# Gutachten
# zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse
# von

**Prof. Stephen I. Vladeck,**
**University of Texas School of Law**

**vom**

**15. November 2021**

Dieses Gutachten wurde unter Federführung der Berliner Beauftragten für Datenschutz und die Informationsfreiheit im Auftrag der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) erstellt.

Die in diesem Gutachten dargelegten Informationen und Ansichten sind die des Verfassers. Die Datenschutzkonferenz übernimmt keine Gewähr für die Richtigkeit der in diesem Gutachten enthaltenen Daten. Das Gutachten bindet weder die Datenschutzkonferenz noch die Datenschutzaufsichtsbehörden des Bundes und der Länder in ihrer Beurteilung von Grundsatzfragen oder Einzelfällen.

Es handelt sich bei diesem Dokument um eine deutsche Übersetzung des Gutachtens als unverbindliche Arbeitshilfe. Maßgeblich ist ausschließlich das englischsprachige Original.

Weitere Informationen zur Datenschutzkonferenz:

www.datenschutzkonferenz-online.de

**Kontakt**:

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Graurheindorfer Straße 153
53117 Bonn
E-Mail: pressestelle@bfdi.bund.de

SCHOOL OF LAW
THE UNIVERSITY OF TEXAS AT AUSTIN

727 East Dean Keeton Street | Austin, Texas 78705-3299 | (512) 475-9198 | svladeck@law.utexas.edu

STEPHEN I. VLADECK
STEPHEN I. VLADECK
Charles Alan Wright-Lehrstuhl für Bundesgerichte

15. November 2021

Matthias Bergt
Leiter Referat I B (Recht)
Berliner Beauftragte für Datenschutz und Informationsfreiheit
Friedrichstraße 219
10969 Berlin, Deutschland

**Re: Memo zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbehörden**

Sehr geehrter Herr Bergt,

Sie haben mich gebeten, eine Reihe von Fragen zum aktuellen Stand des US-Überwachungsrechts und der US-Behörden mit einem Gutachten zu beantworten. Wie Sie wissen, war ich einer der Sachverständigen für Facebook im Schrems-Verfahren vor den irischen Gerichten. [1] Als Referenz füge ich diesem Memorandum eine Kopie meines Expertenberichts in diesem Fall bei (und werde ihn hier als "Vladeck Schrems Report" bezeichnen). [2] Dieser Bericht gibt unter anderem auch einen detaillierteren Überblick über meine Qualifikationen und Fachkenntnisse, siehe Vladeck Schrems Report.

FRAGEN:

I. ZUSÄTZLICHE FRAGEN ZU ABSCHNITT 702 FISA

1. Enthält FISA 702 nur die Erlaubnis für US-Geheimdienste, Daten von Anbietern elektronischer Kommunikationsdienste zu erhalten, oder verpflichtet er auch Anbieter elektronischer Kommunikationsdienste, Daten an US-Geheimdienste, die solche Daten anfordern, weiterzugeben oder ihnen Zugang zu den Daten zu gewähren?

Auf den Anwendungsbereich von Abschnitt 702 des FISA (das Kernstück des FISA Amendments Act von 2008) gehe ich in den Ziffern 39-43 des Vladeck Schrems Report ein. Um es kurz zu machen: Abschnitt 702 ist in dem Sinne verbindlich, dass, wenn die Vereinigten Staaten einem Anbieter von elektronischen Kommunikationsdiensten eine Anweisung erteilt haben, die durch ihre jährliche Zertifizierung vor dem FISA-Gericht gemäß Abschnitt 702 genehmigt wurde, der Anbieter entweder (1) die Anweisung befolgen oder (2) die Anweisung vor dem FISA-Gericht anfechten muss.

1. Die Analyse in diesem Memorandum gibt meine beste Expertenmeinung zu den objektiven Antworten auf die von Ihnen gestellten Fragen wieder - und zwar völlig unabhängig von den Interessen einer bestimmten Person, Organisation oder Gruppe.
2. Eine elektronische Kopie des Berichts ist auch verfügbar unter https://iapp.org/media/pdf/_resource center/Schrems-testimony-Vladeck.pdf.

Anders ausgedrückt: Eine gemäß Abschnitt 702 erlassene Anweisung kann den Anbieter elektronischer Kommunikationsdienste, der sie erhält, dazu verpflichten, Daten an einen US-Geheimdienst weiterzugeben oder ihm Zugang zu den Daten zu gewähren. Aber es ist die Anweisung, die die Offenlegung erzwingt. Abschnitt 702 an sich verpflichtet die Anbieter elektronischer Kommunikationsdienste nicht zur proaktiven Offenlegung von Daten oder zur Gewährung eines allgemeinen Zugangs zu Daten für US-Geheimdienste.

2. Falls die Antwort auf Frage 1 lautet, dass die Anbieter elektronischer Kommunikationsdienste verpflichtet sind, Daten offenzulegen oder Zugang zu ihnen zu gewähren: Verfügen die US-Behörden über Mittel zur Durchsetzung dieser Verpflichtung? Wenn ja, beschreiben Sie bitte diese Mittel.

Abschnitt 702 geht speziell auf diese Frage ein. Wenn der Anbieter die Anweisung vor Gericht anfechtet und verliert, kann die Nichtbefolgung der daraufhin ergangenen gerichtlichen Anordnung ausdrücklich mit Missachtung geahndet werden, was erhebliche (ansteigende) Geldstrafen nach sich ziehen kann, siehe 50 U.S.C. § 1881a(i)(4)(G). Wenn der Anbieter die Anweisung nicht vor Gericht anfechtet, sondern sich ebenfalls weigert, sie zu befolgen, kann der Attorney General vor dem FISA-Gericht ein kontradiktorisches Gerichtsverfahren zur Durchsetzung der Anweisung anstrengen, siehe id. § 1881a(i)(5). Auch hier gilt: Wenn der Attorney General eine Anordnung erwirkt, die die Einhaltung der Richtlinie erzwingt, wird die Nichteinhaltung als Missachtung geahndet, siehe id. § 1881a(i)(5)(D). Unabhängig davon, ob der Anbieter die Anweisung (erfolglos) anfechtet oder sich einfach weigert, sie zu befolgen, droht ihm also in jedem Fall ein Verfahren wegen Missachtung (das darauf abzielt, seine Befolgung durch steigende Geldstrafen und andere Maßnahmen zu erzwingen).

3. Welche Arten von Daten kann die Regierung von Anbietern elektronischer Kommunikationsdienste gemäß FISA 702 anfordern? Erlaubt das Gesetz der US-Regierung, die Metadaten und den Inhalt der Kommunikation zu erfassen? Erlaubt das Gesetz der US-Regierung, andere Arten oder Formen von Daten zu erfassen?

Der Wortlaut des Gesetzes sagt nichts über die spezifischen Arten von Daten aus, die gemäß Abschnitt 702 erfasst werden können. Wir wissen jedoch, dass das FISA-Gericht die Erfassung von Metadaten und Kommunikationsinhalten gemäß Abschnitt 702 zumindest unter bestimmten Umständen genehmigt hat - was bedeutet, dass es die Auslegung des Gesetzes durch die US-Regierung, die eine solche Erfassung zulässt, formell bestätigt hat. Nach den Bestimmungen des Gesetzes ist die US-Regierung nicht befugt, andere Arten oder Formen von Daten zu erheben - was aber nicht unbedingt bedeutet, dass die Regierung nicht befugt ist, solche Daten zu erheben. Wie bei den Inhalten und Metadaten ist dies in erster Instanz eine Frage der Gesetzesauslegung durch das FISA-Gericht. Das Gesetz bezieht sich nur auf den "Inhalt" von Kommunikationen, 50 U.S.C. § 1881a(f)(3)(A), und "Inhalt", wie in 18 U.S.C. § 2510(8) definiert, "wenn er in Bezug auf eine drahtgebundene, mündliche oder elektronische Kommunikation verwendet wird, schließt alle Informationen über den Inhalt, den Sinn oder die Bedeutung dieser Kommunikation ein". (Hervorhebung hinzugefügt).

4. Gilt FISA 702 für Daten im Übermittlungsstadium und/oder für Daten im Ruhezustand? Umfassen diese beiden Begriffe zusammen alle Daten, die verarbeitet werden können?

Abschnitt 702 wurde sowohl auf Daten im Übermittlungsstadium als auch auf Daten im Ruhezustand angewandt. Die Erhebung im Übermittlungsstadium wird als "vorgelagerte" Erhebung bezeichnet, die Erhebung im Ruhezustand wird oft als "nachgelagerte" Erhebung beschrieben. (Das PRISM-Programm ist ein Beispiel für Letzteres.) Soweit öffentlich bekannt ist, decken diese beiden Begriffe alle Daten ab, die gemäß Abschnitt 702 erfasst werden können, obwohl es innerhalb dieser beiden Begriffe mehrere Erfassungsprogramme geben kann.

5. Welche Personen oder Einrichtungen fallen unter den Begriff "Anbieter elektronischer Kommunikationsdienste" in 50 U.S.C. § 1881(b)(4)?

Die Definitionen in § 1881(b)(4) sind erschöpfend, aber auch recht umfangreich, einschließlich:

(A) ein Telekommunikationsunternehmen, wie dieser Begriff in Abschnitt 153 von Titel 47 definiert ist; [3]

(B) ein Anbieter von elektronischen Kommunikationsdiensten, wie dieser Begriff in Abschnitt 2510 von Titel 18 definiert ist; [4]

(C) ein Anbieter eines Ferncomputerdienstes, wie dieser Begriff in Abschnitt 2711 von Titel 18 definiert ist; [5]

---

3. Gemäß 47 U.S.C. § 153(51) "bedeutet der Begriff 'Telekommunikationsanbieter' jeden Anbieter von Telekommunikationsdiensten, mit der Ausnahme, dass dieser Begriff keine Aggregatoren von Telekommunikationsdiensten (wie in Abschnitt 226 dieses Titels definiert) umfasst". Und "Telekommunikationsdienste" "bedeutet das Anbieten von Telekommunikationsdiensten gegen eine Gebühr direkt an die Öffentlichkeit oder an solche Gruppen von Nutzern, die unabhängig von den verwendeten Einrichtungen tatsächlich direkt für die Öffentlichkeit verfügbar sind." Id. § 153(53).

4. Gemäß 18 U.S.C. § 2510(15) ist ein "elektronischer Kommunikationsdienst" jeder Dienst, der seinen Nutzern die Möglichkeit bietet, drahtgebundene oder elektronische Nachrichten zu senden oder zu empfangen. Und "elektronische Kommunikation" sind:

   jede Übertragung von Zeichen, Signalen, Schrift, Bildern, Tönen, Daten oder Informationen jeglicher Art, die ganz oder teilweise über ein Draht-, Funk-, elektromagnetisches, fotoelektronisches oder fotooptisches System übertragen werden und den zwischenstaatlichen oder ausländischen Handel beeinträchtigen, jedoch nicht-

   a. jede drahtgebundene oder mündliche Kommunikation;

   b. jede Kommunikation, die über ein reines Tonrufgerät erfolgt;

   c. jegliche Kommunikation von einem Ortungsgerät (wie in Abschnitt 3117 dieses Titels definiert); oder

   d. Informationen über elektronische Geldtransfers, die von einem Finanzinstitut in einem Kommunikationssystem gespeichert werden, das für die elektronische Speicherung und den elektronischen Transfer von Geldern verwendet wird.

   Id. § 2510(12).

5. Gemäß 18 U.S.C. § 2711(2) "bedeutet der Begriff 'Ferncomputerdienst' die Bereitstellung von Computerspeicher- oder -verarbeitungsdiensten für die Öffentlichkeit mittels eines elektronischen Kommunikationssystems".

(D) jeder andere Anbieter von Kommunikationsdiensten, der Zugang zu drahtgebundener oder elektronischer Kommunikation hat, entweder während der Übertragung oder während der Speicherung solcher Kommunikationen; oder

(E) ein leitender Angestellter, ein Angestellter oder ein Beauftragter einer unter Buchstabe A, B, C oder D beschriebenen Einrichtung.

Es ist schwierig, den Inhalt dieser Definitionen erschöpfend oder umfassend zu beschreiben, da sie sich auf andere Gesetze mit eigenen Definitionen beziehen und viele der in diesen Definitionen verwendeten Begriffe zumindest bis zu einem gewissen Grad mehrdeutig sind. In dieser Hinsicht funktioniert das US-Rechtssystem eher wie ein Common-Law-System als ein Civil-Law-System, in dem gesetzliche Definitionen oft zu Unstimmigkeiten und konkurrierenden (wenn nicht gar widersprüchlichen) gerichtlichen Auslegungen führen. Es gibt einige allgemeine Grundsätze, die sich aus diesen Definitionen ableiten lassen (und die ich im Folgenden zu extrahieren versuche), aber der wichtigere Punkt ist, dass viele Anwendungsfragen zumindest einige Unsicherheiten hinsichtlich des wahrscheinlichen Ergebnisses mit sich bringen, einschließlich (1) der Frage, ob die US-Regierung jemals eine solche Auslegung annehmen würde; und (2) wenn ja, ob ein überprüfendes Gericht sie billigen würde.

a. Im Besonderen: Umfasst der Begriff Unternehmen wie Banken, Fluggesellschaften, Hotels, Schifffahrtsgesellschaften und dergleichen?

Wie die obigen Definitionen nahelegen, gibt es zumindest einige Kontexte, in denen Banken, Fluggesellschaften, Hotels und Schifffahrtsunternehmen zumindest einige der Definitionen in § 1881(b)(4) erfüllen können. Die wichtigsten Möglichkeiten sind die als Anbieter von elektronischen Kommunikationsdiensten (ECS) oder Fernkommunikationsdiensten (RCS). Ob ein Unternehmen als ECS oder RCS agiert, ist völlig kontextabhängig; die Entscheidung, ob die ECS- oder die RCS-Regelung Anwendung findet, wird auf der Grundlage des jeweiligen Dienstes oder des jeweiligen Teils einer elektronischen Kommunikation zu einem bestimmten Zeitpunkt und in einem bestimmten Kontext getroffen, siehe z.B. in der Sache United States, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009). Um festzustellen, ob ein Unternehmen als Anbieter von elektronischen Kommunikationsdiensten einzustufen ist, würde die Analyse daher jede der verschiedenen Tätigkeiten des Unternehmens gemäß den oben genannten rechtlichen Definitionen gesondert bewerten. In der Praxis werden für die von Ihnen genannten Unternehmen wahrscheinlich nur ECS und RCS relevant sein. Diese beiden Definitionen dürften in der Praxis nur wenige Probleme aufwerfen - zum einen, weil ihre Begriffe relativ klar sind, und zum anderen, weil es eine umfangreiche Rechtsprechung gibt, die einige der Unklarheiten beseitigt.

Der wichtigste Punkt, der bei der Durchführung einer solchen Analyse zu berücksichtigen ist, ist, dass ein Unternehmen in Bezug auf einige Kommunikationen als ECS, in Bezug auf andere Kommunikationen als RCS und in Bezug auf wieder andere Kommunikationen weder als ECS noch als RCS auftreten kann, siehe 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, 1215-16 & n.48 (2004). In Anbetracht

dessen, ja, es wird Umstände geben, unter denen Banken, Fluggesellschaften, Hotels und Schifffahrtsunternehmen alle unter § 1881(b)(4) fallen könnten - je nachdem, welche Dienstleistungen sie anbieten und für wen. Dies gilt umso mehr, als das Justizministerium diese Begriffe recht großzügig ausgelegt hat, siehe z. B. Justizministerium, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 117-19 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanua12009.pdf.

b. Wenn ein Unternehmen ein "Anbieter von elektronischen Kommunikationsdiensten" gemäß der Definition in 50 U.S.C. § 1881(b)(4) ist, gibt es dann ein Gesetz, das bestimmte Informationen, über die das Unternehmen verfügt, von der Erhebung gemäß FISA 702 ausschließt? Gibt es beispielsweise ein Gesetz, das ausdrücklich festlegt, dass der Status als "Anbieter elektronischer Kommunikationsdienste" nur für eine bestimmte Funktion gilt, die ein Unternehmen ausübt? Wenn beispielsweise eine bestimmte Bank ein "Anbieter von elektronischen Kommunikationsdiensten" gemäß 50 U.S.C. § 1881(b)(4) ist, würde FISA 702 der US-Regierung dann erlauben, jegliche Kommunikation oder Daten von dieser Bank zu erfassen, die mit dem Konto der "Zielperson" der US-Regierung verbunden sind?

Sobald ein Unternehmen die Definition eines "Anbieters elektronischer Kommunikationsdienste" gemäß § 1881(b)(4) erfüllt, gibt es kein mir bekanntes Gesetz, das Informationen, über die das Unternehmen verfügt, kategorisch von der Erfassung gemäß Abschnitt 702 ausschließt. Stattdessen würde sich die Frage darauf beschränken, ob die gesuchten Mitteilungen oder Daten (1) in den Anwendungsbereich der genehmigten Richtlinie fallen und (2) nicht den einschlägigen Minimierungsanforderungen unterliegen, die der Bescheinigung der Regierung beigefügt sind. Auch wenn ein Unternehmen aufgrund einer sehr geringen Anzahl von Aktivitäten (und in der Tat Aktivitäten, die nichts mit seiner Hauptfunktion zu tun haben) als "Anbieter elektronischer Kommunikationsdienste" eingestuft werden kann, spielt diese Unterscheidung nach dem Wortlaut von Abschnitt 702 letztlich keine Rolle.

c. 18 U.S.C. § 2711(2) schreibt ausdrücklich vor, dass die dort genannten Dienste der Öffentlichkeit zur Verfügung gestellt werden müssen. Gilt diese Anforderung auch für andere Arten von Anbietern elektronischer Kommunikationsdienste gemäß 50 U.S.C. § 1881(b)(4)?

Die kurze Antwort lautet "Nein". Jede der Definitionen in § 1881(b)(4) ist unabhängig - was bedeutet, dass ein "Anbieter elektronischer Kommunikationsdienste" ein Unternehmen ist, das eine der Definitionen erfüllt. Gemäß meiner obigen Antwort erfordert die RCS-Definition (§ 2711(2)) eindeutig die Bereitstellung von Diensten für die Öffentlichkeit. Dies gilt auch für die Definition von "Telekommunikationsdiensten" in 47 U.S.C. § 153(53), siehe vor 3 Nr. 3.

Die ECS-Definition in 18 U.S.C. § 2510(15) ist jedoch anders. In dieser Bestimmung wird "elektronischer Kommunikationsdienst" definiert als "jeder Dienst, der seinen Nutzern die Möglichkeit bietet, drahtgebundene oder elektronische

Nachrichten zu senden oder zu empfangen", und es wird nicht verlangt, dass der Dienst der Öffentlichkeit oder anderen Dritten zur Verfügung gestellt wird. So haben US-Gerichte beispielsweise entschieden, dass ein Unternehmen die ECS-Definition erfüllt, wenn es seinen Mitarbeitern einen E-Mail-Dienst zur Verfügung stellt. siehe z.B. Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114-15 (3. Cir. 2003); siehe auch Shefts v. Petrakis, No. 100-1104, 2011 WL 5930469, bei *6 (C.D. 111. Nov. 29, 2011) ("Die Genehmigung für den Zugang zu einer 'Einrichtung' kann von der Einrichtung erteilt werden, die den elektronischen Kommunikationsdienst bereitstellt, wozu auch ein privater Arbeitgeber gehört, der seinen Mitarbeitern einen E-Mail-Dienst zur Verfügung stellt"). Ebenso wurde ein Reisebüro, das seinen Mitarbeitern Computerterminals zur Verfügung stellt, auf denen ein elektronisches Reservierungssystem läuft, als ECS eingestuft, siehe United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993). Es ist also möglich, dass ein Unternehmen die Definition des "Anbieters von elektronischen Kommunikationsdiensten" in 50 U.S.C. § 1881(b)(4) erfüllt, ohne irgendwelche Dienste für die Öffentlichkeit anzubieten.

d. Wenn man prüft, ob ein Unternehmen als "Remote Computing Service" gemäß 50 U.S.C. § 1881(b)(4)(C) in Frage kommt: Wann werden Dienstleistungen für die Öffentlichkeit im Sinne von 18 U.S.C. § 2711(2) erbracht? Z.B. wenn (1) ein Unternehmen seinen Angestellten oder Vertragsarbeitern Zugang zu E-Mail-Diensten gewährt, (i) ausschließlich für die Durchführung der Geschäfte des Unternehmens und/oder (ii) für den privaten Gebrauch des Angestellten oder Vertragsarbeiters und/oder (iii) wenn der private Gebrauch nicht erlaubt ist, aber nicht strafrechtlich verfolgt wird, oder (2) ein Unternehmen ein Messaging-System für die Kommunikation mit seinen Kunden bereitstellt,
z. B. im Rahmen des Online-Banking-Systems einer Bank, stellt dies eine Dienstleistung für die Öffentlichkeit dar? Wenn ein Mitglied einer Unternehmensgruppe Dienstleistungen, die unter 50 U.S.C. § 1881(b)(4) fallen würden, für andere Mitglieder seiner Unternehmensgruppe, aber nicht für Dritte erbringt, werden diese Dienstleistungen dann als für die Öffentlichkeit erbracht angesehen?

Die kurze Antwort lautet, dass keines dieser Beispiele die Definition eines "Remote-Computing-Dienstes" gemäß § 1881(b)(4)(C) erfüllen dürfte. Für eine gute Diskussion des Zwecks der Definition siehe In JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 310 (E.D.N.Y. 2005) (mit der Feststellung, dass eine Fluggesellschaft, die eine Website und Server betreibt, um die Kommunikation mit ihren Kunden zu erleichtern, kein "Remote Computing Service" gemäß § 2711(2) ist), siehe allgemein Kerr, supra, S. 1229-30
(erörtert die RCS-Definition). Ein aufschlussreicher Fall ist Andersen Consulting, LLP v. UOP, 991 F. Supp. 1041, 1042-43 (N.D. Ill. 1998), in dem festgestellt wird, dass ein Unternehmen nicht allein deshalb ein RCS ist, weil es Auftragnehmern, die für das Unternehmen arbeiten, Zugang zu seinem internen E-Mail-System gewährt.

Allgemeiner ausgedrückt, der Senatsbericht zum Gesetz über die gespeicherte Kommunikation macht deutlich, dass das Gesetz nicht nur auf die Erbringung von Dienstleistungen für "die Öffentlichkeit" abzielt, sondern auf "Lagerungs- oder Verarbeitungsdienstleistungen". 18 U.S.C. § 2711(2), siehe allgemein S. Rep. No. 99-

541, at 8, 10-11 (1986). Wie der oben zitierte Fall JetBlue deutlich macht, reicht es also nicht aus, dass ein Unternehmen öffentlich zugängliche Messaging-Plattformen anbietet, selbst wenn diese sicher sind. Entscheidend ist, ob das Unternehmen der Öffentlichkeit die Möglichkeit bietet, Daten zu speichern oder zu verarbeiten. Ein Unternehmen, das Dienste für ein verbundenes Unternehmen erbringt, ohne diese Dienste auf dem freien Markt zur Verfügung zu stellen, würde also den öffentlichen Teil der Definition nicht erfüllen; und ein Unternehmen, das seinen Kunden lediglich einen Mechanismus zum Austausch von Nachrichten mit dem Unternehmen zur Verfügung stellt, bietet keine "Speicher- oder Verarbeitungsdienste" an.

Wenn die Begrenztheit dieser Antwort mit dem Umfang der Antwort auf Frage 5.c unvereinbar zu sein scheint, so liegt das ausschließlich an den sehr unterschiedlichen Definitionen von ECS und RCS. RCS ist im Allgemeinen eine viel engere Kategorie von Dienstleistungen als ECS. Das mag für Unternehmen, die beides anbieten, keine große Rolle spielen, hat aber in einer Reihe von Fällen, in denen es nur um RCS ging, einen Unterschied gemacht, wie sowohl der oben zitierte Fall von JetBlue als auch die darin zitierten Fälle deutlich machen.

e. Alles in allem: Gibt es praktische Beispiele für Unternehmen oder Branchen, die nicht in den Anwendungsbereich von 50 U.S.C. § 1881 fallen? Welche?

Wie die obigen Antworten deutlich machen, glaube ich, dass die Antwort "ja" lautet, aber vielleicht für weit weniger Unternehmen und Branchen, als wir denken. Was bei der abstrakten Lektüre von Abschnitt 702 vielleicht nicht offensichtlich ist, ist die Tatsache, dass zumindest hier bewährte (und wiederholt interpretierte) Definitionen aus dem Stored Communications Act von 1986 übernommen wurden. Der Kongress hat in diesem Gesetz nicht heimlich versucht alle Unternehmen als angreifbare Anbieter zu behandeln; im Gegenteil, er hat versucht, zwischen den Unternehmen zu unterscheiden, und zwar auf der Grundlage eines (längst überholten) Verständnisses der verschiedenen Arten, wie Unternehmen Kommunikationsdienste nutzen und/oder anbieten. Das Problem ist, dass diese Definitionen selbst heute weit mehr Unternehmen abdecken, als dies bei ihrer Verabschiedung der Fall war (und als sie wohl auch gedacht warenhaben). Abschnitt 702 macht sich diese Entwicklungen zunutze.

f. Wenn eine Einrichtung selbst nicht dem FISA 702 unterliegt, aber einen Anbieter von elektronischen Kommunikationsdiensten zur Verarbeitung bestimmter Daten einsetzt, ist es dann möglich, dass die US-Geheimdienste gemäß FISA 702 Zugang zu diesen Daten erhalten?

Ja. Sofern sich die Daten im Besitz des Anbieters elektronischer Kommunikationsdienste befinden, können sie gemäß Abschnitt 702 erhoben werden, und zwar unabhängig davon, ob die Daten einer anderen Stelle als dem Anbieter "gehören" oder anderweitig von ihm kontrolliert werden. Das heißt, die Frage ist nicht, woher die Daten kommen, sondern ob sie zum Zeitpunkt der Abfrage in der

Infrastruktur des Anbieters elektronischer Kommunikationsdienste ruhen oder in Bewegung sind.

6. Unterliegen US-amerikanische Anbieter elektronischer Kommunikationsdienste und/oder deren Tochtergesellschaften außerhalb der USA (insbesondere in der EU) dem FISA 702, wenn sie personenbezogene Daten außerhalb der USA, insbesondere in der EU/EWR, verarbeiten? Gilt der Grundsatz des Besitzes, der Verwahrung oder der Kontrolle für FISA 702, und wenn ja, was bedeutet dies? Wann wird eine Nicht-US-Tochtergesellschaft als unter der Kontrolle eines US-Unternehmens stehend betrachtet?

Die Antwort auf diese Frage ist ein wenig kompliziert. Einerseits ist Abschnitt 702 auf die Erhebung von Daten von Anbietern elektronischer Kommunikationsdienste in den USA ausgerichtet. In der Tat besteht der Sinn des Gesetzes darin, die Lücke zwischen der Erfassung der Kommunikation von Nicht-US-Personen außerhalb der Vereinigten Staaten (die durch die Executive Order 12.333 geregelt ist) und der Erfassung der Kommunikation von US-Personen innerhalb der Vereinigten Staaten (die durch das "traditionelle" FISA geregelt ist) zu schließen.
Wenn die fraglichen Daten ausschließlich von Nicht-US-Personen außerhalb der Vereinigten Staaten gespeichert werden, fallen sie möglicherweise überhaupt nicht unter Abschnitt 702 - und können stattdessen den weniger regulierten (und weitaus geheimnisvolleren) Überwachungsbefugnissen des EO 12.333 unterliegen. Werden die Daten jedoch von US-Unternehmen (einschließlich deren EU-Tochtergesellschaften) außerhalb der Vereinigten Staaten gespeichert, können sie sehr wohl unter die Bestimmungen von Abschnitt 702 fallen. Schließlich schränkt dieses Gesetz die Datenerhebung nur in Fällen ein, in bekannt ist, dass sich die Zielperson zum Zeitpunkt der Erfassung in den Vereinigten Staaten befindet oder eine US-Person ist, siehe 50 U.S.C. § 1881a(b). Handelt es sich bei der Zielperson um eine Nicht-US-Person, von der man vernünftigerweise annimmt, dass sie sich außerhalb der Vereinigten Staaten befindet, und handelt es sich bei dem Anbieter von elektronischen Kommunikationsdiensten um ein US-amerikanisches Unternehmen, scheint es durchaus ein Argument dafür zu geben, dass Abschnitt 702 auf Daten anwendbar ist, die auf europäischen Servern gespeichert sind - und dass die oben beschriebene Regelung zur Einhaltung der Vorschriften verwendet werden könnte, um die Zusammenarbeit auch in Bezug auf im Ausland gespeicherte Daten zu erzwingen. [6]

7. Kann ein US-amerikanischer Anbieter elektronischer Kommunikationsdienste und/oder eine Nicht-US-Tochtergesellschaft eines solchen Anbieters die Anwendung von FISA 702 mit dem Argument verhindern, dass eine solche Anwendung gegen das Recht der EU oder eines EU-Mitgliedstaats verstoßen würde?

---

6. Diese Frage stellte sich kürzlich im Zusammenhang mit dem Stored Communications Act, als Microsoft argumentierte, dass es nicht verpflichtet werden könne, einer von einem Bundesbezirksgericht in New York erlassenen SCA-Anordnung für Daten auf einem Server in Irland nachzukommen, siehe United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (per curiam). Bevor der Oberste Gerichtshof diese Frage klären konnte, verabschiedete der Kongress den Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, div. V, §§ 101-106, 132 Stat. 348, 1213 (kodifiziert in verstreuten Abschnitten des 18 U.S.C.). Siehe id. Das CLOUD-Gesetz befasst sich nur mit einem solchen Erwerb im Rahmen des SCA, nicht des FISA.

Nicht als solche, nein. Abschnitt 702 selbst macht keine der darin vorgesehenen Befugnisse davon abhängig, ob die Erhebung mit dem Recht der EU oder der EU-Mitgliedstaaten vereinbar ist; im Gegenteil, es heißt ausdrücklich, dass die Erhebung, zu der er ermächtigt, "Ungeachtet anderer gesetzlicher Bestimmungen". 50 U.S.C. § 1881a(a). Der einzige Vorbehalt ist hier die Presidential Policy Directive 28 ("PPD-28"), die ein gewisses Maß an Schutz für bestimmte Daten von Nicht-US-Personen bietet, siehe Vladeck Schrems Report ¶ 62-64. Die Grenzen der PPD-28 hängen jedoch nicht davon ab, ob die Erhebung mit dem Recht der EU oder der EU-Mitgliedstaaten vereinbar ist oder nicht (sie richten sich stattdessen nach dem Zweck der Erhebung). Und in jedem Fall schafft die PPD-28 keine einklagbaren Rechte, die ein US-amerikanischer Anbieter elektronischer Kommunikationsdienste oder eine nicht-amerikanische Tochtergesellschaft eines solchen Anbieters vor Gericht durchsetzen könnte.

8. Gilt FISA 702 für Anbieter elektronischer Kommunikationsdienste außerhalb der USA (d.h. ohne Hauptsitz in den USA), z.B. (i) wenn sie überhaupt in den USA tätig sind und/oder (ii) wenn sie eine Tochtergesellschaft in den USA haben, sei es eine abhängige Tochtergesellschaft oder eine nach US-Recht gegründete juristische Person?

Auf den ersten Blick geht es nach dem Wortlaut und dem allgemeinen Verständnis von Abschnitt 702 nicht um die Frage, wo sich der Anbieter befindet, sondern darum, wo sich die Daten befinden. Das liegt wiederum daran, dass Abschnitt 702 in Fällen, in denen Daten von Nicht-US-Personen von Nicht-US-Unternehmen außerhalb des Hoheitsgebiets der Vereinigten Staaten gespeichert werden, überhaupt nicht anwendbar ist - und jede Sammlung von Daten zur Überwachung ausländischer Nachrichtendienste stattdessen durch die Executive Order 12.333 geregelt wird (die, wie wir bereits erörtert haben, Vor- und Nachteile hat).

Allerdings hat die US-Regierung in anderen Zusammenhängen (z. B. im Microsoft-Streit, der zum CLOUD-Gesetz führte) den Standpunkt vertreten, dass die einzige relevante Überlegung darin besteht, ob sich die Daten im Besitz oder unter der Kontrolle eines US-Kommunikationsdienstleisters gemäß der Definition in 50 U.S.C. § 1881(b)(4) befinden. Ein EU-Unternehmen mit einer US-Tochtergesellschaft könnte also durchaus unter die Regelung von Abschnitt 702 fallen, und zwar wiederum aufgrund der Definition in § 1881(b)(4), die die "Agenten" von qualifizierten Anbietern elektronischer Kommunikationsdienste umfasst.

Es gibt also keine klare, kategorische Antwort auf diese Frage. Sofern die Daten auf US-Servern ruhen oder über eine US-Infrastruktur übertragen werden, können sie gemäß Abschnitt 702 erfasst werden, unabhängig davon, wo sich das Unternehmen befindet, dem die Server und/oder die Infrastruktur gehören. Wenn ein EU-Unternehmen eine US-Tochtergesellschaft hat (oder selbst eine Niederlassung in den Vereinigten Staaten unterhält), können die oben erwähnten Zwangsmaßnahmen leicht eingesetzt werden, um die Einhaltung der Richtlinien gemäß Abschnitt 702 zu erzwingen. Und soweit die Daten auf Nicht-US-Servern ruhen oder über eine Nicht-US-Infrastruktur übertragen werden, über die kein US-Unternehmen Kontrolle hat, scheint Abschnitt 702 weniger eindeutig zu sein, je nachdem, ob ein US-Unternehmen Kontrolle ausüben könnte.

Wenn ja:

a. Gilt FISA 702 nur für eine solche Tochtergesellschaft oder ein Unternehmen, das in den USA Geschäfte tätigt, oder erstreckt sich die Anwendung auch auf die nichtamerikanische Muttergesellschaft und/oder andere verbundene Unternehmen (z. B. ein europäisches Unternehmen, das personenbezogene Daten in der EU verarbeitet und eine Tochtergesellschaft in den USA hat)?

Die Definition in § 1881(b)(4) definiert den Begriff "Anbieter elektronischer Kommunikationsdienste" so, dass sie "Beamte, Angestellte oder Bevollmächtigte einer Einrichtung" umfasst, die ansonsten die gesetzliche Definition erfüllen. 50 U.S.C. § 1881(b)(4)(E). Zu diesem Zweck wird allgemein davon ausgegangen, dass eine Tochtergesellschaft eines Anbieters zu einem elektronischen Kommunikationsdienst zählt. Es ist jedoch keineswegs klar, dass eine Muttergesellschaft oder ein verbundenes Unternehmen die Definition erfüllt, da sie kein Vertreter ihrer Tochtergesellschaft/ihres verbundenen Unternehmens ist.

b. Falls die Antwort auf Frage 2 "Ja" lautet: Können Verpflichtungen zur Weitergabe von Daten an US-Geheimdienste oder zur Gewährung von Zugang gegen Nicht-US-Personen oder -Einrichtungen durchgesetzt werden? Wie und in welchem Umfang? Würde ein Eigentümer, Direktor, Vertreter, Angestellter o.ä. Gefahr laufen, den Forderungen der USA nach Offenlegung, Aufbewahrung oder Zugang nicht nachzukommen, z.B. Gefahr, dass ihm die Einreise in die USA verweigert wird, dass er verhaftet wird, dass gegen ihn Sanktionen verhängt werden usw.? Könnten die US-Behörden an die US-Tochtergesellschaft herantreten, wenn die Nicht-US-Person oder -Einrichtung den Aufforderungen zur Offenlegung oder zum Zugang nicht nachkommt?

Auch hier ist die Antwort ein wenig kompliziert. Wenn die US-Regierung Daten von Servern oder Infrastrukturen erhebt, die sich physisch in den Vereinigten Staaten befinden, ist der Eigentümer dieses Materials vermutlich in den Vereinigten Staaten ansässig. Daraus sollte folgen, dass die US-Regierung gegen jede Einrichtung mit einer US-Präsenz vorgehen könnte, um die Einhaltung einer gemäß Abschnitt 702 erlassenen Richtlinie zu erzwingen, so wie ich es in meiner Antwort auf Frage 2 oben dargelegt habe. Es fällt mir allerdings schwer, mir einen Sachverhalt vorzustellen, bei dem die US-Regierung versuchen könnte, gemäß Abschnitt 702 Daten von einem Anbieter elektronischer Kommunikationsdienste zu beschaffen, der in den Vereinigten Staaten keine Niederlassung hat. Aber es ist möglich, dass es Fälle am Rande gibt, in denen es Nicht-US-Unternehmen gibt, deren Daten zumindest theoretisch dem Erwerb nach Abschnitt 702 unterliegen, gegen die aber die Zwangsmechanismen des FISA unwirksam wären - und sei es aus keinem anderen Grund als dem Fehlen einer bedeutenden rechtlichen Präsenz in den Vereinigten Staaten.

## II. WEITERE ZUGRIFFSRECHTE, OFFENLEGUNGS- UND AUFBEWAHRUNGSPFLICHTEN

1. Erlauben es die US-Gesetze oder -Vorschriften über FISA 702 hinaus den Behörden (seien es Nachrichtendienste, Gerichte oder andere Behörden) oder anderen Stellen in den USA, auf personenbezogene Daten zuzugreifen, die von Europa in die USA übermittelt werden, solange sie sich im Empfangsbereich des vorgesehenen Empfängers oder eines weiteren Empfängers befinden, an den die personenbezogenen Daten weitergegeben wurden (unabhängig davon, ob es sich um den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter handelt), indem sie entweder auf die Verarbeitungseinrichtungen zugreifen (mit oder ohne Wissen des Empfängers) oder den Empfänger auffordern, den Behörden (z. B. FISA 501, National Security Letters) oder Dritten (z. B. Pre-Trial Discovery) Daten zu übermitteln?

Die kurze Antwort auf diese Frage lautet "Ja". Lokale, nationale und bundesstaatliche Behörden in den Vereinigten Staaten verfügen über eine breite Palette rechtlicher Befugnisse, die es ihnen unter den richtigen Umständen erlauben könnten, personenbezogene Daten zu sammeln, indem sie entweder auf in den USA ansässige Verarbeitungseinrichtungen zugreifen oder den Empfänger auffordern, die Daten den Behörden offenzulegen, solange sie sich auf amerikanischem Boden befinden. Die Bandbreite reicht von einem gewöhnlichen Durchsuchungsbefehl in einem Strafverfahren (der mindestens 57 verschiedenen Gesetzen unterliegt) über eine Abhörmaßnahme (deren Befugnis sich aus einzelstaatlichen oder bundesstaatlichen Gesetzen ergeben kann) bis hin aus einem Schreiben zur nationalen Sicherheit und einem "traditionellen" FISA-Beschluss. Es wird daher schwierig sein, die folgenden Fragen zu all diesen Befugnissen umfassend zu beantworten. In der Tat würde es wahrscheinlich Monate dauern, jede dieser Befugnisse einzeln aufzulisten.

Um die Behörden, nach denen Sie speziell gefragt haben, kurz zu beschreiben: FISA § 501 ist umgangssprachlich als die Bestimmung über "Geschäftsunterlagen" (oder "greifbare Dinge") bekannt und in 50 U.S.C. § 1861 kodifiziert. Eine Zeit lang (von der Verabschiedung des USA PATRIOT Act von 2001 bis Anfang letzten Jahres) bot diese Bestimmung der Bundesregierung eine unglaublich weitreichende Befugnis zur (heimlichen) Beschaffung von Nicht-Inhaltsdaten (einschließlich Telefon-Metadaten) von Unternehmen. Die schwerwiegendste dieser Befugnisse lief jedoch im Jahr 2020 aus und wurde bisher nicht neu genehmigt. Die derzeit geltende Fassung ist die Version vor 2001, die viel enger gefasst ist.

Ein weiteres Beispiel sind die National Security Letters (NSLs). Dabei handelt es sich um administrative Vorladungen, die von der US-Regierung ausgestellt werden, um Informationen für Zwecke der nationalen Sicherheit zu sammeln. Anders als bei FISA § 501 ist für NSLs keine vorherige Genehmigung durch einen Richter erforderlich. Der Stored Communications Act, der Fair Credit Reporting Act und der Right to Financial Privacy Act ermächtigen die US-Regierung, solche Informationen anzufordern, wenn sie für genehmigte nationale Sicherheitsuntersuchungen "relevant" sind. Laut Gesetz können NSLs nur Informationen anfordern, die nicht den Inhalt betreffen, z.B. Transaktionsdatensätze und gewählte Telefonnummern, aber niemals den Inhalt von Telefonaten oder E-Mails.

Die vorprozessuale Offenlegung ist sowohl spezifischer als auch unbefristeter. Sie ist spezifischer in dem Weise, dass sie nur im Zusammenhang mit einem bestimmten Zivilrechtsstreit erfolgt - einem Rechtsstreit, der einen Antrag auf Klageabweisung überstanden hat. Und die Offenlegung muss sich auf die tatsächlichen oder rechtlichen Fragen beziehen, um die es in dem konkreten Fall geht. Solange dies der Fall ist, kann die Offenlegung recht weitreichend sein und sich auch auf den Inhalt von Mitteilungen erstrecken (wenn diese nicht durch ein Privileg geschützt sind).

2. Erlauben es US-Gesetze, wie z. B. 18 U.S.C. § 2703(f), oder gesetzliche Vorschriften, dass die US-Regierung oder Dritte von einem Unternehmen verlangen können, personenbezogene Daten zu speichern?

Im Allgemeinen lautet die Antwort: Ja. Es gibt Dutzende von Gesetzen und Bundesverordnungen, die Unternehmen verpflichten, bestimmte Arten von personenbezogenen, kundenbezogenen oder internen Daten aufzubewahren. Die meisten davon dienen jedoch Zwecken, die zumindest nach außen hin nichts mit der Überwachung und/oder nachrichtendienstlichen Erfassung zu tun haben (z.B. Führung von Mitarbeiterakten, Einhaltung von Sicherheitsvorschriften etc.). Es gibt nicht annähernd so viele Gesetze oder Vorschriften, die sich mit der Aufbewahrung von Kommunikationsdaten befassen, die gemäß Abschnitt 702 erfasst werden könnten. Ein Beispiel für letzteres ist die Federal Communications Commission, die von Telefongesellschaften verlangt, bestimmte Gesprächsaufzeichnungen bis zu 18 Monate lang aufzubewahren, siehe 47 C.F.R. § 42.6.

Abschnitt 2703(f), der Teil des Stored Communications Act ist, ist vielleicht das wichtigste und treffendste Beispiel. Nach diesem Gesetz muss "ein Anbieter von drahtgebundenen oder elektronischen Kommunikationsdiensten oder eines Ferncomputerdienstes auf Ersuchen einer staatlichen Stelle alle erforderlichen Maßnahmen ergreifen, um die in seinem Besitz befindlichen Aufzeichnungen und sonstigen Beweismittel bis zum Erlass einer gerichtlichen Anordnung oder eines anderen Verfahrens aufzubewahren", und diese Aufzeichnungen 90 Tage lang aufbewahren (ein Zeitraum, der auf Antrag verlängert werden kann). 18 U.S.C. § 2703(f). Der Zweck dieser Bestimmung besteht darin, der Regierung Zeit zu geben, die Unterlagen auf dem Rechtsweg zu beschaffen - und die Aufbewahrungspflicht kann sogar durch informelle Anfragen ausgelöst werden, siehe z. B. United States v. Bach, No. CRIM.01-221, 2001 WL 1690055, at *1 (D. Minn. Dec. 14, 2001), rev'd, 310 F.3d 1063 (8th Cir. 2002). Das Gesetz schreibt nicht vor, dass der Antrag alle Unterlagen eines Unternehmens betreffen muss. Vielmehr scheint es im Einklang mit dem Gesetz zu stehen, dass die Regierung ein Unternehmen auffordern kann, nur eine bestimmte Untergruppe von Unterlagen vorübergehend aufzubewahren - darunter vielleicht Unterlagen, die sich auf einen bestimmten Mitarbeiter oder Kunden beziehen.

3. Wenn ja, beschreiben Sie bitte ausführlich die unter 1. und 2. genannten Gesetze oder Vorschriften. insbesondere:

    a. Welche Ziele werden mit der Zugangsgenehmigung oder der Aufbewahrungspflicht verfolgt?

Ich verallgemeinere hier notwendigerweise ein wenig (auch hier wäre es ein ziemliches Unterfangen, einen umfassenden Überblick über alle Gesetze und

Vorschriften zu geben, die den Antworten auf die ersten beiden Fragen genügen würden). Die meisten dieser Gesetze und Vorschriften haben jedoch eines von drei Zielen: Entweder die Vorlage von Beweismitteln in einer strafrechtlichen Untersuchung, die Vorlage von Informationen, die für eine Spionageabwehruntersuchung relevant sind, oder die Überwachung bestimmter Branchen, um die Einhaltung zivilrechtlicher Vorschriften zu gewährleisten.

Am Beispiel von § 2703(f) wird deutlich, dass die Aufbewahrungspflicht dazu dient, der Regierung die Möglichkeit zu geben, Anträge auf Herausgabe solcher Informationen gezielt und rechtzeitig zu verfolgen - und nicht durch beschleunigte Notverfahren, um ihre Vernichtung zu verhindern.

b. Für wen gilt das Gesetz oder die Vorschrift?

Sie variiert erheblich, je nachdem, um welches Gesetz es sich handelt. Die meisten Aufbewahrungspflichten gelten nur für Unternehmen in bestimmten Branchen (z. B. Telefongesellschaften, die der FCC-Verordnung unterliegen, oder Kreditauskunfteien, die unter den Fair Credit Reporting Act fallen). Der Stored Communications Act gilt ebenfalls nur für bestimmte Arten von Dienstleistern, wie in § 2703(f). Aber Durchsuchungsbefehle, nationale Sicherheitsbriefe und andere vergleichbare Befugnisse können theoretisch für jede Person oder Einrichtung gelten, die der Gerichtsbarkeit der US-Gerichte unterliegt.

c. Für welche Art von Daten gilt das Gesetz oder die Vorschrift?

Die Anforderungen an die Vorratsdatenspeicherung sind in der Regel eng und spezifisch, z. B. müssen Telefongesellschaften nur "den Namen, die Adresse und die Telefonnummer des Anrufers, die angerufene Telefonnummer, das Datum, die Uhrzeit und die Dauer des Anrufs" aufbewahren. Die zwingenderen Offenlegungsvorschriften können je nach den Umständen für weitaus breitere Datenkategorien gelten. Tatsächlich kann normalerwise ein Durchsuchungsbefehl (der bei hinreichendem Verdacht auf eine Straftat ausgestellt werden kann) in einem geeigneten Fall verwendet werden, um praktisch alle Daten im Besitz des Empfängers zu erhalten.

d. Unter welchen Umständen erlaubt das Gesetz oder die Vorschrift den Zugang zu den Daten (bzw. deren Speicherung)?

Die Aufbewahrungsanforderungen sind in der Regel kategorisch; wenn sie zutreffen, ist die Aufbewahrung erforderlich. Die Vorratsspeicherung und der Zugang der Regierung zu den aufbewahrten Daten sind jedoch völlig unterschiedliche rechtliche Regelungen. Der Zugang zu Daten durch die eher zwangsweisen Erhebungsverfahren ist stärker eingeschränkt. Anordnungen nach dem SCA und nationale Sicherheitsbriefe erfordern zumindest den Nachweis einer laufenden Untersuchung, für die die angeforderten Daten relevant sind. Und normalerweise erfordern Durchsuchungsbefehle erfordern die richterliche Feststellung eines wahrscheinlichen Grundes für die Annahme, dass die Durchsuchung Beweise für eine Straftat aufdecken wird. Ein Grund, warum die Aufbewahrungsanforderungen in der Regel kaum geprüft werden, liegt darin, dass die Aufbewahrungsanforderung an sich den Zugang der Regierung nicht erlaubt; sie bewahrt lediglich bestehende Quellen von Aufzeichnungen für den Fall, dass die Regierung in der Lage ist, mit herkömmlichen Mitteln Zugang zu erhalten.

e. Welche Verpflichtungen und Beschränkungen der den Behörden oder Dritten übertragenen Befugnisse gelten?

Zusätzlich zu den oben beschriebenen Beschränkungen der Befugnisse werden die Befugnisse zur zwangsweisen Beschaffung durch eine Vielzahl externer Befugnisse eingeschränkt, einschließlich des Privacy Act (der die Sammlung, Pflege, Verwendung und Verbreitung von persönlich identifizierbaren Informationen über Einzelpersonen regelt, die von Bundesbehörden in Aufzeichnungssystemen aufbewahrt werden) und des vierten Zusatzes zur US-Verfassung (der "unangemessene" Durchsuchungen und Beschlagnahmen verbietet).

f. Sind die geltenden Gesetze oder Vorschriften öffentlich zugänglich?

Soviel ich weiß, ja.

g. Sind die geltenden Gesetze oder Vorschriften klar und präzise?

Im Großen und Ganzen, ja. Der Stored Communications Act ist bekanntlich etwas veraltet, was die darin verwendete Terminologie und die darin getroffenen Unterscheidungen angeht, siehe Kerr, oben. Es gibt jedoch eine umfangreiche Rechtsprechung zur Auslegung des Gesetzes, die herangezogen werden kann, wenn sich Fragen zu seinem Anwendungsbereich ergeben.

h. Verfügen die US-Behörden oder Dritte über Mittel zur Durchsetzung solcher Zugangsrechte, Offenlegungspflichten oder Aufbewahrungspflichten? Wenn ja, beschreiben Sie bitte diese Mittel.

In fast allen Fällen, ja. Die Nichteinhaltung gesetzlicher oder behördlicher Aufbewahrungspflichten wird mit zivilrechtlichen Sanktionen geahndet. Und die Nichteinhaltung eines Gerichtsbeschlusses, der die Offenlegung bestimmter Informationen vorschreibt, zieht für die nicht einhaltende Partei eine Missachtung nach sich - was wiederum zu erheblichen (und sich häufenden) Geldstrafen führen kann.

i. Gilt das jeweilige Gesetz oder die jeweilige Vorschrift auch für US-Personen oder -Einrichtungen und/oder Nicht-US- (insbesondere: EU-) Tochtergesellschaften solcher Personen oder Einrichtungen, wenn sie personenbezogene Daten außerhalb der USA, insbesondere in der EU/im EWR, verarbeiten? Wenn ja, was sind die genauen Voraussetzungen?

Die Behörden vertreten hier teilweise unterschiedliche Auffassungen. Aber die Kurzfassung ist, dass zumindest einige dieser rechtlichen Regeln nicht für Daten außerhalb der Vereinigten Staaten gelten, sowohl im Allgemeinen als auch aufgrund der starken Voreingenommenheit, welche die US-Gerichte gegen die extraterritoriale Anwendung von Gesetzen haben, siehe z.B. RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2099-100 (2016).

Allerdings gibt es auch bedeutende Ausnahmen. An erster Stelle ist hier das CLOUD-Act von 2018 zu nennen, das, wie bereits erwähnt, speziell für die Fälle erlassen wurde, in denen das SCA die US-Regierung ermächtigt, Daten von einem Unternehmen zu erheben, das in den Vereinigten Staaten tätig ist und die Daten außerhalb der Vereinigten Staaten gespeichert sind. Obwohl das Gesetz die Anwendung einer SCA-Anordnung auf solche Daten generell zulässt, sieht es auch Mechanismen vor, mit denen die Unternehmen oder die Gerichte diese Anfragen

zurückweisen oder anfechten können, wenn die Forderung die Datenschutzrechte des Landes verletzt, in dem die Daten gespeichert sind. (Der CLOUD Act sieht auch eine alternative Datenerhebung durch Rechtshilfeabkommen vor).

Ob die Vermutung gegen eine extraterritoriale Anwendung auch für einige der oben genannten spezifischeren Befugnisse zur Vorratsdatenspeicherung gilt, wie z. B. 18 U.S.C. § 2703(f), scheint eine offene Frage zu sein. Hier würde viel davon abhängen, ob ein Ersuchen beispielsweise an ein EU-Unternehmen, auf einem US-Server gespeicherte Daten aufzubewahren, überhaupt als extraterritorial gelten würde. Falls nicht, könnte das Ersuchen um Vorratsdatenspeicherung vermutlich ohne Schwierigkeiten an das EU-Unternehmen gerichtet werden.

j. Kann eine US-Person oder -Einrichtung und/oder eine Nicht-US-Tochtergesellschaft einer solchen Person oder Einrichtung die Anwendung eines solchen Gesetzes oder einer solchen Vorschrift mit dem Argument verhindern, dass eine solche Anwendung gegen das Recht der EU oder eines EU-Mitgliedstaats verstoßen würde?

Im Allgemeinen nicht. Aber im Rahmen des CLOUD-Gesetzes,

> Ein Anbieter eines elektronischen Kommunikationsdienstes für die Öffentlichkeit oder eines Ferninformationsdienstes, einschließlich eines ausländischen elektronischen Kommunikationsdienstes oder Ferninformationsdienstes, der aufgrund eines nach diesem Abschnitt eingeleiteten Gerichtsverfahrens verpflichtet ist, den Inhalt einer drahtgebundenen oder elektronischen Kommunikation eines Teilnehmers oder Kunden offenzulegen, kann einen Antrag auf Änderung oder Aufhebung des Gerichtsverfahrens stellen, wenn der Anbieter vernünftigerweise glaubt, dass-
>
> (i) dass der Kunde oder Abonnent keine US-Person ist und seinen Wohnsitz nicht in den Vereinigten Staaten hat; und
>
> (ii) dass die geforderte Offenlegung ein wesentliches Risiko schaffen würde, dass der Anbieter gegen die Gesetze einer qualifizierten ausländischen Regierung verstoßen würde.

18 U.S.C. § 2703(h)(2)(A). Eine "qualifizierte ausländische Regierung" ist wiederum eine Regierung, mit der die Vereinigten Staaten ein Abkommen speziell im Rahmen des CLOUD-Act geschlossen haben, das ähnliche Schutzmaßnahmen wie das CLOUD-Act vorsieht. Bisher bin ich der Meinung, dass nur das Vereinigte Königreich eine "qualifizierte ausländische Regierung" im Sinne dieser Formulierung ist.

k. Gilt das jeweilige Gesetz oder die jeweilige Vorschrift für nicht-US- (d.h. nicht in den USA ansässige) Personen oder Unternehmen/ Organisationen, z.B. (i) wenn sie jedenfalls in den USA geschäftlich tätig sind und/oder (ii) wenn sie eine Niederlassung in den USA haben, sei es eine abhängige Tochtergesellschaft oder eine nach US-Recht gegründe wurde juristische Person?

Meine eigenen Recherchen legen nahe, dass die Rechtslage in vielen der wichtigsten Fälle in dieser Frage unklar ist. Sicherlich würden an US-Tochtergesellschaften gerichtete Anträge auf Vorratsdatenspeicherung in keiner Weise durch die Tatsache beeinflusst, dass sich die Muttergesellschaft außerhalb der Vereinigten Staaten

befindet. Wenn der Antrag jedoch direkt an die ausländische Muttergesellschaft gerichtet wird, kann es Streitigkeiten hinsichtlich der Anwendung der Vermutung gegen eine extraterritoriale Anwendung geben (Streitigkeiten, die nicht zu FISA passen – weil FISA ausdrücklich extraterritorial ist). So kann beispielsweise ein Ersuchen um Vorratsspeicherung gemäß 18 U.S.C. § 2703(f) möglicherweise nicht an eine Nicht-US-Person gerichtet werden - sei es formal (weil das Gesetz nicht anwendbar ist) oder praktisch (weil dem Empfänger keine realistische Sanktion für die Nichtbefolgung droht). Im Allgemeinen haben die US-Gerichte keine Befugnis, Zwangsmaßnahmen gegen juristische Personen außerhalb ihrer "persönlichen" Zuständigkeit zu ergreifen. US-Tochtergesellschaften wären somit von solchen Befreiungsregelungen betroffen, Muttergesellschaften, die nicht in den Vereinigten Staaten ansässig sind, jedoch wohl nicht.

Wenn ja:

i. Gilt das Gesetz oder die Vorschrift nur für die Tochtergesellschaft oder das Unternehmen, das in den USA geschäftlich tätig ist, oder gilt es auch für die Nicht-US-Muttergesellschaft oder andere verbundene Unternehmen (z. B. ein Europäisches Unternehmen, das personenbezogene Daten in der EU verarbeitet und eine Tochtergesellschaft in den USA hat)?

Auch hier gibt es nicht viel publiziertes Recht, um diese Frage zu beantworten. Nach meinem Verständnis der einschlägigen Behörden gilt die Verpflichtung jedoch höchstwahrscheinlich nur für die Tochtergesellschaft oder das Unternehmen, das in den Vereinigten Staaten geschäftlich tätig ist. 18 U.S.C. § 2703(f) ist wieder einmal ein anschauliches Beispiel. Diese Vorschrift gestattet die Einbehaltung von Daten gegenüber "Anbietern elektronischer Kommunikationsdienste", ein Begriff, der, wie oben erörtert, EU-Muttergesellschaften wahrscheinlich nicht einschließt, nur weil sie US-Tochtergesellschaften haben, die der Definition entsprechen (aufgrund der Definition des Begriffs). In diesem Zusammenhang würde der Antrag auf Vorratsdatenspeicherung, sowohl formell als auch praktisch, höchstwahrscheinlich an das Unternehmen mit einer tatsächlichen rechtlichen Präsenz in den Vereinigten Staaten gerichtet werden - nicht nur, weil die zuständige Behörde beschränkt sein könnte, sondern auch, weil die Möglichkeiten der Regierung, die Einhaltung der Vorschriften zu erzwingen, ebenfalls begrenzt sein könnten. Diese Regel ist jedoch nicht verbindlich. Die US-Regierung könnte versuchen, gegenüber der EU-Muttergesellschaft eine Einbehaltung der Daten zu verlangen - mit der Begründung, dass das Vorhandensein irgendeiner rechtlichen Präsenz in den Vereinigten Staaten als Grundlage für eine gerichtliche Zwangsmaßnahme dienen könnte. Hier gibt es viele Grauzonen - und mir ist nicht klar, wie die Gerichte in einem solchen Fall entscheiden würden, insbesondere wenn die Befugnisse aus Gründen der Extraterritorialität angefochten werden würden.

ii. Können Verpflichtungen zur Offenlegung oder Vorratsspeicherung von Daten oder zur Gewährung von Zugang gegen Nicht-US-Personen oder Einrichtungen durchgesetzt werden? Wie und in welchem Umfang? Besteht für Betroffene, Verantwortliche, Vertreter, Angestellte o.ä., wenn sie den Forderungen der USA nach Offenlegung, Aufbewahrung oder Zugang nicht nachkommen, z.B. das Risiko, dass ihnen die

Einreise in die USA verweigert wird, dass sie verhaftet werden, gegen sie Sanktionen verhängt werden usw.? Könnten die US-Behörden an die US-Tochtergesellschaft herantreten, wenn das Nicht-US-Unternehmen den Aufforderungen zur Offenlegung, Aufbewahrung oder zum Zugang nicht nachkommt?

Die Vollstreckung ist etwas unkomplizierter. US-Gerichte sind im Allgemeinen nicht in der Lage, Zwangsmaßnahmen gegen Stellen oder Körperschaften außerhalb ihrer territorialen Zuständigkeit zu ergreifen - nach der Doktrin der "persönlichen Zuständigkeit". Es ist durchaus denkbar, dass ein US-Gericht seine Befugnis gegenüber einer US-Tochtergesellschaft nutzt, um zu versuchen, Zwangsmaßnahmen gegen die Muttergesellschaft zu ergreifen, aber es ist nicht klar, warum die Tochtergesellschaft nicht selbst in der Lage sein sollte, die geforderten Maßnahmen zu ergreifen. Entscheidend ist auch hier, dass die US-Einrichtung mit einer Niederlassung auf US-Boden diejenige wäre, die potenziellen (und möglicherweise erheblichen) Sanktionen ausgesetzt wäre. Und in Fällen, in denen es keine US-Tochtergesellschaft gibt, ist es nicht klar, wie die US-Regierung vor US-Gerichten ein Zwangsverfahren gegen ein Unternehmen erwirken kann, das keine Kontakte zu den Vereinigten Staaten hat.

4. Gibt es andere rechtliche Verpflichtungen, die der Einhaltung der Verpflichtungen (insbesondere zur Vertraulichkeit) in den Standardvertragsklauseln entgegenstehen würden? Wenn ja, beschreiben Sie diese bitte im Detail.

Zumindest auf der Grundlage der alten Standardvertragsklauseln (und nicht der Standardvertragsklauseln von 2021, mit denen ich weniger vertraut bin) ist es schwer, die Antwort eindeutig mit Nein zu beantworten, angesichts des breiten Spektrums an staatlichen Behörden, die involviert werden könnten. Aber mir fällt auf Anhieb nichts ein. Die zentralen Streitpunkte betreffen die lokalen Behörden, die Behörden der einelnden Bundesstaaten und die Bundesbehörden, die solche Informationen zwingend zu erhalten, und alle oben (zumindest in allgemeiner Form) genannt wurden.

## III. WEITERE PRAXIS

1. Gibt es eine Zugriffspraxis auf personenbezogene Daten oder eine Verpflichtung zur Aufbewahrung von personenbezogenen Daten in den USA, die über die in I. und II. beschriebene Rechtslage hinausgeht?

Mir ist nicht bekannt, dass staatliche Behörden die Aufbewahrung personenbezogener Daten in einer Art und Weise vorgeben, die über meine obigen Antworten hinausgeht. Es ist jedoch bei vielen großen US-Unternehmen, insbesondere bei solchen mit einem großen Kundenstamm, zunehmend üblich, freiwillig große Mengen an Kunden- und Transaktionsdaten aufzubewahren. In den meisten Fällen verbieten Bundesgesetze eine solche freiwillige Vorratsspeicherung nicht, obwohl sie einige Bedingungen für die Speicherung und Verwendung solcher Daten vorschreiben.

## IV. RECHTSBEHELF

1. Steht allen Betroffenen in der EU/im EWR ein Rechtsbehelf gegen den Zugriff auf ihre personenbezogenen Daten oder deren Speicherung zur Verfügung? Wenn ja, beschreiben Sie bitte die Bedingungen, die Einschränkungen und das Verfahren. Wer wird über den Rechtsbehelf entscheiden? Falls es sich nicht um einen unabhängigen, unparteiischen Richter handelt, der in einem Standardverfahren gewählt wird, beschreiben Sie bitte die Rechtsstellung der Entscheidungsinstanz, mögliche Abhängigkeiten und das Ernennungsverfahren. Hat das Entscheidungsgremium Zugang zu allen relevanten Dokumenten, einschließlich nichtöffentlicher Unterlagen? Ist das Entscheidungsgremium mit wirksamen Korrekturbefugnissen ausgestattet? Wenn ja, beschreiben Sie bitte diese Befugnisse.

Wie Sie wissen, ist dies der Schwerpunkt meines Sachverständigengutachtens im Schrems-Verfahren, siehe Vladeck Schrems Report ¶ 79-103. Die kurze Antwort lautet "Nein" - Rechtsbehelfe gegen den Zugriff auf Daten betroffener EU-/EWR-Bürger oder deren Speicherung sind nicht immer verfügbar. Wie in meinem Schrems-Report ausführlich beschrieben, gibt es eine Reihe von Aufsichtsmaßnahmen und Maßnahmen zur Rechenschaftspflicht, die sicherstellen sollen, dass die US-Behörden die gesetzlichen und verfassungsmäßigen Grenzen dieser Befugnisse einhalten sowie beachtliche Korrekturbefugnisse für Fälle, in denen dies nicht der Fall ist, vgl. a.a.O., aber es ist nicht immer der Fall, dass diese Maßnahmen von den betroffenen Personen selbst geltend gemacht werden können.

Ein konkretes Gegenbeispiel ist der Judicial Redress Act von 2016, der darauf ausgerichtet ist, den Schutz der Privatsphäre auf EU/EWR-Bürger auszuweiten, siehe id. ¶¶ 66-67. Der Judicial Redress Act setzt jedoch nicht die im Privacy Act enthaltenen Einschränkungen für das Führen von Gerichtsverfahren außer Kraft, welche es Behörden neben anderen Dingen erlauben, ihre Akten den gesetzlichen Offenlegungspflichten unter bestimmten Voraussetzungen vollständig zu entziehen - unter anderem, wenn die Aufzeichnungen im Interesse der nationalen Sicherheit als geheim eingestuft werden, siehe z.B. 5 U.S.C. § 552a(k)(1). Die NSA hat beispielsweise von dieser Befugnis Gebrauch gemacht, siehe 32 C.F.R. § 322.7(a) (2016) ("Alle Aufzeichnungssysteme, die von der NSA/CSS und ihren Bestandteilen unterhalten werden, sind gemäß 5 U.S.C. 552a(k)(1) von den Anforderungen von 5 U.S.C. 552a(d) ausgenommen, soweit das System Informationen enthält, die gemäß der Executive Order 12958 ordnungsgemäß als Verschlusssache eingestuft sind und die gemäß der Executive Order im Interesse der nationalen Verteidigung oder der Außenpolitik geheim gehalten werden müssen."). Damit es nicht den Anschein hat, dass diese Vorgehensweise umstritten sei: "Es ist schwer vorstellbar, wie es anders sein könnte, (…) wenn die NSA Daten eines Terroristen erhält, der sich in Paris aufhält und möglicherweise einen Anschlag plant, sollte sie der Zielperson keinen Zugriff auf ihre Daten und die Möglichkeit geben müssen, diese zu korrigieren" - der Kernzweck des Privacy Act. Tim Edgar, Redress for NSA Surveillance: The Devil is in the Details, LAWFARE, Oct. 19, 2015, https://www.lawfareblog.com/redress-nsa-surveillance-devil-details.

Was die Frage betrifft, "wer" über den Rechtsbehelf entscheidet, so sind alle Richter, soweit diese Streitigkeiten vor den Bundesgerichten landen, "Artikel III"-Bundesrichter - das bedeutet, dass sie vom Präsidenten ernannt und vom Senat bestätigt wurden und ihr Amt bei "gutem Benehmen" auf unbestimmte Zeit innehaben.

2. Stellt sich die US-Regierung auf den Standpunkt, dass betroffene Personen in der EU/im EWR außerhalb der USA keine Rechte nach dem Vierten Verfassungszusatz haben? Welchen Umfang haben die Rechte, die betroffene Personen aus der EU/dem EWR in einem Gerichtsverfahren geltend machen können?

Die US-Regierung vertritt in der Regel den Standpunkt, dass alle "Nicht-US-Personen" keine Rechte nach dem Vierten Verfassungszusatz haben, siehe auch den Präzedenzfall Agency for Int'l Dev. v. Alliance for Open Soc'y Int'l, Inc., 140 S. Ct. 2082, 2086 (2020) ("Entsprehcend dem amerikanischen Verfassungsrecht ist seit langem entschieden, dass ausländische Bürger außerhalb des US-Territoriums keine Rechte nach der US-Verfassung haben."). Wie ich jedoch in meinem Schrems-Report feststellte, gibt es zahlreiche gesetzliche und nicht-gesetzliche Rechtsbehelfe, die Betroffenen aus der EU/dem EWR zumindest in einigen dieser Zusammenhänge theoretisch zur Verfügung stehen - einschließlich der Geltendmachung, dass die zuständigen US-Behörden ihre gesetzlichen Befugnisse überschritten haben, siehe z.B. Vladeck Schrems Report ¶ 81-83. Schließlich beruhte die erfolgreiche Anfechtung der Massenerfassung von Telefon-Metadaten durch die ACLU nicht auf einer Verfassungsklage, sondern auf der Behauptung, dass die Regierung ihre gesetzlichen Befugnisse überschritten habe - eine Klage, die einem EU-Bürger ebenso zur Verfügung stehen würde, siehe z.B. ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).

3. Kann das Erfordernis einer Klagebefugnis ein Hindernis für Rechtsmittel gegen rechtswidrige Überwachungsmaßnahmen sein? Inwiefern?

Ja, aber nicht aus dem offensichtlichen Grund. Es ist selbstverständlich, dass diejenigen, deren Daten unrechtmäßig von der Regierung erlangt wurden, die Art von "tatsächlichem Schaden" erleiden, die in der Regel das Erfordernis der Klagebefugnis vor den Bundesgerichten der USA erfüllt. Das Problem, das sich in diesem Zusammenhang stellt, ist das Fehlen einer Benachrichtigung. Solange die betroffene Person plausibel behaupten kann, dass ihre Daten unrechtmäßig erworben wurden, erfüllt sie diese Anforderung, siehe z.B. Wikimedia Found. v. Nat'l Security Agency, 857 F.3d 193 (4th Cir. 2017) (Bestätigung der Klagebefugnis einer Medienorganisation, die die Rechtmäßigkeit der "vorgelagerten" Datenerhebung gemäß Abschnitt 702 anfechten wollte).

Problematisch wird es, wenn die erlangten Daten als Verschlusssache eingestuft wurden, wie es bei Informationen in der Regel der Fall ist, die durch die Überwachungsbehörden ausländischer Nachrichtendienste erlangt wurden, siehe Vladeck Schrems Report ¶ 89-95. Da der Kläger in diesen Fällen nicht plausibel darlegen kann, dass seine Kommunikation abgefangen wurde, kann er die Klagebefugnis insofern nicht begründen, als dass er nicht nachweisen kann, dass der von ihm behauptete Schaden tatsächlich eingetreten ist, siehe Clapper vs. Amnesty Int'l, 568 U.S. 398 (2013). In dieser Hinsicht ist die Klagebefugnis zwar ein

Hindernis, aber das bedeutendere Problem ist die Schwierigkeit, die fehlende Benachrichtigung zu überwinden - was mehr mit der Privilegierung von Staatsgeheimnissen zu tun hat, die als nächstes behandelt wird, als mit der Klagebefugnis.

4. Können die Regelungen für Staatsgeheimnisse ein Hindernis für gerichtliche Rechtsbehelfe bei unrechtmäßiger Überwachung darstellen? Inwiefern?

Das ist durchaus möglich, wie ich in meinem Schrems-Report erläutert habe, siehe Vladeck Schrems Report ¶ 100-02. Selbst wenn ein Kläger plausibel behaupten kann, dass seine Daten im Rahmen einer der Überwachungsmaßnahmen der US-Regierung für ausländische Nachrichtendienste unrechtmäßig erhoben wurden, können seine Möglichkeiten, einen solchen Erwerb zu beweisen, dadurch eingeschränkt sein, dass er die Regierung nicht dazu zwingen kann, geheime Details über ihre Überwachungsaktivitäten herauszugeben. Ein Beispiel für dieses Problem findet sich in Wikimedia Found. v. Nat'l Security Agency, 14 F.4th 276 (4th Cir. 2021). In diesem Fall war das Berufungsgericht zunächst der Ansicht, dass Wikimedia gemäß Artikel III befugt war, die Rechtmäßigkeit der "vorgelagerten" Erhebung gemäß Abschnitt 702 anzufechten, weil sie plausibel behauptet hatte, dass ihre Kommunikation abgefangen wurde. Als Wikimedia jedoch tatsächlich beweisen musste, dass ihre Kommunikation abgefangen worden war, berief sich die Regierung auf das Staatsgeheimnis - und der Fourth Circuit befand, dass die Berufung auf das Privileg es Wikimedia unmöglich machte, ihren Fall vorzubringen.

Am 8. November 2021 fand vor dem Obersten Gerichtshof der USA die mündliche Verhandlung in der Rechtssache FBI gegen Fazaga statt, dem wichtigsten Fall zum Thema FISA im Zusammenhang mit dem Staatsgeheimnisprivileg, mit dem sich der Gerichtshof seit einiger Zeit befasst hat. Eine der konkreten Fragen, die Fazaga aufwirft, ist die, ob FISA das Privileg des Staatsgeheimnisses in Fällen außer Kraft setzt, in denen Kläger behaupten, dass ihre Kommunikation unrechtmäßig unter Verstoß gegen das Gesetz abgehört wurde - weil es ein bestimmtes Verfahren vorsieht, mit dem Gerichte prüfen können, ob Verschlusssachen als Beweismittel zugelassen werden können und sollten (aus diesem Grund beschränkt sich diese Argumentation auf Klagen, die sich darauf richten, dass die Überwachung durch FISA unzulässig ist, im Gegensatz zu Klagen, dass die Überwachung verfassungswidrig oder gemäß der Executive Order 12.333 unzulässig ist). Der Neunte Bundesberufungsgerichtshof hatte entschieden, dass Klagen, die sich aus dem FISA ergeben, nicht unter das Staatsgeheimnisprivileg fallen, da der FISA das Privileg aufhebt. Ob und inwieweit das Staatsgeheimnisprivileg ein Hindernis für gerichtliche Klagen wegen rechtswidriger Überwachung darstellt, hängt in hohem Maße davon ab, wie der Oberste Gerichtshof in diesem Fall entscheidet. Eine Entscheidung ist nicht vor Mai 2022 zu erwarten.

Ich hoffe, dass diese Antworten für Sie und Ihre Kollegen von Nutzen sind, und würde mich freuen, sie mit Ihnen weiter zu diskutieren.

Mit freundlichen Grüßen,

Stephen I. Vladeck