NIEDERER KRAFT FREY

Cloud Act und dessen Risiken bei der Zusammenarbeit mit Cloud Service Providern

Webinar @Weblaw zum Cloud Act

Zürich — 6. März 2019

Übersicht

1. Was ist der CLOUD Act?
2. Terminologie
3. Hintergrundinformationen
4. Anwendungsbereich
5. Welche Daten sind betroffen?
6. Welche CSP sind betroffen?
7. Wie können US-Cloud warrants abgewehrt werden?
8. Exkurs: Bilateraler Vertrag USA-CH
9. Reaktionen auf den CLOUD Act
10. Was gilt es bei Verträgen mit CSP zu beachten?
11. Ausblick

Was ist der Cloud Act? I

Bild: Time Staff, originally published 29 April 2011

Was ist der Cloud Act? II

- CLOUD Act = "Clarifying Lawful Overseas Use of Data Act"
- Ein US-amerikanisches Gesetz, welches am 6. Februar 2018 verabschiedet und am 23. März 2018 unterzeichnet wurde
- Anpassung des US-Stored Communications Acts (SCA) (Kapitel 121 des Title 18, United States Code): Link
- Zugriff von US-Behörden auf Daten, die bei CSP mit US-Bezug liegen, und zwar unabhängig vom Standort der Server
- Rechtsrahmen für den Abschluss von bilateralen Rechtshilfeabkommen, sogenannte Executive Agreements

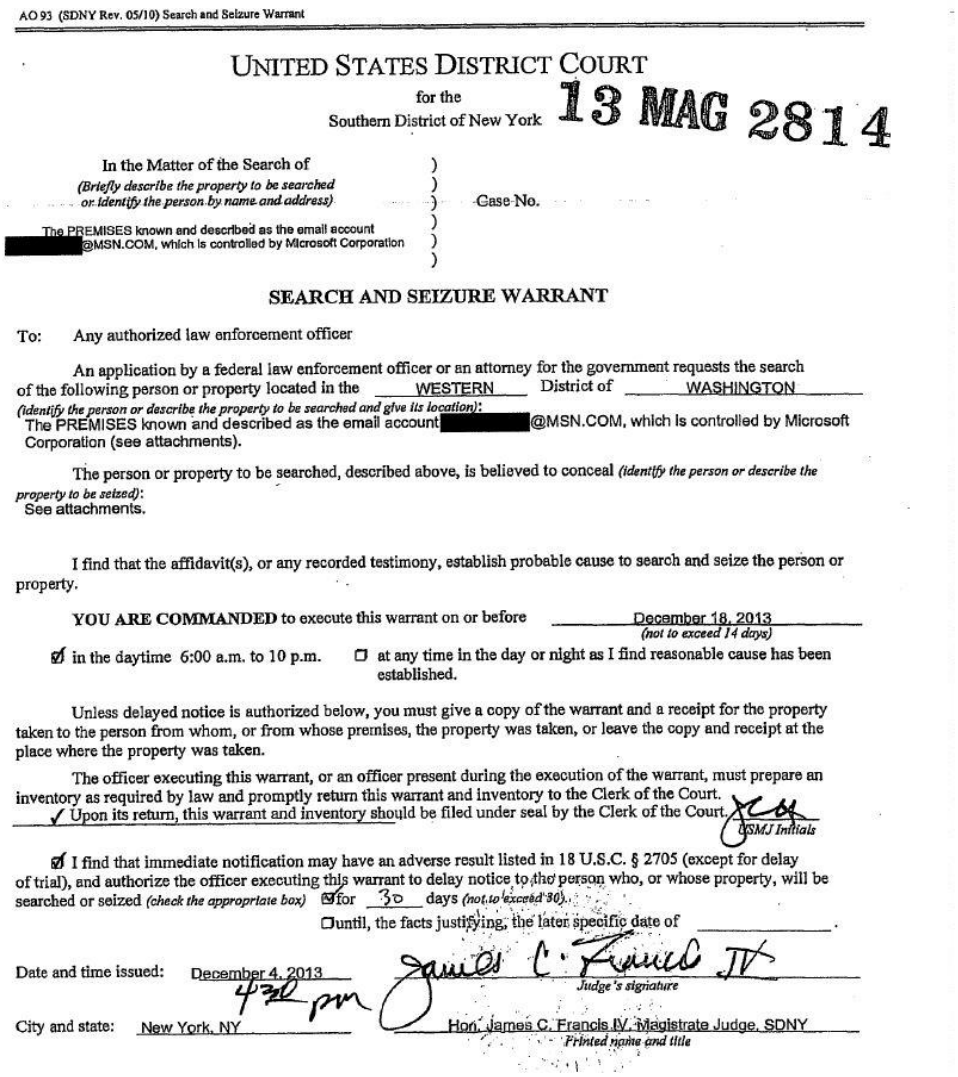
Terminologie I

- Comity Analysis: US-richterliche Abwägung, ob ausländisches Recht und Abkommen beachtet werden müssen
- CLOUD Act: Clarifying Lawful Overseas Use of Data Act
- CSP: Cloud Service Provider
- DoJ: Department of Justice
- Executive Agreement: Bilaterales Rechtshilfeabkommen gemäss CLOUD Act
- ECPA: Electronic Communications Privacy Act
- MLAT: Internationales Rechtshilfeverfahren (zivil- oder strafrechtlich)
- Quash: Aufheben (lassen) [einer Anordnung]

Terminologie II

- QFG: Qualifying foreign government = Land, welches ein Executive Agreement abgeschlossen hat
- SCA: Stored Communications Act
- Subpoena: Behördliche Aufforderung (z.B. Herausgabeverfügung)
- U.S.C.: United States Code
- US-Person: Natürliche oder juristische Person, die Staatsbürger der USA ist oder dort ansässig ist. Je nach US-Gesetz kann der Begriff aber eine andere Bedeutung haben.
- Warrant: Behördliche Massnahme (z.B. Durchsuchungsbefehl)

US-Amerikanische Verwaltung vs. Microsoft



AO 93 (SDNY Rev. 05/10) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of New York

13 MAG 2814

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation

Case No.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the WESTERN District of WASHINGTON
(identify the person or describe the property to be searched and give its location):
The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation (see attachments).

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See attachments.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before December 18, 2013 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.

✓ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court. *USMJ Initials*

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☑ for 30 days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: December 4, 2013 4:30 pm

Judge's signature

City and state: New York, NY

Hon. James C. Francis IV, Magistrate Judge, SDNY
Printed name and title

Hintergrundinformationen I

- Aufhänger für den Erlass des CLOUD Acts ist ein Streit aus dem Jahr 2013 über den Zugriff von US-Strafverfolgern auf Daten auf einem Microsoft Server in Irland
- E-mail-Austausch von zwei auf amerikanischem Boden handelnden Drogendealern, der auf Servern von Microsoft in Irland gespeichert war
- Microsoft überreichte den in den USA gespeicherten Teil der Nachrichten, weigerte sich aber, auch auf Servern in Irland gespeicherte Daten auszuhändigen
- Vor dem Berufungsgericht hatte Microsoft bereits Recht erhalten, das Berufungsgericht war der Auffassung, der SCA finde keine Anwendung für Fälle mit Datenhaltung im Ausland

Hintergrundinformationen II

- Begründung: Verfügungen gestützt auf SCA sind nicht gültig/vollstreckbar ausserhalb der USA
- US-Verwaltung ging an den Supreme Court, zog ihr Rechtsmittel nach Erlass des CLOUD Act zurück
- Unentschieden, inwiefern die US-amerikanische Verfassung (Fourth Amendment) und SCA auf diesen und ähnlich gelagerte Fälle Anwendung gefunden hätten
- CLOUD Act schafft rechtliche Grundlage für den extraterritorialen Zugriff
- CLOUD Act löst "Problem" der US-amerikanischen Administration in Bezug auf Daten von "US-Persons". Zugriff auf Daten ermöglicht, die zuvor nach US-amerikanischem Recht nicht rechtmässig zugänglich waren

The Washington Post

National Security

Supreme Court grapples with access to globalized data in U.S. investigations

By Ellen Nakashima

February 27

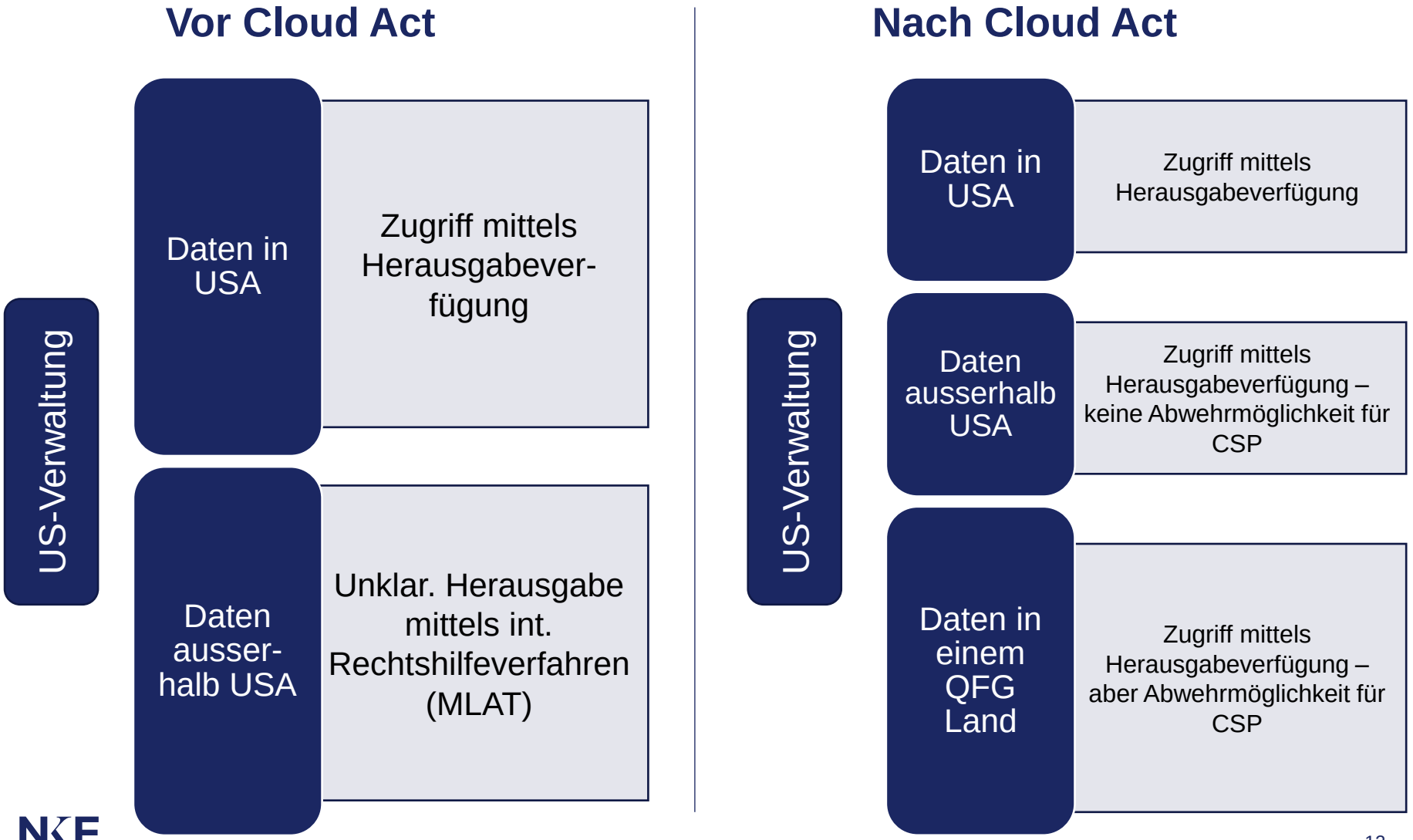
The Supreme Court on Tuesday wrestled with a digital-age legal quandary: Can the U.S. government use a warrant to compel a U.S. company — in this case, Microsoft — to turn over data stored in a server overseas?

The case has far-reaching implications for law enforcement, which relies on access to emails and other data in criminal investigations, and the U.S. tech industry, which needs the trust of foreign governments to operate globally.

Anwendungsbereich I

- Der CLOUD Act dient der Aufklärung von Straftaten
- US-Strafverfolgungsbehörden können gestützt auf den CLOUD Act mittels Herausgabeverfügungen oder Ermittlungsanordnungen Informationen von CSP mit US-Bezug erlangen, die diese im Ausland speichern
- Keine Pflicht der CSP automatisch Kundendaten an US-Ermittlungsbehörden herauszugeben
- Begriff des "US-Bezuges" (*subject to the jurisdiction of the United States of America*) ist sehr weit gefasst: Interpretation und Qualifikation untersteht der Kompetenz der US-Gerichte
- Neu Zugriff unter Umgehung der internationalen Rechtshilfeabkommen

Anwendungsbereich II



Welche Daten sind betroffen?

- Section 3, §2713: Required preservation and disclosure of communications and records:

  "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States".

- Viele Definitionen im ECPA
- Sämtliche Kommunikationsdaten über Kunden, die mit einer Warrant/Subpoena herausverlangt werden können
- Speicherungsort der Daten ist unabhängig vom Server Standort (USA und Ausland)
- Kommunikationsdaten, die "in possession, custody or control" des CSP sind

Welche CSP sind betroffen? I

- *“A provider of electronic communication service or remote computing service … subject to jurisdiction of the United States”*
- Betroffen sind:
  - Anbieter elektronischer Kommunikationsdienste (wie E-Mail, Social Media) und "remote computing"-Angebote (Cloud)
  - Soweit diese der US-amerikanischen Jurisdiktion unterstehen
- Was bedeutet “US-amerikansiche Jurisdiktion”?
  - Gericht muss “personal jurisdiction” über den Provider haben
  - Vorliegen von “minimum contacts” zur USA (International Shoe vs. Washington, 326 US 310 (1945))
  - US-amerikanisches Gericht entscheidet gestützt auf US-amerikanische Rechtsprechung, ob solche “minimum contacts” vorliegen

Welche CSP sind betroffen? II

- "Minimum contacts" Test:
  - *“…defendant has sufficient contacts with the forum such that maintaining the suit in that forum does not offend “traditional notions of fair play and substantial justice”.*
- "Minimum contacts" kann daher vieles heissen:
  - Holdinggesellschaft in den USA
  - Tochtergesellschaft in den USA
  - Zweigniederlassung in den USA
  - Werbung, die an US-Amerikaner gerichtet ist
  - Etc.
- Plixer International, Inc. v. Scrutinizer GmbH Fall: US-Umsatz hat gereicht

NKF

Abwehren von US-Cloud warrants und subpoenas? I

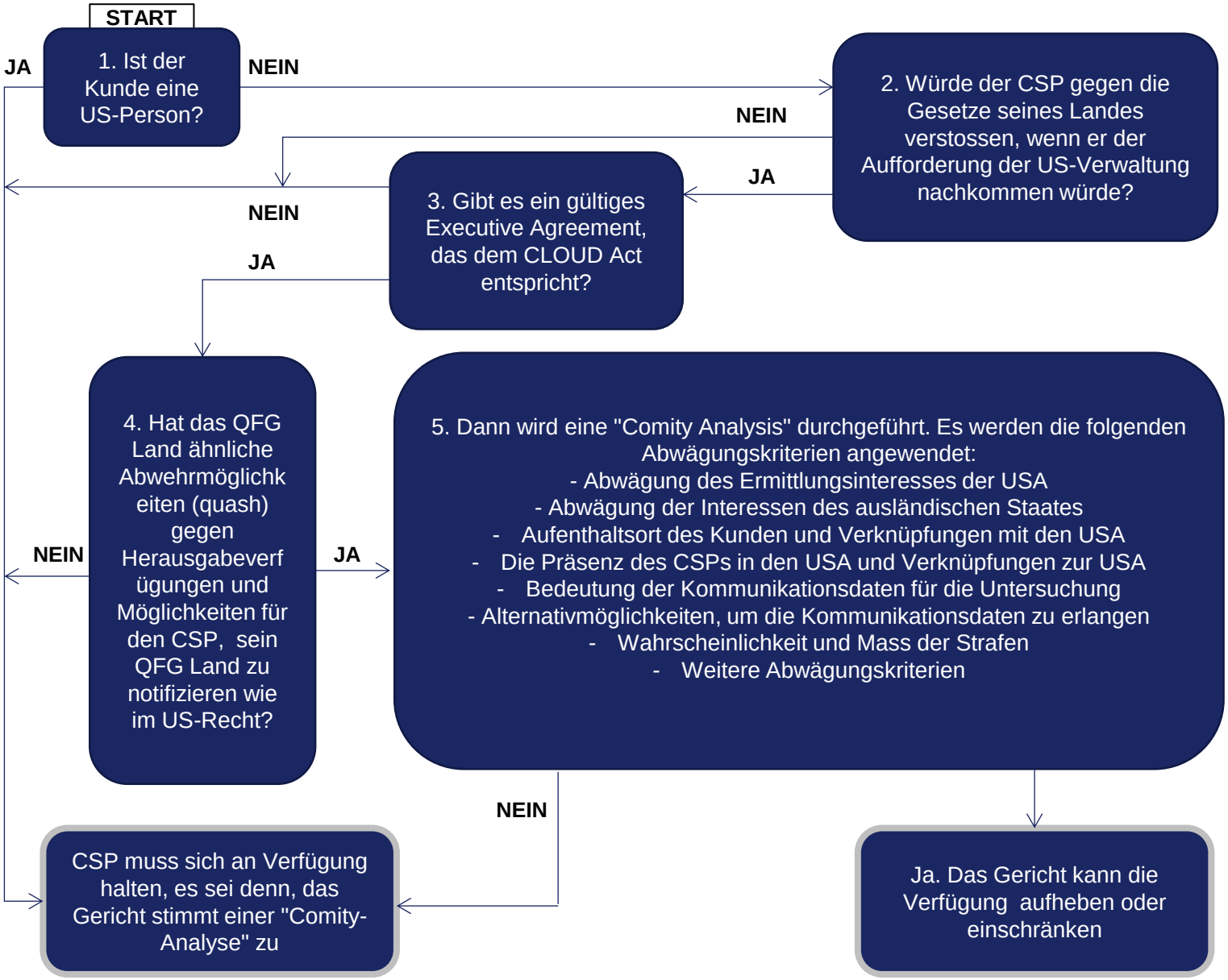
- Was sind warrants und subpoenas?
  - Subpoena: Eine mit einer Sanktion versehene Aufforderung an eine Person, eine im Rahmen eines Verfahrens relevante Handlung vorzunehmen, z.B. Dokumente herauszugeben (wie eine Herausgabeverfügung) oder zu einem Termin zu erscheinen (wie eine Vorladung).
  - Warrant: Eine Massnahme, die einer Behörde erlaubt, ohne Mitwirkung der Person, um die es geht, eine Handlung vorzunehmen, d.h. in deren geschützte Rechtsposition einzugreifen (wie Durchsuchungs- oder Haftbefehl).

Abwehren von US-Cloud warrants und subpoenas? II

- Keine Abwehrmöglichkeit der betroffenen Person/des Kunden gegen einen Herausgabebefehl, da nicht Partei
- Begrenzte Abwehrmöglichkeiten des Providers:
  - bei Nachweis, dass subpoena/warrant sich gegen Personen richtet, die "not a US-Person" sind und die sich nicht in den USA aufhalten und
  - wenn Datenherausgabe eine Verletzung nationalen Rechts hervorruft (z.B. in CH: Art. 271 und 273 StGB)
- Abwehrmöglichkeiten gelten nur, wenn das betreffende Land, dessen nationales Recht verletzt wird, ein bilaterales Rechtshilfeabkommen (Executive Agreement) mit den USA geschlossen hat

Abwehren von US-Cloud warrants und subpoenas? III

- US-Gericht führt sogenannte "Comity Analysis" durch:
  - Liegt Verstoss gegen das internationale "comity" vor?
  - Ist das betroffene Land eine sogenannter QFG, d.h. hat einen bilateralen Vertrag (Executive Agreement) abgeschlossen?
  - Bietet das QFG Land reziproke Rechte?
  - Abwägung des Ermittlungsinteresses der USA
  - Abwägung der Interessen des ausländischen Staates
  - Bedeutung der Kommunikationsdaten für die Untersuchung
  - Alternativmöglichkeiten, um die Kommunikationsdaten zu erlangen
  - Wahrscheinlichkeit und Mass der Strafen, etc.
- Nur wenn "Comity Analysis" ergibt, dass Datenübermittlung unbillig ist, wird Anordnung aufgehoben oder abgeändert


START
1. Ist der Kunde eine US-Person?
JA
NEIN
2. Würde der CSP gegen die Gesetze seines Landes verstossen, wenn er der Aufforderung der US-Verwaltung nachkommen würde?
NEIN
JA
3. Gibt es ein gültiges Executive Agreement, das dem CLOUD Act entspricht?
NEIN
JA
4. Hat das QFG Land ähnliche Abwehrmöglichkeiten (quash) gegen Herausgabeverfügungen und Möglichkeiten für den CSP, sein QFG Land zu notifizieren wie im US-Recht?
NEIN
JA
5. Dann wird eine "Comity Analysis" durchgeführt. Es werden die folgenden Abwägungskriterien angewendet:
- Abwägung des Ermittlungsinteresses der USA
- Abwägung der Interessen des ausländischen Staates
- Aufenthaltsort des Kunden und Verknüpfungen mit den USA
- Die Präsenz des CSPs in den USA und Verknüpfungen zur USA
- Bedeutung der Kommunikationsdaten für die Untersuchung
- Alternativmöglichkeiten, um die Kommunikationsdaten zu erlangen
- Wahrscheinlichkeit und Mass der Strafen
- Weitere Abwägungskriterien
NEIN
CSP muss sich an Verfügung halten, es sei denn, das Gericht stimmt einer "Comity-Analyse" zu
Ja. Das Gericht kann die Verfügung aufheben oder einschränken

Exkurs: Bilateraler Vertrag USA-CH I

- Eckpunkte des Bilateralen Vertrages werden im CLOUD Act vorgegeben
- Nationales Recht des "qualifying foreign government" muss:
  - "Robustes" System zum Datenschutz und den Verfahrensrechten vorsehen
  - Zureichende Massnahmen ergreifen, um das Sammeln und Verbreiten von Informationen über "US-Persons" zu minimieren
  - Unterbinden, dass Verfügungen gestützt auf den Bilateralen Vertrag in unlauterer Art und Weise "US-Persons" zur Zielscheibe haben, US-Recht absichtlich zu verletzen, etc.
  - Den USA gegenseitige Rechte einräumen
- Genehmigungsverfahren durch Attorney General des Bilateralen Vertrags sehr aufwendig

Exkurs: Bilateraler Vertrag USA-CH II

- CLOUD Act zwingt Provider sich zu entscheiden entweder sein nationales Recht oder US-Recht zu verletzen
- Ohne Abschluss Verletzung von Schweizer Recht und Internationalen Abkommen:
  - Art. 271 und 273 StGB (Blocking Statutes)
  - Art. 6 DSG, Art. 48 DSGVO
  - Art. 27 IRSG
  - Cyber Crime Convention
  - Mutual Legal Assistance Treaty CH-USA
  - Swiss-US Privacy Shield
- Analoges Beispiel: CH-USA Abkommen für die Herausgabe von Daten der UBS an die IRS

Exkurs: Bilateraler Vertrag USA-CH III

- Vorteile des Abschluss eines Executive Agreements:
  - Einsprachemöglichkeiten für Schweizer CSP und natürliche Personen/Kunden
  - Direkter Zugriff auf US-Server für Schweizer Behörden unter gleichen Voraussetzungen – unter Umgehung des int. Rechtshilfeverfahren
  - Keine Verletzung von Schweizer Recht und internationalen Abkommen
- Erstes Executive Agreement zwischen UK und USA in Verhandlung: Link

Exkurs: Bilateraler Vertrag USA-CH IV

US and UK Governments propose a series of bilateral agreements between jurisdictions

1. Creating a less bureaucratic conduit for cross-border requests
2. Recognising common, high standards of rule of law and judicial independence
3. Lifting legal barriers to compliance where requests are made under an agreement – but not creating a compulsion to comply
4. Clearly specifying the scope of requests which are permitted
5. Excluding requests where the receiving party has an interest (e.g. targeting of people in their territory)
6. Providing a dispute resolution mechanism

Reaktionen auf Cloud Act

- Joint Letter von Apple, Facebook, Google, Microsoft, and Oath (Yahoo!) am 6. Februar 2018:

  “The new Clarifying Lawful Overseas Use of Data (CLOUD) Act reflects a growing consensus in favor of protecting Internet users around the world and provides a logical solution for governing cross-border access to data. Introduction of this bipartisan legislation is an important step toward enhancing and protecting individual privacy rights, reducing international conflicts of law and keeping us all safer.”

- Microsoft begrüsst CLOUD Act, verlangt aber in einem Katalog mit 6 Prinzipien strengere Regeln

- Letter to Congress von 24 Parteien gegen den CLOUD Act am 12. März 2018: Link

- E-Evidence Verordnung der EU: Alternativvorschlag für europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen

Was gilt es bei Verträgen mit CSP zu beachten? I

- Falls nicht schon gemacht – feststellen, wo überall Cloud Daten des Unternehmens gespeichert werden
- Durchsicht bestehender Verträge mit CSP im Hinblick auf Notifikationspflichten bei Datenherausgabe an Dritte und Behörden
- Intern abklären mit den Legal und IT Teams, welche möglichen Auswirkungen der CLOUD Act heute und zukünftig für das Geschäftsmodell des eigenen Unternehmens haben kann
- Interne Taskforce erstellen, um die Entwicklungen betreffend Datenherausgabe gestützt auf CLOUD Act zu beobachten
- Regelmässige Berichte über Entwicklungen an Management / Geschäftsleitung

Was gilt es bei Verträgen mit CSP zu beachten? II

- Abklären, ob der eigene CSP vom CLOUD Act betroffen ist und/oder Stellungnahme vom CSP verlangen
- Falls ja:
  - Allfällige Leitlinien der CSP zum Thema CLOUD Act und geplante Reaktionen auf Herausgabeverfügungen einsehen oder diese verlangen
  - Server Standorte anschauen
  - Verschiedene Datenpool kreieren: Muss alles in die Cloud?
  - Lösungsvorschläge des CSP's ansehen: Treuhand-/Private Cloud
  - Oft Server Standorte nur in der Schweiz oder EU nicht machbar oder praktikabel bei weltweit operierenden Unternehmen

Was gilt es bei Verträgen mit CSP zu beachten? III

- Notifikationspflichten bei Datenherausgabe
- Verschiedene Server Standorte für verschiedene Datenpools
- Starke Verschlüsselung der Daten?
- Andere Lösungsansätze?

Offene Fragen und Ausblick

- Es gibt noch keine Gerichtsurteile gestützt auf den CLOUD Act
- Kann die EU als QFG anerkannt werden? CLOUD Act sieht Executive Agreements nur für einzelne Länder
- Werden viele Staaten den QFG-Status erwerben wollen?
- Wie werden US-Gerichte QFG-Staaten und nicht QFG-Staaten behandeln?
- Wie wird der Konflikt zwischen CLOUD Act und DSGVO (Art. 48) gelöst werden?
- Werden sich die betroffenen CSP an die Herausgabeverfügungen halten? Anfechten?
- Schweiz sollte asap Executive Agreement mit den USA aushandeln

THANK YOU

Your Contact

Clara-Ann Gordon
clara-ann.gordon@nkf.ch
D +41 58 800 84 26

Niederer Kraft Frey Ltd Bahnhofstrasse 53 CH-8001 Zurich T +41 58 800 80 00 F +41 58 800 80 80 nkf.ch