23850

In Kooperation mit:
bitkom e.V.
BvD e.V.
davit im DAV
eco e.V.
VPRT e.V.

ZD ZEITSCHRIFT FÜR DATENSCHUTZ

AUS DEM INHALT

www.zd-beck.de

Seiten 457–504
6. Jahrgang 4. Oktober 2016
Verlag C.H.BECK München

10/2016

O850201610

US Court of Appeals for the Second Circuit: Keine Vorlagepflicht bei US-Beschlagnahmebeschluss für in Irland belegene Daten

18 U.S.C. §§ 2701, 2703, 2707
Entscheidung (Richter Lynch, Carney und Bolden) vom 14.7.2016 – 14-2985 (US-District Court Southern District of New York)

Leitsatz der Redaktion

Ein gegen ein Unternehmen mit Sitz in den USA erlassener strafrechtlicher Beschlagnahmebeschluss zur Vorlage von E-Mail-Verkehr (SCA-Warrant) umfasst nicht Daten, die in Irland auf einem Server des Adressaten abgespeichert sind.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2016, 12719. Die Entscheidung wurde mitgeteilt und der Leitsatz verfasst von RA *Dr. Axel Spies*, Morgan Lewis & Bockius, Washington DC. Zur Vorinstanz vgl. *Schröder/Spies*, ZD-Aktuell 2014, 04315 und *Bezirksgericht Southern District of New York* ZD 2014, 346 m. Anm. *Schröder/Spies*; ferner *Spies*, ZD-Aktuell 2015, 04588.

Sachverhalt

Microsoft Corp. (Microsoft) hatte Berufung gegen einen Beschluss des *US-District Court Southern District of New York (SDNY)* eingelegt (zu den Einzelheiten s. ZD 2014, 346 m. Anm. *Schröder/Spies*). Dieses *Untergericht* hatte einen Antrag von *Microsoft* gegen einen Beschlagnahmebeschluss („Warrant") nach § 2703 des Stored Communications Act (SCA) mit dem Ziel der Herausgabe bestimmter Datensätze abgelehnt; es belegte *Microsoft* darüber hinaus mit einer Strafe (Contempt of Court) wegen Missachtung des *Gerichts* auf Grund der Weigerung zur Ausführung des Warrant. Der Warrant sah die Herausgabe von E-Mails eines bestimmten E-Mail-Kontos vor, die *Microsoft* für den Kunden auf einem E-Mail-Server in Irland abgespeichert hatte. Mit den E-Mails möchte die *US-Strafverfolgungsbehörde* beweisen, dass der E-Mail-Account-Inhaber in bestimmte Drogengeschäfte verwickelt war. Der Warrant war *Microsoft* an seinem Hauptsitz in Redmond im Bundesstaat Washington zugestellt worden.

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

Aus den Gründen

I. Standard of Review: We will vacate a finding of civil contempt that rests on a party's refusal to comply with a court order if we determine that the *district court* relied on a mistaken understanding of the law in issuing its order. United States ex rel. Touhy v. Ragen, 340 U.S. 462, 464-70 (1951). Similarly, we will vacate a district court's denial of a motion to quash ... [The Warrant was issued under the provisions of the Stored Communications Act (SCA), legislation enacted as Title II of the Electronic Communications Privacy Act of 1986 (ECPA).]

II. Whether the SCA Authorizes Enforcement of the Warrant as to Customer Content Stored in Ireland. ...

B. Morrison and the Presumption Against Extraterritoriality: When interpreting the laws of the United States, we presume that legislation of *Congress* "is meant to apply only within the territorial jurisdiction of the United States," unless a contrary intent clearly appears. Id. at 255 (internal quotation marks omitted); see also RJR Nabisco, Inc. v. European Cmty., ..., 2016 WL 3369423, at *7 (June 20, 2016). This presumption rests on the perception that "Congress ordinarily legislates with respect to domestic, not foreign matters." Id. The presumption reflects that *Congress*, rather than the courts, has the "facilities necessary" to make policy decisions in the "delicate field of international relations." Kiobel v. Royal Dutch Petroleum Co., 133 S. Ct. 1659, 1664 (2013) (quoting Benz v. Compania Naviera Hidalgo, S.A., 353 U.S. 138, 147 (1957)). In line with this recognition, the presumption is applied to protect against "unintended clashes between our laws and those of other nations which could result in international discord." Equal Emp't Opportunity Comm'n v. Arabian American Oil Co., 499 U.S. 244, 248 (1991) ("Aramco"); see generally Park Central Global Hub Ltd. v. Porsche Auto. Holdings SE, 763 F.3d 198 (2d Cir. 2014) (per curiam). ...

C. Whether the SCA's Warrant Provisions Contemplate Extraterritorial Application: ... When *Congress* intends a law to apply extraterritorially, it gives an "affirmative indication" of that intent. Morrison, 561 U.S. at 265. It did so, for example, in the statutes at issue in Weiss v. National Westminster Bank PLC, 768 F.3d 202, 207 & n.5 (2d Cir. 2014) (concluding that definition of "international terrorism" within 18 U.S.C. § 2331(1) covers extraterritorial conduct because *Congress* referred to acts that "occur primarily outside the territorial jurisdiction of the United States") and United States v. Weingarten, 632 F.3d 60, 65 (2d Cir. 2011) (concluding that 18 U.S.C. § 2423(b) applies to extraterritorial conduct because it criminalizes "travel in foreign commerce undertaken with the intent to commit sexual acts with minors" that would violate United States law had the acts occurred in the jurisdiction of the United States). We see no such indication in the SCA. ... *Congress's* use of the term of art "warrant" also emphasizes the domestic boundaries of the Act in these circumstances. ... The magistrate judge took a different view of the legislative history of certain amendments to the SCA. He took special notice of certain legislative history related to the 2001 amendment to the warrant provisions enacted in the USA Patriot Act. A House committee report explained that "(c)urrently, Federal Rules (sic) of Criminal Procedure 41 requires that the 'warrant' be obtained 'within the district' where the property is located. An investigator, for example, located in Boston ... might have to seek a suspect's electronic e-mail from an Internet service provider (ISP) account located in California." In re Warrant, 15 F. Supp. 3d at 473 (quoting H.R. Rep. 107-236(I), at 57 (2001)). The *magistrate judge* reasoned that this statement equated the location of property with the location of the service provider, and not with the location of any server. Id. at 474.

But this excerpt says nothing about the need to cross international boundaries; rather, while noting the "cross-jurisdictional nature of the Internet," it discusses only amendments to Rule 41 that allow magistrate judges "within the district" to issue warrants to be executed in other "districts" – not overseas. Id. at 473 (quoting H.R. Rep. 107-236(I), at 58). Furthermore, the *Committee* discussion reflects no expectation that the material to be searched and seized would be located any place other than where the service provider is located. Thus, the *Committee's* hypothetical focuses on a situation in which an investigator in Boston might seek e-mail from "an Internet service provider (ISP) account located in California." To our reading, the Report presumes that the service provider is located where the account is – within the United States. ... *Microsoft* convincingly observes that

our *Court* has never upheld the use of a subpoena to compel a recipient to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item. Appellant's Br. at 42-43. The *government* does not identify, and our review of this *Court's* precedent does not reveal, any such cases. ...

D. Discerning the "Focus" of the SCA: ... When we find that a law does not contemplate or permit extraterritorial application, we generally must then determine whether the case at issue involves such a prohibited application. Id. at 266-67. As we recently observed in Mastafa v. Chevron Corp., "An evaluation of the presumption's application to a particular case is essentially an inquiry into whether the domestic contacts are sufficient to avoid triggering the presumption at all." 770 F.3d 170, 182 (2d Cir. 2014). ...

From this statutory framework we find further reason to conclude that the SCA's focus lies primarily on the need to protect users' privacy interests. The primary obligations created by the SCA protect the electronic communications. Disclosure is permitted only as an exception to those primary obligations and is subject to conditions imposed in § 2703. Had the Act instead created, for example, a rebuttable presumption of law enforcement access to content premised on a minimal showing of legitimate interest, the *government's* argument that the Act's focus is on aiding law enforcement and disclosure would be stronger. Cf. Morrison, 561 U.S. at 267. But this is not what the Act does.

The SCA's procedural provisions further support our conclusion that the Act focuses on user privacy. As noted above, the SCA expressly adopts the procedures set forth in the Federal Rules of Criminal Procedure. 18 U.S.C. § 2703(a), (b)(1)(A). Rule 41, which governs the issuance of warrants, reflects the historical understanding of a warrant as an instrument protective of the citizenry's privacy. See Fed. R. Crim. P. 41. Further, the Act provides criminal penalties for breaches of those privacy interests and creates civil remedies for individuals aggrieved by a breach of their privacy that violates the Act. See 18 U.S.C. §§ 2701, 2707. These all buttress our sense of the Act's focus.

We find unpersuasive the *government's* argument, alluded to above, that the SCA's warrant provisions must be read to focus on "disclosure" rather than privacy because the SCA permits the government to obtain by mere subpoena the content of e-mails that have been held in ECS storage for more than 180 days. Gov't Br. at 28-29; see 18 U.S.C. § 2703(a). In this vein, the *government* submits that reading the SCA's warrant provisions to focus on the privacy of stored communications instead of disclosure would anomalously place newer e-mail content stored on foreign servers "beyond the reach of the statute entirely," while older e-mail content stored on foreign servers could be obtained simply by subpoena, if notice is given to the user. Gov't Br. at 29. This argument assumes, however, that a subpoena issued to *Microsoft* under the SCA's subpoena provisions would reach a user's e-mail content stored on foreign servers. Although our Court's precedent regarding the foreign reach of subpoenas (and Marc Rich in particular) might suggest this result, the protections rightly accorded user content in the face of an SCA subpoena have yet to be delineated. Today, we need not determine the reach of the SCA's subpoena provisions, because we are faced here only with the lawful reach of an SCA warrant. ...

We believe this legislative history tends to confirm our view that the Act's privacy provisions were its impetus and focus. Although *Congress* did not overlook law enforcement needs in formulating the statute, neither were those needs the primary motivator for the enactment. See S. Rep. No. 99-541, at 3 (in drafting SCA, *Senate Judiciary Committee* sought "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs"). ...

E. Extraterritoriality of the Warrant: ... The *magistrate judge* noted the ease with which a wrongdoer can mislead a service provider that has overseas storage facilities into storing content outside the United States. He further noted that the current process for obtaining foreign-stored data is cumbersome. That process is governed by a series of Mutual Legal Assistance Treaties ("MLATs") between the United States and other countries, which allow signatory states to request one another's assistance with ongoing criminal investigations, including issuance and execution of search warrants. See U.S. Dep't of State, 7 Foreign Affairs Manual (FAM) § 962.1 (2013), available at fam.state.gov/FAM/07FAM/07FAM0960.html (last visited May 12, 2016) (discussing and listing MLATs). And he observed that, for countries with which it has not signed an MLAT, the United States has no formal tools with which to obtain assistance in conducting law enforcement searches abroad. These practical considerations cannot, however, overcome the powerful clues in the text of the statute, its other aspects, legislative history, and use of the term of art "warrant," all of which lead us to conclude that an SCA warrant may reach only data stored within United States boundaries. Our conclusion today also serves the interests of comity that, as the MLAT process reflects, ordinarily govern the conduct of crossboundary criminal investigations. Admittedly, we cannot be certain of the scope of the obligations that the laws of a foreign sovereign – and in particular, here, of Ireland or the E.U. – place on a service provider storing digital data or otherwise conducting business within its territory. But we find it difficult to dismiss those interests out of hand on the theory that the foreign sovereign's interests are unaffected when a United States judge issues an order requiring a service provider to "collect" from servers located overseas and "import" into the United States data, possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the United States. Thus, to enforce the Warrant, insofar as it directs *Microsoft* to seize the contents of its customer's communications stored in Ireland, constitutes an unlawful extraterritorial application of the Act.

Conclusion: We conclude that *Congress* did not intend the SCA's warrant provisions to apply extraterritorially. The focus of those provisions is protection of a user's privacy interests. Accordingly, the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States. The SCA warrant in this case may not lawfully be used to compel *Microsoft* to produce to the *government* the contents of a customer's e-mail account stored exclusively in Ireland. Because *Microsoft* has otherwise complied with the Warrant, it has no remaining lawful obligation to produce materials to the government. We therefore reverse the District Court's denial of *Microsoft's* motion to quash; we vacate its order holding *Microsoft* in civil contempt of court; and we remand this cause to the *District Court* with instructions to quash the warrant insofar as it demands user content stored outside of the United States. ...

Anmerkung

RA Dr. Christian Schröder, Orrick Herrington & Sutcliffe, Düsseldorf / RA Dr. Axel Spies, Morgan Lewis & Bockius, Washington DC

Die Entscheidung des *US Court of Appeals for the Second Circuit* ist eine bedeutende Entscheidung, da das *Gericht* die extraterritoriale Anwendung von US-amerikanischem Recht auf solche Gesetze beschränkt, bei denen der *US-Kongress* ausdrücklich

eine solche extraterritoriale Anwendung vorsieht. Nach dem *US Court of Appeals for the Second Circuit* gelten nun die Befugnisse der *US-Regierung* in Bezug auf den Stored Communications Act nicht, wenn die Daten in anderen Ländern gespeichert sind. Stattdessen ist die *US-Regierung* auf zwischenstaatliche Rechtshilfeabkommen angewiesen, wenn sie Zugriff auf Daten erhalten möchte, die außerhalb der USA gespeichert sind. Mit dieser Entscheidung reduziert das *Gericht* die Reichweite der ohne eine ausdrückliche Anweisung des *US-Kongresses* zur extraterritorialen Anwendung erlassenen Gesetze, stärkt den Souveränitätsanspruch von Drittstatten und reduziert Rechtskonflikte mit Europäischem Datenschutzrecht.

I.E. führt dieses Urteil, sofern es rechtskräftig wird, dazu, dass Daten, die von US-Diensteanbietern auf außerhalb der USA befindlichen Servern gelagert sind, besser gegen den Zugriff durch US-Behörden geschützt sind. Im Einzelnen:

Der *US Court of Appeals for the Second Circuit* folgt der Ansicht von *Microsoft* und hebt die Entscheidung des *US-District Court für den südlichen Bezirk von New York* (vgl. die Analysen von *Schröder/Spies,* ZD-Aktuell 2014, 04315 und *Bezirksgericht Southern District of New York* ZD 2014, 346 m. Anm. *Schröder/Spies*; *Spies,* ZD-Aktuell 2015, 04588) nach einer detaillierten Diskussion der Entstehungsgeschichte des SCA auf. Der *US-Kongress* habe im Jahr 1986 den SCA als Teil des weitergehenden Electronic Communications Privacy Act mit dem Ziel verabschiedet, die Privatsphäre der Bürger gegen neue Technologien zu schützen. Eine Erstreckung der Zugriffsbefugnisse von US-Strafverfolgungsbehörden auf Daten, die im Ausland belegen sind, sei nicht beabsichtigt gewesen. Dies müssten die Richter akzeptieren, solange der US-Gesetzgeber den SCA nicht abändere. Der *US-Kongress* müsse eine Erstreckung auf Sachverhalte im Ausland ausdrücklich anordnen. Nur so könne sichergestellt werden, dass im sensiblen Bereich der internationalen Beziehungen ausschließlich dem US-Gesetzgeber und nicht Gerichten eine Entscheidung über den Anwendungsanspruch des US-Rechts vorbehalten ist. Es gebe daher eine Vermutung, dass die Warrant-Provision (Sec. 2307 SA) nicht extraterritorial gelte.

Indem der *US Court of Appeals for the Second Circuit* nun in Bezug auf SCA Warrants bei internationalen Sachverhalten auf Rechtshilfeabkommen verweist, führt die Entscheidung (mit einer hier nicht abgedruckten Concurring Decision eines Richters) zu einer verstärkten Achtung der Souveränität von Drittstaaten und reduziert offensichtliche Konflikte mit dem europäischen Datenschutzrecht. Sofern das Urteil rechtskräftig wird, wird so auch ein aus europäischer Sicht naheliegender zukünftiger Konflikt mit der Regelung des Art. 48 DS-GVO vermieden. Art. 48 untersagt bei Fehlen anderer Ermächtigungen verantwortlichen Stellen oder Auftragsverarbeitern ausdrücklich die Herausgabe von personenbezogenen Daten an Behörden aus Drittstaaten und verweist auf in Kraft befindliche internationale Übereinkünfte wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der EU oder dem betroffenen Mitgliedstaat.

Die Entscheidung des *US Court of Appeals for the Second Circuit* steht in einer Linie mit weiteren neueren Gerichtsentscheidungen zu Gunsten eines besseren Schutzes der Privacy (z.B. *US-Supreme Court* U.S. v. Jones – verbotene heimliche GPS-Überwachung (s. *Spies*, http://blog.beck.de/2012/01/23/us-supreme-court-verfolgung-von-taetern-mit-angebrachtem-gps-ohne-durchsuchungsbeschluss-unzulaessig (23.1.2012)) und *US Court of Appeals for the Second Circuit in New York* (s. *Spies,* ZD-Aktuell 2015, 04668 – keine anlasslose Sammlung von TK-Daten). Diese neue Entscheidung könnte das derzeit sehr angespannte Verhältnis zwischen US- und europäischem Datenschutzrecht deutlich verbessern. Jedenfalls wären Daten, die von US-Anbietern im EU-Inland gespeichert werden, deutlich besser gegen den Zugriff von US-Strafverfolgungsbehörden geschützt.

Die *US-Regierung* könnte allerdings bei dem *US-Supreme Court* Revision einlegen oder beim *Second Circuit Court of Appeals* eine Petition für eine erneute Anhörung vor allen Richtern einreichen. Grundsätzlich kann der *US-Supreme Court* eine Rechtsfrage letztverbindlich klären, wenn US-Berufungsgerichte zu unterschiedlichen Entscheidungen kommen. Der *US-Supreme Court* ist nicht verpflichtet eine Revision anzunehmen und überprüft regelmäßig in vergleichbaren Fällen keine Entscheidungen.

Das Urteil des *Second Circuit Court of Appeals* mag zwar die Entscheidungen anderer Berufungsgerichte beeinflussen, sie sind hieran aber nicht gebunden. Darüber hinaus könnte der *US-Kongress* seinerseits den SCA zu Gunsten der Strafverfolgungsbehörden ergänzen und ihm ausdrücklich eine extraterritoriale Wirkung in manchen Fällen zuweisen. *Microsoft* hat tatsächlich selbst Gesetze unterstützt, die einen Zugriff durch US-Behörden auf Daten, die US-Staatsbürgern und Einwohnern mit ständigem Wohnsitz in den USA (permanent residents) gehören, ermöglichen, wenn diese außerhalb der USA gespeichert sind.

Der wohl einzige gangbare Weg zur Vermeidung von Rechtskonflikten wäre jedoch für alle betroffenen Länder eine schon lange ins Auge gefasste Überarbeitung der Mutual Legal Assistance Treaties (MLATs) entweder in Form von Ergänzungen (Amendments) oder durch eine ganz neue, mehrseitige internationale Vereinbarung. Auch Art. 50 DS-GVO verlangt ausdrücklich, dass mehr Rechtshilfeabkommen geschlossen werden, um den notwendigen internationalen Datenaustausch auf beidseitig rechtskonforme Grundlagen zu stellen. Dies setzt allerdings auch voraus, dass kleinere Länder bereit und in der Lage sind, MLAT-Anfragen zügig zu bearbeiten. Derzeit gibt es nur wenige solcher Rechtshilfeabkommen. Auf jeden Fall rückt die Zusammenarbeit der Strafverfolgungsbehörden in Bereichen wie dem Cloud Computing weiter nach oben auf der Agenda.

BVerfG: Erfolglose Verfassungsbeschwerde gegen BayPAG und BayVSG

BayPAG Art. 34-34e; BayVSG Art. 6a-g; BVerfGG § 93a Abs. 2
Beschluss vom 15.6.2016 – 1 BvR 2544/08

Leitsätze der Redaktion

1. Berufsgeheimnisträgern kann die gegenwärtige Selbstbetroffenheit fehlen, wenn sie mit der Verfassungsbeschwerde Befugnisnormen rügen, die einen besonderen Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger vorsehen. Dies gilt insbesondere für Abgeordnete, die sich darauf berufen, auf Grund ihrer politischen Arbeit und Abgeordnetentätigkeit mit Dritten in Kontakt zu stehen, welche von Polizei und Verfassungsschutz beobachtet werden, und nicht darlegen, warum sie gleichwohl mit einiger Wahrscheinlichkeit davon ausgehen, Objekt einer Online-Durchsuchung zu werden.

2. Im Übrigen sind die wesentlichen von den Beschwerdeführern aufgeworfenen Fragen durch das Urteil des BVerfG zum BKAG v. 20.4.2016 (ZD 2016, 374 m. Anm. Petri) geklärt.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2016, 48109. Vgl. hierzu *BverfG* ZD 2016, 374 m. Anm. *Petri.*