil so, dass der Richter damit „unfreiwillige Schützenhilfe für die Idee einer europäischen Cloud" gibt, die in Europa mit Unterstützung der Politik vorgebracht wird (abrufbar unter: http://www.welt.de/politik/deutschland/article127462262/Google-amp-Co-muessen-Europa-Daten-an-NSA-liefern.html). Einerseits ist der Zugriff auf klar umrissene Datensätze zum Zweck der Strafverfolgung nicht mit einem intransparenten und exzessiven Zugriff durch Geheimdienste vergleichbar. Andererseits dürfte auch die „Festung Europa" gar nicht so sicher sein, wie ihr Begriff andeutet. So ist keineswegs sicher, dass europäische Diensteanbieter schon dann nicht dem Zugriff von US-Behörden unterliegen, wenn sie ihre Dienste ausschließlich in Europa anbieten und dort ihre Server haben. Nach dem US-Patriot Act genügt schon eine Beteiligung von US-Unternehmen an dem europäischen Dienstleister, um auch dessen Informationen ungeachtet ihres Speicherorts herauszuverlangen.

Darüber hinaus kann bereits eine bloße Niederlassung oder Repräsentanz in den USA genügend Anknüpfungspunkte auch z.B. für die Anwendung des ECPA und des SCA geben. So ist der Wortlaut des ECPA durchaus offen und könnte z.B. auch einen europäischen ISP erfassen, wenn dieser über eine Niederlassung in den USA verfügt. Die einschlägige Vorschrift des 18 U.S.C. § 2703(b)(1)(B)(i) unterscheidet nämlich nicht zwischen inländischen und ausländischen Anbietern: „A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable." Auch der Begriff des „remote computing service" kann vom Wortlaut her jeden in der Welt ansässigen Diensteanbieter erfassen: „any service which provides to users thereof the ability to send or receive wire or electronic communications." Der Terminus „provider" ist gesetzlich in Sec. 50 U.S.C. § 1885 (6) wie folgt definiert: „The term 'electronic communication service provider' means
(A) a telecommunications carrier ...;
(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18;
(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18;
(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored;
(E) a parent, subsidiary, affiliate, successor, or assignee of an entity described in subparagraph (A), (B), (C), or (D); or
(F) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), (D), or (E)."

4. Was folgt hieraus für europäische Anbieter?

Sofern Rechtszuständigkeit (Jurisdiction) nach US-Recht besteht, könnte auch einem EU-Cloud-Anbieter (oder dessen US-Vertreter – s. Unterpunkt „F" der genannten Definition) ein SCA-Warrant zugestellt werden – egal wo die Daten tatsächlich gespeichert werden. In den USA wird der Begriff „Jurisdiction" sehr weit ausgelegt. *Voigt* (MMR 2014, 158,160) hat kürzlich dazu ausgeführt: „Sogar die Anwesenheit von Mitarbeitern in den USA, z.B. bei einer Dienstreise, kann die Anwendbarkeit des US-Rechts eröffnen." Wo die Grenzen genau liegen, ob z.B. eine Repräsentanz in den USA ausreicht, während die Server des Unternehmens in Europa liegen, muss im Einzelfall entschieden werden. Ein Zugriff auf Daten des Anbieters i.R.d. internationalen Rechtshilfe über die sog. zwischenstaatlichen MLATs (Mutual Legal Assistance Agreements) ist ebenfalls denkbar, kommt aber, wie der *Einzelrichter* näher ausführt, häufig zu spät.

Unabhängig hiervon wird eine „Festung Europa" kaum den Mobilitätsbedürfnissen der Nutzer gerecht und es drohen weitere transatlantische Konflikte: Der dem *Weißen Haus* zugeordnete *US-Handelsbeauftragte* (*USTR*) hat sich (vgl. im Beck-Blog v. 17.4.2014, abrufbar unter: http://blog.beck.de/2014/04/17/usa-handelsbeauftragter-ustr-sieht-wto-handelshemmnis-in-schengen-cloud) bereits sehr kritisch öffentlich zu den Plänen einer „Schengen-Cloud" geäußert (s.a. http://www.ustr.gov/about-us/press-office/press-releases/2014/March/USTR-Targets-Telecommunications-Trade-Barriers). Das viel diskutierte neue *Google*-Urteil des *EuGH* (ZD 2014, 350 m. Anm. *Karg* – in diesem Heft = MMR 7/2014 m. Anm. *Sörup*) zum Recht auf Vergessenwerden wird die Auseinandersetzung eher noch verschärfen. Sinnvoll wäre daher eine intensivere transatlantische Diskussion darüber, ob der geschilderte Prozess der MLAT, den der Einzelrichter als „mühsam" erachtet, für das Cloud Computing angemessen ist. Bei US-Zivilklagen gibt es diese Diskussion über den direkten Zugriff aus den USA auf EU-Daten schon seit Jahren (vgl. *Spies,* in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, S. 934 ff. – Kap. zur „E-Discovery").

EuGH: Löschungsanspruch gegen Google – „Recht auf Vergessen"

RL 95/46/EG Art. 2 lit. b u. lit. d, 12 lit. b, 14 Abs. 1 lit. a; AEUV Art. 267; GRCh Art. 8
Urteil vom 13.5.2014 – C-131/12 – Google Spain und Google

Leitsätze

1. Art. 2 lit. b und d der RL 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahin auszulegen, dass die Tätigkeit einer Suchmaschine, die darin besteht, von Dritten ins Internet gestellte oder dort veröffentlichte Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen, sofern die Informationen personenbezogene Daten enthalten, als „Verarbeitung personenbezogener Daten" i.S.v. Art. 2 lit. b der RL 95/46/EG einzustufen ist und dass der Betreiber dieser Suchmaschinen als für diese Verarbeitung „Verantwortlicher" i.S.v. Art. 2 lit. d der RL 95/46/EG anzusehen ist.
2. Art. 4 Abs. 1 lit. a der RL 95/46/EG ist dahin auszulegen, dass im Sinne dieser Bestimmung eine Verarbeitung personenbezogener Daten i.R.d. Tätigkeiten einer Niederlassung ausgeführt wird, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedstaats besitzt, wenn der Suchmaschinenbetreiber in einem Mitgliedstaat für die Förderung des Verkaufs der Werbeflächen der Suchmaschine und diesen Verkauf selbst eine Zweigniederlassung oder Tochtergesellschaft gründet, deren Tätigkeit auf die Einwohner dieses Staats ausgerichtet ist.
3. Art. 12 lit. b und Art. 14 Abs. 1 lit. a der RL 95/46/EG sind dahin auszulegen, dass der Suchmaschinenbetreiber zur Wahrung der in diesen Bestimmungen vorgesehenen Rechte, sofern deren Voraussetzungen erfüllt sind, dazu verpflichtet ist, von der Ergebnisliste, die im Anschluss an eine anhand des Namens einer Person durchgeführte Suche angezeigt wird, Links zu von Dritten veröffentlichten Internetseiten mit Informationen zu dieser Person zu entfernen, auch wenn der Name oder die Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht werden und gegebenenfalls auch dann, wenn ihre Veröffentlichung auf den Internetseiten als solche rechtmäßig ist.
4. Art. 12 lit. b und Art. 14 Abs. 1 lit. a der RL 95/46/EG sind dahin auszulegen, dass i.R.d. Beurteilung der Anwendungsvoraussetzungen dieser Bestimmungen u.a. zu prüfen ist, ob die betroffene Person ein Recht darauf hat, dass die Information über sie zum gegenwärtigen Zeitpunkt nicht mehr durch eine Ergebnisliste, die im Anschluss an eine anhand ihres Namens durchgeführte Suche angezeigt wird, mit ihrem Namen in Verbindung gebracht wird, wobei die Feststellung eines solchen Rechts nicht voraussetzt, dass der betroffenen Person durch die Einbeziehung der betreffenden Information in die Ergebnisliste ein Schaden entsteht. Da die betroffene Person in Anbetracht ihrer Grundrechte aus den Art. 7 und 8 GRCh verlangen kann, dass die betreffende Information der breiten Öffentlichkeit nicht mehr durch Einbeziehung in eine derartige Ergebnisliste zur Verfügung gestellt wird, überwiegen diese Rechte grundsätzlich nicht nur gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetrei-