Die Regulierung transatlantischer Datenströme: zwischen Diktat und Blockade?

Andreas Busch

1. Einleitung

Die Nutzung des Internets, sei es zu Zwecken der Arbeit oder aus privatem Interesse, ist in den letzten Jahren völlig alltäglich geworden und heute eine Selbstverständlichkeit.[1] Das gilt zumindest für die Menschen in den entwickelten Ländern der Erde, in denen 64 Prozent Zugang zur Online-Welt haben (ITU 2010).[2] Außerhalb dieser Ländergruppe liegt der Anteil mit lediglich 18 Prozent deutlich niedriger; aber insgesamt lag die Zahl der Menschen mit Internet-Zugang mit 1,7 Milliarden im Jahr 2009 so hoch wie noch nie. Und ein immer größerer Prozentsatz der weltweit 4,6 Milliarden Nutzer von Mobiltelefonen hat ebenfalls (zumindest teilweisen) Zugang zum Angebot des Internets.

Wenn diese Nutzer Nachrichten oder Informationen über Fakten suchen, Geschäfte über das Internet abwickeln, über soziale Netzwerke Nachrichten mit Freunden und Bekannten austauschen, die nächste Reise buchen, ihre Lieblingsmusik kaufen oder eine Vielzahl anderer Tätigkeiten verfolgen, sind sie sich nicht unbedingt bewusst, dass dadurch oft Datenströme über nationale Grenzen hinweg ausgelöst werden; tatsächlich ist das aber so, denn viele Dienstleistungen im IT-Verkehr sind international stark vernetzt. So mag etwa das Reservierungszentrum für eine innereuropäische Flugreise in den Vereinigten Staaten stehen; die Verbuchung einer Überweisung bei einer in Deutschland beheimateten Bank über einen IT-Dienstleister etwa in Irland vorgenommen werden; oder die Abwicklung des Geschäftsauftrages eines in Großbritannien beheimateten internationalen Unternehmens über einen firmeneigenen Server erfolgen, der in Indien steht. Solche (vermutlich täglich in die Millionen gehenden und für das moderne Wirtschaftsle-

1 Dieser Artikel verdankt seine Entstehung u.a. der Unterstützung durch ein vom *Economic and Social Research Council* finanziertes Forschungsprojekt zum Thema „Coping with innovation: The political regulation of personal information in comparative perspective“ (RES-062-23-0536) sowie zahlreichen Diskussionen mit einer Vielzahl von Kolleginnen und Kollegen über einen ungewöhnlich langen Zeitraum. Erste Schritte zur Analyse der hier betrachteten Fragen wurden bei der Konferenz “Safety & Security in a Networked World: Balancing Cyber-Rights & Responsibilities” am Oxford Internet Institute (8.-10. September 2005) vorgelegt und diskutiert; analytische und inhaltliche Ausweitungen wurden dann bei Tagungen und Vorträgen an den Universitäten Edinburgh, Freie Universität Berlin, am Department of Politics and International Relations der University of Oxford sowie am Wissenschaftszentrum Berlin für Sozialforschung (WZB) präsentiert. Für Hilfen und Diskussionen bei der Erstellung der hier vorgelegten Fassung gilt mein besonderer Dank Dr. Tobias Jakobi (Universität Göttingen).

2 Vgl. ITU 2010: (ix-1) hierzu und zu den folgenden Angaben. Genauere statistische Daten auf Länderbasis finden sich in World Bank (2011). In Deutschland sind laut einer Mitteilung des Industrieverbandes BITKOM vom April 2011 rund 51 Mio. Bürger online; das entspricht 72 Prozent der Altersgruppe über 14 Jahren (http://www.bitkom.org/de/presse/8477_67654.aspx, 12.4.2011).

ben längst unverzichtbaren[3]) Transaktionen lösen also Datenströme aus, die nationale Grenzen und damit oft auch die Grenzen von Jurisdiktionen überschreiten. Doch die übermittelten Daten sind oft schützenswert, sei es, weil sie von hohem wirtschaftlichem Wert sind oder weil sie personenbezogen sind und deshalb Datenschutzerfordernissen unterliegen. Das Schutzniveau für solche Daten kann sich zwischen unterschiedlichen Jurisdiktionen aber deutlich unterscheiden. Der internationale Datenverkehr bedarf also länderübergreifender Regeln. Die Erstellung solcher Regeln ist das Thema dieses Aufsatzes.

Der vorliegende Beitrag beschreibt und analysiert die Konflikte, Verhandlungen und Übereinkünfte im Bereich der Regulierung des transatlantischen Datenverkehrs seit Mitte der 1990er Jahre. Dabei geht es konkret um die Verhandlungen zwischen den USA und der Europäischen Union sowie um die unterschiedlichen Interessen, Akteurkonstellationen, Druckmittel sowie die jeweiligen Perspektiven auf das Problem des Schutzes der dabei übermittelten (oft personenbezogenen) Daten. Die Darstellung fußt auf einer Reihe von Fallstudien – dem ‚Safe Harbor'-Abkommen, den Verhandlungen über die Übermittlung von Flugpassagierdaten sowie den Streitigkeiten über den Zugriff auf Daten über Finanztransaktionen im Rahmen des SWIFT-Netzwerkes –, die in den letzten anderthalb Jahrzehnten die empirische Realität dieses Themas gebildet haben. Sie sind die Grundlage der hier vorgenommenen Analyse.

In der politikwissenschaftlichen Literatur ist das Thema des transatlantischen Disputs über die Regulierung des Austauschs personenbezogener Daten bisher nur recht kursorisch behandelt worden. Die vergleichsweise spärliche diesbezügliche Fachliteratur hat sich v.a. auf die Darstellung der Ansätze zur Regulierung von personenbezogenen Daten sowie die in diesem Bereich vorzufindenden Unterschiede zwischen der Europäischen Union und den Vereinigten Staaten von Amerika konzentriert (Shaffer 1999; Zwick u. Dholakia 2001; Whitman 2004). Bei der Analyse konkreter Verhandlungen über die beim transatlantischen Austausch personenbezogener Daten einzuhaltenden Standards sowie ihrer Ergebnisse steht bisher ganz überwiegend der Fall des sogenannten ‚Safe Harbor'-Abkommens im Mittelpunkt des Interesses, das Ende der 1990er Jahre verhandelt wurde, im November 2000 in Kraft trat und sich auf Datenaustausch im damals im Entstehen begriffenen Bereich des elektronischen Handels (*e-commerce*) bezieht (Long u. Quek 2002; Farrell 2003; Regan 2003; Drezner 2004). Doch seit den Terroranschlägen vom 11. September 2001 hat sich der Fokus beim Problem des grenzüberschreitenden Datenaustauschs vom kommerziellen Interesse in Richtung Sicherheit verschoben; im letzten Jahrzehnt haben sich deshalb neue transatlantische Meinungsverschiedenheiten über die Regulierung von grenzüberschreitenden Datenströmen ergeben. Diese sind aber in der Literatur bisher kaum beachtet worden, obwohl sie in einem stark veränderten Kontext stattgefunden haben – und mit deutlich anderen Ergebnissen, als das nach den Analysen zum ‚Safe Harbor'-Abkommen zu erwarten gewesen wäre.[4]

3 Der globale ICT-Markt belief sich im Jahr 2005 auf 3,13 Billionen US-Dollar oder 7,6 Prozent des Welt-BIP, mit einer durchschnittlichen jährlichen Wachstumsrate von 6 Prozent (ITU 2006, S. 70).

4 Ausnahmen sind hier lediglich Heisenberg (2005) und Newman (2008).

Der hier vorgelegte Aufsatz erweitert daher in dreierlei Hinsicht die bisher vorliegenden politikwissenschaftlichen Analysen zum transatlantischen Datenverkehr:

- zum einen nimmt er eine Analyse aller drei bisherigen Konfliktbereiche zu diesem Thema vor, indem er Fallstudien zu den Themen ‚Safe Harbor', Passagierdatenaustausch und Zugriff auf die Finanzdaten von SWIFT integriert;
- zum anderen wird die bisher in der Literatur dominierende theoretische Perspektive eines konstruktivistisch orientierten Erklärungsansatzes um weitere theoretische Ansätze erweitert, um die Ergebnisse der Auseinandersetzungen jenseits des Themas ‚Safe Harbor' besser verstehen zu können;
- und drittens bemüht sich der Aufsatz, auch die innereuropäische Dimension in den Streitigkeiten (d.h. die Konflikte zwischen der Europäischen Kommission und dem Europäischen Parlament) in den Blick zu nehmen, da diese in der Konfliktdynamik der letzten Jahre einen großen Einfluss gespielt haben.

Im ersten Teil des Aufsatzes wird zunächst ein einführender Überblick in die Probleme der Regulierung des Internets unter dem Gesichtspunkt des entstehenden *e-commerce* gegeben, bevor die unterschiedlichen regulativen Ansätze in den Vereinigten Staaten und Europa thematisiert werden. Der zweite Teil des Aufsatzes bildet mit einer Reihe von Fallstudien den empirischen Kern des Beitrages. Zunächst werden die Verhandlungen im Gefolge der EU-Datenschutz-Richtlinie von 1995 geschildert, die im ‚Safe Harbor'-Abkommen endeten. Es folgen zwei weitere Fallstudien zu den Themen Austausch von Passagierdaten und Zugriff auf Bestände des Finanzdienstleisters SWIFT, bevor im dritten Teil des Aufsatzes theoretische Perspektiven auf das Thema im Mittelpunkt stehen. Hier wird zunächst kurz der politikwissenschaftliche Forschungsstand zum Thema resümiert und dann argumentiert, dass eine Ausweitung der bisher dominierenden analytischen Perspektive notwendig ist, die insbesondere die Wichtigkeit institutioneller Faktoren in Betracht zieht. In einem letzten Teil wird dann der Einfluss sich ändernder Akteurkonstellationen untersucht. Zum Schluss des Beitrags wird argumentiert, dass eine auf institutionelle und machtpolitische Faktoren abstellende Analyse am besten geeignet ist, die drei Fälle von Streitigkeiten über die Regulierung transatlantischer Datenströme zusammenfassend zu erklären.

2. Die Regulierung des Internet

Heute sehen wir im Internet vor allem ein Medium für kommerzielle Transaktionen (*e-commerce*) und für sozialen Austausch; doch die Ursprünge dieses weltweiten Kommunikationsmediums liegen auf einem ganz anderen Gebiet. Zu Beginn der 1970er Jahre initiierte DARPA (der auf Forschung spezialisierte Teil des U.S.-Verteidigungsministeriums, die *Defense Advanced Research Projects Agency*) Arbeiten an einem dezentralisierten Kommunikationssystem das – im Kontext des damaligen Kalten Krieges essentiell – auch einen massiven, möglicherweise nuklearen Angriff unbeschadet würde überstehen können. Dazu war die Erstellung einer dezentralen Kommunikationsstruktur von größter Wichtigkeit. Mitte der 1980er Jahre förderte dann die *National Science Foundation* (NSF) der Vereinigten Staaten die Weiterentwicklung dieser Kommunikations-Infrastruktur zu Zwe-

cken der Forschung, indem sie die nationalen Hauptforschungszentren mit ihren lokalen Netzwerken miteinander verband. Das Ergebnis wurde schließlich als das ‚Internet' bekannt.[5] Diese Entwicklungen wurden damals von einer kleinen Gemeinschaft technisch kompetenter Experten vorangetrieben, und es gab daher wenig Bedarf für Regulierung. Die wenigen Regeln, die es gab, entsprangen einem egalitären Diskussionsprozess mit allgemeiner Teilhabe;[6] Beziehungen basierten vor allem auf Vertrauen; und die existierenden Hierarchien in der Verwaltung des Netzes auf anerkannter Expertise.

In den frühen 1990er Jahren, als die Nutzung des Internet zu wachsen begann (allerdings damals noch unter Namen wie ‚Global Information Infrastructure' [GII] und ‚information superhighway'), träumte die Gründergeneration des Internet von einer Entwicklung des langsam die Welt umspannenden Kommunikationsnetzes ohne Staatseinfluss und Regulierung. Organisationen wie die ‚Electronic Frontier Foundation' (EFF), 1990 von Technologieexperten und Vertretern der Alternativbewegung gegründet, beschworen bewusst die Mythen der Gründerväter der Vereinigten Staaten herauf, wenn sie in Anlehnung an die Landgewinnung im damaligen Westen von einer ‚digital frontier' sprachen und von der Verteidigung der Rechte des Einzelnen im neuen ‚cyberspace'. Ihre utopischen Ideen sahen in dem neuen Medium ein Mittel zur Verbesserung der Welt sowie zur Ausweitung der individuellen Freiheit, und sie lehnten eine von außen aufgezwungene Regulierung ab. John Perry Barlow, Gründungsmitglied der EFF und Texter der Kultband *The Grateful Dead* in den 1960er Jahren, formulierte diesen Geist beispielhaft in der „Unabhängigkeitserklärung des Cyberspace" im Jahr 1996, als Kommerzialisierung und aufgezwungene Regelsetzung den bis dahin vorherrschenden Geist der Freiheit bedrohte:

> „Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind.
>
> On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> […]
>
> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks.
>
> I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us.
>
> You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear." (Barlow 1996)

Doch weder die Eloquenz dieses noch diejenige vergleichbarer anderer Manifeste konnten die schließlich stattfindende staatliche Regulierung des ‚cyberspace' ver-

5 Ein kurzer geschichtlicher Überblick zur technischen Entwicklung des Internet findet sich z.B. bei http://www.isoc.org/internet/history/ [Zugriff 19. Juli 2005]. Instruktiv ist auch das Buch von Hafner u. Lyon (2000).

6 Hier sind vor allem die „Requests for Comments" (RFC) zu nennen. Mehr hierzu unter http://de.wikipedia.org/wiki/Request_for_Comments [Zugriff 25. Juli 2011].

hindern[7]. Hauptgrund dafür war, dass das Internet einfach zu wichtig wurde, als dass Staaten es weiter hätten ignorieren können. Denn zwischen dem Internet und staatlichen Regeln und Gesetzen gab es eine Menge Reibungsflächen. Im Jahr 1996 etwa gab ein Gericht in New York dem Antrag der in den Vereinigten Staaten beheimateten Zeitschrift *Playboy* gegen eine italienische Firma statt, die eine Website unter dem Namen *Playmen* betrieb. *Playboy* hatte argumentiert, dass diese Website für Besucher aus den Vereinigten Staaten zugänglich sei und somit ein Gerichtsurteil aus dem Jahr 1981 unterlaufe, das der italienischen Firma den Vertrieb ihrer Zeitschrift *Playmen* in den Vereinigten Staaten aus markenrechtlichen Gründen untersagte. Die italienische Firma wurde verpflichtet, ihre Website dahingehend zu modifizieren, dass alle Zugriffsversuche von Benutzern aus den Vereinigten Staaten zurückgewiesen würden. Im Jahr 2000 urteilte ein französisches Gericht, dass die in den Vereinigten Staaten ansässige Firma *Yahoo!* französische Bürger am Zugang zu Websites hindern müsse, auf denen Versteigerungen von Nazi- und Ku Klux Klan-Andenken durchgeführt wurden, da ein französisches Gesetz den Verkauf und das Anpreisen von zum Rassismus anstachelnden Gütern verbiete. Ebenso übten deutsche Stellen Druck auf das U.S.-Internet-Auktionshaus *eBay* aus, keine Nazi-Andenken zu verkaufen – obwohl dies in den Vereinigten Staaten (aus Gründen von *freedom of speech*) durchaus legal ist. Beide U.S.-Firmen fügten sich schließlich den Anforderungen, obwohl *Yahoo!* sich zunächst durch ein U.S.-Gericht bestätigen ließ, dass das französische Urteil nicht vollstreckbar sei. Danach jedoch verbot die Firma *allen* ihren Kunden den Handel mit Nazi-Andenken und behauptete zudem, dies habe nichts mit den juristischen Drohungen aus Frankreich zu tun (u.a. einer Strafe von pro Tag 100.000 Französischen Francs bei Missachtung des Urteils).[8] Sowohl *Yahoo!* wie auch *eBay* erwarteten wahrscheinlich, dass sie durch nachteilige Öffentlichkeitswirkung und Gerichtskosten mehr verlieren würden, als sie durch den Verkauf dieser Güter erlösen könnten, und dass die Konzentration auf den Verkauf unkontroverser Güter gekoppelt mit einer Ausweitung ihrer Geschäfte sowohl in den Vereinigten Staaten wie in Europa eine klügere Geschäftsstrategie sei. Denn der elektronische Handel war ab Ende der 1990er Jahre einer der am raschesten wachsenden Geschäftszweige überhaupt: So wuchs der elektronische Einzelhandel beispielsweise im ersten Quartal 2004 mit einer Rate von 28,1 Prozent, während diese im konventionellen Handel lediglich 8,8 Prozent betrug; der gesamte Verkauf über das Internet betrug in Europa im Jahr 2001 bereits 86 Mrd. Dollar, und in den Vereinigten Staaten 120 Mrd. Dollar im Jahr 2004; bezieht man Handel zwischen den Unternehmen ein (*business-to-business*), so betrug der gesamte *e-commerce* im Jahr 2001 in den Vereinigten Staaten 1080 Mrd. Dollar und 430 Mrd. Dollar in der Europäischen Union.[9]

7 Aktueller Überblick zum Thema Regulierung des Internets bei Murray (2007).

8 Einzelheiten zu diesem Fall finden sich z.B. bei BBC News (2000) wo sich auch weitere Verweise finden. Generell zur Analyse der Rolle des Staates bei der Regulierung des Internet siehe auch Drezner (2004).

9 Alle Daten nach UNCTAD (2004) und The Economist (15. Mai 2004, S. 9).

3. Unterschiedliche Ansätze im Datenschutz

Angesichts des im vorangegangenen Abschnitt beschriebenen Ausmaßes an wirtschaftlichen Werten ist es verständlich, dass der Zugang zu den elektronischen Märkten des jeweils anderen sowohl für die Vereinigten Staaten wie für die Europäische Union von größter Wichtigkeit war. Doch das Problem unterschiedlicher gesetzlicher und regulativer Regeln stellte sich mit neuer Schärfe im Kontext der kommerziellen Nutzung des Cyberspace, bei der grenzüberschreitende Transaktionen den Kontrast zwischen dem grenzenlosen Wirtschaftsraum einerseits und den territorial gebundenen Rechtsräumen andererseits besonders akzentuieren. Und da *e-commerce* zu einem erheblichen Teil auf dem Austausch von Informationen beruht, war das Problem besonders akut im Bereich von Datenschutz und *privacy*, wo auf beiden Seiten des Atlantiks substantiell unterschiedliche Regulierungsansätze zur Anwendung gekommen waren.[10]

In den Vereinigten Staaten ist der Schutz von *privacy* durch gesetzliche Regelungen nicht sehr hoch entwickelt. Trotz einer seit langem anhaltenden Debatte über das Thema (die ihren Ausgangpunkt im späten 19. Jahrhundert mit dem wegweisenden Artikel von Warren u. Brandeis (1890) nahm) wird die gesetzliche Situation von Kennern als „Patchwork-Decke" (Holvast et al. 1999, USA-1), „dünnes Flickwerk" (Froomkin 2000, S. 1539) bzw. als „fragmentiert, *ad hoc* und eng auf spezifische Sektoren und Probleme ausgerichtet" (Shaffer 1999, S. 422) beschrieben.[11] Da es keine umfassende Datenschutz-Gesetzgebung gab und man in den Vereinigten Staaten auch nicht gewillt war, eine solche zu erlassen, gleichzeitig jedoch erkannte, dass Schutz von Daten und Privatsphäre notwendige Voraussetzung für einen Erfolg von *e-commerce* waren, setzte das Land auf den Ansatz von Selbstregulierung durch die Industrie. Das „Framework for Global Electronic Commerce", von Präsident Clinton und Vize-Präsident Gore verfasst und im Juli 1997 vom Weißen Haus veröffentlicht, drückt es wie folgt aus:

> "Americans treasure privacy, linking it to our concept of personal freedom and well-being. Unfortunately, the GII's great promise – that it facilitates the collection, re-use, and instantaneous transmission of information – can, if not managed carefully, diminish personal privacy. It is essential, therefore, to assure personal privacy in the networked environment if people are to feel comfortable doing business. […]
>
> The Administration supports private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes. These include mechanisms for facilitating awareness and the exercise of choice online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution." (Clinton u. Gore 1997)

10 Siehe zur Analyse der Differenzen etwa Reidenberg (2000); Whitman (2004) oder Feick u. Werle (2010, S. 535-537). Ein Überblick über die Regulierung von *privacy* findet sich bei Busch (2011a).

11 Alle Zitate aus dem Englischen sind vom Autor übersetzt. Umfassendere Darstellungen und Vergleiche internationaler privacy-Regulierungen finden sich bei Michael (1994) und Electronic Privacy Information Center and Privacy International (2004).

In Europa hingegen wählte man mit nationalstaatlicher und supranationaler Regulierung einen deutlich anderen Ansatz. Ab den frühen 1970er Jahren hatten Länder wie die Bundesrepublik Deutschland, Schweden, Frankreich und Dänemark begonnen, Gesetze zum ‚Datenschutz' zu erlassen, und diese Art der Gesetzgebung hatte sich über den ganzen Kontinent verbreitet. Sie zielte darauf ab, Gefährdungen der Privatsphäre zu verhindern, die durch die Einführung von computergestützten Technologien – wie etwa umfassender Datenbanken – entstehen könnten, und stellten das Recht auf den Schutz der eigenen Daten in den Mittelpunkt.[12] Diese Schutzregimes unterschieden sich jedoch von Land zu Land in der Europäischen Union, was ein potentielles Hindernis sowohl für den Handel zwischen ihnen wie für die Entwicklung des *e-commerce* darstellen konnte.

Dieses Problem wurde im Umfeld der Vollendung des europäischen Binnenmarktes in den frühen 1990er Jahren besonders relevant. Nach fünfjährigen Verhandlungen wurde deshalb im Oktober 1995 die Richtlinie 95/46/EU „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" verabschiedet, die im Oktober 1998 in Kraft trat. Die Richtlinie stellte klar, dass die Mitgliedsstaaten forthin „aufgrund des gleichwertigen Schutzes, der sich aus der Angleichung der einzelstaatlichen Rechtsvorschriften ergibt, den freien Verkehr personenbezogener Daten zwischen ihnen nicht mehr aus Gründen behindern, die den Schutz der Rechte und Freiheiten natürlicher Personen und insbesondere das Recht auf die Privatsphäre betreffen" (Präambel Abschnitt 9), führte aber gleichzeitig Bestimmungen ein, die die Übertragung solcher Daten in Drittländer (d.h. Länder ausserhalb der EU) von der dort existierenden „Angemessenheit des Schutzniveaus" abhängig machten (Artikel 25). Mit anderen Worten erleichterte die Richtlinie den Handel *innerhalb* der EU, doch konnte sie für den elektronischen Handel mit Staaten *außerhalb* der EU (wie etwa den Vereinigten Staaten) ein ernsthaftes Hindernis darstellen, sollten ihre Datenschutzbestimmungen als nicht angemessen bewertet werden.

4. Fallstudien zur Regulierung von Datenübertragungen

4.1 Transatlantischer Datenstreit I: e-commerce und das ‚Safe Harbor'-Abkommen

Die unterschiedlichen Regulierungsphilosophien, die Initiative zum Erlass einer EU-Richtlinie für den Datenschutz und das mit Verve entstehende Feld des elektronischen Handels bildete, wie in den voranstehenden Abschnitten gezeigt, den Hintergrund für den ersten transatlantischen Disput zur Angleichung der Regulierung in diesem Bereich. Angesichts der engen Handels- und Wirtschaftsverflechtungen zwischen der EU und den Vereinigten Staaten hätte man erwarten können, dass Verhandlungen über das Thema des transatlantischen Datenverkehrs unmittelbar nach Verabschiedung der Datenschutz-Richtlinie im Jahr 1995 aufgenommen worden wären. Dies war jedoch nicht der Fall. Vielmehr gingen die Vereinigten Staaten zunächst wie selbstverständlich davon aus, dass die Ausnahmeklausel des Artikels 26 der Richtlinie den Datenverkehr ohne Probleme gewährleisten würde. Zu ernst-

12 Überblicke über die gesetzlichen Entwicklungen in diesem Bereich in Europa finden sich bei Mayer-Schönberger (1997) sowie bei Bennett (1992), insbesondere in den Tabellen auf S. 57 und 59.

haften Diskussionen kam es erst in der ersten Hälfte des Jahres 1998, als die U.S.-Regierung gewahr wurde, dass dem eventuell nicht so sein könnte.

Die Verhandlungspositionen beider Seiten waren zunächst durch ein Beharren auf der eigenen Position sowie die Erwartung gekennzeichnet, dass die jeweils andere Seite den eigenen Regulierungsansatz übernehmen solle. Die EU-Vertreter ließen erkennen, dass ihrer Ansicht nach nur die Einführung entsprechender formeller gesetzlicher Regelungen (also eines allgemeinen Datenschutzgesetzes) und Aufsichtsbehörden (also des Äquivalents eines Datenschutzbeauftragten) durch die USA ein angemessenes Schutzniveau für Daten sicherstellen könne. Die Vereinigten Staaten verfolgten hingegen weiter ihre im oben zitierten „Framework" niedergelegte Strategie des Vertrauens auf unabhängige Zertifizierungsstellen für den Schutz der Privatsphäre. Diese sollten Websites mit einem Gütesiegel ausstatten, und man erwartete – wie es der für die *e-commerce*-Politik zuständige Berater des Weißen Hauses, Ira Magaziner, ausdrückte – dass eine internationale Verbreitung dieses Ansatzes schließlich die Meinungsverschiedenheiten mit der Europäischen Union hinfällig machen werde (Farrell 2003, S. 288). Doch selbst in den Vereinigten Staaten war der Selbst-Zertifizierungs-Ansatz nur von sehr mäßigem Erfolg gekrönt: nur wenige Firmen beantragten eine Zertifizierung ihrer Websites durch Gütesiegel-Agenturen wie TRUSTe oder BBBOnline, was natürlich die Skepsis über die Wirksamkeit des amerikanischen Selbstregulierungs-Ansatzes noch weiter bestärkte.

Tabelle 1: 'Safe Harbor'-Verpflichtungen (Europäische Kommission 2000)

Informationspflicht: Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen.
Wahlmöglichkeit: Die Organisation muss Privatpersonen die Möglichkeit geben zu wählen (‚opt out'), ob ihre personenbezogenen Daten (a) an Dritte weitergegeben werden sollen oder (b) für einen Zweck verwendet werden sollen, der mit dem ursprünglichen oder dem nachträglich von der betreffenden Person genehmigten Erhebungszweck unvereinbar ist. Der betroffenen Person muss die Ausübung ihres Wahlrechts durch leicht erkennbare und verständliche, leicht zugängliche und kostengünstige Verfahren ermöglicht werden. Bei sensiblen Daten (wie z. B. Angaben über den Gesundheitszustand, über Rassen- oder ethnische Zugehörigkeit, über politische, religiöse oder philosophische Überzeugungen, über die Mitgliedschaft in einer Gewerkschaft oder über das Sexualleben) benötigen die Organisationen die ausdrückliche Zustimmung ('opt in') der betroffenen Personen.
Weitergabe: Eine Organisation darf Daten nur dann an Dritte weitergeben, wenn sie die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwendet. Möchte eine Organisation Daten an einen Dritten weitergeben, der in ihrem Auftrag und auf ihre Anweisung tätig ist, kann sie dies tun, sofern der Dritte entweder dem 'sicheren Hafen' angehört oder der Richtlinie unterliegt, oder von einer anderen Feststellung angemessenen Schutzniveaus erfasst wird oder sich schriftlich in einer Vereinbarung mit der Organisation dazu verpflichtet, zumindest das Maß an Schutz personenbezogener Daten zu

gewährleisten, das in den entsprechenden Grundsätzen des ‘sicheren Hafens’ gefordert wird. Eine Organisation, die diese Forderungen erfüllt, kann nicht haftbar gemacht werden (sofern sie nichts anderes vereinbart hat), wenn ein Dritter, an den sie Daten übermittelt hat, Beschränkungen der Verarbeitung dieser Daten missachtet.

Sicherheit:

Organisationen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, müssen angemessene Sicherheitsvorkehrungen treffen, um sie vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung zu schützen.

Datenintegrität:

In Übereinstimmung mit den Grundsätzen müssen personenbezogene Daten für den beabsichtigten Verwendungszweck erheblich sein. Eine Organisation darf personenbezogene Daten nicht in einer Weise verarbeiten, die mit dem ursprünglichen Erhebungszweck oder mit dem Zweck unvereinbar ist, dem der Betroffene nachträglich zugestimmt hat. In dem für diese Zwecke notwendigen Umfang muss die Organisation durch angemessene Maßnahmen gewährleisten, dass die Daten für den vorgesehenen Zweck hinreichend zuverlässig, genau, vollständig und aktuell sind.

Auskunftsrecht:

Privatpersonen müssen Zugang zu den personenbezogenen Daten haben, die eine Organisation über sie besitzt, und sie müssen die Möglichkeit haben, diese zu korrigieren, zu ändern oder zu löschen, wenn sie falsch sind, es sei denn, die Belastung oder die Kosten für die Gewährung des Zugangs würden in dem jeweiligen Fall in einem Missverhältnis zu den Nachteilen für den Betroffenen stehen, oder Rechte anderer Personen als des Betroffenen würden verletzt.

Durchsetzung:

Für einen effektiven Schutz der Privatsphäre müssen Mechanismen geschaffen werden, die die Einhaltung der Grundsätze des sicheren Hafens gewährleisten, Rechtsbehelfe für Betroffene vorsehen, bei deren Daten die Grundsätze nicht eingehalten wurden, sowie Sanktionen für die Organisation, die die Grundsätze nicht befolgt. Diese Mechanismen müssen mindestens folgendes umfassen (a) leicht zugängliche, erschwingliche und von unabhängigen Stellen durchgeführte Verfahren; (b) Kontrollmaßnahmen, um zu überprüfen, ob die Bescheinigungen und Behauptungen der Unternahmen über ihre Datenschutzmaßnahmen der Wahrheit entsprechen und ob diese Maßnahmen wie angegeben durchgeführt werden; (c) Verpflichtungen zur Lösung von Problemen sowie entsprechende Sanktionen für diese Organisationen. Die Sanktionen müssen hinreichend streng sein, um sicherzustellen, dass die Organisationen die Grundsätze einhalten.

Die drohende Blockade der Verhandlungen verschwand jedoch erst, als der amerikanische Verhandlungsführer David Aaron das Konzept eines ‚Safe Harbor‘ (wörtlich: sicherer Hafen) vorschlug – eine Reihe von Prinzipien, zu deren Einhaltung sich Unternehmen verpflichten konnten, was wiederum als „angemessener Schutz“ im Sinne der EU-Richtlinie anerkannt werden würde. Dieser Vorschlag verwandelte die Verhandlungen grundlegend, da er erstmals einen Ausweg zeigte, wie den europäischen Sachbedenken über Schutz von Privatsphäre und Daten ohne den Erlass umfassender Datenschutz-Gesetzgebung samt Errichtung diesbezüglicher Institutionen Rechnung getragen werden könnte. Trotz weiterbestehender Skepsis einiger EU-Mitgliedsstaaten wurde schließlich eine Übereinkunft zwischen den Vereinigten Staaten und der EU-Kommission erzielt, die sich weitgehend auf Aarons Vorschlag stützte. Unternehmen konnten sich demnach alljährlich zur Einhaltung einer Reihe von sieben durch das U.S.-Handelsministerium festgelegten und mit der EU vereinbarten Datenschutz-

Prinzipien verpflichten (siehe Tabelle 1). Die *Federal Trade Commission* würde auf ihrer Website eine Liste dieser Unternehmen veröffentlichen, und Mängel bei der Einhaltung der Selbstverpflichtung würden einen Bruch des *Federal Trade Commission Act* darstellen, der rechtlich verfolgt würde. Im Gegenzug verabschiedete die Europäische Kommission einen Beschluss, der diese Prozedur als „angemessenes Schutzniveau" im Sinne der Datenschutz-Richtlinie anerkannte.

Das ‚Safe Harbor'-Abkommen stellte also weder eine Anerkennung des zuvor von den USA praktizierten Systems durch die Europäische Union dar, noch war es eine Ausweitung des EU-Systems formeller Gesetzgebung auf die Vereinigten Staaten gekoppelt mit der Einführung von Datenschutz-Behörden. Vielmehr unterschied es sich qualitativ von beiden und stellte ein neues System dar, das in vielen Kommentaren als besonders passend für die spezifischen Bedingungen der Inkongruenz zwischen wirtschaftlichen und politischen Räumen sowie das Problem des regulativen *spill-over* zwischen verschiedenen Jurisdiktionen angesehen wurde. Sowohl in der politischen wie in der akademischen Bewertung wurde es als Erfolg angesehen und als Modellfall für zukünftige Einigungen in diesem Bereich, als es im November 2000 in Kraft trat.

4.2 Transatlantischer Datenstreit II: Terrorismus und Flugpassagierdaten

Weniger als ein Jahr später veränderten sich die Kontextbedingungen für Einigungen über die Regulierung transatlantischer Datenströme allerdings stark durch die Terroranschläge vom 11. September 2001. Das wurde zunächst im Bereich der Flugpassagierdaten deutlich.

Bei der Buchung, Abrechnung und Durchführung von Flugreisen fallen für jeden Passagier personenbezogene Daten an, die elektronisch gespeichert und informationstechnisch verarbeitet werden. Solche Flugpassagierdaten existieren in der Form von sogenannten *passenger name records* (PNR), und ein solcher Datensatz wird jedes Mal angelegt, wenn ein Passagier eine Reise bucht. PNRs werden in computerisierten Reservierungssystemen (CRS) gespeichert und enthalten den Namen des Reisenden, Details des Fluges, Hotel- und Mietwagenbuchungen sowie weitere gebuchte Leistungen. Sie enthalten daneben Wohn- und Geschäftsadresse (postalisch und elektronisch), Telefonnummern, Kreditkartendetails und die Namen und persönlichen Informationen für Kontakte im Notfall. Zudem können aus Rechnungs-, Tagungs- und Rabattcodes aus PNRs Informationen über Mitgliedschaften und Zugehörigkeit zu Organisationen abgeleitet werden, und schließlich können religiöse Diätvorschriften und Details über physische Behinderungen und medizinischen Status abgespeichert sein. PNRs sind deshalb als sehr persönliche Informationen zu betrachten.[13]

13 Es gibt vier große CRS-Systeme weltweit, und nur eines – AMADEUS – liegt in der EU, die anderen in den Vereinigten Staaten. Die Informationen in diesem Abschnitt basieren auf dem Bericht des Europäischen Parlaments A6-0226/2005 (4.7.2005), dem Kapitel über *privacy* beim Reisen in Electronic Privacy Information Center and Privacy International (2004), und der „Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States" der EU Article 29 Working Group (verabschiedet am 24. Oktober 2002).

Nach den Anschlägen vom 11. September 2001 beschlossen die Vereinigten Staaten, PNR-Daten für ihren Kampf gegen den internationalen Terrorismus zu nutzen. Am 19. November 2001 verabschiedete der U.S.-Congress den „Aviation and Security Act", der Fluggesellschaften, die nach, aus, oder durch die USA fliegen, verpflichtete, dem *US Bureau of Customs and Border Protection* (CBP) noch vor dem Abflug oder spätestens 15 Minuten danach direkten elektronischen Zugang zu den PNR-Daten in ihren Flugreservierungs- und Abfertigungssystemen zu gewähren. Da PNRs, wie oben geschildert, sehr persönliche Daten enthalten und somit unter die EU Datenschutz-Richtlinie fallen, entstand so ein regulativer Konflikt zwischen den USA und der EU, der Verhandlungen notwendig machte. Um ihrer Position Nachdruck zu verleihen, drohten die USA mit dem Entzug der Landerechte für alle EU-Fluggesellschaften, falls dieser Zugang nicht gewährt werde (Busch 2006, S. 317).

Zunächst kam es im März 2003 zu einer vorläufigen Übereinkunft, die den europäischen Fluggesellschaften die Übertragung der PNRs gestattete, ohne dass sie dafür von der EU bestraft werden würden. Weitere Verhandlungen über die Datentransfers fanden dann zwischen der EU Generaldirektion Binnenmarkt und Dienstleistungen (zuständig für das Thema Datenschutz) auf der einen Seite und dem U.S.-Heimatschutz-Ministerium auf der anderen Seite statt. Das strategische Verhandlungsziel der amerikanischen Seite wurde in einem Dokument des U.S.-Außenministeriums beschrieben als „ein Abkommen mit der EU das dem CBP und der TSA [*Transport Security Administration*, A.B.] dauerhaften Zugang zu den PNRs verschafft". Danach sei zu versuchen, diesen Zugang weltweit zu erlangen.[14] Mit anderen Worten: das amerikanische Politikziel war vollständiger und unkontrollierter Zugang zu ausländischen PNRs. Von EU-Seite her wurden diese Forderungen als inakzeptabel betrachtet, wie Binnenmarkt-Kommissar Frits Bolkestein mehrfach klarstellte. In einer Rede vor dem Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments erklärte er am 9. September 2003, dass die Kommission die Erfordernis eines „angemessenen Schutzniveaus" bisher nicht als erfüllt betrachten könne und legte vier prinzipielle Defizite der bis dato erfolgten Verhandlungen dar:[15]

- die Vereinigten Staaten seien nicht bereit, die übertragenen PNRs ausschließlich zur Verfolgung von Terrorismus und terrorismusbezogenen Verbrechen zu verwenden;
- die 39 von den USA geforderten PNR-Datenvariablen seien mehr als für den vorliegenden Zweck erforderlich sei;

14 Siehe den "FY 2005 Performance Plan", zugänglich unter http://www.state.gov/s/d/rm/rls/perfplan/2005/html/29302.htm [1.8.2011]. Dort heißt es in großer Offenheit: „Ensure access to PNR data on a global basis for border and passenger screening. Use demarches, high-level meetings, conferences, and all other appropriate occasions to disseminate information about the USGs data and privacy protection regimes. Work with DHS to negotiate agreements for access to these data."

15 Siehe auch seinen Kommentar „Resisting U.S. demands: Passenger privacy and the war on terror" auf der Op-Ed-Seite des *International Herald Tribune* am 24. Oktober 2003, der ähnliche Argumente vorbringt.

- die von den Vereinigten Staaten geforderte Speicherungszeit für die übermittelten PNR-Daten von sechs bis sieben Jahren sei zu lang;[16]
- und schließlich kritisierte er die „unzureichende rechtliche Verbindlichkeit der U.S.-Zusicherungen" (d.h. die vereinbarten Rechte waren in den USA nicht gerichtlich durchsetzbar).

Nach weiteren Verhandlungen verkündete Bolkestein jedoch am 16. Dezember 2003, dass man sich auf einen Kompromiss geeinigt habe. Die Europäische Kommission veröffentlichte am 14. Mai 2004 einen „Angemessenheitsbefund" im Sinne der Datenschutz-Richtlinie, und zwei Wochen später wurde die Vereinbarung zwischen beiden Seiten in Washington unterzeichnet. Vergleicht man deren Text jedoch mit dem der Kriterien, die Bolkestein noch sechs Monate zuvor genannt hatte, so wird deutlich, dass sich die U.S.-Seite mit ihren Forderungen weitgehend durchgesetzt hatte:

- PNR-Daten konnten zur Verhinderung und Bekämpfung von 1.) Terrorismus und terrorismusbezogenen Straftaten; 2.) anderen schweren Verbrechen, inklusive länderübergreifender organisierter Kriminalität; und 3.) zur Verfolgung Flüchtiger für die obengenannten Straftaten benutzt werden;
- 34 PNR-Elemente sollten übertragen werden (siehe Tabelle 2), von denen u.a. Adresse, frühere Reisen, allgemeine Bemerkungen sowie das Feld über besondere Informationen hochgradig personenbezogen sind;
- PNRs durften dreieinhalb Jahre gespeichert werden; danach sollten die Daten, auf die währenddessen nicht zugegriffen wurde, gelöscht werden; die anderen Daten sollten weitere acht Jahre aufbewahrt werden;
- Beschwerden gegen die Handhabung der PNRs konnten schriftlich an den *Chief Privacy Officer* des Heimatschutz-Ministeriums gerichtet werden – der den Fall untersuchen und sich bemühen würde, den Grund für die Beschwerde auszuräumen.

Daneben sollten die an die CBP übermittelten Daten auch dem Heimatschutz-Ministerium zur Verfügung gestellt werden können – einer riesigen Behörde, die 22 früher unabhängige Bundesbehörden umfasst (unter ihnen das CBP) und mehr als 170.000 Angestellte beschäftigt (Kettl 2004). Zusicherungen des Heimatschutz-Ministeriums, es werde nicht zu weitreichender Verbreitung der Daten unter anderen Bundesbehörden kommen, erschienen daher von fraglichem Wert.

In der Folge wurde das Abkommen sowohl von der Arbeitsgemeinschaft der EU-Datenschutzbehörden (der sogenannten *Article 29 Working Group*) wie vom Europäischen Parlament heftig kritisiert (Article 29 Data Protection Working Party 2004). Das Europäische Parlament hatte bereits das vorläufige Abkommen kritisiert und mit 445 zu 31 Stimmen (bei 21 Enthaltungen) im Oktober 2003 gefordert, die PNR-Übertragungen den EU-Datenschutz-Gesetzen entsprechend zu gestalten. Im Juni 2004 klagte das Europäische Parlament deshalb gegen die Kommission vor dem Europäischen Gerichtshof und verlangte, sowohl das Ab-

16 Ursprünglich hatten die USA eine 50jährige Datenspeicherung verlangt.

kommen wie auch den ‚Angemessenheitsbefund' für nichtig zu erklären. Beinahe zwei Jahre später, am 30. Mai 2006, annullierte der Europäische Gerichtshof sowohl die Entscheidung des Ministerrates über den Abschluss des Abkommens mit den USA als auch die Entscheidung der Kommission über die Angemessenheit (Fälle C-317/04 und C-318/04). Doch traf der Gerichtshof diese Entscheidungen lediglich auf der Basis der Beurteilung rechtlicher Kompetenzen: danach mangelte es dem Ministerrat an der Befugnis zum Abschluss des Abkommens, und die Kommission überschritt ihre Kompetenzen, indem sie das Abkommen als „angemessen" im Rahmen der Datenschutz-Richtlinie erklärte. Der Gerichtshof entschied demnach *nicht* über die inhaltliche Richtigkeit der Beschwerde des Parlaments hinsichtlich Recht auf Privatsphäre und Bruch von Grundrechten.

Tabelle 2: **Zu übermittelnde PNR-Variablen nach dem Abkommen von Juni 2003 (Europäische Kommission 2004)**

1. PNR-Buchungscode (Passenger Name Record)
2. Datum der Reservierung
3. Geplante Abflugdaten
4. Name
5. Andere Namen im PNR
6. Anschrift
7. Zahlungsart
8. Rechnungsanschrift
9. Telefonnummern
10. Gesamter Reiseverlauf für den jeweiligen PNR
11. Vielflieger-Eintrag (beschränkt auf abgeflogene Meilen und Anschrift(en))
12. Reisebüro
13. Bearbeiter
14. Codeshare-Information im PNR
15. Reisestatus des Passagiers
16. Informationen über die Splittung/Teilung einer Buchung
17. E-Mail-Adresse
18. Informationen über Flugscheinausstellung (Ticketing)
19. Allgemeine Bemerkungen
20 Flugscheinnummer
21. Sitzplatznummer
22. Datum der Flugscheinausstellung
23. Historie über nicht angetretene Flüge (no show)
24. Nummern der Gepäckanhänger
25. Fluggäste mit Flugschein aber ohne Reservierung (Go show)
26. Spezielle Service-Anforderungen (OSI - Special Service Requests)
27. Spezielle Service-Anforderungen (SSI/SSR - Sensitive Security Information/Special Service Requests)
28. Information über den Auftraggeber (received from)

29. Alle Änderungen der PNR (PNR-History)
30. Zahl der Reisenden im PNR
31. Sitzplatzstatus
32. Flugschein für einfache Strecken (one-way)
33. Etwaige APIS-Informationen (Advance Passenger Information System)
34. ATFQ-Felder (automatische Tarifabfrage)

4.3 Transatlantischer Datenstreit III: Terrorismus und Finanztransaktionsdaten

Nur drei Wochen, nachdem der Europäische Gerichtshof Ende Mai 2006 sein Urteil über den Transfer von Flugpassagierdaten gesprochen hatte, schob sich bereits der nächste Fall im Bereich transatlantischer Datenübermittlung (und damit: eines potentiellen Konfliktes zwischen dem Vereinigten Staaten und der Europäischen Union) auf die Agenda. Am 23. Juni 2006 veröffentlichte die *New York Times* einen Bericht darüber, dass die amerikanische Regierung sich Zugriff auf Daten über weltweite Finanztransaktionen verschafft hatte, und zwar über die *Society for Worldwide Interbank Financial Telecommunicatio*n (SWIFT) (Lichtblau u. Risen 2006). SWIFT ist eine in Belgien inkorporierte Genossenschaft der Finanzindustrie mit mehr als 2200 Teilhabern, die seit ihrer Gründung im Jahr 1973 internationale Finanztransaktionen für ihre Kunden vermittels eines elektronischen Transfersystems durchführt. Die Firma hat über 8000 Finanzinstitutionen in über 200 Ländern als Kunden, und verarbeitet bis zu 12 Mio. Transaktionen pro Tag mit einem Volumen von bis zu 6 Billionen US-Dollar. SWIFT kann deshalb zu Recht als das Rückgrat des internationalen Zahlungsverkehrs bezeichnet werden, über das alle formalen internationalen Finanztransaktionen abgewickelt werden – nicht zuletzt, weil dies die einzige solche Firma ist. Da die von SWIFT übermittelten Nachrichten sowohl personenbezogene Daten beinhalten wie auch potentiell strategisch wertvolle Unternehmensdaten, ist in diesem Bereich der Datenschutz von hoher Wichtigkeit.

Nach den Terroranschlägen auf die Vereinigten Staaten vom 11. September 2001 beschloss die amerikanische Regierung, sich Zugang zu diesen Transaktionsdaten für das von ihr betriebene ‚*Terrorist Finance Tracking Program*' (TFTP) zu verschaffen. Durch juristische Mittel (*subpoena*) wurde SWIFT gezwungen, der amerikanischen Justiz Daten für den Zweck Terrorismus-bezogener Nachforschungen zur Verfügung zu stellen; Adressat der juristischen Zwangsmaßnahmen war das SWIFT-Rechenzentrum in den Vereinigten Staaten, eines von zwei Rechenzentren der Firma (das andere befindet sich in einem Mitgliedsstaat der Europäischen Union). Die Firmendaten von SWIFT wurden nämlich zum Zweck der Datensicherung zwischen beiden Rechenzentren gespiegelt und 124 Tage vorgehalten; das bedeutet, dass in beiden Computersystemen dieselben Daten existierten und folglich auf US-Territorium auch alle Daten zugänglich waren, die sich auf Geschäfte in Europa und der gesamten restlichen Welt bezogen.

SWIFT musste der Anordnung auf Überlassung der Daten Folge leisten. Während das Ausmaß der den amerikanischen Behörden überlassenen Daten zunächst

unklar war, stand außer Frage, dass die SWIFT-Firmenleitung in der Folge weder ihre Teilhaber noch sonst irgendwen von den juristischen Zwangsmitteln der amerikanischen Regierung (nicht weniger als 64 zwischen September 2001 und November 2006 – im Durchschnitt also eine pro Monat – vgl. Article 29 Working Party Opinion 10/2006, S. 8.) in Kenntnis gesetzt hatte und somit die Übergabe der Daten an die US-Regierung niemandem bekannt war. Nachdem die Existenz des TFTP-Programms öffentlich gemacht und von der amerikanischen Regierung im Juni 2006 bestätigt worden war, folgte daher harsche Kritik von europäischer Seite. Das Europäische Parlament verabschiedete am 6. Juli 2006 eine Resolution, in der es vollständige Information von den EU-Institutionen über deren Kenntnis des Programms verlangte, und betonte sein Missfallen und seine tiefe Besorgnis hinsichtlich der ergriffenen Maßnahmen, da diese insgeheim den Schutz personenbezogener Daten von europäischen Bürgern unterlaufen habe; die europäischen Regierungen verneinten jegliche vorherige Kenntnis des TFTP-Programms; die Parlamente in zahlreichen Mitgliedsstaaten der EU debattierten die Vorfälle und äußerten scharfe Kritik am Vorgehen der US-Regierung[17]; und Wirtschaftsverbände und Finanzpresse äußerten ihre Besorgnis, dass die übergebenen Daten auch zum Zweck der Wirtschaftsspionage genutzt werden könnten.[18]

Festzuhalten bleibt jedenfalls, dass das Handeln der amerikanischen Regierung sowie die Geheimhaltung der Konfiszierung der Daten ein außerordentlich einseitiges Vorgehen darstellte, das bei den um Datenschutz besorgten Europäern höchste Besorgnis auslösen musste. Zwar war sehr wahrscheinlich genau das Wissen darum (und die Erwartung, dass die Institutionen der Europäischen Union sowie die Regierungen der Mitgliedsstaaten versuchen würden, den Datentransfer zu verhindern, falls sie davon erführen) ein Hauptgrund für die Bush-Regierung, so zu handeln; jedoch muss diese Vorgehensweise auf jeden Fall als keineswegs auf Ausgleich der Interessen bedacht und als wenig partnerschaftlich vorgehend eingestuft werden.

5. Theoretische Perspektiven auf das Thema

Politikwissenschaftliche Untersuchungen zu Regulierung des Datenverkehrs zwischen den Vereinigten Staaten von Amerika und der EU haben sich bisher vor allem auf den Fall des ‚Safe Harbor'-Abkommens konzentriert und ihn vornehmlich aus konstruktivistischer Perspektive analysiert (vgl. etwa Long u. Quek 2002; Farrell 2003; Regan 2003; eine Ausnahme bildet die Studie von Heisenberg 2005). Diese Sichtweise betont die Wichtigkeit von Werten, Normen, und Diskursen gegenüber konventionellen, einer ‚realistischen' Perspektive im Bereich der Internationalen Beziehungen folgenden Analysen von Macht. Mit Bezug auf den ‚Safe Harbor'-Fall wurde dabei argumentiert, dass – insbesondere unter Bedingungen annähernd gleicher Macht – Dialog Verhandlungsblockaden auflösen sowie die Dominanz einer Seite oder die Eskalation eines (Handels-)Konfliktes

17 Vgl. etwa die Debatte im Deutschen Bundestag am 27. März 2007.

18 Siehe etwa die entsprechenden Berichte im *Handelsblatt* (11. Juli 2006) sowie in der österreichischen Zeitung *Die Presse* (11. Juli 2006).

verhindern könne, und dass durch Überzeugungsarbeit und Argumente Ergebnisse erreichbar seien, die durch die herkömmliche Verhandlungstheorie nicht erklärbar seien. Im Angesicht einer schwierigen Verhandlungssituation, so besagt diese Analyse, sei es den USA und der EU gelungen, „durch einen Argumentationsprozess neue Handlungswege zu entdecken sowie eine vorläufige Übereinkunft über einen neuen institutionellen Ansatz zur Lösung des vertrackten Disputs zur Regelung des Datenschutzes zu erlangen, der nun auf andere Bereiche des *e-commerce* übertragen werden könne" (Farrell 2003, S. 302).[19]

Dies mag im Fall des ‚Safe Harbor'-Abkommens tatsächlich so gewesen sein. Da in den erwähnten Analysen keine Einschränkungen bezüglich des Kontexts gemacht werden, wird damit jedoch zugleich implizit eine generalisierte Aussage über das Verhalten der transatlantischen Akteure in Disputen über grenzüberschreitende Datentransfers gemacht. Deren Gültigkeit muss allerdings fraglich erscheinen, wenn man weitere Fälle aus dieser Klasse betrachtet wie die oben geschilderten Fallstudien zum Transfer von Flugpassagier- und Finanztransaktionsdaten. In beiden Fällen findet man wenig Überzeugungsarbeit und Argumentation, vielmehr scheint eine einseitige Durchsetzung von Interessen zu dominieren. Wenn es aber zwischen Politikepisoden, die jeweils Fragen des grenzüberschreitenden Datenverkehrs betreffen, deutliche Unterschiede in Verhandlungsdynamik und -ergebnissen gibt, dann müssen zusätzliche Differenzierungen in die Betrachtung eingeführt werden, wenn man die Gemeinsamkeiten und Unterschiede der Fälle erklären will. In den nächsten Abschnitten wird deshalb argumentiert, dass dies am besten über die Unterscheidung unterschiedlicher Sichtweisen auf die zugrundeliegende Problematik geschieht – weil aus unterschiedlichen Sichtweisen auch unterschiedliche Problemdefinitionen und -lösungen folgen – sowie durch die Einbeziehung institutioneller Faktoren in die Analyse.

5.1 Drei „frames" zur Analyse der Positionen

Der Disput über grenzüberschreitende Datenströme ist einer, dem man sich unter verschiedenen Gesichtspunkten nähern kann, und in dem unterschiedliche Akteure daher unterschiedliche Positionen hinsichtlich dieser Gesichtspunkte einnehmen können. Das bedeutet, dass sowohl die relevanten Fakten des umstrittenen Themenfeldes wie auch die in den sie betreffenden Auseinandersetzungen und Verhandlungen anzustrebenden Ziele nicht von vorneherein feststehen, sondern dass es über sie legitimerweise Meinungsverschiedenheiten geben kann. In der sozialwissenschaftlichen Terminologie hat sich zur Analyse dieses wichtigen Sachverhalts der Ausdruck des *framing* eingebürgert (Rein u. Schön 1996; Schön u. Rein 1994). Die den Politikpositionen der Akteure zugrundeliegenden Überzeugungen, Wahrnehmungen und Wertungen werden als *frames* bezeichnet, und Politikkontroversen zwischen den Akteuren werden als Konflikte zwischen den jewei-

19 Im Original: „Through a process of argument, these actors succeeded in discovering new possibilities of action, reaching a provisional understanding about a new institutional approach to resolving the vexing dispute over privacy regulation, which may be applied to other areas of e-commerce."

ligen *frames* interpretiert (vgl. zum Folgenden Schön u. Rein 1994, S. 23-26). Diese jeweiligen *frames* liefern Interpretationen, die aus einer diffusen und komplexen Realität erst eine bestimmte Situation machen, indem sie Tatsachen auswählen und für wichtig erklären. Denn erst durch diesen Prozess der Auswahl, Benennung und Bewertung wird ein Problem verstehbar und behandelbar gemacht. *Frames* definieren also zum einen die genaue Natur des Problems, und zudem, was als Tatsache zählt und welche Argumente als relevant und überzeugend gelten. Wenn Akteure ein Themengebiet durch unterschiedliche *frames* interpretieren, wird die zugrundeliegende Kontroverse demzufolge nur schwer lösbar sein, zumal wenn diese *frames* nicht offen ausgesprochen bzw. definiert werden. In Verhandlungen der internationalen Politik zeigt sich oft, dass die Definition des Problems ein entscheidender Schritt für das Setzen der Agenda und den Fortschritt im Politikprozess darstellt (Mitchell 2002, S. 503-504).

Auch für das Thema grenzüberschreitender Datenströme lässt sich aufgrund theoretischer Überlegungen die Existenz unterschiedlicher *frames* annehmen, die vor allem durch die unterschiedlichen Charakteristika und vielgestaltigen Verwendungsmöglichkeiten solcher Datenströme bestimmt sind. Dies sind

- zum einen eine Perspektive *ökonomischer Interessen*, die Aspekte wie Kosteneffizienz, Profitabilität und Ausweitung des Marktanteils in den Mittelpunkt stellt;
- zum anderen eine Perspektive von *Sicherheitsinteressen*, die das Thema unter den Gesichtspunkten von Risikominimierung und Verhinderung von Missbrauch sieht;
- und schließlich eine Perspektive von *Bürgerrechtsinteressen*, die sich auf den Schutz der Privatsphäre sowie auf Informationsfreiheit (*freedom of information*) konzentriert.

Die unterschiedlichen *frames* werden mutmaßlich von unterschiedlichen Klassen von Akteuren verwendet, und ihre Wahl durch jeweilige Interessen und Situationsdefinitionen bestimmt:

- Die Perspektive *ökonomischer Interessen* wird wahrscheinlich von kommerziell interessierten Akteuren wie Unternehmen[20] und marktnahen Akteuren in der staatlichen Verwaltung (wie etwa Wirtschaftsministerien oder Regulierungsagenturen von Märkten etc.) eingenommen werden. Ihr Interesse wird sich auf eine Minimierung von Transaktionskosten richten; man wird sich der wohlfahrtssteigernden Vorteile von Handel und Austausch bewusst sein und diese auch öffentlich betonen; und man wird deshalb versuchen, regulative Vorschriften gering zu halten und dabei gleichzeitig ein hohes Maß an Schutz für personenbezogene Daten zu erreichen, weil man sich der Wichtigkeit der Glaubwürdigkeit dieses Schutzes für die Attraktivität von *e-commerce* bewusst ist.

20 Eine Ausnahme wird es hier wahrscheinlich für Unternehmen aus der Sicherheitsindustrie geben, da diese aus ökonomischen Interessen eher eine die Vordringlichkeit von Sicherheit betonende Perspektive einnehmen werden.

- Die Betonung von *Sicherheitsinteressen* wird vermutlich bei Sicherheitsbehörden (also Polizei- und Geheimdiensten sowie deren Vorgesetzten in der staatlichen Verwaltung wie etwa Innenministerien), bei Vertretern des Militärs sowie kommerziellen Interessen aus der Sicherheitsindustrie vorherrschen. Diese Akteure werden vor allem auf die Minimierung von Risiken und die Maximierung von Sicherheit zielen – und dabei dem Problem von Transaktionskosten nur wenig Beachtung schenken; schließlich, so wird man vermutlich äußern, geht es letztlich um den Schutz menschlichen Lebens, dem gegenüber andere Gesichtspunkte zurücktreten müssen. Deshalb kann auch auf den Schutz personenbezogener Daten nur wenig Rücksicht genommen werden – vielmehr wird man sich von deren Sammlung und Auswertung die Identifikation potentieller Gefährder versprechen, die dann zielgerichtet überwacht werden können.
- Auf den Schutz von *Bürgerrechtsinteressen* werden sich vermutlich Akteure konzentrieren, die einen Auftrag oder ein besonderes Interesse am Schutz von Menschen- und Bürgerrechten sowie Privatsphäre haben. Dazu werden wahrscheinlich Datenschutzbeauftragte auf staatlicher und supranationaler Ebene, aber auch in Unternehmen gehören, bürgerrechtlich orientierte NGOs, sowie politische Kräfte, deren Anhänger bürgerrechtliche Interessen über wirtschaftliche und Sicherheitsinteressen stellen, also vermutlich solche libertärer Orientierung.

Eine Differenzierung der Akteure, ihrer Interessen und der damit in Verbindung stehenden Perspektiven auf das Thema der Regulierung transatlantischer Datenströme ermöglicht eine genauere und trennschärfere Analyse der Fallstudien zur Regulierung transatlantischer Datenströme als die bisher in der Literatur dominante Interpretation aus der Perspektive eines konstruktivistischen Ansatzes. Dieser analytische Ansatz beherrscht, wie bereits oben erwähnt, die politikwissenschaftliche Literatur zum ‚Safe Harbor'-Fall (vgl. zum Folgenden Long u. Quek 2002, S. 338 ff.; Regan 2002, S. 264; Farrell 2003, S. 297-302), und die Autoren hatten stets auf die wichtige Rolle hingewiesen, die soziale Normen bei der Lösung dieses Konflikts gespielt hatten. Zudem war betont worden, dass sich das Abkommen dadurch auszeichne, dass es weder eine Anerkennung der U.S.-Präferenz für Selbstregulierung durch die EU darstelle noch eine Ausweitung des europäischen Systems umfassender Datenschutzgesetzgebung auf die Vereinigten Staaten, sondern etwas genuin Neues. Durch Deliberation sei es gelungen, trotz zunächst unvereinbarer Verhandlungspositionen eine gemeinsame Lösung zu finden, die wahrscheinlich sogar Rückwirkungen auf die ursprünglichen Regulierungssysteme in der EU und den USA haben werde. Der Lösungsansatz eines iterativen Dialogs zeige, dass Kooperation zwischen Nationalstaaten möglich sei, ohne dass eine Seite ihre Interessen einseitig durchsetze oder es zu Blockade und Handelskonflikt komme. Deshalb könne die ‚Safe Harbor'-Lösung als Modell für zukünftige Lösungen im Bereich der Regulierung transatlantischer Datenströme dienen. Auch von politischer Seite gab es solche Erwartungen, etwa durch den ehemaligen Präsidenten des Europäischen Parlaments, Pat Cox, der dem ‚Safe

Harbor'-Abkommen eine „Vorbildfunktion für die Zukunft" zusprach (vgl. das diesbezügliche Zitat in Farrell 2003, S. 298).

Aus heutiger Perspektive klingen diese Erwartungen und Heilszuschreibungen an das dialogische Prinzip sehr optimistisch. Denn die Entwicklung im Bereich der Regulierung transatlantischer Datenströme ist im letzten Jahrzehnt deutlich anders verlaufen als man das nach dem Abschluss des ‚Safe Harbor'-Abkommens prognostiziert hatte. Im Lichte der neueren Dispute zwischen den beiden transatlantischen Seiten – dem über die Übermittlung von Flugpassagierdaten sowie dem über den Zugriff auf internationale Finanztransaktionsdaten – werden daher auch diese Erwartungen wohl neu evaluiert werden müssen.

5.2 Änderungen der Akteurkonstellation

Stand bei Beginn der Verhandlungen über die Regulierung von transatlantischen Datenströmen ab 1998 die Perspektive von ökonomischen Interessen und beiderseitigem Gewinn durch internationalen Handel im Mittelpunkt, so machen die beiden weiter oben geschilderten Fälle zur Übertragung von Flugpassagier- und Finanztransaktionsdaten deutlich, dass nach den Terroranschlägen vom 11. September 2001 in diesem Themenfeld eine deutliche Änderung eintrat. Der *frame* der Sicherheitsinteressen wurde dominant – insbesondere für die Vereinigten Staaten von Amerika. Entsprechend den oben geäußerten Erwartungen standen nun Risikominimierung und Maximierung von Sicherheit im Vordergrund, und die bei dem angestrebten Ziel der Sammlung möglichst umfassender Daten anfallenden Kosten in Bezug auf Privatheits- und Bürgerrechte wurden weitgehend ignoriert.[21] Auf der europäischen Seite stießen die amerikanischen Forderungen hingegen auf eine Position, die bestrebt war, die etablierten Standards beim Datenschutz aufrechtzuerhalten und zu verteidigen. Dabei spielte die Europäische Kommission eine wichtige Rolle, die (zumindest im Fall der Flugpassagierdaten) als Ansprechpartner der Vereinigten Staaten agierte und den neuen Konflikt intern durch die gleichen Kanäle verarbeitete wie den ‚Safe Harbor'-Fall, nämlich in der für den Binnenmarkt zuständigen Generaldirektion. Während man es auf der Seite der USA also (aufgrund der fehlenden Institutionalisierung von Datenschutz) mit anderen Akteuren als im ‚Safe-Harbor'-Fall zu tun hatte (dem CBP und dem neuen *Department of Homeland Security* oder DHS), blieben auf der europäischen Seite mit der DG Binnenmarkt die Akteure gleich – und damit auch die Dominanz eines *frame* ökonomischer Interessen. Angesichts der amerikanischen Drohung mit einem Landeverbot für die europäischen Fluglinien in den Vereinigten Staaten kam man den Forderungen nach einer Datenübertragung sehr weitgehend entgegen.

Innerhalb Europas hatte diese Nachgiebigkeit der EU-Kommission allerdings erhebliche Konsequenzen. Denn sie führte dazu, dass das Europäische Parlament

21 Ein extremes Beispiel für den Umfang von Datenerfassung, der hier zunächst in Erwägung gezogen wurde, bildet das *Total Information Awareness*-Projekt, das von der DARPA nach den Terroranschlägen betrieben wurde und schlicht alle verfügbaren Daten miteinander verknüpfen sollte (vgl. O'Harrow 2006, S. 190-213 sowie Anhang J in National Research Council 2008). Es wurde später zunächst in *Terrorist Information Awareness* umbenannt und dann nicht weiter finanziert.

der Kommission eine Missachtung der europäischen Rechtslage zum Datenschutz vorwarf und beschloss, die Kommission vor dem Europäischen Gerichtshof zu verklagen. Diese Klage machte zum einen deutlich, dass es innerhalb der Europäischen Union Interessen- und Positionsdivergenzen zum Thema Regulierung der transatlantischen Datenströme gab, mithin neben dem Konflikt über den Atlantik hinweg noch ein innereuropäischer Konflikt existierte;[22] wichtige Konsequenzen hatte dieser Konflikt vor allem dadurch, dass das Urteil des Europäischen Gerichtshofs Mitte 2006 eine Veränderung der zuständigen Akteure auf der europäischen Seite der transatlantischen Verhandlungen erzwang. Denn da der Gerichtshof unter Bezugnahme auf die geltenden EU-Verträge dem Ministerrat und der Kommission sowohl die Kompetenz zum Abschluss eines Abkommens mit den USA wie auch zur Anerkennung der ‚Angemessenheit' der amerikanischen Maßnahmen mit Hinblick auf die Datenschutz-Richtlinie absprach, wurde der gesamte Sachverhalt (in der Terminologie des Maastrichter Vertrages) aus der vergemeinschafteten ‚ersten Säule' der europäischen Kooperation in die ‚dritte Säule' (die intergouvernementale Kooperation in den Bereichen Justiz und Inneres) verlegt. Mit diesem *forum shift* wechselten die Akteure auf der europäischen Seite: anstelle der DG Binnenmarkt waren es nun die nationalen Innen- und Justizminister sowie der für das Justiz-Portfolio zuständige EU-Kommissar Franco Frattini, welche die Weichen für die weiteren Verhandlungen stellten; ihre Präferenzen orientierten sich viel deutlicher an einem sicherheitspolitischen *frame* als das bei der DG Binnenmarkt der Fall gewesen war.

Mit seiner Klage gegen die Kommission hatte das Europäische Parlament somit zwar zunächst einen Erfolg erreicht, da das bestehende Abkommen mit den USA über Flugpassagierdaten gekündigt werden musste (EuGH 2006). Dieser Erfolg hatte jedoch unbeabsichtigte Konsequenzen insoweit, als die in der Folge notwendigen Verhandlungen auch auf der europäischen Seite nun von Akteuren geführt wurden, die das Thema der Datenübertragung eher durch den *frame* der Sicherheitsinteressen betrachteten. Das lag zwar in inhaltlicher Hinsicht nicht im Interesse des Parlaments, war jedoch nach dem Beschreiten des Weges über das Gericht nun nicht mehr zu ändern. Für das Parlament war ärgerlich, dass durch die Verschiebung der Entscheidungsmaterie von der ersten in die dritte Säule eine deutliche Schwächung seiner Mitwirkungsrechte erfolgt war und es deshalb auf die Ergebnisse der neuen Verhandlungen kaum Einfluss würde nehmen können.

Man hätte nun annehmen können, dass die Verschiebung der Verhandlungskompetenz in die dritte Säule und zu Akteuren, bei denen die Dominanz eines sicherheitspolitischen *frame* angenommen werden kann, plausiblerweise zu einer deutlichen Annäherung der transatlantischen Positionen und einer Erleichterung bei der Einigung auf ein neues Abkommen führen würde. Wie weiter unten in der Schilderung des Verlaufs deutlich wird, war das nur eingeschränkt der Fall. Und als man beinahe so weit war (gegen Ende des Jahres 2009), kam es zu einer noch-

22 Dabei soll hier offen bleiben, ob dieser innereuropäische Konflikt auf genuinen Unterschieden bei den Präferenzen beruht oder als Teil des Ringens um Macht und Einfluss zwischen Parlament und Kommission zu sehen ist; beide Motive sind denkbar und aus der Beobachtung des Handelns der Akteure kaum zu unterscheiden.

maligen Änderung der Akteurkonstellation, die eine Einigung weiter hinauszögerte: Der Vertrag von Lissabon trat am 1. Dezember 2009 in Kraft und erweiterte die Kompetenzen des Europäischen Parlaments auch in Sachverhalten, die unter die dritte Säule fallen.[23] Da es vor dem Inkrafttreten der neuen Kompetenzen zu einer Polarisierung zwischen dem Parlament auf der einen Seite und der Kommission und dem Rat auf der anderen Seite gekommen war (das Parlament argwöhnte, eine von ihm abgelehnte Regelung hinsichtlich der Übertragung von Finanzdaten an die USA solle noch unter den alten Regeln durchgesetzt werden, s.u.), kam es bereits im Februar 2010 zu einer ersten Demonstration der neuen Vetomacht des Parlaments, das das SWIFT-Interimsabkommen mit deutlicher Mehrheit ablehnte.

Die Akteurkonstellation hat sich somit zwischen 2006 und 2010 zweimal entscheidend geändert, einmal durch den *forum shift* von der ersten in die dritte Säule der Europäischen Union und das zweite Mal durch das Inkrafttreten des Vertrages von Lissabon mit seiner Aufwertung der Entscheidungsmacht des Europäischen Parlaments. Während die erste Veränderung Konsequenzen hatte für die von den europäischen Verhandlungspartnern eingenommene Perspektive auf das Thema, war das bei der zweiten Änderung nicht der Fall. Dennoch machen beide Veränderungen deutlich, dass neben dem *framing* des Themas auch institutionelle Variablen (wie beispielsweise die Zusammensetzung der Verhandlungsgruppe sowie die Entscheidungsbefugnisse und Vetomacht der einzelnen Akteure) für die Analyse der Regulierung transatlantischer Datenströme von essentieller Wichtigkeit ist.

Der Einfluss der in diesem Teil des Beitrags benannten Variablen wird auch im folgenden Teil des Beitrags anhand der weiteren Entwicklung der in den Themenbereichen Übermittlung von Flugpassagierdaten sowie Finanztransaktionsdaten nach dem *forum shift* von 2006 deutlich.

6. Die Konflikte seit 2006

Das Urteil des EuGH vom 30. Mai 2006 hatte das Abkommen über Fluggastdaten zwischen der Europäischen Union und den Vereinigten Staaten für ungültig erklärt, allerdings nicht (wie vom klagenden Europäischen Parlament erhofft) wegen eines Verstoßes gegen die europäischen Datenschutzgesetze, sondern wegen mangelnder Kompetenz von Kommission und Ministerrat zum Abschluss eines Abkommens in diesem Bereich (s.o.). In inhaltlicher Hinsicht hatte der Klageerfolg des Europäischen Parlaments demnach keine Entscheidung gebracht; die Verschiebung in den Bereich der intergouvernementalen Zusammenarbeit der EU ließ vielmehr eine Verstärkung der sicherheitspolitischen Perspektive auf das Thema erwarten.

23 Nach Art. 14 EU-Vertrag wurde das Ko-Dezisionsverfahren, das erstmals mit dem Vertrag von Maastricht (1992) eingeführt worden war, nun zum „ordentlichen Gesetzgebungsverfahren" auf der europäischen Ebene und bezog nun auch die polizeiliche und justizielle Zusammenarbeit im Rahmen der dritten Säule ein, wodurch das Europäische Parlament eine faktische Vetoposition im europäischen Gesetzgebungsverfahren erhielt.

Bereits im September 2006 hatten neue Verhandlungen mit den USA begonnen, und im Juni 2007 einigte man sich auf ein neues Abkommen – rechtzeitig vor dem Auslaufen des Interimsabkommens im Juli 2007. Das neue Abkommen (Rat der EU 2007) veränderte gegenüber den existierenden Regeln einige Parameter, und Beobachter bewerteten es insgesamt als ein Entgegenkommen gegenüber den Wünschen der USA.[24] So war die Speicherfrist der Daten von dreieinhalb auf bis zu 15 Jahre verlängert worden, und zudem wurde der Zugriff mehr amerikanischen Behörden gestattet (und somit eine Verknüpfung mit anderen Informationen zur Erstellung von Risikoprofilen möglich). Die europäische Seite konnte als Erfolg verzeichnen, dass den US-Behörden nun nicht mehr der direkte Zugriff auf die Buchungssysteme erlaubt war (*pull*-Verfahren), sondern ihnen die Daten übermittelt wurden (*push*-Verfahren); die ebenfalls als Erfolg dargestellte Reduktion der Zahl der übermittelten Daten aus den PNR-Datensätzen von 34 auf 19 wurde hingegen fast vollständig durch eine Zusammenfassung der Positionen erreicht.[25]

Auch jenseits der Verhandlungen mit den USA hatte der *forum shift* Folgen für die Haltung der Europäischen Union zum Thema Nutzung von Flugpassagierdaten. Das einst bekämpfte Verfahren sollte nun auch im eigenen Hoheitsgebiet angewandt werden. Im November 2007 schlug Justizkommissar Frattini nämlich vor, dass zukünftig auch in Europa Flugpassagierdaten im Rahmen der Bekämpfung des internationalen Terrorismus sowie der organisierten Kriminalität genutzt werden sollten (EU-Kommission 2007; SZ 6.11.2007, S. 6). Bereits im Sommer 2007 hatte der deutsche Innenminister Schäuble als amtierender Präsident des Ministerrates einen entsprechenden Vorschlag gemacht, und auch die französische Ratspräsidentschaft lancierte im Sommer 2008 eine ähnliche Initiative.

Schon das Abkommen mit den USA war beim Europäischen Parlament auf erhebliche Kritik in fast allen Fraktionen gestoßen (FAZ-Net 2007). Dabei spielte neben inhaltlichen Erwägungen auch der Umstand eine Rolle, dass der Rat das Abkommen in die Form eines Rahmenbeschlusses gefasst hatte, bei dem das Parlament zwar seine Meinung äußern kann, aber keinen Einfluss auf die Entscheidung hat, da diese die Form eines Abkommens der Mitgliedsstaaten hat. Allerdings müssen alle Vertragspartner (und das heißt auch alle 27 EU-Mitgliedsstaaten) ihre internen Ratifikationsverfahren abschließen, bevor das bis dahin nur provisorisch angewandte Abkommen in Kraft treten kann. Hierbei kam es zu Verzögerungen. Irland hatte im September 2006 vor dem EuGH gegen die Richtlinie über die Vorratsdatenspeicherung (2006/24/EG) geklagt,[26] und die zu erwartende Entscheidung war relevant für die rechtliche Grundlage der geplanten Regelung. Insbesondere die deutsche Regierung drang darauf, weitere Schritte bis nach den Entscheidungen des EuGH (der die Sache erst im Sommer 2008 verhandelte) sowie des Bundesverfassungsgerichts zur Vorratsdatenspeicherung zurückzustel-

24 Vgl. http://www.heise.de/newsticker/meldung/print/91861; Zugriff 1.8.2011.

25 Das wird ersichtlich, wenn man die in Abschnitt III des Abkommens aufgeführten Variablen mit den in Tabelle 2 dieses Aufsatzes aufgeführten Variablen vergleicht.

26 Die Dokumente – Klageschrift, Anträge, Urteil – dazu finden sich unter http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=DE&Submit=Rechercher$docrequire=alldocs&numaff=C-301/06&datefs=&datefe=&nomusuel=&domaine=&mots=&resmax=100; Zugriff: 19.5.2011. Der EuGH sah in seiner Entscheidung vom 10. Februar 2009 im Übrigen eine geeignete Rechtsgrundlage gegeben.

len; Österreich forderte, zunächst die Notwendigkeit einer zusätzlichen, europäischen Datenbank zu belegen.[27] Und schließlich stellte sich die deutsche Regierung, die wegen der hohen Sensibilität der heimischen Öffentlichkeit das Thema aus dem Wahlkampf heraushalten wollte, gegen eine neue Vereinbarung vor Ablauf der Legislaturperiode in Deutschland im Herbst 2009.[28]

Im Dezember 2009 ergriff dann die Kommission die Initiative, einen erneuten Vorschlag für einen Beschluss des Rates vorzulegen (EU-Kommission 2009). Nach diesem sollte das PNR-Abkommen nach den Regeln des (am 1.12.2009 in Kraft getretenen) Vertrags von Lissabon – und daher mit Zustimmung des Parlaments – endgültig beschlossen werden, wie zugleich auch entsprechende Abkommen mit weiteren Staaten wie Australien und Kanada (mit denen bisher ebenfalls nur vorläufige Abkommen bestanden). Im Mai 2010 lehnte das Europäische Parlament eine Zustimmung zu den vorliegenden PNR-Abkommen mit den USA und Australien ab und forderte die Kommission auf, bei neuen Verhandlungen auf die Einhaltung bestimmter Mindestanforderungen zu achten (EU-Parlament 2010).

Vorangegangen war dieser Entscheidung im Februar 2010 die Ablehnung des Abkommens über die Datentransfers in Sachen SWIFT durch das Europäische Parlament, ebenfalls unter seinen neuen Kompetenzen im Rahmen des Vertrages von Lissabon. Diese Entscheidung bildete den vorläufigen Schlusspunkt in dem Konflikt über den Transfer von Finanztransaktionsdaten, der 2006 entstanden war. Im September 2006 hatte die belgische Datenschutzkommission festgestellt, dass SWIFT mit seiner Praxis der Überlassung von Daten in den USA gegen die EU-Datenschutzrichtlinie verstoßen hatte. Die *Article 29 Working Group* kam zu demselben Ergebnis und setzte SWIFT eine Frist bis zum 1. September 2007, um wieder eine rechtmäßige Situation herzustellen. SWIFT beschloss daraufhin, dem ‚Safe Harbor'-Abkommen beizutreten, was die Kommission als hinreichend ansah (EU-Kommission 2007). Zudem gestand das US-Finanzministerium (nach öffentlichem Druck sowie dem des Europäischen Parlaments (EU-Parlament 2007) zu, dass man auf die europäischen Transaktionsdaten ausschließlich zu Zwecken der Terrorbekämpfung zugreifen werde und die dabei gewonnenen Daten nach fünf Jahren wieder löschen werde (U.S.-Treasury 2007).

Mit der Überprüfung dieser Verpflichtungen beauftragte die Kommission den französischen Richter Jean-Louis Bruguière. Er legte im Februar 2009 seinen ersten Bericht an die Kommission vor, in dem er die Wirksamkeit der Vorkehrungen in den USA bestätigte (EU-Kommission 2009a). Damit hätte die SWIFT-Episode beendet sein können, denn die Regierungen der EU-Mitgliedsstaaten waren grundsätzlich damit einverstanden, Finanzdaten zur Terrorbekämpfung zu benutzen. Die europäischen Innenminister wollten nun sogar selbst auf die europäischen Finanzdaten zugreifen; dies forderte die sogenannte EU-Zukunftsgruppe

27 Vgl. http://www.heise.de/newsticker/meldung/EU-Rat-verfolgt-eigenen-Weg-bei-Fluggastdaten-194308.html und http://www.statewatch.org/news/2008/jul/eu-pnr-11281-08.pdf; Zugriff: 19.5.2011.

28 Dies war zwischen Bundesjustizministerin Zypries und Bundesinnenminister Schäuble abgesprochen. Vgl. http://www.heise.de/newsticker/meldung/EU-Plaene-zur-Fluggastdatenspeicherung-liegen-auf-Eis-218699.html; Zugriff: 19.5.2011.

unter Leitung von Wolfgang Schäuble.[29] Im Themenbereich Finanztransaktionsdaten hatte also ein Prozess des *policy learning* bzw. der Imitation aus dem Bereich der Passagierdaten stattgefunden.[30]

Doch bereits im September 2007 hatte SWIFT angekündigt, die europäischen Finanztransaktionsdaten ab Ende 2009 nur noch auf einem in der Schweiz aufgestellten Server zu speichern. Dies hätte den USA den direkten Zugriff entzogen – eine Reaktion sowohl auf die Kritik von Datenschützern und Europäischem Parlament, aber auch auf die Wünsche der europäischen Finanzindustrie, der dieser Zugriff ebenfalls missfiel.[31] Dadurch wurde nun aber eine neue Vereinbarung zwischen der EU und den USA nötig, da die amerikanischen Behörden weiterhin auf diese Daten zugreifen wollten. Es ging nun also um die Weitergabe von europäischen Daten an Drittstaaten; die diesbezüglichen Verhandlungen verliefen bis zum Sommer 2009 weitgehend von der Öffentlichkeit unbeachtet.

Das änderte sich, als der Rat der Außenminister der schwedischen Ratspräsidentschaft ein Verhandlungsmandat erteilte und das Thema im beginnenden deutschen Bundestagswahlkampf große Aufmerksamkeit erhielt. Es kam zu einer starken Politisierung, da sich einerseits Parteien wie FDP und Grüne besorgt über die Einhaltung der Bürgerrechte äußerten (und auch die CSU Kritik der Datenschutzbeauftragten teilte), während andererseits Banken, Wirtschaftsunternehmen und der Bundesrat Wirtschaftsspionage durch das Abkommen befürchteten. Hinzu kam, dass Politiker auf der europäischen Ebene den Verdacht hegten, das neue Abkommen solle rasch verabschiedet werden, bevor der am 1. Dezember 2009 in Kraft tretende Vertrag von Lissabon das Mitentscheidungsverfahren (und damit die Ausweitung der Befugnisse des Europäischen Parlaments) auch für den Bereich Justiz und Inneres einführen würde. Einige EU-Parlamentarier, darunter der Vorsitzende der Grünen-Fraktion Daniel Cohn-Bendit, verknüpften die Bestätigung von Kommissionspräsident Barroso explizit mit seinem Verhalten beim SWIFT-Abkommen.[32] Das Parlament machte seine Einwände in einer Resolution am 17.9.2009 noch einmal deutlich. Und obwohl Frattinis Amtsnachfolger als Innen- und Justizkommissar, Jacques Barrot, den vorläufigen Charakter der neuen Vereinbarung betonte – ein endgültiges Abkommen sollte demnach erst nach Inkrafttreten des Vertrags von Lissabon und mit der dann notwendigen Beteiligung

29 Die Gruppe wurde auf Anregung von Schäuble und Frattini Anfang 2007 eingerichtet. Sie sollte Nachfolgeregelungen für das „Haager Programm" erarbeiten, das die europäische Innenpolitik bis Ende 2009 bestimmte. Das „Stockholmer Programm" wurde im Dezember 2009 von den Staats- und Regierungschefs der EU verabschiedet (Rat der EU 2009). Schäuble hat auch zusammen mit Frattini die Zugeständnisse der USA verhandelt, weil Deutschland im ersten Halbjahr 2007 die Ratspräsidentschaft inne hatte.

30 Das gilt auch für die PNR, bei denen Frattini ein eigenes europäisches System anstrebte, das das amerikanische exakt kopiert, vgl. http://futurezone.orf.at/stories/252094/; Zugriff 1.8.2011.

31 So der Country-Manager von SWIFT für Österreich im Juli 2008 in einem Interview, unter : http://futurezone.orf.at/stories/294809/; Zugriff 1.8.2011.

32 Die Attacke gegen die Kommission richtete sich allerdings wohl eher auf die Zukunft, führte doch zu diesem Zeitpunkt die Ratspräsidentschaft (und nicht die Kommission) die Verhandlungen zu SWIFT. Ziel war wohl eher die gesamte Innenpolitik der EU und insbesondere das so genannte Stockholmer Programm, mit dem deren Leitlinien für 2010 bis 2014 festgelegt wurden.

des Europäischen Parlaments geschlossen werden (Europäisches Parlament 2009)[33] – irritierte die plötzliche Eile des Vorhabens.

Die Folge war eine deutliche Verschlechterung der politischen Atmosphäre zwischen Parlament und Rat, nachdem letzterer am 30. November 2009 das SWIFT-Abkommen für die Dauer von neun Monaten ab dem 1. Februar 2010 angenommen hatte. Neben inhaltlichen Unklarheiten war man von Seiten des Parlaments vor allem empört, dass das Abkommen nicht bis zur Abstimmung im Parlament ausgesetzt wurde. Zudem wurde kritisiert, dass durch amerikanische Regierungsvertreter und die Kommission deutlicher Druck auf die Abgeordneten ausgeübt wurde,[34] das Abkommen anzunehmen – obwohl die Kritik aus dem Parlament in keiner Weise aufgenommen worden war. Als Folge ließ am 11. Februar 2010 eine deutliche Mehrheit der Abgeordneten (378 gegen 196) das Interimsabkommen scheitern.[35] Die Kommission wurde beauftragt, bei neuen Verhandlungen auf strengere Auflagen (wie etwa kürzere Speicherzeiten) zu dringen; nach umfangreichen Verhandlungen, in denen beide Seiten ein erneutes Scheitern vor dem Parlament verhindern wollten, kam es dann am 8. Juli 2010 zur Annahme, nachdem die Fraktionen der Liberalen, der Christdemokraten und der Sozialdemokraten für das Abkommen stimmten. Grüne, Linke und Datenschützer wie die *Article 29 Working Party* hielten ihre Kritik am Abkommen hingegen aufrecht. Sie bemängelten insbesondere, dass mit Europol eine Polizei- und keine Datenschutzstelle die Gesuche aus den USA überwachen solle, die auf Anfrage zu übermittelnden Datenpakete immer noch sehr umfangreich seien und die Umsetzung des Auskunftsverfahrens vollkommen unklar sei.[36]

Auswertungen der tatsächlichen Umsetzung des Abkommens haben in der Tat Schwachstellen offengelegt. So wurde Anfang Februar 2011 bekannt, dass die USA, anders als die Befürworter des Abkommens im EU-Parlament als angenommen hatten, auch auf die Daten des innereuropäischen Zahlungsverkehrs zugreifen konnten (FTD 2011). Auch wurde bekannt, dass Europol auf sehr unspezifische Anfragen aus den USA große Datenmengen transferiert hatte;[37] und es zeigte sich, dass die Auskunftsrechte nicht einmal in Ansätzen wahrgenommen werden konnten. Von europäischer Seite wird dies als Vertragsverletzung interpretiert (Spiegel Online 2011).

Zusammenfassend lässt sich sagen, dass die nach 2006 geänderten Akteurkonstellationen deutlichen Einfluss auf den Fortgang und die Ergebnisse der transatlantischen Verhandlungen über die Regulierung von personenbezogenen Daten gehabt haben; allerdings waren diese komplexer, als man bei oberflächlicher Be-

33 In einem Bericht der *New York Times* (2008) wird von diesem Vorhaben bereits im Frühsommer 2008 berichtet.

34 Vgl. http://www.heise.de/newsticker/meldung/SWIFT-Streit-Druck-auf-EU-Parlamentarier-waechst-923094.html; Zugriff: 18.5.2011.

35 Vgl. http://www.heise.de/newsticker/meldung/EU-Parlament-kippt-SWIFT-Abkommen-zum-Bankdatentransfer-927932.html; Zugriff: 18.5.2011. Im Dezember 2009 hatte eine Ablehnung noch als unwahrscheinlich gegolten.

36 Vgl. http://www.heise.de/newsticker/meldung/Praktisch-keine-Auskuenfte-fuer-EU-Buerger-ueber-ihre-in-den-USA-gespeicherten-Finanzdaten-1039937.html; Zugriff: 18.05.2011.

37 Vgl. http://www.heise.de/newsticker/meldung/EU-Kommission-wiegelt-Bedenken-gegen-Bankdaten-Transfer-in-die-USA-ab-1209949.html; Zugriff: 18.05.2011.

trachtung vielleicht erwartet hätte. So ist durch das *forum shifting* in die dritte Säule und die Dominanz des Rates als Akteur die Wichtigkeit des Sicherheits*frame* deutlich gestiegen und der allgemein in der Innen- und Rechtspolitik nach dem 11. September 2001 zu beobachtende Trend zur Sekuritisierung (vgl. Busch 2011) auch im Bereich der Regulierung transatlantischer Datenströme sichtbar. Doch führt die damit gestiegene Wichtigkeit der exekutivischen Perspektive keinesfalls zu einer völligen Übereinstimmung und Abwesenheit von Konflikten mit den amerikanischen Verhandlungspartnern; vielmehr bleibt auch in dieser Akteurkonstellation ein deutlicher Unterschied zwischen europäischer und amerikanischer Herangehensweise sichtbar. Diese Unterschiede werden nicht zuletzt deutlich bei dem Unvermögen der amerikanischen Seite, die mit dem Vertrag von Lissabon in diesem Themenbereich deutlich gestiegene Entscheidungskompetenz des Europäischen Parlaments wahrzunehmen und in der eigenen Verhandlungstaktik zu berücksichtigen. Auf der europäischen Seite wird die (durch Folgen der Klage vor dem EuGH vom Parlament selbst verschuldete) Abschwächung der Entscheidungskompetenzen durch Verlagerung der Materie in die dritte Säule nach einigen Jahren durch die generelle Aufwertung der Parlamentsbefugnisse im Rahmen des Vertrags von Lissabon kompensiert. Bleibender Effekt der verstärkten Rolle des Rates ist jedoch der geänderte Ansatz, personenbezogene Daten auch innerhalb Europas für den Kampf gegen den Terrorismus zu nutzen und ein eigenes europäisches Überwachungs- und Auswertungssystem aufzubauen. Dagegen bestehen, vor allem im Europäischen Parlament und bei den Datenschutzbehörden, weiter Bedenken. Der ursprüngliche Ansatz, den US-Behörden nur den Zugriff auf ein Minimum von Daten zu gewähren, ist nun durch den Aufbau eigener Datenverarbeitungskapazitäten in diesem Bereich sowie einer kontrollierten Weitergabe ersetzt worden.

7. Schluss

Die technologische und ökonomische Entwicklung der letzten beiden Jahrzehnte hat zu einem enormen Anstieg des Ausmaßes und der Dichte des internationalen Datenverkehrs geführt und damit auch der Frage nach der Regulierung des Austausches oft sehr sensibler Daten große Wichtigkeit zukommen lassen. Wie in diesem Beitrag geschildert, ist eine Vielzahl von alltäglichen Tätigkeiten im heutigen wirtschaftlichen und privaten Leben mit der Initiierung von Datenströmen verbunden, die oft über nationale Grenzen gehen; gleichzeitig sind jedoch die Schutzniveaus, denen solcher Datenaustausch unterliegt, im internationalen Vergleich weiterhin von erheblicher Unterschiedlichkeit. Zwar hat es deutliche regionale Harmonisierungsbestrebungen und auch -erfolge (beispielsweise innerhalb der Europäischen Union, aber auch innerhalb der APEC) gegeben, doch sind diese Schutzbestimmungen weiterhin weit von einer Einheitlichkeit entfernt (Busch 2011a).

Die Frage nach dem Umgang mit unterschiedlichen Regelungen für den grenzüberschreitenden Datenverkehr im Angesicht einer steigenden politischen und wirtschaftlichen Wichtigkeit desselben stand im Mittelpunkt der hier vorgelegten Analyse, wobei der Fokus auf dem Bereich der transatlantischen Beziehungen,

also der Auseinandersetzungen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union, lag. Aufgrund der engen wirtschaftlichen Verflechtungen zwischen diesen beiden hochentwickelten Märkten und der Tatsache, dass das Thema zunächst als ein vor allem kommerzielles gesehen wurde, lag eine Einigung über die Regulierung des grenzüberschreitenden Datenverkehrs zwischen beiden Jurisdiktionen im Interesse aller Beteiligten. In Gestalt des ‚Safe Harbor'-Abkommens trat sie im November 2000 in Kraft und wurde sowohl in der akademischen Literatur wie auch von Seiten der Politik als innovative Lösung und Vorbild für zukünftige Regelungen in diesem Bereich gefeiert, wie Abschnitt 5 dieses Beitrages im Detail darlegt.

Doch die Terroranschläge vom 11. September 2001 führten nur kurze Zeit später zu einer Verschiebung der *frames* im Bereich der Regulierung des grenzüberschreitenden Datenverkehrs vom Kommerz auf die Sicherheit. Wie im vorliegenden Beitrag ausführlich dargelegt, bedeutete dieser Framewechsel auch das Ende des Einvernehmens zwischen USA und Europäischer Union in diesem Bereich. Anstelle von Kompromissen kam es nun in wachsendem Maße zu einseitigem Vorgehen und sogar zu Androhungen (etwa mit dem Entzug von Landerechten für europäische Fluggesellschaften) durch die sich in ihrer Sicherheit bedroht sehenden USA, die zunehmend die Bedingungen für den transatlantischen Datenzugang diktieren wollten.

In der politikwissenschaftlichen Literatur zur Analyse des Themenbereichs Regulierung grenzüberschreitenden Datenverkehrs dominiert bislang ein konstruktivistischer Ansatz, der den Fokus auf Werte und Normen legt und die Wichtigkeit von Diskurs und Dialog betont. Doch die durch die Sekuritisierung des Themenbereichs ausgelösten veränderten Reaktionen der beteiligten Akteure kann ein solcher Ansatz nur unzureichend erklären. Eine Ergänzung – nicht Ersetzung! – durch weitere Analyseperspektiven ist daher notwendig, und wie im vorliegenden Beitrag gezeigt, empfehlen sich insbesondere zwei Ansätze in dieser Hinsicht:

- zum einen eine Unterscheidung der verschiedenen *frames*, durch die die Akteure das Themenfeld betrachten und interpretieren (und darauf aufbauend ihre Interessen verfolgen), sowie
- eine Berücksichtigung der institutionellen Gegebenheiten, insbesondere im Hinblick auf Kompetenzen der Akteure sowie der Interessenkonvergenzen und -divergenzen zwischen ihnen. Im Lauf des letzten Jahrzehnts sind deutliche Änderungen der Akteurkonstellationen eingetreten, vor allem auf der europäischen Seite. Durch den Machtzuwachs des Europäischen Parlaments im Rahmen des Vertrags von Lissabon ist diesem ein Blockadepotential zugewachsen, das den durch das *forum switching* nach dem EuGH-Urteil begründeten Bedeutungsverlust mehr als ausgleicht, aber von der amerikanischen Verhandlungsseite bisher kaum berücksichtigt zu werden scheint (Stand Sommer 2011).

Aufbauend auf diesen Ergänzungen konnte im vorliegenden Beitrag erklärt werden, warum sich in den drei betrachteten Fallstudien zur Regulierung des transatlantischen Datenverkehrs so unterschiedliche Dynamiken und Ergebnisse finden. Deutlich wurden darüber hinaus, dass die heutigen Positionen der Akteure in er-

heblichem Maße beeinflusst sind durch historisch tief verwurzelte Unterschiede in den Ansätzen zu Staatstätigkeit allgemein und zur Regulierung des Zugangs zu personenbezogenen Daten im Besonderen. Dem in Europa dominierenden Ansatz, diese Regulierung als Aufgabe des Staates zu sehen und über Gesetze zu regeln sowie dabei den Schutz des Individuums in den Mittelpunkt zu stellen, steht dabei ein in den Vereinigten Staaten bevorzugter Ansatz gegenüber, der die Vertragsfreiheit des Einzelnen auch in diesem Bereich als vorrangig betrachtet und daher freiwillige Vereinbarungen als das angemessene Instrument ansieht.

Im Bereich der transatlantischen Verhandlungen lässt sich aus letzterem ein Vorzug für konkrete, themenbezogene Regelungen ableiten, während der ersten Position eine Präferenz für allgemeine, umfassende Abkommen entspricht. Beides ist jedoch nur schwer zu vereinbaren, wie auch in weiteren, in diesem Beitrag bisher nicht berücksichtigten Verhandlungen zwischen den USA und der Europäischen Union in den letzten fünf Jahren deutlich wird. Seit November 2006 wird nämlich der Versuch unternommen, im Rahmen einer *High Level Contact Group on Information-Sharing and Privacy and Personal Data Protection* ein allgemeines EU-US-Datenschutzabkommen voranzutreiben. Auf der Basis eines Berichts zu gemeinsamen Prinzipien (vom Mai 2008 bzw. Oktober 2009) (Rat der EU 2009a) wird seit Anfang 2010 verhandelt; doch die jeweiligen Verhandlungsschwerpunkte der beiden Seiten haben eine Einigung bisher verhindert. So steht für die EU-Kommission ein gerichtlich durchsetzbarer Rechtsschutz im Vordergrund; und spezifische Abkommen wie die zu SWIFT und PNR sollen zwar bestehen bleiben, aber ausdrücklich den Vereinbarungen des Rahmenabkommens entsprechen (EU-Kommission 2010);[38] die USA hingegen wollen die bestehenden Abkommen auf keinen Fall durch ein Rahmenabkommen berührt sehen.[39]

Zum Zeitpunkt des Abschlusses dieses Beitrags (Spätsommer 2011) dauern die Verhandlungen noch an – und alle Erwartungen über ihren Ausgang sind daher notwendig spekulativer Natur. Dennoch lässt sich auf Grund der vorgenommenen Analyse die begründete Erwartung äußern, dass sich die Interessengegensätze zwischen den transatlantischen Partnern auf dem Gebiet der Regulierung grenzüberschreitenden Datenverkehrs auch in Zukunft fortdauern werden. Die Herausforderung an die Verhandlungspartner ist dabei, aus dem bisherigen Kreislauf von versuchtem Diktat einer Lösung, Blockade eines dauerhaften Abkommens und Zuflucht zu einer temporären Praxis auszubrechen. Für zukünftige politikwissenschaftliche Studien zu diesem Thema wird es daher wohl noch genügend Material und Anlässe geben.

38 Vgl. auch die nicht offiziell veröffentlichte Empfehlung unter http://www.statewatch.org/news/2010/aug/eu-usa-dp-general-em.pdf; Zugriff: 26.05.2011.

39 Das wurde bereits im Oktober 2010 bei einer Anhörung im Ausschuss für Bürgerliche Freiheiten des Europäischen Parlaments deutlich. Vgl. http://www.heise.de/newsticker/meldung/EU-und-USA-uneins-ueber-Datenschutz-Abkommen-1125752.html; Zugriff: 19.05.2011.

Literatur

Article 29 Data Protection Working Party. 2004. *Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)*, Brüssel. 29. Januar. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp87_en.pdf. Zugegriffen: 15.09.2011.

BBC News. 2000. *Yahoo hits back at Nazi ruling*. 21. November 2000. http://news.bbc.co.uk/2/hi/europe/1032605.stm. Zugegriffen: 15.09.2011.

Barlow, John Perry. 1996. *A Declaration of the Independence of Cyberspace*. http://homes.eff.org/~barlow/Declaration-Final.html. Zugegriffen: 15.09.2011.

Bennett, Colin J. 1992. *Regulating privacy. Data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press.

Bolkestein, Frits. 2003. Resisting U.S. demands - Passenger privacy and the war on terror. *International Herald Tribune* 24.10.2003.

Busch, Andreas. 2006. From Safe Harbour to the Rough Sea? Privacy Disputes across the Atlantic. *SCRIPT-ed. A Journal of Law and Technology* 3: 304–321. http://www.law.ed.ac.uk/ahrc/script%2Ded/vol3-4/busch.asp. Zugegriffen: 15.09.2011.

Busch, Andreas. 2011. Freiheits- und Bürgerrechte nach 9/11. *Zeitschrift für Außen- und Sicherheitspolitik* 4: 861–881.

Busch, Andreas. 2011a. The Regulation of Privacy. In *Handbook on the Politics of Regulation*, Hrsg. David Levi-Faur, 227–240. Cheltenham UK/Northampton MA: Edward Elgar.

Clinton, William J., und Albert Gore Jr. 1997. *A Framework for Global Electronic Commerce*. Washington D.C. http://clinton4.nara.gov/WH/New/Commerce/. Zugegriffen: 15.09.2011.

Drezner, Daniel W. 2004. The Global Governance of the Internet. Bringing the State Back In. *Political Science Quarterly* 119: 477–498.

Electronic Privacy Information Center, und Privacy International. 2004. *Privacy & Human Rights. An International Survey of Privacy Laws and Developments*. Washington, D.C./London: Electronic Privacy Information Center/Privacy International.

Europäische Gemeinschaften (Parlament und Rat). 1995. Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. 95/46/EG. 24.10.1995. *Amtsblatt der Europäischen Gemeinschaften* L 281/31, 23.11.1995.

Europäischer Gerichtshof. 2006. *Urteil des Gerichtshofes in den verbundenen Rechtssachen C-317/04 und C-318/04. Pressemitteilung 46/06*. 30.05.2006. http://curia.europa.eu/jcms/upload/docs/application/pdf/2009-02/cp060046de.pdf. Zugegriffen: 11.10. 2011.

Europäische Kommission. 2000. *Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (2000/520/EG)*. 26.07.2000. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2000D0520:20000825:DE:HTML. Zugegriffen: 15.09.2011.

Europäische Kommission. 2004. Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection, 2004/535/EC. 14.05.2004. *Amtsblatt der Europäischen Union* L 235/11, 06.07.2004. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:235:0011:0022:EN:PDF. Zugegriffen: 15.09.2011.

Europäische Kommission. 2007. *The SWIFT case and the American Terrorist Finance Tracking Program. Presseerklärung MEMO/07/266*. Brüssel. 28.06.2007. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/266&format=HTML&aged=0&language=EN&guiLanguage=en. Zugegriffen: 15.09.2011.

Europäische Kommission. 2009. *Vorschlag für einen Beschluss des Rates über den Abschluss des Abkommens zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Record – PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS) (PNR-Abkommen von 2007)*. Kom(2009) 702 endgültig. 2009/0187 (NLE). Brüssel. 17.12.2009. http://register.consilium.europa.eu/pdf/de/09/st17/st17697.de09.pdf. Zugegriffen: 01.08.2011.

Europäische Kommission. 2009a. *EU-Überprüfung des US-Programms zur Fahndung nach Finanzquellen des Terrorismus bestätigt Wirksamkeit der Datenschutzvorkehrungen*. IP/09/264. Brüssel. 17.02.2009. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/264&format=PDF&aged=0&language=DE&guiLanguage=en. Zugegriffen: 15.09.2011.

Europäische Kommission. 2010. *Europäische Kommission will Datenschutzabkommen mit den USA mit strengen Regeln für den Schutz der Privatssphäre. Pressemitteilung IP/10/609*. Brüssel. 26.05.2010. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/609&format=PDF&aged=1&language=DE&guiLanguage=en. Zugegriffen: 11.10.2011.

Europäisches Parlament. 2007. *PNR-SWIFT – European Parliament resolution on SWIFT, the PNR agreement and the transatlantic dialogue on these issues*. P6_TA(2007)0039. 14.02.2007. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:287E:0349:0353:EN:PDF. Zugegriffen: 15.09.2011.

Europäisches Parlament. 2009. *SWIFT: EU-US bank data-sharing will be an „interim" one, says Jacques Barrot*. Pressemitteilung. 22.07.2009. http://www.europarl.europa.eu/sides/getDoc.do?language=en&type=IM-PRESS&reference=20090720IPR58611. Zugegriffen: 15.09.2011.

Europäisches Parlament. 2010. *Fluggastdatensätze (PNR) – Entschließung des Europäischen Parlaments vom 5. Mai 2010 zum Start der Verhandlungen über Abkommen über Fluggastdatensätze mit den USA, Australien und Kanada*. P7_TA(2010)0144. 05.05.2010. http://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/definitif/2010/05-05/0144/P7_TA(2010)0144_DE.pdf. Zugegriffen: 15.09.2011.

Europäische Union (Kommission). 2004. Entscheidung der Kommission vom 14. Mai 2004 über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Passenger Name Records enthalten sind, welche dem United States Bureau of Customs and Border Protection übermittelt werden. 2004/535/EC. 14.05.2004. *Amtsblatt der Europäischen Union* L 235/11, 06.07.2004.

Europäische Union (Parlament und Rat). 2006. Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG. 15.03.2006. *Amtsblatt der Europäischen Union* L 105/54, 13.04.2006.

Farrell, Henry. 2003. Constructing the international foundations of E-commerce. The EU-US Safe Harbor arrangement. *International Organization* 57: 277–306.

FAZ-Net. 2007. *Datenschutz. Europäisches Parlament kritisiert Speicherung der Fluggastdaten*. 12.07.2007. http://www.faz.net/aktuell/politik/europaeische-union/datenschutz-europaeisches-parlament-kritisiert-speicherung-der-fluggastdaten-1461860.html. Zugegriffen: 15.09.2011.

Feick, Jürgen, und Raymund Werle. 2010. Regulation of Cyberspace. In *The Oxford Handbook of Regulation*, Hrsg. Robert Baldwin, Martin Cave und Martin Lodge, 523–547. Oxford: Oxford Univ. Press.

Financial Times Deutschland. 2011. *Swift-Vertrag: US-Einblick in europäische Bankdaten unterschätzt*. 01.02.2011. http://www.ftd.de/politik/international/:swift-vertrag-us-einblick-in-europaeische-bankdaten-unterschaetzt/60005765.html. Zugegriffen: 15.09.2011.

Froomkin, A. Michael. 2000. The Death of Privacy? *Stanford Law Review* 52: 1461–1543.

Hafner, Katie, und Matthew Lyon. 2000. *ARPA Kadabra oder die Geschichte des Internet*. 2., korr. Aufl. Heidelberg: dpunkt-Verl.

Heisenberg, Dorothee. 2005. *Negotiating Privacy. The European Union, the United States, and Personal Data Protection*. Boulder (CO): Lynne Rienner Publishers.

Holvast, Jan, Wayne Madsen, und Paul Roth (Hrsg.). 1999. *The global encyclopaedia of data protection regulation*. The Hague/London: Kluwer Law International.

International Telecommunication Union. 2006. *digital.life. ITU internet report 2006*. Geneva: International Telecommunication Union.

International Telecommunication Union. 2010. *Measuring the information society. 2010*. Geneva: International Telecommunication Union.

Kettl, Donald F. 2004. *System under stress. Homeland security and American politics* (Public affairs and policy administration series). Washington, D.C.: CQ Press.

Kommission der Europäischen Gemeinschaften. 2007. *Vorschlag für einen Rahmenbeschluss des Europäischen Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken*. Kom(2007) 654 endgültig. 2007/0237 (CNS). Brüssel, 06.11.2007. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0654:FIN:DE:PDF. Zugegriffen: 15.09.2011.

Lichtblau, Eric, und James Risen. 2006. Bank Data Sifted in Secret by US. to Block Terror. *The New York Times* 23.06.2006: 1.

Long, William J., und Marc Pang Quek. 2002. Personal data privacy protection in an age of globalization: the US - EU safe harbor compromise. *Journal of European Public Policy* 9: 325–344.

Mayer-Schönberger, Viktor. 1997. Generational Development of Data Protection in Europe. In *Technology and privacy. The new landscape*, Hrsg. Philip Agre und Marc Rotenberg, 219–241. Cambridge (MA)/London: MIT Press.

Michael, James R. 1994. *Privacy and human rights. An international and comparative study, with special reference to developments in information technology*. Aldershot, Hampshire: Dartmouth/Unesco Publishing.

Mitchell, Ronald B. 2002. International Environment. In *Handbook of international relations*, Hrsg. Walter Carlsnaes, Thomas Risse und Beth A. Simmons, 500–516. London/Thousand Oaks/New Delhi: SAGE.

Murray, Andrew. 2011. Internet Regulation. In *Handbook on the Politics of Regulation*, Hrsg. David Levi-Faur, 267–279. Cheltenham UK/Northampton MA: Edward Elgar.

National Research Council (Hrsg.). 2008. *Protecting individual privacy in the struggle against terrorists. A framework for program assessment*. Washington D.C.: National Academies Press.

Newman, Abraham L. 2008. *Protectors of privacy. Regulating personal data in the global economy*. Ithaca et al.: Cornell University Press.

New York Times. 2008. *U.S. and Europe Near Agreement on Private Data*. 28.06.2008. http://www.nytimes.com/2008/06/28/washington/28privacy.html. Zugegriffen: 15.09.2011.

O'Harrow, Robert. 2006. *No Place to Hide. Behind the Scenes of of our Emerging Surveillance Society*. New York, NY: Free Press.

Rat der Europäischen Union. 2007. *Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) Data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)*, 11595/07. Brüssel. 18.07.2007. http://register.consilium.europa.eu/pdf/en/07/st11/st11595.en07.pdf. Zugegriffen: 15.09.2011.

Rat der Europäischen Union. 2009. *Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger*. 17024/09. Brüssel. 02.12.2009. http://register.consilium.europa.eu/pdf/de/09/st17/st17024.de09.pdf. Zugegriffen: 15.09.2011.

Rat der Europäischen Union. 2009a. *Final Report by the EU-U.S. High Level Contact Group on Information Sharing and Privacy and Personal Data Protection*. 15851/09. Brüssel. 23.11.2009. http://www.dhs.gov/xlibrary/assets/privacy/-privacy_hlcg_reports_infosharing_personal_data_protection.pdf. Zugegriffen: 15.09. 2011.

Regan, Priscilla M. 2002. Privacy as a Common Good in the Digital World. *Information, Communication and Society* 5: 382–405.

Regan, Priscilla M. 2003. Safe harbors or free frontiers? Privacy and transborder data flows. *Journal of Social Issues* 59: 263–282.

Reidenberg, Joel R. 2000. Resolving Conflicting International Data Privacy Rules in Cyberspace. *Stanford Law Review* 52: 1315–1371.

Rein, Martin, und Donald A. Schön. (1996). Reframing Policy Discourse. In *The Argumentative Turn in Policy Analysis and Planning*, Hrsg. Frank Fischer und John Forester, 145–166. 2. Auflage. London: Duke Univ. Press.

Schön, Donald A., und Martin Rein. 1994. *Frame reflection. Toward the resolution of intractable policy controversies*. New York: Basic Books.

Shaffer, Gregory. 1999. The power of EU collective action. The impact of EU data privacy regulation on US business practice. *European Law Journal* 5: 419–437.

Spiegel Online. 2011. *Bankdaten-Debakel: Amerikaner verstoßen gegen Swift-Abkommen*. 31.03.2011. http://www.spiegel.de/politik/ausland/0,1518,754150,00.html. Zugegriffen: 15.09.2011.

Süddeutsche Zeitung. 2007. *EU sammelt Flugdaten*. 06.11.2007: 6.

The Economist. 2004. 15.05.2004: 9.

UNCTAD. 2004. *E-Commerce and Development Report 2004*. New York/Geneva: United Nations.

U.S. State Department. 2005. *FY 2005 Performance Plan*. http://www.state.gov/s/d/rm/rls/perfplan/2005/html/29302.htm. Zugegriffen: 15.09.2011.

U.S. Department of the Treasury. 2007. Schreiben des Finanzministeriums der Vereinigten Staaten zum Thema SWIFT/Programm zum Aufspüren der Finanzierung des Terrorismus (TFTP). 28.06.2007. *Amtsblatt der Europäischen Union*. Informationen von Drittstaaten. 2007/C166/08. 20.07.2007. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:166:0017:0017:DE:PDF. Zugegriffen: 15.09.2011.

Warren, Samuel D., und Louis D. Brandeis. 1890. The Right to Privacy. *Harvard Law Review* 4: 193–220.

Whitman, James Q. 2004. The Two Western Cultures of Privacy: Dignity Versus Liberty. *Yale Law Journal* 113: 1151–1221.

Zwick, Detlev, und Nikhilesh Dholakia. 2001. Contrasting European and American approaches to privacy in electronic markets: Property right versus civil right. *Electronic markets* 11: 116–120.