UNIVERSITÄT
ZU KÖLN

Universität zu Köln • Albertus-Magnus-Platz • 50923 Köln

Rechtswissenschaftliche
Fakultät

[redacted]

Telefon: [redacted]

Anschrift
[redacted]
50931 Köln
Deutschland

Rechtsgutachten zur US-Rechtslage zum weltweiten Datenzugriff durch US-Behörden bei Nutzung von Cloud-Diensten

vorgelegt von [redacted]

im Auftrag der Bundesrepublik Deutschland, vertreten durch das Bundesministerium des Innern und für Heimat

am 21. März 2025

Servicezeiten
Mo. Di. Do 9.00 – 16.00 Uhr
Mi. 9.00 – 18.00 Uhr
Fr. 9.00 – 13.00 Uhr
und nach Vereinbarung

UNIVERSITÄT
ZU KÖLN

A. Gutachtenauftrag

Mit Vertrag vom 23.12.2024 hat die Bundesrepublik Deutschland, vertreten durch das Bundesministerium des Innern und für Heimat (Auftraggeberin), [redacted] (Auftragnehmer), damit beauftragt, ein Rechtsgutachten zur Rechtslage in den Vereinigten Staaten von Amerika hinsichtlich des weltweiten Zugriffs auf Daten durch US-Behörden, insbesondere bei der Nutzung von Cloud-Diensten, zu erstellen. Hintergrund ist der Bedarf der Bundesverwaltung, Informationen in Clouds verarbeiten zu können, und die Frage, ob Verschlusssachen in Clouds amerikanischer Hyperscaler ausreichend geschützt sind.

Im Einzelnen wurden folgende Fragen gestellt:

1. Wie ist die aktuelle Rechtslage in den USA? Ist es richtig, dass amerikanische Nachrichtendienste ein Direktzugriffsrecht auf die in Clouds enthaltenen Informationen und ein Herausgaberecht gegenüber den Cloud-Anbietern haben bzw. unter welchen Voraussetzungen ist dies der Fall?

2. Unterliegen auch ausländische Provider der amerikanischen Jurisdiktion?

3. Besteht ein solches Zugriffsrecht auch dann, wenn das US-amerikanische Unternehmen eine deutsche Tochter nach deutschem Recht gründet und die Cloud auf deutschem Hoheitsgebiet betreibt (sich also die Hardware in Deutschland befindet)?

Mit E-Mail vom 15. Januar 2025 hat die Auftraggeberin zusätzlich gefragt, ob es rechtlich möglich ist, dass sich ein US-Cloud-Betreiber seinen Verpflichtungen zur Speicherung und Herausgabe von Daten und Informationen aus der Cloud dadurch entzieht, dass er sich selbst technisch aus der Cloud ausschließt, sodass ihm kein eigener Zugriff auf die darin enthaltenen Daten verbleibt.

Die Untersuchung erfolgt somit unter der Annahme, dass die Bundesregierung beabsichtigt, eigene sensible Daten in Clouds zu speichern und den Zugriff durch US-amerikanische Behörden auszuschließen.

B. Zusammenfassung der Gutachtenergebnisse

I. Wie ist die aktuelle Rechtslage in den USA? Ist es richtig, dass amerikanische Nachrichtendienste ein Direktzugriffsrecht auf die in Clouds enthaltenen Informationen und ein Herausgaberecht gegenüber den Cloud-Anbietern haben bzw. unter welchen Voraussetzungen ist dies der Fall? (Fragestellung 1)

Kurzantwort: US-amerikanische Sicherheitsbehörden verfügen weitreichende Herausgabe- und Zugriffsrechte auf Kommunikationsdaten sowie in Clouds gespeicherte Informationen. Der Zugriff auf solche Informationen ist sehr umfassend, wenn sich die Server auf US-Territorium befinden. Aber auch ausländische Server und Cloud-Betreiber können der Herausgabepflicht unterworfen sein. Nicht in allen Fällen muss dafür ein gerichtlicher Durchsuchungsbeschluss vorliegen. Die Rechtschutzmöglichkeiten gegen eine Herausgabeanordnung sind für europäische Unternehmen eingeschränkt. Darüber hinaus können amerikanische Geheimdienste unter Voraussetzungen, die nicht öffentlich bekannt sind, auf im Ausland gespeicherte Daten auch ohne die Mitwirkung von Cloud-Anbietern zugreifen.

Zusammenfassung: US-amerikanische Sicherheitsbehörden – sowohl die Nachrichtendienste als auch die Strafverfolgungsbehörden – können auf der Grundlage von Section 702 FISA und Sections 2701-2713 SCA von bestimmten Unternehmen die Herausgabe von in Clouds gespeicherten Informationen verlangen. Section 502 FISA ist auf Cloud Computing und Data Centers hingegen nicht anwendbar. Die Rechtsgrudlage zum Abhören von Daten außerhalb der USA auch ohne Mitwirkung der Cloud-Betreiber bietet Executive Order 12.333.

Section 702 FISA findet auf alle Cloud Computing Dienstleister und Data Center Anwendung. Nach dieser Vorschrift müssen US-amerikanische Dienstleister aller Art – also nicht nur Telekommunikationsdienstleister – geheimdienstrelevante Informationen über Nicht-US-Personen, die sich außerhalb der USA befinden, nach einem mehrschrittigen Verfahren an die Sicherheitsbehörden herausgeben.

Dieses Verfahren erfolgt weitgehend ohne nachvollziehbare gerichtliche Überprüfung; nur der unter Ausschluss der Öffentlichkeit tagende FISC erhält die Gelegenheit, die behördliche Anordnung zu bestätigen oder abzulehnen. Zur Anordnung der Herausgabe von Informationen unter Section 702 FISA ist somit grundsätzlich kein richterlicher Durchsuchungsbeschluss erforderlich. Es findet lediglich eine jährliche Zer-

tifizierung durch den FISC statt, die die Rahmenbedigungen der Herausgabeanordnungen festsetzt. Aufgrund dieser mangelnden Rechtsschutzmöglichkeiten hatte der EuGH den Transfer personenbezogener Daten unter dem EU-USA Privacy Shield Abkommen für rechtswidrig befunden.

Für die Herausgabepflicht kommt es nicht auf den Ort der Niederlassung des Unternehmens, sondern vielmehr auf den Ort des Servers an. Sobald Daten auf US-Territorium gespeichert oder verarbeitet werden, unterliegen sie Section 702 FISA. Da diese Daten ausschließlich Nicht-US-Personen betreffen dürfen, hat Section 702 FISA eine extraterritoriale Anwendungskomponente.

Wenn hingegen der Server außerhalb des US-Territoriums belegen ist, dann kommt es auf die mögliche Kontrolle des US-amerikanischen Unternehmens über diesen Server an (dazu Fragestellung 2). Auch leitende Angestellte, Mitarbeitende, Verwalter und Vertreter sind umfasst. Das bedeutet, dass eine (ausländische) Tochtergesellschaft in der Regel der Herausgabepflicht unterliegt (dazu Fragestellung 3). Ob hingegen auch die Muttergesellschaft oder ein mit einem verpflichteten Unternehmen verbundenes Unternehmen zwingend umfasst ist, ist weniger eindeutig.

Unter Exekutive Order 12333 sind US-Geheimdienste dazu ermächtigt, geheimdienstrelevante Informationen auch von Servern im Ausland zu sammeln. Dabei ist die Mitwirkung der Serverbetreiber grundsätzlich nicht erforderlich, vielmehr werden Sicherheitslücken in der IT-Infrastruktur ausgenutzt.

Nach dem SCA müssen elektronische Kommunikationsdienste und Remote-Computing-Dienste ebenfalls Daten herausgeben. Die herauszugebenden Daten umfassen den Inhalt elektronischer Kommunikation und von in Clouds gespeicherten Dokumenten sowie nicht-inhaltliche Informationen wie Nutzerdaten und Übermittlungsdaten, aber keine sonstigen personenbezogenen oder Geschäftsdaten. Dazu bedarf es grundsätzlich einer richterlichen Anordnung, welche den Anforderungen der US-Verfassung an Durchsuchungen unterliegt.

Allerdings besteht für deutsche Unternehmen zurzeit kein Rechtschutz gegen solche Anordnungen. Das vorgesehene Widerspruchsrecht nach Section 2703(h)(2)(A) SCA gegen ein solches Herausgabeverlangen steht europäischen Unternehmen nicht zu, da es dafür an einem entsprechenden Abkommen zwischen den USA und der EU fehlt.

Zudem gibt es im SCA auch Ausnahmen von dem Erfordernis einer gerichtlichen Anordnung. Auf der Grundlage von *National Security Letters*, einer Art behördlichen Anordnung, die das FBI ohne richterliche Vorprüfung erlässt und die (nur im Nachgang) eingeschränkter gerichtlicher Überprüfbarkeit unterliegen, kann die Herausgabe von Daten verlangt werden. Die Herausgabepflicht nach dieser Vorschrift bezieht sich auf Telefonteilnehmerdaten, Rechnungsdaten und andere elektronischen Transaktionsdaten, nicht aber den Inhalt der abgefragten Kommunikation.

II. Besteht ein solches Zugriffsrecht auch dann, wenn das US-amerikanische Unternehmen eine deutsche Tochter nach deutschem Recht gründet und die Cloud auf deutschem Hoheitsgebiet betreibt (sich also die Hardware in Deutschland befindet)? (Fragestellung 3)

Kurzantwort: Die Regelungen des CLOUD-Acts stellen klar, dass einem Herausgabeverlangen von US-Strafverfolgungsbehörden auch dann Folge zu leisten ist, wenn die Daten auf einem Server außerhalb der USA gespechert sind. Dies ist auch der Fall, wenn der Server durch eine europäische Tochtergesellschaft eine US-Konzerns betrieben wird, soweit das US-Unternehmen eine Herausgabe der Daten bei der Tochtergesellschaft veranlassen kann.

Zusammenfassung: Die Vorschriften des SCA – insbesondere Section 2703 – finden zweifellos auch extraterritoriell Anwendung. Dies entspricht dem eindeutigen Willen des CLOUD-Act Gesetzgebers. Darüber hinaus ist es ständige Rechtsprechung von US-Bundesgerichten, dass Dokumente auch dann herauszugeben sind, wenn sie sich zwar außerhalb der USA befinden, der Verpflichtete aber die Kontrolle über diese Dokumente hat. Der Begriff der Kontrolle wird dabei weit ausgelegt, sodass jeder leitende Angestellte, der eine Übersendung der Informationen veranlassen kann, über Kontrolle in diesem Sinne verfügt. In Bezug auf Tochterunternehmen ist somit davon auszugehen, dass der Mutterkonzern Kontrolle über diese im Sinne dieser Rechtsprechung hat. US-Gerichte könnten somit anordnen, dass US-Unternehmen ihre ausländischen Tochterunternehmen anweisen, Daten an die Behörden herauszugeben. Kommt der Mutterkonzerne dieser Aufforderung nicht nach, können durch das Gericht Bußgelder sowie strafrechtliche Maßnahmen angeordnet werden.

III. Unterliegen auch ausländische Provider der amerikanischen Jurisdiktion? (Fragestellung 2)

Kurzantwort: Die Reichweite der Jurisdiktion US-amerkanischer Gerichte bemisst sich daran, welche Kontakte ein Unternehmen zu den USA pflegt. Bereibt ein europäisches Unternehmen eine Niederlassung in den USA, ist davon auszugehen, dass die US-amerikanischen Gerichte ihre Zuständigkeit über das Unternehmen ausüben werden. Nach den Umständen des Einzelfalls, kann auch das Bestehen geschäftlicher Kontake bereits ausreichend sein.

Zusammenfassung: Der Umfang der Zuständigkeit von US-Gerichten über ausländische Entitäten wird stets von den Umständen des Einzellfalls bestimmt. Generell betrachten die Gerichte dabei den Umfang und die Intensität der Kontakte, die ein bestimmtes Unternehmen mit den USA hat. Dabei wird zwischen *general* und *specific personal jurisdiction* unterschieden, wobei die Annahme von *general personal jurisdiction* intensivere Kontakte mit den USA voraussetzt als *specific personal jurisdiction*, jedoch dann die Gerichte dazu berechtigt, Klagen aller Art gegen ein Unternehmen zuzulassen.

Bezogen auf die konkrete Frage, ob auch EU-Unternehmen, die ihre Serverdaten in der EU speichern, der Jurisdiktion US-amerikanischer Gerichte unterliegen, ist dies nach Art und Umfang der Geschäftsbeziehungen des Unternehmens in den USA zu bestimmen. So reicht es nach Rechtsprechung der US-Gerichte noch nicht aus, dass ein EU-Unternehmen eine Tochtergesellschaft in den USA betreibt, um die Annahme von *general personal jurisdiction* zu rechtfertigen, eine Niederlassung des Mutterkonzerns hingegen könnte jedoch ausreichend sein. Auch das Betreiben einer Website, die sich zumindest auch an US-Kunden richtet bzw. diese vom Zugriff auf die Website nicht explizit ausschließt, kann für die Annahme von *specific personal jurisdiction* bereits ausreichen. Für einen Cloud-Anbieter kann mitunter bereits das Anbieten seiner Dienstleistungen für US-Kunden ausreichend sein, wenn es in dem Verfahren um eben jene Tätigkeit geht.

IV. Ist es rechtlich möglich, dass sich ein US-Cloud-Betreiber seinen Verpflichtungen zur Speicherung und Herausgabe von Daten und Informationen aus der Cloud dadurch entzieht, dass er sich selbst technisch aus der Cloud ausschließt, sodass ihm kein eigener Zugriff auf die darin enthaltenen Daten verbleibt. (Zusatzfrage)

Kurzantwort: Während es zwar technisch möglich erscheint, sich vom Datenzugriff auf die Cloud auszuschließend, könnte dies Sanktionen durch US-Gerichte nach sich ziehen. Im US-amerkanischen prozessrecht besteht die Pflicht zur Bereithaltung und Herausgabe von Informationen an die gegnerische Prozesspartei. Wird dieser Pflicht nicht nachgegangen, so können Geldbußen oder sogar Haftstrafen angeordnet werden.

Zusammenfassung: Es erscheint fraglich, ob eine Herausgabeverpflichtung dadurch vermieden werden kann, dass sich Cloud-Anbieter technisch aus der Cloud ausschließen. Das ist zwar technisch denkbar, z.B. indem der Cloud-Betreiber die Daten verschlüsselt speichert, ohne selbst die Entschlüsselungstechnologie vorzuhalten, sodass nur Dritte, die sich im Besitz dieser Entschlüsselungstechnologie befinden, auf die Daten faktisch zugreifen können. In diesem Fall wäre wohl der Tatbestand der Herausgabepflicht aus dem SCA nicht erfüllt.

Im US-amerikanischem Prozessrecht sind Parteien jedoch dazu verpflichtet, schon vor Beginn eines Rechtsstreits verfahrensrelevante Informationen zu speichern und dem Gericht sowie den anderen Prozessparteien bei Bedarf im Rahmen der Beweisaufnahme zur Verfügung zu stellen. Bei Nichtbefolgung drohen Sanktionen in Form von teils erheblichen Bußgeldern durch die Gerichte. Dies gilt unter Umständen auch, wenn verfahrensrelevante Informationen aus Versehen oder absichtlich vernichtet werden (sog. *Spoliation*). US-Gerichte haben in der Vergangenheit eine Speicherpflicht für Daten dann anerkannt, wenn das Unternehmen wusste oder wissen konnte, dass die Daten für ein späteres Gerichtsverfahren relevant sein könnten. Ein Cloud-Anbieter, der regelmäßig Herausgabeverlangen von US-Strafverfolgungsbehörden nachzukommen hat, könnte mithin verpflichtet sein, Informationen für diese aufzubewahren. Darüber hinaus besteht nach Section 2703(f) SCA die Möglichkeit, dass eine Speicherung durch Strafverfolgungsbehörden gesondert angeordnet wird. Schließt sich ein Cloud-Anbieter durch technische Maßnahmen von seinem Zugang zum Cloud-Server aus, kann er diesen Verpflichtungen nicht mehr nachkommen und riskiert mitunter erhebliche Bußgelder, strafrechtliche Konsequenzen, oder beides.

C. Gutachten

I. US-Rechtslage zum Herausgaberecht US-amerikanischer Sicherheitsbehörden gegenüber Cloud-Anbietern auf in Clouds gespeicherte Informationen (Fragestellung 1)

Die Rechtslage bezüglich des Zugriffsrechts von US-Behörden auf Cloud-Daten ist sehr komplex und durch eine Fülle unterschiedlicher Gesetze, welche im Lauf der letzten Jahre zahlreiche Änderungen erfahren haben, geprägt. Hierbei sind insbesondere die folgenden Bundesgesetze relevant: Der Foreign Intelligence Surveillance Act of 1978 (FISA)[1], der USA PATRIOT Act of 2001[2], der USA FREEDOM Act of 2015[3], der CLOUD Act of 2018[4], der Electronic Communications Privacy Act of 1986 (ECPA)[5], und der Stored Communications Act (SCA)[6] (der SCA ist selbst Teil des ECPA und in Titel II der Norm kodifiziert).

Zunächst ist festzuhalten, dass es sich beim USA PATRIOT Act, USA FREEDOM Act und CLOUD Act jeweils um Änderungsgesetze zu bereits bestehenden Gesetzen handelt. Die maßgeblichen Befugnisse von US-Strafverfolgungsbehörden zur Anordnung der Herausgabe von Daten ergeben sich aus dem FISA und dem ECPA. Grundsätzlich kann

---

1 Publ. L. No. 95-511, 92 Stat. 1783 (abrufbar unter: https://uscode.house.gov/statutes/pl/95/511.pdf, Stand: 06.02.2025); die aktuelle Version von FISA gilt als 50 U.S. Code Chapter 36 – "Foreign Intelligence Surveillance" (abrufbar unter: https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title50-chapter36&saved=%7CZ3JhbnVsZWlkOlVTQy1wcmVsaW0tdGl0bGU1MC1zZWN0aW9uMTg4MWE%3D%7C%7C%7C0%7Cfalse%7Cprelim&edition=prelim, Stand: 31.7.2020).

2 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001 vom 26. Oktober 2001, H.R. 3162, Publ. L. No. 107–56, 115 Stat. 272 (abrufbar unter: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf, Stand: 31.7.2020).

3 Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act, Publ. L. No. 114-23, 129 Stat. 268 (abrufbar unter: https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf).

4 Clarifying Lawful Overseas Use of Data of 2018, Publ. L. No. 115-141, Stat. 2383 (abrufbar unter: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text, Stand: 31.7.2020).

5 Pub. L. No. 99–508, 100 Stat. 1848, kodifiziert in 18 U.S.C. §§ 2510-2725 (abrufbar unter: https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf, Stand: 31.7.2020).

6 Kodifiziert in 18 U.S.C. §§ 2701-2712.

hier zwischen Eingriffsbefugnissen zum Zwecke der nationalen Sicherheit der USA und Eingriffsbefugnissen zum Zwecke der Strafverfolgung unterschieden werden. Die Eingriffsmöglichkeiten des FISA gelten zugunsten der US-amerikanischen Nachrichtendienste zum Zwecke der nationalen Sicherheit und Terrorismusabwehr und sind in den Sections 502 und 702 FISA sowie in Executive Order (EO) 12.333 (1981)[7] statuiert. Die Eingriffsbefugnisse regulärer Strafverfolgungsbehörden sind in den Sections 2701-2713 SCA geregelt. Auf die einzelnen Zugriffsnormen und deren Voraussetzungen wird im Folgenden eingegangen.

1. Section 502 FISA

Section 502 FISA[8] ermächtigt das Federal Bureau of Investigation (FBI), von bestimmten Unternehmen – Transportgesellschaften (*common carrier*), Einrichtungen zur temporären Unterbringung von Menschen wie etwa Hotels (*public accommodation facility*), Lager- und Logistikunternehmen (*physical storage facility*) und Mietwagenunternehmen (*vehicle rental facility*) – die Herausgabe von Unterlagen (*records*) für Ermittlungen zur Sammlung Geheimdienst-relevanter Informationen aus dem Ausland (*foreign intelligence information*) oder für die Terrorismusabwehr zu verlangen. Der Direktor des FBI oder ein Vertreter, der im Rang mindestens ein *Assistant Special Agent in Charge* sein muss, stellt dafür einen Antrag bei dem *Foreign Intelligence Surveillance Court* (FISC)[9] oder bei einem besonders dazu ermächtigten US *Magistrate Judge*[10]. Dieser erlässt die entsprechende Anordnung, wenn die Voraussetzungen der Vorschrift erfüllt sind. Der FISC ist ein besonderes Bundesgericht, das in nichtöffentlichen Sitzungen, an denen nur die Regierung teilnimmt (sog. *ex parte* Verhandlung), über die Anträge berät.[11] Der gesamte Vorgang (Antragstellung, Herausgabe der Daten) ist von dem Adressaten des Herausgabeverlangens geheim zu halten.[12]

---

7 Executive Order 12333 vom 04.12.1981, 46 FR 59941, abrufbar hier: https://www.federalregister.gov/citation/46-FR-59941.

8 Kodifiziert in 50 U.S.C. § 1862.

9 Dieses Gericht wurde durch 50 U.S.C. § 1803(a) errichtet.

10 Diese Richter werden unter den Voraussetzungen des 28 U.S.C. Chapter 43 ernannt.

11 The Foreign Intelligence Surveillance Act of 1978 (FISA), US Department of Justice, Office of Justice Programs, abrufbar unter: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286. Stand: 5.2.2025.

12 50 U.S.C. § 1862(d)(2).

Section 501 FISA[13] enthält in Ergänzung zu Section 101 FISA[14] weitere Definitionen für die Anwendung dieser Vorschrift. Dort werden insbesondere die Adressaten des Herausgabeverlangens nach Section 502 FISA (*common carrier*, *physical storage facility*, *public accommodation facility* und *vehicle rental facility*) definiert. Cloud-Anbieter in Deutschland und anderswo dürften von den Definitionen dieser Begriffe nicht umfasst sein. Die Herausgabeverpflichteten sind unter der geltenden Rechtslage relativ eng umrissen.

Dies war während der Geltung des USA PATRIOT Act (2001) und des USA FREEDOM Act (2015) anders. Der Anwendungsbereich und die Zugriffsbefugnisse aus Sections 501, 502 FISA waren durch Section 215 USA PATRIOT Act erheblich ausgeweitet worden. Section 101 USA FREEDOM Act schränkte diese nur geringfügig wieder ein. Während der Geltung dieser Vorschriften hatten die Sicherheitsbehörden eine sehr weitgehende Befugnis zur (geheimen) Abfrage von nicht-inhaltlichen Daten, einschließlich Telefonie-Metadaten, von Unternehmen.[15] So stützte sich die NSA etwa bei ihren Anordnungen an Telefongesellschaften, Kommunikationsdaten herauszugeben, auf die in der damaligen Fassung geltenden Sections 501, 502 FISA.[16] Beide Vorschriften sind durch Fristablauf mittlerweile außer Kraft getreten.[17] Während ei-

---

13 Kodifiziert in 50 U.S.C. § 1861.

14 Kodifiziert in 50 U.S.C. § 1801.

15 Stephen I. Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15.11.2021, Seite 10, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf.

16 Ausführlich siehe USA Freedom Act 2015: Überblick über die Änderungen der nachrichtendienstlichen Befugnisse, Wissenschaftliche Dienste des Deutschen Bundestages, WD 3 - 3000 - 144/15, 17.6.2015, Seite 3, abrufbar unter: https://www.bundestag.de/resource/blob/959552/11f8d330a6d6c6cc1529dd1d1fe5cd1e/WD-3-144-15-pdf-data.pdf; vgl. auch US-Datenrecht: Zugriff US-amerikanischer Behörden auf Daten, Wissenschaftliche Dienste des Deutschen Bundestages, WD 3 - 3000 - 181/20, 3.8.2020, Seite 4, abrufbar unter: https://www.bundestag.de/resource/blob/796102/ea53ffe8e08a9ab11e270719263d8c53/WD-3-181-20-pdf-data.pdf.

17 Section 101 USA FREEDOM Act trat am 15.3.2020 außer Kraft.

nige der durch die Vorschrift bewirkten Kompetenzerweiterungen aufgrund anderer Gesetze weiterhin wirksam sind,[18] wurden die viel kritisierten, als uferlos wahrgenommenen Befugnisse nicht verlängert.[19] Zuletzt wurde Section 502 FISA durch den Reforming Intelligence and Securing America Act (RISAA)[20] (2024) verändert.

2. Section 702 FISA

Eine weitere Eingriffsbefugnis enthält Section 702 FISA[21]. Diese Vorschrift ermöglicht den US-Behörden die Überwachung von Nicht-US-Bürgern außerhalb des US-amerikanischen Staatsgebiets, deren Kommunikationsdaten sich im Besitz US-amerikanischer Dienstleister befinden, zum Zwecke der nationalen Sicherheit/Terrorismusabwehr. Sie schließt damit die Lücke zwischen der von EO 12.333 umfassten Kommunikation von Nicht-US-Bürgern, die sich ausschließlich außerhalb des US-amerikanischen Staatsgebiets befindet, und der Erfassung von Kommunikation von US-Personen (US-Staatsbürger, Aufenthaltsberechtigte, u.a.) innerhalb der USA, die von anderen Teilen des FISA abgedeckt ist.[22]

Die Norm ermächtigt ausschließlich zur Datenerhebung von Nicht-US-Bürgern, bei denen vernünftigerweise davon ausgegangen wird, dass sie sich außerhalb des US-amerikanischen Territoriums befinden. Ob Deutsch/US-amerikanische Doppelstaater im Ausland aus Sicht von Section 702 FISA als US-Bürger behandelt werden, kann nicht abschließend beurteilt werden, dürfte aber davon abhängen, welche Staatsangehörigkeit als dominant angesehen wird.[23]

---

18 Vgl. Electronic Privacy Information Center, Surveillance Oversight: Patriot Act, abrufbar unter: https://epic.org/issues/surveillance-oversight/patriot-act/ (Stand 10.02.2025).

19 Stephen I. Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15.11.2021, Seite 10, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf.

20 Publ. L. 118-49, 138 Stat. 862 (abrufbar unter: https://www.congress.gov/118/plaws/publ49/PLAW-118publ49.pdf).

21 Kodifiziert in 50 U.S.C. § 1881a.

22 Stephen I. Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15.11.2021, Seite 8, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf.

23 Soweit ersichtlich, ist diese Frage im Hinblick auf die Definition der „United States person" gemäß 50 U.S.C. § 1801(i) bislang nicht Gegenstand der US-amerikanischen Rechtsprechung gewesen. In anderen Kontexten wird in

Das Verfahren ist wie folgt ausgestaltet. In einem ersten Schritt erlassen der Generalbundesanwalt/Justizminister[24] (*Attorney General*) und der Direktor der Nachrichtendienste der USA (*Director of National Intelligence*) nach freiem Ermessen ein Zertifikat (*certification*) mit einer maximalen Geltungsdauer von einem Jahr, in dem sie bestimmte Kategorien Geheimdienst-relevanter Informationen aus dem Ausland (*foreign intelligence information*[25]) identifizieren, die die US-amerikanischen Geheimdienste erheben dürfen.[26] Darin werden auch Vorgaben zum Verfahren und dem Gegenstand der Untersuchung gemacht, die den Schutz von personenbezogenen Daten von US-Personen[27] bezwecken sollen. Der FISC prüft diese *certification* auf ihre Vereinbarkeit mit dem FISA und dem 4. Zusatzartikel zur Verfassung der USA, der Vorgaben zum Schutz personenbezogener Daten enthält. Die Prüfung erfolgt unter Ausschluss der Öffentlichkeit. Das Besondere an dieser *certification* ist, dass sie pauschal und für alle denkbaren Anwendungsfälle gilt. Anders als beispielsweise bei dem Erlass eines Durchsuchungsbeschlusses erfolgt gerade keine Einzelfallprüfung auf der Grundlage eines hinreichenden Verdachts (*probable cause*) gegenüber einer konkreten Person.[28]

---

der Regel auf die „dominante Staatsangehörigkeit" abgestellt, siehe etwa *Sadat v. Mertes*, 615 F.2d 1176 (7th Cir.) (1980) (Kläger, der eingebürgerter US-Staatsangehöriger ist und den Ägypten weiterhin als Ägypter ansieht, der den USA die Treue geschworen hat, im Rahmen des Einbürgerungsprozesses auf jegliche Zugehörigkeit zu ausländischen Staaten verzichtet hat und sich während Auslandsaufenthalten bei der US-Botschaft registriert, ist aus Sicht der US-Gerichte nicht Ägypter zu Zwecken der Bestimmung der Bundesgerichtsbarkeit). Die dominante Staatsangehörigkeit eines Doppelstaaters aus Sicht der Section 702 FISA dürfte anhand der folgenden Kriterien ermittelt werden: gewöhnlicher Aufenthaltsort, Arbeitsstätte, Vermögenswerte, Familie. Dieses Vorgehen dürfte auch der Grundregel im internationalen Privatrecht entsprechen, dass in Staatsangehörigkeitssachen diejenige Staatsangehörigkeit mit dem engsten Anknüpfungspunkt Anwendung findet (vgl. etwa Art. 5 EGBGB im deutschen Rechtsraum).

24 Der U.S. Attorney General ist als Leiter des U.S.-Justizministeriums Teil des Kabinetts, ohne jedoch als Minister bezeichnet zu werden, und nimmt zugleich Aufgaben wahr, die in Deutschland durch den Generalbundesanwalt ausgeführt werden.

25 Definiert in 50 U.S.C. § 1801(e).

26 50 U.S.C. § 1881a(h)(1)(A), (2).

27 Definiert in 50 U.S.C. § 1801(i).

28 So hat ein Gericht die gerichtliche Überprüfung von Anordnungen nach 50 U.S.C. § 1881a(h) als „programmatic pre-clearance" bezeichnet, *United States v. Hasbajrami*, 945 F.3d 641, 652 (2d Cir. 2019). Siehe auch Noah C. Chauvin, *Increasing Congressional Oversight of FISA Section 702 After RISAA*, Widener Law Commonwealth Research Paper No. 25-1, 2025, Seiten

Nach dieser Prüfung durch den FISC und seiner Zustimmung ohne Vorbehalte in Form eines Beschlusses (*order*)[29] können der *Attorney General* und der *Director of National Intelligence* die Überwachung und Herausgabeverpflichtung autorisieren.[30] Auf der Grundlage dieser Autorisation können sie dann Telekommunikationsanbieter (*electronic communication service provider*) anweisen (*direct*), Informationen und Daten über Nutzer herauszugeben.[31] Für die Herausgabeanordnung (*directive*) ist kein (weiterer) individualisierter gerichtlicher Durchsuchungsbeschluss und auch keine Beschlagnahmeanordnung erforderlich. Gegen die Herausgabeanordnung kann der betroffene Telekommunikationsanbieter den FISC anrufen.[32] Kommt er der darauf ergehenden gerichtlichen Entscheidung nicht nach, macht er sich wegen Missachtung des Gerichts (*contempt of court*) strafbar.[33] Kommt der Adressat des Herausgabeverlangens diesem nicht ausreichend nach (*fails to comply*), so kann er auf Antrag des *Attorney General* durch einen weiteren Beschluss des FISC dazu angehalten werden.[34] Wiederum ist die Missachtung dieses Gerichtsbeschlusses strafbar.[35] Die Herausgabeverpflichtung und ihre Durchsetzbarkeit folgen also nicht unmittelbar aus dem Gesetz, sondern beruhen auf einer Reihe von behördlichen und gerichtlichen Entscheidungen.[36]

Wenn der FISC die *certification* des *Attorney General* und des *Director of National Intelligence* für fehlerhaft oder unvollständig hält, kann er Korrekturen anordnen.[37] Den Beschluss des FISC kann die Regierung vor dem Foreign Intelligence Surveillance Court of Review (FISCR) anfechten.[38]

7-8 und 12 ff., abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5084391.

29 50 U.S.C. § 1881a(j)(3)(A).

30 50 U.S.C. § 1881a(a).

31 50 U.S.C. § 1881a(i)(1).

32 50 U.S.C. § 1881a(i)(4).

33 50 U.S.C. § 1881a(i(4)(G).

34 50 U.S.C. § 1881a(i)(5).

35 50 U.S.C. § 1881a(i)(5)(D).

36 Vgl. dazu Stephen I. Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15.11.2021, Seiten 1-2, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf.

37 50 U.S.C. § 1881a(j)(3)(B).

38 50 U.S.C. § 1881a(j)(4).

Der *Attorney General* und der *Director of National Intelligence* können im Eilfall (*exigent circumstances*) eine Entschließung (*determination*) erlassen, wenn ohne die unverzügliche Autorisation Informationen verloren gehen oder nicht rechtzeitig gewonnen werden würden, die für die nationale Sicherheit der USA wichtig sind, und ein Beschluss des FISC nicht rechtzeitig vor einer solchen Autorisation erlangt werden könnte.[39] In diesem Fall müssen der *Attorney General* und der *Director of National Intelligence* innerhalb von sieben Tagen nach Erlass der Entschließung eine *certification* erlassen.[40]

Der Begriff der *electronic communication service provider*[41] – welche die Adressaten konkreter Herausgabeanordnungen sein können – wird vom Gesetz legaldefiniert.[42] Dazu zählen unter anderem Telekommunikationsanbieter (*telecommunications carrier*)[43], Anbieter von elektronischen Kommunikationsdiensten (*provider of electronic communication service*)[44] (ECS) und Anbieter von Remote-Computing-Diensten (*provider of a remote computing service*)[45] (RCS). Darüber hinaus ist „jeder sonstige Anbieter von Diensten, der Zugang zu Geräten hat, die zur Übertragung oder Speicherung drahtgebundener oder elektronischer Kommunikation verwendet werden oder verwendet werden können" (*any other service provider who has access to equipment that is being or may be used to transmit or store wire or electronic communications*[46]) erfasst.[47] „Zugang" zu solchen Geräten hat heutzutage wohl jeder Dienstleister, der in seinem Unternehmen z. B. Smartphones, Computer und W-LAN-Router verwendet. Die Dienstleister müssen also keine *Telekommunikations*anbieter mehr sein.[48] Vielmehr ist eine unüberschaubare Vielzahl von Dienstleistern erfasst, etwa auch

---

39 50 U.S.C. § 1881a(c)(2).
40 50 U.S.C. § 1881a(h)(1)(B).
41 Der Begriff wird in 50 U.S.C. § 1881a(i)(1) verwendet.
42 50 U.S.C. § 1881(b)(4).
43 50 U.S.C. § 1881(b)(4)(A), der auf 47 U.S.C. § 153(51) verweist.
44 50 U.S.C. § 1881(b)(4)(B), der auf 18 U.S.C. § 2510(15) verweist.
45 50 U.S.C. § 1881(b)(4)(C), der auf 18 U.S.C. § 2711 verweist.
46 50 U.S.C. § 1881(b)(4)(E).
47 Ausgenommen sind lediglich öffentliche Beherbergungs- und Wohneinrichtungen, öffentliche Betriebe wie Wasser- und Abfallwerke, Polizei- und Feuerwehrstationen, Bibliotheken, Krankenhäuser usw., und Gastronomiebetriebe, 50 U.S.C. § 1881(b)(4)(E)(i)-(iv).
48 Noah C. Chauvin, *Increasing Congressional Oversight of FISA Section 702 After RISAA*, Widener Law Commonwealth Research Paper No. 25-1, 2025, Seite 41, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5084391.

Waschsalons, Friseure, Fitnesscenter, Zahnarztpraxen, Baumärkte und kommerzielle Vermieter von Büroräumen.[49]

Hintergrund der Erweiterung des Kreises der Herausgabeverpflichteten durch Section 25 RISAA war eine Herausgabeanordnung aus dem Jahr 2022 an ein Rechenzentrum für Cloud-Computing-Dienste. Die Rechtslage vor 2024 sah noch eine enge Definition der *„electronic communication service provider"* vor und umfasste nur solche Unternehmen, die direkten Zugang zu Kommunikation zwischen Privaten haben. Das – nicht identifizierte – Rechenzentrum für Cloud-Dienste sah sich als von dieser Definition nicht erfasst an. Der FISC befand die Herausgabeanordnung auf die Rüge des betroffenen Unternehmens hin für rechtswidrig und blockierte sie.[50] Aus diesem Grund entschloss sich die Biden-Regierung, die Vorschrift zu reformieren. In diesem Kontext beteuerte das Justizministerium, durch die neue Vorschrift (vor allem) den Zugriff auf Rechenzentren für Cloud-Dienste ermöglichen zu wollen.[51]

Vor dem Hintergrund dieser Gesetzgebungsgeschichte besteht kein Zweifel daran, dass die Vorschrift den Zugriff auf die Anbieter von Cloud-Diensten und Rechenzentren bzw. deren Betreiber ermöglicht.[52]

---

49 Elizabeth Goitein, *Is Secret Law the Solution to an Overbroad Surveillance Authority?*, JUST SEC. (June 11, 2024), abrufbar unter: https://www.justsecurity.org/96638/secret-law-overbroad-surveillance-authority/.

50 *In re* Petition to Set Aside or Modify Directive Issued to [Redacted], Slip Op. at 20 (FISC Ct. Rev. 2023), abrufbar unter: https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf; *In re* Petition to Set Aside or Modify Directive Issued to [Redacted], Slip Op. at 20 (FISC 2022). Die maßgeblichen Stellen sind zwar geschwärzt und das betroffene Unternehmen ist nicht identifizierbar, aber es ist bekannt, dass es sich um ein *cloud computing data center* handelte, vgl. Charlie Savage, *Secret Rift Over Data Center Fueled Push to Expand Reach of Surveillance Program*, 17.4.2024, New York Times, abrufbar unter: https://www.nytimes.com/2024/04/16/us/fisa-surveillance-bill-program.html.

51 Siehe zu alledem Noah C. Chauvin, *Increasing Congressional Oversight of FISA Section 702 After RISAA*, Widener Law Commonwealth Research Paper No. 25-1, 2025, Seiten 42 f., abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5084391.

52 Vgl. dazu u.a. Preston Marquis, *FISA Section 702 Reauthorized for Two Years*, 30.04.2024, abrufbar unter: https://www.lawfaremedia.org/article/fisa-section-702-reauthorized-for-two-years#:~:text=Lawmakers%20were%20tight%2Dlipped%20about,data%20center%20under%20Section%20702; Patrick G. Eddington, *FISA Fight Final Score: Surveillance State 1, Bill of Rights 0*, 22.04.2024, abrufbar unter: https://www.cato.org/blog/fisa-fight-final-score-surveillance-state-1-bill-rights-0; John Miller, *Expansion of*

Ob ein bestimmtes Unternehmen als ECS oder RCS in Anspruch genommen werden kann, ist anhand der konkreten Umstände des Einzelfalls zu bewerten.[53] So erbringen die meisten Internetanbieter heutzutage sowohl elektronische Kommunikationsdienste als auch Remote-Computing-Dienste. Welcher Definition sie unterfallen, bestimmt sich dann nach der konkreten Information, die abgefragt wird, zu der bestimmten Zeit und in dem bestimmten Kontext. Das Unternehmen als solches kann also hinsichtlich der einen Kommunikation wie ein ECS agieren, hinsichtlich der anderen Kommunikation wie ein RCS, und hinsichtlich einer weiteren Kommunikation weder als ECS noch als RCS.[54]

Um unter die gesetzliche Definition eines RCS zu fallen, muss ein Unternehmen seine Tätigkeit auf die Öffentlichkeit ausrichten, d.h. der Öffentlichkeit anbieten und zur Verfügung stellen (*means the provision to the public of computer storage or processing services by means of an electronic communications system*[55]). Eine Fluggesellschaft, die eine Website und Server betreibt, um Kommunikation mit ihren Kunden zu ermöglichen, betreibt keinen Remote-Computing-Dienst.[56] Das Gleiche gilt für ein Unternehmen, das seinen freien Mitarbeitenden (*contractors*) Zugang zu einem internen E-Mail-System gewährt.[57] Die Definition des RCS ist mithin relativ eng und erfordert, dass das Unternehmen seine Dienste der Speicherung oder Verarbeitung von Daten der *uneingeschränkten Öffentlichkeit* zur Verfügung stellt. Damit unterfällt auch ein Unternehmen, das (nur) seiner Mutter- oder Tochtergesellschaft eben diese Dienste zur Verfügung stellt, der Definition eines RCS nicht.[58]

FISA Electronic Communications Service Provider Definition Must Be Removed, 16.04.2024, abrufbar unter: https://www.itic.org/news-events/techwonk-blog/expansion-of-fisa-electronic-communications-service-provider-definition-must-be-removed.

53 *In re* United States, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009).

54 Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it*, 72 Geo. Wash. L. Rev. 1208, 1215-1216 (2004).

55 18 U.S.C. § 2711(2).

56 *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 310 (E.D.N.Y. 2005).

57 *Andersen Consulting, LLP v. UOP*, 991 F. Supp. 1041, 1042-1043 (N.D. Ill. 1998).

58 Stephen I. Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15.11.2021, Seiten 6-7, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf.

Das Erfordernis der Ausrichtung auf die Öffentlichkeit gilt für ECS nicht. So haben US-Gerichte die Eigenschaft als ECS bei einem Unternehmen als erfüllt angesehen, das seinen Mitarbeitern die Möglichkeit eingeräumt hat, unternehmensinterne E-Mails zu verschicken.[59] Ebenso wurde eine Reiseagentur als ECS angesehen, das seinen Mitarbeitenden elektronische Reservierungssysteme zur Verfügung gestellt hat.[60]

Inhaltlich muss sich die Überwachung und Herausgabeanordnung auf „Geheimdienst-relevante Informationen aus dem Ausland" (*foreign intelligence information*) beziehen. Dieser Begriff ist legaldefiniert[61] und umfasst neben Bedrohungen aus Krieg, Terrorismus, Massenvernichtungswaffen, Spionage und internationalem Drogenhandel auch alle sonstigen Informationen zu einem fremden Staat oder Staatsgebiet, die „mit der nationalen Verteidigung oder Sicherheit oder mit der Führung der auswärtigen Angelegenheiten der USA in Zusammenhang stehen" (*relates to [...] the national defense or the security of the United States; or the conduct of the foreign affairs of the United States*).[62] Eine Auslegung des „Zusammenhangs mit den auswärtigen Angelegenheiten der USA" kann denkbar weit erfolgen. Durch diese Auffangklausel dürfte der Überwachungsbefugnis der US-Geheimdienste kaum mehr eine echte Grenze gesetzt sein.[63] Im Ernstfall lässt sich nahezu jede Information mit der Führung der auswärtigen Angelegenheiten der USA kreativ in Zusammenhang bringen.

Der FISC hat in der Vergangenheit sowohl die Herausgabe von Metadaten als auch von Kommunikations*inhalten* autorisiert. Das ist möglich aufgrund der Legaldefinition von „Inhalten" (*contents*), die im Zusammenhang mit drahtgebundener, mündlicher oder elektronischer Kommunikation „alle Informationen einschließen, die den Inhalt, Zweck oder die Bedeutung dieser Kommunikation betreffen" (*includes any in-*

59 *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114-115 (3d Cir. 2003); *Shefts v. Petrakis*, No. 10-cv-1104, 2011 WL 5930469, at 13 (C.D. Ill. Nov. 29, 2011).

60 *United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993).

61 50 U.S.C. § 1801(e).

62 50 U.S.C. § 1801(e)(2).

63 Noah C. Chauvin, *The Warrant Exception that Isn't: FISA Section 702, "Defensive" Searches, and the Fourth Amendment*, 74 Am. U. L. Rev., im Erscheinen 2025, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4914365.

formation concerning the substance, purport, or meaning of that communication).[64] Section 702 FISA betrifft sowohl Daten, die sich in der Übermittlung befinden, als auch Daten, die bereits gespeichert sind.

Section 24 RISAA hat Section 702(f)(6) FISA geschaffen. Hiernach müssen Nachrichtendienste, die Zugang zu Section 702-generierten Daten haben, Suchmechanismen schaffen, die die Überprüfung von Nicht-US-Personen ermöglichen, die zum Zwecke der Reise in die USA überprüft werden, und zwar unter Verwendung von Begriffen, die keine US-Personen-Begriffe sind. Das ist eine erhebliche Erweiterung der Befugnisse und weckt Zweifel, ob das EU-US *Data Privacy Framework* mit den Europäischen Menschenrechten vereinbar ist.[65] Beide Vorgänger des *Privacy Frameworks* hat der EuGH bereits gekippt: das EU-US *Safe-Harbor-Abkommen* aus dem Jahr 2000, das der EuGH 2015 für ungültig erklärt hat,[66] und dessen Nachfolgeregelung EU-US *Privacy Shield* aus dem Jahr 2016, das der EuGH 2020 für ungültig erklärt hat.[67] Die Begründung des EuGH war schlicht, dass die Regelungen der Section 702 FISA dem europäischem Datenschutzniveau nicht entsprechen.[68]

Section 702 FISA ermächtigt die Behörden, Daten zu sammeln, die von US-amerikanischen Dienstleistern gespeichert oder verarbeitet werden. Dabei kommt es nicht so sehr auf den Ort der Niederlassung des Unternehmens, sondern vielmehr auf den Ort des Servers an. Sobald Daten auf US-Territorium gespeichert oder verarbeitet werden, unterliegen sie Section 702 FISA. Da diese Daten ausschließlich Nicht-US-Personen betreffen dürfen (d.h. insbesondere keine Person, die sich

---

64 Stephen I. Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15.11.2021, Seite 2, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf.

65 Noah C. Chauvin, *Increasing Congressional Oversight of FISA Section 702 After RISAA*, Widener Law Commonwealth Research Paper No. 25-1, 2025, Seiten 40 f., abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5084391.

66 EuGH, Schrems v. Data Protection Commissioner, Urt. v. 06.10.2015, ECLI:EU:C:2015:650, abrufbar unter: https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1 (Schrems I).

67 EuGH, Data Protection Commissioner v. Facebook Ireland Ltd., Urt. v. 16.07.2020, ECLI:EU:C:2020:559, abrufbar unter: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1 (Schrems II).

68 EuGH, ECLI:EU:C:2020:559, Schrems II, Rn. 180.

auf US-Territorium befindet), ist Section 702 FISA zwangsläufig extraterritorial.

Wenn hingegen der Server außerhalb des US-Territoriums belegen ist, dann kommt es auf die mögliche Kontrolle des US-amerikanischen Unternehmens über diesen Server an (dazu unten, III., Fragestellung 2).[69]

Außerdem ist zu berücksichtigen, dass die Definition auch leitende Angestellte, Mitarbeitende, Verwalter und Vertreter (*officer, employee, custodian, or agent of an entity*) umfasst. Das bedeutet, dass eine (ausländische) Tochtergesellschaft eines ECS in der Regel von der Definition umfasst ist (dazu unten, II., Fragestellung 3). Ob hingegen auch die Muttergesellschaft eines ECS oder ein mit einem ECS verbundenes Unternehmen zwingend umfasst ist, ist weniger eindeutig.[70]

Infolgedessen stellt sich die Frage nach der Durchsetzbarkeit einer etwaig bestehenden Herausgabeverpflichtung. Jedes Unternehmen mit einer physischen Präsenz in den USA wird den oben dargelegten Sanktionsmechanismen (Strafbarkeit wegen Missachtung des Gerichts) unterliegen. Es wäre zwar denkbar, dass Unternehmen, die überhaupt gar keinen Bezugspunkt in den USA haben, auch von einer Anordnung nach Section 702 FISA betroffen sein könnten. Eine Durchsetzbarkeit in Form von Sanktionen ist aber schwer vorstellbar.[71]

Section 702 FISA ist seit der Einführung mit einem Ablaufdatum versehen, um die Befassung des Kongresses mit der Vorschrift in regelmäßigen Abständen zu gewährleisten. Die Geltungsdauer der Vorschrift wurde bislang dreimal und zuletzt im Jahr 2024 verlängert. Das Außerkrafttreten der Vorschrift ist derzeit für den 20.04.2026 vorgesehen.[72] Die Vorschrift unterlag in der Vergangenheit einigen Ände-

---

69 Stephen I. Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15.11.2021, Seite 9, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf.

70 Stephen I. Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15.11.2021, Seite 9, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf.

71 Stephen I. Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15.11.2021, Seite 9, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf.

72 Section 19(a)(1)(A) RISAA.

rungen und sieht sich teils massiver Kritik ausgesetzt, weil sie die Überwachung von US-amerikanischen Staatsbürgern durch die Hintertür („*backdoor searches*") ermögliche.[73] So fordern einige, dass der Kongress eine Verlängerung der Geltungsdauer nicht ohne substanzielle Reformen der Vorschrift beschließen solle.[74]

3. Executive Order 12.333

Die Executive Order (EO) 12.333 wurde 1981 durch Präsident Ronald Reagan erlassen und ermächtigt die National Security Agency (NSA), Kommunikationsdaten von Nicht-US-Personen zu sammeln, speichern und verarbeiten, wenn sich diese Daten außerhalb der USA befinden. EO 12.333 wurde seit ihrem Erlass mehrfach geändert, zuletzt 2008 durch Präsident George W. Bush.[75] Das Instrument der Executive Order ist ein formloser Erlass des US-Präsidenten zur Ausführung seiner verfassungsrechtlichen Exekutivfunktion. Dieser kann rein verwaltungsinterne Anweisungen sowie allgemein-rechtsverbindliche Regelungen ähnlich einer Rechtsverordnung im deutschen Recht enthalten. Eine Zustimmung der Legislative ist nicht erforderlich, jedoch kann der US-Kongress eine Exekutive Order durch den Erlass eines entgegenstehenden Gesetzes überstimmen.

Während FISA US-Geheimdienste zur Überwachung innerhalb der USA ermächtigt, stellt EO 12.333 die Grundlage für Überwachungsaktivitäten außerhalb der USA dar. EO 12.333 ermächtigt US-Geheimdienste dazu, Kommunikationsinformationen und anderen Daten, die über Funk, Draht und elektromagnetische Mittel übermittelt werden oder zugänglich sind und die sich im US-Ausland befinden, zu sammeln.

---

73 Kürzlich entschied ein US-Gericht, dass die Durchsuchung der Datenbanken und die Ermittlung von Daten von US-Personen auf Grundlage von nach Section 702 FISA erlangten Datensätzen ohne Durchsuchungsbeschluss gegen den Vierten Zusatzartikel verstoßen und somit verfassungswidrig sind, *United States v. Hasbajrami*, Case 1:11-cr-00623-LDH (E.D.N.Y., 02.12.2024), abrufbar unter: https://assets.aclu.org/live/uploads/2025/01/2025.01.21-U.S.-v.-Hasbajrami-Opinion.pdf.

74 Statt vieler Noah C. Chauvin, *Increasing Congressional Oversight of FISA Section 702 After RISAA*, Widener Law Commonwealth Research Paper No. 25-1, 2025, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5084391.

75 Vgl. Executive Order 13470, 30.07.2008, abrufbar unter: https://www.govinfo.gov/content/pkg/WCPD-2008-08-04/pdf/WCPD-2008-08-04-Pg1064.pdf).

Im Gegensatz zu Section 702 des FISA stützt sich die Überwachung gemäß EO 12.333 nicht auf die erzwungene Unterstützung von ECS und begründet keine Aufgaben oder Verpflichtungen für private Unternehmen.[76]

Die technischen Details sind geheim und undurchsichtig, aber die NSA hat bestätigt, dass EO 12.333 die Sammlung von Daten unter Ausnutzung von Schwachstellen in der Telekommunikationsinfrastruktur beinhaltet.[77] Außerhalb der von der NSA veröffentlichten Informationen ist über die Überwachungspraxis unter EO 12.333 wenig bekannt und Versuche von Bürgerrechtsorganisationen, Informationen auf dem Klageweg zu erlangen, wurden bisher durch US-Gerichte abgewiesen.[78]

4. Stored Communications Act

Der Stored Communications Act (SCA), kodifiziert in 18 U.S.C. §§ 2701-2713, ist der Title II des Electronic Communications Privacy Acts of 1986 (ECPA), dieser wiederum kodifiziert in 18 U.S.C. §§ 2510-2725. Der CLOUD Act ist lediglich ein Änderungsgesetz, das Vorschriften im ECPA geändert hat. Der SCA regelt die Herausgabeverpflichtung bestimmter Anbieter von digitalen Dienstleistungen gegenüber den US-Strafverfolgungsbehörden und bestimmt die Voraussetzungen, unter denen Regierungsbehörden auf die Daten zugreifen können.

Adressaten des SCA sind Anbieter von elektronischen Kommunikationsdiensten (*electronic communication services (ECS)*) und von Remote-Computing-Diensten (*remote computing services (RCS)*). Die Definitionen sind dabei deckungsgleich mit denen des FISA.

Die herauszugebenden Daten umfassen den Inhalt elektronischer Kommunikation (*contents of a wire or electronic communication*) und von in Clouds gespeicherten Dokumenten sowie nicht-inhaltliche Informationen wie Nutzerdaten und Übermittlungsdaten (*record or other*

76 Lawne, Richard, *Schrems II: FISA and EO 12333 Overview*, Practical Law Article w-028-0691, (2020).
77 NSA-Pressestatement vom 09.08.2013 (abrufbar unter: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1618729/the-national-security-agency-missions-authorities-oversight-and-partnerships/).
78 Am. C.L. Union v. Nat'l Sec. Agency, No. 13CIV09198KMWJCF, 2017 WL 1155910, (S.D.N.Y. Mar. 27, 2017), aff'd, 925 F.3d 576 (2d Cir. 2019).

information pertaining to a subscriber to or customer of [ECS/RCS]), aber keine sonstigen personenbezogenen oder Geschäftsdaten.[79] Section 2703 SCA ermächtigt staatliche Stellen (*government entity*), ECS und RCS unter bestimmten Voraussetzungen zur Herausgabe von Inhalten und/oder Nutzerdaten drahtgebundener oder elektronischer Kommunikation zu verpflichten.

Neuere Kommunikationsinhalte, die seit 180 oder weniger Tagen elektronisch gespeichert sind, dürfen nur auf Grundlage eines gerichtlichen Durchsuchungsbeschlusses (*warrant*) herausverlangt werden.[80] Ältere Kommunikationsinhalte können hingegen unter den gleichen Voraussetzungen herausverlangt werden, wie die Inhalte drahtgebundener oder elektronischer Kommunikation von Nutzern von Remote-Computing-Diensten. Die Voraussetzungen hierfür sind gelockert; so ist die Herausgabeanordnung nicht nur auf Grundlage eines gerichtlichen Durchsuchungsbeschlusses möglich, sondern – mit vorheriger Benachrichtigung des betroffenen Nutzers durch die staatliche Stelle – auch auf Grundlage einer behördlichen Vorladung (*administrative subpoena*) oder eines sonstigen Gerichtsbeschlusses (*court order*).[81] Oftmals wird die staatliche Stelle indes eine Geheimhaltungsanordnung mit der Folge erwirken, dass die Benachrichtigung der Person, gegen die ermittelt wird, erst später erfolgt.[82] Nutzerdaten von ECS- oder RCS-Nutzern sind ebenfalls unter diesen Voraussetzungen zu erlangen, oder zusätzlich bei Zustimmung des Nutzers.[83]

Für den Erlass eines Durchsuchungsbeschlusses ist ein hinreichender Verdacht (*probable cause*) erforderlich.[84] Dies entspricht dem Standard des 4. Zusatzartikels zur Verfassung der USA zum Schutz gegen unbegründete Durchsuchungsbeschlüsse. Die Regierung muss mithin darlegen, dass die Kommunikationsdaten zur Beweisführung in einem Strafverfahren genutzt werden. In *Carpenter v. United States*[85] stellte

---

79 Office of Legal Education, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2009, Seiten 120 ff., abrufbar unter: https://www.justice.gov/d9/criminal-ccips/legacy/2015/01/14/ssmanual2009_002.pdf.

80 18 U.S.C. § 2703(a).

81 18 U.S.C. § 2703(b).

82 18 U.S.C. § 2705.

83 18 U.S.C. § 2703(c).

84 18 U.S.C. § 2703(a) und 18 U.S.C. § 2703(b)(1)(A) in Verbindung mit Fed. R. Crim. Pro. Rule41(c)(1).

85 Carpenter v. United States, 585 U.S. 296 (2018).

der Supreme Court fest, dass der *probable cause*-Standard auch für sonstige Gerichtsbeschlüsse (s.o.) gilt, da die Abfrage von Telefonzellendaten als „Durchsuchung" im Sinne des 4. Zusatzartikels zu werten ist. Das Gericht beschränkte seine Entscheidung jedoch explizit auf Telefonzellendaten, so dass eine Abfrage anderer Datentypen theoretisch auch ohne den *probable cause*-Standard denkbar ist.

Während der U.S. Supreme Court in *Carpenter* zwar feststellte, dass die Sicherheitsbehörden grundsätzlich nur auf der Grundlage eines Gerichtsbeschlusses Unternehmen zur Herausgabe der gewünschten Daten verpflichten – zwingen – dürfen, läuft diese Gerichtsentscheidung in der Praxis teilweise ins Leere. Solange die Unternehmen die Daten „freiwillig" herausgeben, so die Interpretation durch die Sicherheitsbehörden, bedarf es keines Gerichtsbeschlusses. Die Freiwilligkeit der Unternehmen erkaufen die Sicherheitsbehörden indes mit barem Geld, wie ein von der US-Regierung angefertigter Bericht 2022 ermittelte.[86]

Im Vorfeld der Datenabfrage kann das betroffene Unternehmen auch zur Speicherung und Vorhaltung der Daten verpflichtet werden.[87] Pflichten zur Speicherung und Vorhaltung von Daten stehen eigenständig neben der Pflicht zur Herausgabe auf Anordnung. Die Speicherpflicht betrifft voraussichtlich keine Nicht-US-Personen, da entweder der SCA keine Anwendung findet oder eine Durchsetzbarkeit mangels Sanktionsmöglichkeiten fehlt.[88]

Der SCA enthält in Section 2709 eine weitere Ermächtigungsgrundlage zur Verpflichtung von ECS zur Herausgabe bestimmter Daten auf der

---

86 Siehe den Bericht über „Käuflich Erwerbliche Informationen" (Commercially Available Information") an den DNI, unbekannter Autor (geschwärzt), 27.01.2022, abrufbar unter: https://www.documentcloud.org/documents/23844477-odni-declassified-report-on-cai-january2022/. Vgl. auch Kevin Collier, U.S. government buys data on Americans with little oversight, report finds, 13.06.2023, abrufbar unter: https://www.nbcnews.com/tech/security/us-government-buys-data-americans-little-oversight-report-finds-rcna89035; Elizabeth Goitein, The Government Can't Seize Your Digital Data. Except by Buying It., 28.04.2021, abrufbar unter: https://www.brennancenter.org/our-work/analysis-opinion/government-cant-seize-your-digital-data-except-buying-it.

87 18 U.S.C. § 2703(f).

88 Stephen I. Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15.11.2021, Seite 14, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf.

Grundlage eines *National Security Letters*, einer Art behördlichen Anordnung (*administrative subpoena*), die das FBI ohne richterliche Beteiligung erlässt und die (nur im Nachgang) eingeschränkter gerichtlicher Überprüfbarkeit unterliegt.[89] Die Herausgabepflicht nach dieser Vorschrift bezieht sich auf Telefonteilnehmerdaten (*subscriber information*), Zahlungsdaten (*toll billing records information*) und andere elektronische Transaktionsdaten (*electronic communication transactional records*). Ausgeschlossen ist die Erhebung des Inhalts der abgefragten Kommunikation.

National security letters können auch auf der Grundlage anderer Vorschriften erlassen werden. So ermächtigen neben dem SCA auch der Fair Credit Reporting Act (1970)[90] und der Right to Financial Privacy Act (1978)[91] die US-Regierung, auf Daten zuzugreifen, die für die innere Sicherheit „relevant" sind.[92]

Im Jahr 2023 stellte das FBI nach eigenen Angaben 11.158 *National Security Letters* aus.[93] Viele *National Security Letters* enthalten eine Klausel, die es dem Adressaten verbietet, die Person, über die Daten durch das FBI abgefragt werden, über diesen Vorgang zu informieren. Dies hat in der Vergangenheit Zweifel an der Verfassungsmäßigkeit der Vorschrift aufkommen lassen.[94]

---

89 18 U.S.C. § 2709.

90 So wird Title IV des Consumer Credit Protection Acts bezeichnet. Publ. L. 91-507, 84 Stat. 1127, kodifiziert als 15 U.S.C. §§ 1681-1681x. Die hier gemeinten Vorschriften sind Sections 626, 627, kodifiziert als 15 U.S.C. §§ 1681u, 1681v. Herausgegeben werden müssen hiernach die von Verbraucherkreditwürdigkeitsagenturen (*consumer reporting agency*, definiert in 15 U.S.C. § 1681a(f)) gesammelten Informationen über Verbraucher.

91 Publ. L.115-174, 132 Stat. 1335, kodifiziert als 12 U.S.C. §§ 3401-3423. Die hier gemeinte Vorschrift ist Section 1114, kodifiziert als 12 U.S.C. § 3414. Herausgegeben werden müssen hiernach Finanzinformationen.

92 Stephen I. Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15.11.2021, Seite 11, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf.

93 https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

94 Siehe etwa zur alten Fassung des § 2709(c): In re National Sec. Letter, United States District Court, N.D. California, 930 F.Supp.2d 1064. In Doe v. Mukasey, 549 F.3d 861 (2d Cir. 2008) hat der Second Circuit entschieden, dass die Geheimhaltungsklauseln der National Security Letters den 1. Zusatzartikel zur Verfassung der USA verletzten. In der Konsequenz wurden die Vorschriften geändert, um eine stärkere gerichtliche Kontrolle der Geheimhaltungsvereinbarung zu ermöglichen.

II. Herausgaberecht gegenüber ausländischen Tochtergesellschaften US-amerikanischer Unternehmen auf außerhalb der USA gespeicherte Daten (Fragestellung 3)

Durch den CLOUD Act von 2018 wurde unter anderem die Vorschrift in Section 2713 SCA eingefügt, die bereits bestehende Verpflichtungen des SCA dahingehend konkretisiert bzw. ergänzt, dass die Daten unabhängig davon, ob sie in den USA oder im Ausland gespeichert sind, herauszugeben sind.[95] Nach Auffassung des US-amerikanischen Justizministeriums hat die Norm lediglich eine klarstellenden Funktion.[96] Es beruft sich auf den Grundsatz, dass maßgeblicher Faktor für die Durchsetzbarkeit eines Herausgabeverlangens durch US-Behörden nicht der Ort der Speicherung, sondern die tatsächliche Kontrolle über die Daten sei.
Tatsächlich entspricht es der Rechtsprechung von US-Bundesgerichten, dass einem gerichtlichen Beweisbeschluss über Dokumente, welche sich im Ausland befinden, auch dann nachzukommen ist, wenn das Gericht zuständig ist und sich die angeforderten Dokumente in der Kontrolle der verpflichteten Person befinden.[97]
Der Begriff der „Kontrolle" wird dabei durch die US-Gerichte unterschiedlich ausgelegt. Teilweise wird auf die tatsächliche Zugriffsmöglichkeit (*pracical ability*) und teilweise auf die rechtliche Möglichkeit (*legal right*) abgestellt.[98]
In *First Nat. City Bank of N.Y. v. I.R.S. of U.S. Treasury Dep't* erläuterte der U.S. Court of Appeals (2nd Cir.):

> *Die „Kontrolle" über ihre Aufzeichnungen, auf die sich die Verpflichtung einer Gesellschaft gründet, sie auf Vorladung oder subpoena duces tecum vorzulegen, ist kein esoterisches Kon-*

---

95 Vgl. U.S. Department of Justice (DOJ), *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (CLOUD Act Whitepaper), FAQ 18, Seite 13 (April 2019), abrufbar unter: https://www.justice.gov/archives/opa/press-release/file/1153446/dl.

96 DOJ, Whitepaper, S. 9.

97 Siehe etwa: U.S. v. First Nat. City Bank, United States Court of Appeals Second Circuit, June 26, 1968, 396 F.2d 897.

98 Possession, Custody, and Control of ESI in Federal Civil Litigation, Westlaw Pratical Law, abrufbar unter: https://www.skadden.com/-/media/files/publications/2023/11/possession_custody_and_control_of_esi_in_federal_civil_litigation.pdf?rev=c2e655de6b9d4a469f6301347d41fb40.

> *zept, und jeder leitende Angestellte oder Vertreter, der die Befugnis hat, zu veranlassen, dass die Aufzeichnungen einer Zweigstelle zu einem beliebigen Unternehmenszweck an die Hauptniederlassung geschickt werden, hat eine ausreichende „Kontrolle", um zu veranlassen, dass sie auf Wunsch zu einem behördlichen Zweck weitergeschickt werden [...]*[99]

Die Verpflichtung zur Herausgabe wird auch nicht dadurch ausgeschlossen, dass der Verpflichtete durch die Herausgabe das Recht des Landes bricht, in dem die Daten gelagert sind. In *U.S. v. First Nat. City Bank* war das Gericht mit der Frage konfrontiert, ob eine US-Bank auch dann Informationen bereitstellen muss, wenn sie dadurch in Deutschland einer zivilrechtlichen Haftung ausgesetzt wäre. Das Gericht stellte fest, dass für den Fall, dass die Rechtsnormen zweier Staaten von einem Adressaten ein widersprüchliches Verhalten verlangen, das Vollzugs-interesse anhand folgender Faktoren abzuwägen ist:

> *(a) grundlegende nationale Interessen eines jeden Staates,*
> *(b) das Ausmaß und die Art der Härte, die widersprüchliche Vollstreckungsmaßnahmen für die betreffende Person mit sich bringen würden,*
> *(c) das Ausmaß, in dem das verlangte Verhalten im Hoheitsgebiet des anderen Staates stattfinden soll,*
> *(d) die Staatsangehörigkeit der Person, und*
> *(e) das Ausmaß, in dem vernünftigerweise erwartet werden kann, dass die Vollstreckung durch Maßnahmen eines der beiden Staaten die Einhaltung der von diesem Staat vorgeschriebenen Regelung erreicht.*[100]

---

99 Im Original: „The "control" over its records upon which is founded the obligation of a corporation to produce them upon summons or *subpoena duces tecum* is not an esoteric concept, and any officer or agent who has the power to cause the branch records to be sent from a branch to the home office for any corporate purpose has sufficient "control" to cause them to be sent on when desired for a governmental purpose properly implemented by subpoena [...] (First Nat. City Bank of N.Y. v. I.R.S. of U.S. Treasury Dep't, 271 F.2d 616 (2d Cir. 1959)).

100 (a) vital national interests of each of the states,
(b) the extent and the nature of the hardship that inconsistent enforcement actions would impose upon the person,
(c) the extent to which the required conduct is to take place in the territory of the other state,
(d) the nationality of the person, and
(e) the extent to which enforcement by action of either state can reasonably be expected to achieve compliance with the rule prescribed by that state.

Da die Herausgabe von Bankdaten in Deutschland nicht strafbewehrt ist, sondern lediglich eine zivilrechtliche Haftung nach sich zieht, kam das Gericht zu dem Schluss, dass das Vollzugsinteresse der US-Strafverfolgungsbehörden überwiegt.

Durch den CLOUD Act wurde zudem die Regelung der Section 2703(h)(2)(A) SCA geschaffen. Danach können ECS und RCS Rechtsmittel gegen einen Durchsuchungsbeschluss nach Section 2703(b) oder (c) SCA erheben, wenn sie durch dessen Ausführung gegen das Recht eines fremden Staats verstoßen würden. Diese Möglichkeit besteht jedoch nur für „qualifizierte ausländische Staaten" (*qualifiying foreign government*) im Sinne von 18 U.S.C. § 2523. Danach können ausländische Staaten mit den USA ein Verwaltungsabkommen schließen, welches den Zugang und Austausch von Daten regelt. Während es mit der Europäischen Union zwar Verhandlungen aber ein solches Abkommen gegeben hat, wurde bisher lediglich mit dem Vereinigten Königreich und Australien ein solches unterzeichnet. Das bedeutet, dass die Bundesrepublik Deutschland zurzeit kein qualifizierter ausländischer Staat im Sinne des CLOUD Act ist. Ein in Deutschland ansässiges Unternehmen könnte der Datenabfrage mithin nicht widersprechen. Im Übrigen obliegt die Entscheidung über einen solchen Widerspruch einem US-Gericht, das u.a. „im Interesse der Gerechtigkeit" darüber entscheiden muss (*the interests of justice dictate that the legal process should be quashed*).[101] Wie die Abwägung eines US-amerikanischen Gerichts zwischen dem deutschen/EU-Datenschutzrecht und der Strafverfolgung durch US-Behörden zum Zwecke der Herstellung von „Gerechtigkeit" (wie in diesem Zusammenhang ausgelegt) ausfallen wird, lässt sich hier nicht abschließend beurteilen.

Diese Art eines Widerspruchsrechts wegen Verstoßes gegen das Datenschutzrecht eines anderen Landes enthält Section 702 FISA übrigens nicht. Im Gegenteil gilt die Vorschrift „ungeachtet anderer gesetzlicher Bestimmungen" (*notwithstanding any other provision of law*).

Die Frage der Extraterritorialität des SCA war zudem Gegenstand eines Rechtsstreit zwischen Microsoft und dem FBI.[102] Das FBI erwirkte einen

---

101 18 U.S.C. § 2703(h)(2)(B)(ii).

102 U.S. v. Microsoft Corp., 584 U.S. 236 (2018).

Durchsuchungsbeschluss unter dem SCA gegen Microsoft und verlangte die Herausgabe von Daten eines E-Mail-Accounts. Microsoft erhobt daraufhin Beschwerde beim zuständigen Bundesgericht mit der Begründung, dass die betreffenden Daten des E-Mail-Accounts beim Tochterunternehmen Microsoft Ireland in Irland gespeichert seien und sich somit außerhalb der Zuständigkeit amerikanischer Gerichte befänden. Microsofts Beschwerde wurde zunächst in erster Instanz verworfen, dann durch ein Berufungsgericht stattgegeben. Das Berufungsgericht wandte dabei die Doktrin der „Vermutung gegen die Extraterritorialität" (*presumption against extraterritoriality*) an.[103] Danach sind Bundesgesetze in Ermangelung eines entgegenstehenden gesetzgeberischen Willens dahingehend auszulegen, dass Ihre Geltung auf die territorialen Grenzen der USA beschränkt sei.

Die US Regierung legte gegen die Entscheidung des Berufungsgerichts Rechtsmittel zum U.S. Supreme Court ein. Während des laufenden Verfahrens trat 2018 der CLOUD Act in Kraft, woraufhin der U.S. Supreme Court das Verfahren als erledigt (*moot*) erklärte, da nun kein Disput über die Frage der Extraterritorialität mehr bestehe.[104]

III. Herausgaberecht gegenüber ausländischen Unternehmen auf außerhalb der USA gespeicherte Daten (Fragestellung 2)

Artikel III, § 2 der US-Verfassung begründet die Zuständigkeit von US-Gerichten über Nicht-US-Bürger. Nach 28 U.S.C. § 1332(a)(2) sind für Streitigkeiten zwischen US-Bürgern und Nicht-US-Bürgern, welche sich nicht dauerhaft auf dem Territorium der USA befinden, die Bundesgerichte (*federal court*) zuständig.
Die Reichweite dieser Zuständigkeit bestimmt sich nach dem Konzept der *personal jurisdiction.* Bei der Bestimmung der Frage, ob *personal jurisdiction* über ein beklagtes Unternehmen vorliegt, untersuchen die Gerichte, ob ausreichende Kontakte zwischen dem Unternehmen und dem in die Zuständigkeit des Gerichts fallenden Gebiet (*forum*) bestehen. Dabei wird zwischen *specific personal jurisdiction* und *general personal jurisdiction* unterschieden.

---

[103] 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," Matter of Warrant to Search a Certain E-Mail Acct. Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 210 (2d Cir. 2016), vacated and remanded sub nom. United States v. Microsoft Corp., 584 U.S. 236, 138 S. Ct. 1186, 200 L. Ed. 2d 610 (2018).
[104] US v. Microsoft Corp., 584 U.S. 236 (2018).

Specific personal jurisdiction besteht dann, wenn der zugrundeliegende Rechtsstreit mit einer spezifischen Handlung des Unternehmens im *forum state* in Verbindung steht oder aus ihr entspringt.[105] Dies wäre etwa dann der Fall, wenn in einem Verfahren wegen Schadensersatzes die deliktische Handlung vom Unternehmen innerhalb der USA begangen wurde. *Specific personal jurisdiction* bezieht sich somit lediglich auf den im Verfahren relevanten Streitgegenstand, so dass auch nur auf diesen US-Recht Anwendung findet. Sie rechtfertigt mithin keine Klagen gegen das Unternehmen, welche aus einem anderen Sachverhalt resultieren.

General personal jurisdiction wiederum ist dann anzunehmen, wenn zwar keine konkrete Handlung des Unternehmens im Zusammenhang mit dem Rechtsstreit vorliegt, das Unternehmen jedoch dauerhaft und systematische Kontakte zum *forum state* pflegt, die die Ausübung der Gerichtsbarkeit rechtfertigen.[106] Im Gegensatz zu *specific personal jurisdiction* rechtfertigt die Annahme von *general personal jurisdiction* die Anwendung von US-Recht auf alle Klagen, die sich gegen das betreffende Unternehmen richten.[107]

Die Antwort auf die Frage, ob *personal jurisdiction* anzunehmen ist, ist einzelfallabhängig. Bei der Beurteilung der Frage, ob *specific personal jurisdiction* vorliegt, prüfen die Gerichte, ob das Unternehmen bestimmte „Mindestkontakte" (*minimum contacts*) zu den USA hat, die die Ausübung der Gerichtsbarkeit rechtfertigen.[108] Diese Prüfung findet regelmäßig in drei Schritten statt:[109]

---

105 „When a controversy is related to or "arises out of" a defendant's contacts with the forum, the Court has said that a "relationship among the defendant, the forum, and the litigation" is the essential foundation of in personam jurisdiction.", Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, at 414 (1984).

106 „[...]the continuous corporate operations within a state were thought so substantial and of such a nature as to justify suit against it on causes of action arising from dealings entirely distinct from those activities." Int'l Shoe Co. v. State of Wash., Off. of Unemployment Comp. & Placement, 326 U.S. 310, at 318 (1945).

107 Goodyear Dunlop Tires Operations, S.A. v. Brown, 564 U.S. 915, at 919, (2011).

108 International Shoe Co., 326 U.S. 310, at 320 (1945).

109 Ford Motor Company, 141 S.Ct. 1017, at 1024.

1. Ergibt sich der Anspruch direkt aus konkreten Aktivitäten des Unternehmens in den USA oder bezieht er sich darauf?
2. Macht sich das Unternehmen durch seine Aktivitäten bewusst die Vorzüge des US-amerikanischen Marktes derart zu eigen, dass es damit rechnen muss, der dortigen Gerichtsbarkeit zu unterliegen?
3. Ist die Ausübung der Gerichtsbarkeit angemessen?

So lehnte der U.S. Supreme Court etwa *specific personal jurisdiction* in folgenden Fällen ab: (1) Ein Autohersteller, dessen einziger Kontakt mit dem *forum state* der Umstand war, dass ein Kunde mit seinem Auto in den Bundesstaat gefahren war,[110] (2) ein geschiedener Ehemann, der wegen Kindesunterhaltes verklagt wurde und dessen Verbindung zum *forum state* allein darin bestand, dass die gemeinsame Tochter dort lebte,[111] (3) ein Nachlassverwalter, dessen einzige Verbindung zum *forum state* darin bestand, dass die Erblasserin dort verstarb.[112]

Andererseits bejahte der U.S. Supreme Court in *Plixer Int'l, Inc. v. Scrutinizer GmbH* die Ausübung von *specific personal jurisdiction* über ein deutsches IT-Unternehmen, welches seine Website international auf Englisch zur Verfügung stellte und dadurch auch Kunden aus den USA anwarb.[113] Scrutinizer unterhielt kein Büro oder Subunternehmen in den USA, betrieb dort kein Vertriebsnetzwerk und sendete seine Mitarbeiter nicht dorthin. Seine Zahlungen wickelte das Unternehmen in Euro ab. Jedoch akquirierte es über seine Website im Zeitraum zwischen 2014-2017 insgesamt 156 Kunden aus den USA. Der US-Umsatz belief sich im Geschäftsjahr 2017 auf knapp 200.000 USD.

Der U.S. Supreme Court erachtete es nicht für notwendig, dass die Website sich spezifisch an US-Kunde richtete; es reiche aus, dass Scrutinizer sie dort verfügbar machte und keine Maßnahmen unternahm, um den Zugriff auf die Website aus den USA zu unterbinden.[114] Zusammen mit der Tatsache, dass Scrutinizer bereitwillig Kunden aus den USA bediente, nahm das Gericht an, dass „die gezielten US-

110 World-Wide Volkswagen Corp., 444 U.S. 286 (1980).
111 Kulko v. Cal. Super. Ct., 436 U.S. 84 (1978).
112 Hanson v. Denckla, 357 U.S. 235, at 253 (1958).
113 Plixer Int'l, Inc. v. Scrutinizer GmbH, 905 F.3d 1, at 8 (1st Cir. 2018).
114 Plixer Int'l, Inc. v. Scrutinizer GmbH, 905 F.3d 1, at 9 (1st Cir. 2018).

Kontakte von Scrutinizer ausreichten, um Scrutinizer darauf aufmerksam zu machen, dass es mit einer Klage vor einem US-Gericht zu rechnen hatte."[115]

Zu der Frage, ob *general personal jurisdiction* über ein ausländisches Unternehmen besteht, gibt es insgesamt weniger Rechtsprechung. In *Daimler AG v. Bauman*[116] verklagte eine argentinische Staatsbürgerin die deutsche Daimler AG vor einem kalifornischen Gericht wegen Menschenrechtsverletzungen zur Zeit der Militärjunta in Argentinien, mit welcher die Daimler AG durch ihre argentinische Tochtergesellschaft mitgewirkt haben soll. Daimlers Verbindung zum Bundesstaat Kalifornien bestand darin, dass Daimlers Tochterunternehmen Mercedes-Benz USA, LLC (MBUSA), welches in Delaware ansässig war, dort Daimlers Autos durch ein Netzwerk unabhängiger Autohäuser vertrieb. Das Berufungsgericht hatte das Vorliegen von *general personal jurisdiction* aufgrund der Tatsache angenommen, dass MBUSA für Daimler Aufgaben derart übernähme, dass diese, wenn es MBUSA nicht gäbe, von Daimler selbst hätten durchgeführt werden müssen.[117] Mithin müsse sich die Daimler AG die Kontakte von MBUSA mit dem *forum* Kalifornien zurechnen lassen. Der U.S. Supreme Court lehnte diese Theorie jedoch ab und hielt fest, dass selbst wenn sich die Daimler AG MBUSA's Kontakte mit dem Bundesstaat Kalifornien zurechnen lassen müsste, diese nicht weitreichend genug seien, um die Annahme von *general personal jurisdiction* zu rechtfertigen.[118]

Andererseits bestätigte der U.S. Supreme Court das Vorliegen von *general personal jurisdiction* in Fällen, in denen ein ausländisches Unternehmen eine Niederlassung in den USA unterhielt, aus welcher es Geschäfte in den USA abwickelte.[119]

Zusammenfassend ist festzuhalten, dass die Zuständigkeit von US-Gerichten über ausländische Entitäten stets von den Umständen des Einzellfalls bestimmt wird. Generell betrachten die Gerichte dabei den

---

115 Plixer Int'l, Inc. v. Scrutinizer GmbH, 905 F.3d 1, at 9 (1st Cir. 2018).

116 Daimler AG v. Bauman, 571 U.S. 117 (2014).

117 „performs services that are sufficiently important to the foreign corporation that if it did not have a representative to perform them, the corporation's own officials would undertake to perform substantially similar services". See, Daimler AG v. Bauman, 571 U.S. 117, at 134. (2014).

118 Daimler AG v. Bauman, 571 U.S. 117, at 138 (2014).

119 Perkins v. Benguet Consol. Min. Co., 342 U.S. 437 (1952).

Umfang und die Intensität der Kontakte, die ein bestimmtes Unternehmen mit den USA hat. Dabei wird zwischen *general* und *specific personal jurisdiction* unterschieden, wobei die Annahme von *general personal jurisdiction* intensivere Kontakte mit den USA voraussetzt als *specific personal jurisdiction*, jedoch dann die Gerichte dazu ermächtigt, Klagen aller Art gegen ein Unternehmen zuzulassen.

Ob EU-Unternehmen, die ihre Serverdaten in der EU speichern, der Jurisdiktion US-amerikanischer Gerichte unterliegen, ist danach zu bestimmen, welche Geschäftsbeziehungen sie in die USA haben. So genügt es nach der Rechtsprechung der US-Gerichte noch nicht für die Annahme von *general personal jurisdiction*, dass ein EU-Unternehmen eine Tochtergesellschaft in den USA betreibt; eine Niederlassung des Mutterkonzerns hingegen könnte jedoch ausreichend sein. Für die Annahme von *specific personal jurisdiction* könnte bereits das Betreiben einer Website, welche sich zumindest auch an US-Kunden richtet, ausreichen.

IV. Vermeidung der Herausgabeverpflichtung durch technischen Ausschluss aus der Cloud (Zusatzfrage)

Es ist rechtlich zunächst denkbar, dass sich ein US-Cloud-Betreiber seinen Verpflichtungen zur Speicherung und Herausgabe von Daten und Informationen aus der Cloud dadurch entzieht, dass er sich selbst technisch aus der Cloud ausschließt, sodass ihm kein eigener Zugriff auf die darin enthaltenen Daten verbleibt. Wenn der Cloud-Betreiber in den USA sich selbst technisch dauerhaft vom Zugriff auf die Cloud-Inhalte ausschließt, ist die Herausgabe von Daten durch ihn nicht möglich. Dies kann der Cloud-Betreiber z. B. dadurch erreichen, dass er die Daten verschlüsselt speichert und selbst keine eigene Entschlüsselungstechnologie vorhält. Dann wäre die Entschlüsselung nur durch Dritte möglich. Dies ist durch den SCA, der keine Form der Speicherung oder Verschlüsselung vorschreibt oder ausschließt, nicht verboten. Rechtlich betrachtet dürfte es dann schon an der Tatbestandsvoraussetzung (etwa der Section 2709(a) oder Section 2713 SCA) fehlen, dass der Cloud-Betreiber die Kontrolle über die Daten ausübt bzw. sie in seinem Besitz hat (*possession, custody, or control*). Darüber hinaus wäre der Cloud-Betreiber im Falle einer Herausgabeanordnung außerstande, zu prüfen, ob in seiner Cloud überhaupt Daten vorliegen, die von der Herausgabeanordnung umfasst sind. Indes besteht weiterhin die (theoretische) Möglichkeit, dass die Regierung die physischen Server des Rechenzentrums beschlagnahmt und nach Entschlüsselung der

Daten selbst auswertet. Dafür wären Voraussetzungen erforderlich, die zum Erlass eines Durchsuchungs- und Beschlagnahmebeschlusses führen. Ein solcher (*warrant*, *subpoena*, o.ä.) wäre in ähnlicher Form bereits für die Herausgabeanordnung erforderlich gewesen. Wie realistisch dieses Szenario ist, kann nicht abschließend beurteilt werden.

Gleichzeitig ließe sich dem Wortlaut aus dem Wortlaut von Section 2713 SCA jedoch auch eine Speicherpflicht ableiten (*preserve, backup, or disclose the contents of a wire or electronic communication*). Ob eine solche generelle Speicherpflicht besteht, lässt sich nicht abschließend beurteilen. Jedoch haben US-Gerichte in der Vergangenheit eine Speicherpflicht für Daten dann anerkannt, wenn das Unternehmen Informationen besaß, wonach die Daten für ein späteres Gerichtsverfahren relevant sein könnten.[120] Zudem besteht nach Section 2703(f) SCA die Möglichkeit, dass eine Speicherung durch Strafverfolgungsbehörden gesondert angeordnet wird. Schließt sich ein Cloud-Anbieter durch technische Maßnahmen von seinem Zugang zum Cloud-Server aus, kann er diesen Verpflichtungen nicht mehr nachkommen.

Deshalb erscheint es zweifelhaft, ob eine Herausgabepflicht dadurch vermieden werden kann, dass sich Cloud-Anbieter technisch aus der Cloud ausschließen. Im US-amerikanischem Prozessrecht sind Parteien dazu verpflichtet, im Rahmen der Beweisaufnahme verfahrensrelevante Informationen offenzulegen und der anderen Partei zur Verfügung zu stellen. Bei Nichtbefolgung drohen Sanktionen in Form von teils erheblichen Bußgeldern durch die Gerichte. Dies gilt unter Umständen auch, wenn verfahrensrelevante Informationen aus Versehen oder absichtlich vernichtet werden (sog. Spoliation). US-Gerichte haben in der Vergangenheit eine Speicherpflicht für Daten dann anerkannt, wenn das Unternehmen wusste oder wissen konnte, dass die Daten für ein späteres Gerichtsverfahren relevant sein könnten. Ein Cloud-Anbieter, der regelmäßig Herausgabeverlangen von US-Strafverfolgungsbehörden nachzukommen hat, könnte mithin verpflichtet sein, Informationen für diese aufzubewahren. Anderenfalls würde er sich der Gefahr teils erheblicher Sanktionen, u.a. Bußgeldern, aussetzen.

---

120 "This obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation", In re NTL, Inc. Sec. Litig., 244 F.R.D. 179, at 193 (S.D.N.Y. 2007), aff'd sub nom. Gordon Partners v. Blumenthal, No. 02 CIV 7377 LAK, 2007 WL 1518632 (S.D.N.Y. May 17, 2007).

UNIVERSITÄT
ZU KÖLN

Haftungsausschluss

Dieses Gutachten wurde nach bestem Wissen und Gewissen erstellt. Es bezieht sich ausdrücklich nur auf die aufgeworfenen Fragen. Der Sachverständige haftet für Schäden, die auf einem mangelhaften Gutachten beruhen – gleich aus welchem Rechtsgrund – nur dann, wenn er oder seine Erfüllungsgehilfen die Schäden durch eine vorsätzliche oder grob fahrlässige Pflichtverletzung verursacht haben. Dies gilt auch für Schäden, die der Sachverständige bei der Vorbereitung seines Gutachtens verursacht hat sowie für Schäden, die nach erfolgter Nacherfüllung entstanden sind. § 639 BGB bleibt unberührt. Alle darüberhinausgehenden Schadensersatzansprüche werden ausgeschlossen.

Ferner ist anzumerken, dass der Verfasser ausschließlich Kenntnisse des Rechts des US-Bundesstaates New York sowie des Bundesrechts (*Federal Law*) hat, jedoch über keinerlei Kenntnisse des deutschen Rechts verfügt. Aus diesem Grunde wurde der Verfasser bei der Erfassung von deutschen Rechtsbegriffen in der Fragestellung durch die wissenschaftlichen Mitarbeiter [redacted] welche mit dem deutschen Recht vertraut sind, unterstützt. Nichtsdestotrotz kann das umfassende Verständnis des Gutachters im Hinblick auf diese deutschen Rechtsbegriffe nicht garantiert werden.

Die vorliegende Fragestellung des Gerichts betrifft das materielle Bundesrecht. Demzufolge wurde vom Gutachter vor allem auf die englischsprachigen Originalquellen des US-amerikanischen Rechts zurückgegriffen. Das zunächst in englischer Sprache verfasste Gutachten wurde sodann von einem wissenschaftlichen Mitarbeiter [redacted] ins Deutsche übersetzt. Es ist darauf hinzuweisen, dass die Übersetzung von Rechtsbegriffen regelmäßig Ungenauigkeiten mit sich bringt, weil sie Rechtskonzepte erfassen, die nur schwer auf ein anderes Rechtssystem übertragbar sind.

Köln, 21. März 2025

[redacted]

[redacted]