

14-2985-CV

IN THE
United States Court of Appeals
FOR THE SECOND CIRCUIT

In the Matter of a Warrant to Search a Certain E-mail Account
Controlled and Maintained by Microsoft Corporation,

MICROSOFT CORPORATION,

Appellant,

— v. —

UNITED STATES OF AMERICA,

Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

**JOINT APPENDIX
VOLUME II OF II
(Pages A145 to A346)**

Bradford L. Smith
David M. Howard
John Frank
Jonathan Palmer
Nathaniel Jones
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052

Guy Petrillo
PETRILLO KLEIN & BOXER LLP
655 Third Avenue
New York, NY 10017

E. Joshua Rosenkranz
Robert M. Loeb
Brian P. Goldman
ORRICK, HERRINGTON &
SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
(212) 506-5000

James M. Garland
Alexander A. Berengaut
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001

Attorneys for Appellant

(Counsel continued on inside cover)

Michael A. Levy
Justin Anderson
Assistant United States Attorneys
UNITED STATES ATTORNEY'S OFFICE
FOR THE SOUTHERN DISTRICT
OF NEW YORK
1 St. Andrew's Plaza
New York, NY 10007
(212) 637-2346

Attorneys for Appellee

TABLE OF CONTENTS

VOLUME I OF II

	Page
Docket entries	A1
Microsoft’s Memorandum in Support of Motion to Vacate, Dkt. No. 6, dated Apr. 25, 2014 (redacted)	A20
Declaration of Microsoft Lead Program Manager, Dkt. No. 7, dated Apr. 25, 2014 (redacted)	A35
Declaration of Microsoft Program Manager, Dkt. No. 8, dated Apr. 25, 2014 (redacted)	A39
Warrant, Exhibit 1 to the Declaration of Microsoft Program Manager, Dkt. No. 8, dated Apr. 25, 2014 (redacted)	A42
Declaration of Authentication of Business Records, Exhibit 2 to the Declaration of Microsoft Program Manager, Dkt. No. 8, dated Apr. 25, 2014 (redacted)	A49
Microsoft’s Reply Memorandum in Support of Motion to Vacate, Dkt. No. 10, dated Apr. 25, 2014 (redacted)	A51
Memorandum and Order, of Magistrate Judge James C. Francis IV Dkt. No. 5, dated Apr. 25, 2014	A71
Endorsed Letter Granting Stay Pending Appeal to the District Court, Dkt. No. 11, dated May 5, 2014.....	A98
United States Letter Not Opposing Stay Pending Appeal to the District Court, Dkt. No. 12, dated May 6, 2014.....	A103
Declaration of Microsoft Ireland Compliance Manager, Dkt. No. 16, dated June 6, 2014 (redacted)	A105

Declaration of Rajesh Jha, Dkt. No. 17, dated June 6, 2014 (redacted)	A107
Declaration of Michael McDowell, Dkt. No. 18, dated June 6, 2014.....	A114
Supplemental Declaration of Microsoft Lead Program Manager, Dkt. No. 19, dated June 6, 2014 (redacted)	A118
Declaration of Claire Catalano, Dkt. No. 20, dated June 6, 2014.....	A120
Email from Christopher B. Harwood to Nathan Wessler (Apr. 19, 2013), Exhibit 1 to the Declaration of Claire Catalano, dated June 6, 2014	A122
<i>How Brazil and The EU are Breaking the Internet</i> , Forbes (May 19, 2014), Exhibit 2 to the Declaration of Claire Catalano, dated June 6, 2014	A124
Letter from Sophie in't Veld to Viviane Reding (Apr. 28, 2014), Exhibit 3 to Declaration of Claire Catalano, dated June 6, 2014.....	A129
<i>Microsoft 'must release' data held on Dublin server</i> , British Broadcasting Corp. (Apr. 29, 2014), Exhibit 4 to Declaration of Claire Catalano, dated June 6, 2014.....	A131
European Commission Memorandum: Restoring Trust in EU-US data flows-Frequently Asked Questions (Nov. 27, 2013), Exhibit 5 to Declaration of Claire Catalano, dated June 6, 2014.....	A134

VOLUME II OF II

Supplemental Declaration of Claire Catalano, Dkt. No. 71, dated July 24, 2014	A145
Letter from Viviane Reding to Ms. in't Veld (June 24, 2014), Dkt. No. 71-1, dated July 24, 2014	A149
Christian Kahle, <i>US Wants to Rule over All Servers Globally</i> (July 24, 2014), Dkt. No. 71-2, dated July 24, 2014	A152

Francesco Lanza, <i>US Government to Microsoft: “Data stored online are not protected under the Fourth Amendment”</i> (July 15, 2014), Dkt. No. 71-3, dated July 24, 2014	A156
<i>US Government: Microsoft Servers Subject to US Laws, Irrespective of Country</i> , Inside Channels (July 15, 2014), Dkt. No. 71-4, dated July 24, 2014	A162
Henning Steier, <i>US Government Accessing Data on Foreign Servers</i> , Neue Zürcher Zeitung (July 15, 2014), Dkt. No. 71-5, dated July 24, 2014	A168
<i>Obama also demands access to data stored outside US</i> , Data News in Dutch (July 15, 2014), Dkt. No. 71-6, dated July 24, 2014	A174
<i>Obama Also Requires Access to Data Stored Outside of the USA</i> , Data News in French (July 15, 2014), Dkt. No. 71-7, dated July 24, 2014	A178
<i>US Government Requests Access to Data Held Abroad</i> , Der Standard (July 15, 2014), Dkt. No. 71-8, dated July 24, 2014	A182
<i>US Government: Access to Foreign Servers is Lawful</i> , Neue Osnabrücker Zeitung (July 15, 2014), Dkt. No. 71-9, dated July 24, 2014	A187
<i>US Government Requests Access to Data in EU Processing Centers</i> , Heise Online (July 15, 2014), Dkt. No.71-10, dated July 24, 2014	A192
<i>USA Also Wants Data from Foreign Servers</i> , Future Zone (July 15, 2014), Dkt. No. 71-11, dated July 24, 2014	A196
Richard Waters, <i>EU slams US over Microsoft privacy case</i> , Financial Times (June 30, 2014), Dkt. No. 71-12, dated July 24, 2014	A200

Ruadhán Mac Cormaic, <i>High Court refers Facebook privacy case to Europe</i> , Irish Times (June 19, 2014), Dkt. No. 71-13, dated July 24, 2014	A202
<i>Maximillian Schrems v. Data Protection Commissioner</i> , 2013 No. 765JR (Irish High Court June 18, 2014), Dkt. No. 71-14, dated July 24, 2014	A205
United Kingdom’s Data Retention and Investigatory Powers Act 2014, Dkt. No. 71-15, dated July 24, 2014	A242
Declaration of Joseph V. DeMarco, Dkt. No. 72, dated July 24, 2014	A254
Supplemental Declaration of Michael McDowell, Dkt. No. 73, dated July 24, 2014	A262
Corrected Transcript of July 31, 2014 Hearing Before Chief Judge Loretta A. Preska, Dkt. No. 93, dated Sept. 9, 2014.....	A264
Endorsed Letter Granting Temporary Stay Pending Appeal, Dkt. No. 79, dated August 1, 2014	A335
Order Confirming Bench Ruling, Dkt. No. 80, dated Aug. 11, 2014	A336
Microsoft’s Notice of Appeal, Dkt. No. 81, dated Aug. 11, 2014.....	A337
Order Holding Microsoft in Contempt, Dkt. No. 92, dated Sept. 8, 2014.....	A339
Microsoft’s Amended Notice of Appeal, Dkt. No. 95, dated Sept. 9, 2014.....	A344

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain
E-Mail Account Controlled and Maintained By
Microsoft Corporation

Case Nos. 13-MAG-2814; M9-150

SUPPLEMENTAL DECLARATION OF
CLAIRE CATALANO

CLAIRE CATALANO, pursuant to 28 U.S.C. § 1746, declares as follows under penalties of perjury:

1. I am an attorney duly admitted to practice before this Court, and an associate of the firm Covington & Burling LLP, counsel for Microsoft Corporation.
2. I submit this supplemental declaration in support of the above-referenced motion.
3. I attach as Exhibit 1 a true and correct copy of a letter from Viviane Reding, Vice-President of the European Commission Justice, Fundamental Rights and Citizenship, to Ms. in't Veld, dated June 24, 2014.
4. I attach as Exhibit 2 a true and correct copy of a certified translation of an article titled "US Wants to Rule over All Servers Globally," written by Christian Kahle on July 24, 2014, *available at* <http://winfuture.de/news,82668.html>.
5. I attach as Exhibit 3 a true and correct copy of a certified translation of an article titled "US Government to Microsoft: 'Data stored online are not protected under the Fourth Amendment'," written by Francesco Lanza on July 15, 2014, *available at* <http://www.downloadblog.it/post/112383/il-governo-usa-contro-microsoft-i-dati-conservati-online-non-sono-protetti-dal-4-emendamento>.

6. I attach as Exhibit 4 a true and correct copy of a certified translation of an article titled “US Government: Microsoft Servers Subject to US Laws, Irrespective of Country,” published by Inside Channels on July 15, 2014, *available at* <http://www.inside-channels.ch/articles/37013>.

7. I attach as Exhibit 5 a true and correct copy of a certified translation of an article titled “US Government Accessing Data on Foreign Servers,” published by Neue Zürcher Zeitung on July 15, 2014, *available at* <http://www.nzz.ch/mehr/digital/usa-microsoft-irland-1.18344021>.

8. I attach as Exhibit 6 a true and correct copy of a certified translation of an article titled “Obama also demands access to data stored outside US,” published by Data News in Dutch on July 15, 2014, *available at* <http://datanews.knack.be/ict/nieuws/obama-eist-ook-toegang-tot-data-opgeslagen-buiten-de-vs/article-4000692430542.htm>.

9. I attach as Exhibit 7 a true and correct copy of a certified translation of an article titled “Obama Also Demands Access to Data Stored Outside of the USA,” published by Data News in French on July 15, 2014, *available at* <http://datanews.levif.be/ict/actualite/obama-reclame-aussi-l-acces-aux-donnees-stockees-en-dehors-des-usa/article-4000692595991.htm>.

10. I attach as Exhibit 8 a true and correct copy of a certified translation of an article titled “US Government Requests Access to Data Held Abroad,” published by Der Standard on July 15, 2014, *available at* <http://derstandard.at/2000003099483/US-Regierung-fordert-Zugriff-auf-Daten-im-Ausland>.

11. I attach as Exhibit 9 a true and correct copy of a certified translation of an article titled “US Government: Access to Foreign Servers is Lawful,” published by Neue

Osnabrücker Zeitung on July 15, 2014, *available at* <http://www.noz.de/deutschland-welt/gut-zu-wissen/artikel/490495/us-regierung-zugriff-auf-server-im-ausland-ist-rechtens>.

12. I attach as Exhibit 10 a true and correct copy of a certified translation of an article titled “US Government Requests Access to Data in EU Processing Centers,” published by Heise Online on July 15, 2014, *available at* <http://www.heise.de/newsticker/meldung/US-Regierung-fordert-Zugriff-auf-Daten-in-EU-Rechenzentren-2260639.html>.

13. I attach as Exhibit 11 a true and correct copy of a certified translation of an article titled “US Also Wants Data from Foreign Servers,” published by Future Zone on July 15, 2014, *available at* <http://futurezone.at/netzpolitik/usa-wollen-auch-daten-von-auswaertigen-servern/75.024.634>.

14. I attach as Exhibit 12 a true and correct copy of an article titled “EU slams US over Microsoft privacy case,” published by the Financial Times on June 30, 2014, *available at* <http://www.ft.com/cms/s/0/1bfa7e90-ff6e-11e3-9a4a-00144feab7de.html>.

15. I attach as Exhibit 13 a true and correct copy of an article titled “High Court refers Facebook privacy case to Europe,” published by the Irish Times on June 19, 2014, *available at* <http://www.irishtimes.com/business/sectors/technology/high-court-refers-facebook-privacy-case-to-europe-1.1836657>.

16. I attach as Exhibit 14 a true and correct copy of the Irish High Court’s decision in *Maximillian Schrems v. Data Protection Commissioner*, dated June 18, 2014.

17. I attach as Exhibit 15 a true and correct copy of the United Kingdom’s Data Retention and Investigatory Powers Act 2014, *available at* http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf.

Dated: July 24, 2014
New York, New York

Claire Catalano

Claire Catalano, Esq.

EXHIBIT 1



Viviane REDING

Vice-President of the European Commission
Justice, Fundamental Rights and Citizenship

Rue de la Loi, 200
B-1049 Brussels
T. +32 2 298 16 00

Brussels, 24 June 2014

Dear Ms in 't Veld,

Thank you for your letter of 13 May concerning the Court of Justice ruling in the Google Spain case.

In its ruling the Court said, in relation to the territoriality of EU rules, that even if the physical server of a company processing data is located outside Europe, EU rules apply to search engine operators if they have a branch or a subsidiary in a Member State.

The Commission has welcomed the Court of Justice's decision. In the global world of digital services, the fundamental rights of EU citizens would be nothing more than empty shells if EU data protection rules were not to apply to non-EU companies. That is why the proposed data protection Regulation, for the first time, leaves no legal doubt that no matter where the physical server of a company processing data is located, non-EU companies, when offering services to EU consumers, must comply with EU data protection law (this is made explicit in Article 3 of the proposed data protection Regulation).

I am grateful for your support and that of fellow Members for this principle in the Parliament's report on the Commission's proposal. Furthermore, I am pleased that Ministers have reached agreement on this principle at their meeting in Luxembourg on 5-6 June 2014, namely that EU rules should apply to all companies, even those not established in the EU (territorial scope), whenever they handle personal data of individuals in the EU. Ministers have also confirmed a partial general approach on the rules governing transfers of personal data outside the EU, which will ensure that individual rights are protected and that transfers will only be allowed where the conditions of the Regulation for a transfer to third countries are met. This may, inter alia, be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject.

*Ms Sophie in 't Veld
Member of the European Parliament*

In your letter you also refer to the Microsoft case, which concerns a request by the United States government to personal data processed by US companies outside the US, e.g. in the EU. The effect of the US District Court order is that it bypasses existing formal procedures that are agreed between the EU and the US, such as the Mutual Legal Assistance Agreement, that manage foreign government requests for access to information and ensure certain safeguards in terms of data protection. The Commission's concern is that the extraterritorial application of foreign laws (and orders to companies based thereon) may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union. In addition, companies bound by EU data protection law who receive such a court order are caught in the middle of such situations where there is, as you say in your letter, a conflict of laws.

The Commission has raised this issue with the US government on a number of occasions. The Commission remains of the view that where governments need to request personal data held by private companies and located in the EU, requests should not be directly addressed to the companies but should proceed via agreed formal channels of co-operation between public authorities, such as the mutual legal assistance agreements or sectorial EU-US agreements authorising such transfers. In the context of the negotiations on the umbrella agreement on data protection in the area of law enforcement and judicial cooperation, the Commission has asked the US to undertake commitments in that regard, in order to avoid these potential conflicts of laws. In parallel, the EU institutions should continue working towards the swift adoption of the EU data protection reform, in order to ensure that personal data is effectively and comprehensively protected.

A handwritten signature in black ink, consisting of a series of loops and a long horizontal stroke at the end.

EXHIBIT 2

[advertisements]

US Wants to Rule over All Servers Globally

In the USA, a discussion has broken out about how far the arm of the US justice department may reach. At least the government is of the opinion that US agencies may access servers anywhere in the world, provided they have the respective court order.

The dispute started following a court order that [software company Microsoft should provide](#) criminal investigators in the USA with information stored on a server in Ireland. The court was of the opinion that the company had to obey the request, regardless of where it had actually stored the data, according to [Ars Technica](#).

The US government had also previously clarified its position on the legal situation: data stored on the Internet could not be compared to information stored in another country on a non-digital medium. Since Microsoft has access to the data in question from inside the USA, the request for release had to be granted.

Microsoft of course sees this differently and has appealed to the US Supreme Court. The company lawyers make it clear that a US court has no right to a decision enabling federal agents to enter a data center in Dublin to seize things. In separate statements, other IT and telecommunications companies such as Apple, AT&T, Cisco and Verizon backed up the software company in Redmond.

US economy threatened

In addition to the fundamental legal questions, Microsoft also brought up the current situation in its field, according to which it would be a great setback for the IT industry if the order was upheld. Due to the revelations by Edward Snowden, the trust of Internet users in US providers has already clearly suffered. Should the US government succeed with its position in the current case, this would constitute moving the US IT industry a further step ahead in losing its leading role in the global market one day.

[text at right]

Date: Thursday, 7/25/2014 10:56am

Further Reading: Rights, Politics & EU

Author: Christian Kahle

Login Registrieren

Startseite Ticker Downloads Videos Forum Preisvergleich Mehr

Wirtschaft > **Recht, Politik & EU** Wirtschaft & Firmen Personen aus der Wirtschaft Handel & E-Commerce

US-Regierung will Verfügungsmacht über alle Server weltweit



In den USA ist eine Debatte darüber entbrannt, wie weit der Arm der US-Justiz reichen kann. Die Regierung zumindest vertritt die Ansicht, dass US-Behörden mit einem entsprechenden gerichtlichen Beschluss auch auf Server zugreifen dürfen, die irgendwo auf der Welt stehen.

Datum: Dienstag, 15.07.2014 10:56 Uhr

Mehr: [Recht, Politik & EU](#)

Autor: [Christian Kahle](#)

523 Empfehlen 45 Twittern 23 +1

90 Kommentare

[Nachricht als E-Mail versenden](#)

[Hinweis einsenden](#)

Wöchentlicher Newsletter

[Beispiel Newsletter](#)

Neueste Downloads

Malwarebytes Anti-Malware 2.0.2 - Schadsoftware finden und löschen

CPU-Z 1.70 - Infos über CPU & Mainboard

CDBurnerXP 4.5.4.4954 (64-Bit) - CDs und DVDs brennen

[Mehr Downloads](#)

Jetzt als Amazon Blitzangebot



Datacolor Spyder4Pro stark reduziert im Blitzdeal

Original Amazon-Preis **136,99 €**

Blitzangebot-Preis **109 €**

Ersparnis 20% oder 27,99 €

[Kaufen bei Amazon.de](#)

Im WinFuture Preisvergleich

Datacolor: Spyder4Pro (multilingual) (PC/MAC)

- € 119,89 bei Foto Erhard
- € 119,90 bei Foto Koch
- € 123,95 bei Comtech
- € 124,50 bei Warsteiner-Fotoversand
- € 124,90 bei Foto Köster

56 Angebote im WinFuture.de Preisvergleich

[Alle Amazon Blitzangebote](#)

Video-Empfehlungen



John McAfee erklärt, wie man McAfee Antivirus wieder entfernt

Start Download

[downloadunzip.com](#)

Instant Free Download: Unzip. Start Here!

Die Auseinandersetzung entbrannte an einer Verfügung, dass der [Software-Konzern Microsoft](#) Informationen an Strafverfolger aus den USA [herausgeben sollte](#), die auf einem Rechner gespeichert sind, der in Irland steht. Das Gericht vertrat die Ansicht, dass das Unternehmen der Aufforderung unabhängig davon nachkommen muss, wo die konkrete Speicherung erfolgte, berichtet [Ars Technica](#).

Auch die US-Regierung hatte zuvor bereits ihre Sicht auf die Rechtslage klargemacht: Daten, die im Internet gespeichert seien, könnten nicht mit Informationen verglichen werden, die auf einem analogen Medium in einem anderen Land liegen. Da Microsoft von den USA aus Zugang zu den fraglichen Daten habe, müsse es einer Aufforderung nach deren Herausgabe nachkommen.

Zip & Unzip Files

- ✓ Totally Free
- ✓ Improved Conversion Ratio

It's FREE!

007 zip

Microsoft sieht dies natürlich anders und hat beim Obersten Gerichtshof der USA Beschwerde gegen die Verfügung eingereicht. Die Anwälte des Unternehmens machten deutlich, dass ein US-Gericht keine Befugnis auf einen Beschluss hat, der es Bundesbeamten ermöglicht, in ein Datenzentrum in Dublin einzudringen und Dinge zu beschlagnahmen. In eigenen Stellungnahmen stellten sich auch andere IT- und Telekommunikations-Konzerne wie Apple, AT&T, Cisco und Verizon hinter den Redmonder Software-Konzern.

US-Wirtschaft in Gefahr

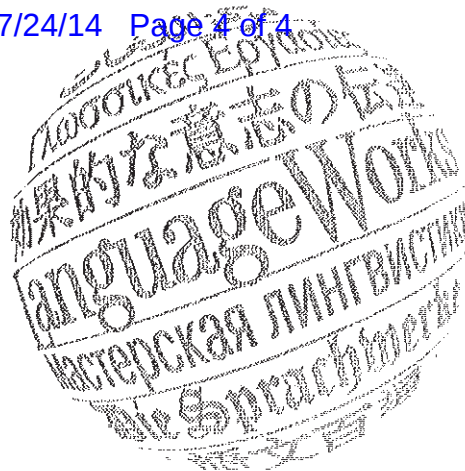
Microsoft führte in seiner Beschwerde neben den grundlegenden rechtlichen Fragen aber auch die aktuelle Situation ins Feld, wonach es für die IT-Industrie ein schwerer Schlag wäre, wenn die Verfügung aufrecht erhalten wird. Durch die Enthüllungen Edward Snowdens sei das Vertrauen der Internet-Nutzer in Anbieter aus den USA ohnehin schon deutlich angeschlagen. Sollte die US-Regierung im aktuellen Fall mit ihrer Haltung durchkommen, wäre es ein weiterer Schritt dahin, dass die IT-Wirtschaft aus den USA ihre führende Rolle auf dem Weltmarkt eines Tages verliert.

Diese Nachricht empfehlen

Empfehlen 523 Twittern 45 +1 23 90

Das könnte Sie auch interessieren

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257




LanguageWorks

STATE OF NEW YORK)
) ss:
COUNTY OF NEW YORK)

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "US-Regierung will Verfügungsmacht über alle Server weltweit" completed on 07/22/2014, originally written in German.



Kevin Hudson
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014



Notary Public

MARCEL HENRIQUE VOTLUCKA
Notary Public, State of New York
No. 01VO6154182
Certificate Filed in New York County
Qualified in Kings County
Commission Expires October 23, 2014

EXHIBIT 3

TECHNOLOGY

Homepage > Digital rights

US Government to Microsoft: “Data stored online are not protected under the Fourth Amendment”

Written by: [Francesco Lanza](#) – Tuesday, July 15, 2014

The Fourth Amendment to the US Constitution prohibits unreasonable searches and seizures, but the US government doesn't want that right applied to data stored online, especially abroad.

Microsoft tried to shield a user whose data are stored in its storage centers in **Dublin**, seeking to have the **international search warrants** issued by a New York judge declared unconstitutional. The US government was completely against this and reacted aggressively to attempts to rein in its wide-ranging powers of investigation.

In an official statement released yesterday, the government stated that data stored in the cloud are not granted the same type of protection afforded to “physical” information, protected under the **Fourth Amendment to the US Constitution**. In fact, according to the Stored Communications Act, such data have always been much more accessible than [normal correspondence and private assets held abroad](#).

READ ALSO: [ProtonMail, the e-mail service the NSA can't penetrate](#)

These days, hackers and scammers who use electronic communication methods both in the United States and abroad in an attempt to get around the law, make this double standard a necessity.

It seems as though the US government is the only party not concerned about the implications of its sprawling control over the entire planet's data, and even **Verizon** has joined forces with **Microsoft** to contend that these arguments are in direct conflict with foreign laws on data protection. **Apple** and **Cisco** have responded similarly, saying that the US government seems fully determined to damage commercial and diplomatic relationships with both allied and non-aligned countries.

INSIGHT: [Obama authorizes the use of software vulnerabilities for espionage and investigations](#)

In fact, the White House's legal argument simply adds fuel to the fire of the media disaster known as the **Snowden** affair.

For its part, the Irish government does not seem at all concerned about the long-term damage caused by US legal rulings; on the contrary, it seems more than willing

to provide US investigators with the personal data and access to e-mail that they seek. Actually, that shouldn't be too surprising: the case involves international drug trafficking.



TECNOLOGIA

Homepage > Diritti digitali

Il Governo USA contro Microsoft: "I dati conservati online non sono protetti dal 4° Emendamento"

Scritto da: [Francesco Lanza](#) - martedì 15 luglio 2014

Mi piace

15

Tweet

9

G+

1

Share

Pin it

0

Il 4° Emendamento della Costituzione degli Stati Uniti d'America stabilisce il diritto di non essere oggetto di perquisizioni irragionevoli e immotivate, un diritto che al Governo statunitense non fa comodo venga applicato ai dati conservati online, specie all'estero





Microsoft ha cercato di difendere un utente i cui dati sono conservati nei suoi centri di stoccaggio a **Dublino**, cercando di far giudicare incostituzionali i **mandati di perquisizione internazionali** ratificati da un giudice newyorkese. Il Governo USA non ne vuole sapere, e regisce con violenza ai tentativi di arginare il proprio strapotere investigativo.

In una dichiarazione ufficiale rilasciata ieri il Governo ha comunicato che per quello che lo riguarda i dati conservati su cloud non hanno lo stesso genere di protezione accordato ai dati “fisici”, coperti dal **4° Emendamento della Costituzione degli Stati Uniti d'America**. Secondo lo Stored Communication Act, infatti, tali dati sono sempre stati molto più accessibili della [normale corrispondenza e dei beni privati conservati all'estero](#).

LEGGI ANCHE: [ProtonMail, il servizio di posta elettronica impenetrabile dall'NSA](#)

La necessità di tale doppio standard deriva dalla presenza di “hacker” e “truffatori” in questa epoca, che usano i mezzi di comunicazione elettronica sia negli USA che all'estero, nel tentativo di aggirare le maglie della legge.

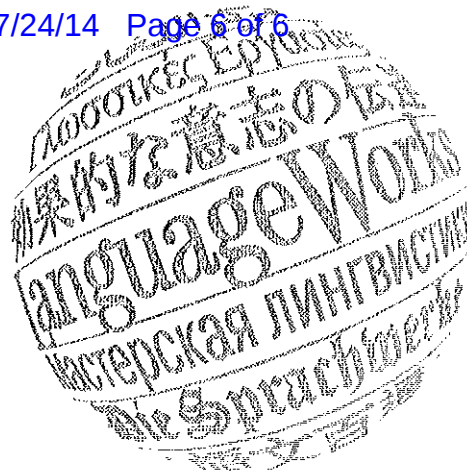
A quanto pare il Governo USA è l'unico a non essere preoccupato dalle implicazioni derivate dal suo dominio tentacolare sui dati dell'intero pianeta Terra, ed anche **Verizon** ha unito la sua voce a quella di **Microsoft** per ribadire che questi ragionamenti entrano direttamente in conflitto con le leggi straniere sulla protezione dei dati. **Apple** e **Cisco** hanno similmente reagito, dicendo che il Governo USA sembra direttamente intenzionato a danneggiare i rapporti commerciali e diplomatici con gli altri paesi alleati e non allineati.

APPROFONDIMENTO: [Obama autorizza l'uso di vulnerabilità software per lo spionaggio e le indagini](#)

Il ragionamento legale dell'esecutivo statunitense, infatti, non fa altro che mettere altra benzina sul fuoco del disastro mediatico che è stato l'affare **Snowden**.

Dal canto suo il Governo irlandese non sembra affatto preoccupato dai danni a lungo termine causati dalle decisioni legali statunitensi, anzi, sembra più che ben disposto a fornire agli inquirenti statunitensi i dati personali e l'accesso alla casella mail che stanno cercando. Non meravigliatevi troppo: si tratta di un caso di commercio di stupefacenti internazionale.

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257



LanguageWorks

STATE OF NEW YORK)
) ss:
COUNTY OF NEW YORK)

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of Il Governo USA contro Microsoft: 'I dati conservati online non sono protetti dal 4° Emendamento'" completed on 07/22/2014, originally written in Italian.

Kevin Hudson
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014

Notary Public

MARCEL HENRIQUE VOTLUCKA
Notary Public, State of New York
No. 01VO6154182
Certificate Filed in New York County
Qualified in Kings County
Commission Expires October 23, 2014

EXHIBIT 4

[advertisement]

Inside-channels.ch

Tuesday, 7/15/2014

US Government: Microsoft Servers Subject to US Laws, Irrespective of Country

An email account is stirring up the world of the Cloud.

In the USA, a dispute between the US Department of Justice and Microsoft has been going on [for a long time](#). While, in concrete terms, this is merely about the content of an email account stored in Ireland, the outcome of this precedent case could strongly impact the future of cloud business across the globe. The question is whether US judges may force domestic companies to release data stored abroad, regardless of where such data are stored and what laws might apply in the respective country.

A US federal judge will have to address the issue soon. In a recent [submission](#) to this judge, the Obama government has now confirmed its legal position and explained that, for criminal prosecution purposes, US agencies need to have access to client data of US companies, even if such data were stored abroad. According to this position, an order by a US judge seeing sufficient indication that certain data could contain relevant data would have to force data to be released. The laws and agencies in the respective country would play no role in this. A "detour" via a legal assistance process and/or cooperation with authorities in the respective country would thus become unnecessary.

To search or not to search?

Throughout, the US government is backing up its request by citing the Stored Communications Act of the Reagan era. Microsoft, on the other hand, argues that this law could not apply abroad. In its view, such a request would correspond to a search warrant, and no US court could order US agents to break open a door at the Microsoft processing center in Dublin, for example, in order to seize data. According to Microsoft, Congress explicitly decided in its favor recently.

The US government, however, considers this argument completely irrelevant since the release of data stored online has nothing in common with a physical search.

In its line of argument, Microsoft is supported by [other IT giants such as Apple, AT&T, Cisco and Verizon](#). A lot of money is at stake for American companies. If the US government prevails, foreign clients' confidence in their cloud-based services, already weakened by the Snowden affair, is likely to decline even further. And employees abroad could end up in a legal dilemma if they had to choose whether to comply with US Justice Department orders or local laws. Foreign branches of US companies have so far adamantly emphasized that they would, of course, always do the latter. (hjm)

More on this topic

[Microsoft not \(yet\) providing data to US government](#)
[US agencies may continue to access cloud data abroad.](#)
[Obama's expert group defends NSA practices](#)

[article comments]

GEFUNDEN WERDEN STATT SUCHEN. ICTJOBS.CH – DIE INTELLIGENTE JOBPLATTFORM FÜR ICT-PROFIS IN DER SCHWEIZ.

DER ONLINE STELLENMARKT FÜR ICT-PROFESSIONALS **ictjobs.ch**



Dienstag, 15.07.2014

US-Regierung: Microsoft-Server unterstehen US-Gesetzen, egal in welchem Land

Ein E-Mail-Account bewegt die Cloud-Welt.

In den USA schwelt [seit einiger Zeit](#) ein Streit zwischen dem US-Justizdepartement und Microsoft. Konkret geht es zwar nur um den Inhalt eines in Dublin gespeicherten E-Mail-Accounts, der Ausgang dieses Streits könnte als Präzedenzfall aber die Zukunft des Cloud-Geschäfts weltweit stark beeinflussen. Es geht darum, ob US-Richter einheimische Unternehmen zur Herausgabe von im Ausland gespeicherten Daten zwingen können, egal wo diese Daten lagern und welche Gesetze im betreffenden Land gelten.

In Kürze wird sich ein US-Bundesrichter den Kopf darüber zerbrechen müssen. In einer [Eingabe](#) an diesen Richter hat die Obama-Regierung nun ihren Standpunkt bekräftigt und vertieft, dass US-Behörden für strafrechtliche Untersuchungen Zugriff auf Daten von Kunden von US-Unternehmen haben müssen, auch wenn diese im Ausland gelagert werden. Eine Anordnung eines US-Richters, der einen hinreichenden Verdacht sehe, dass in bestimmten Daten relevante Informationen enthalten sein könnten, müsse ausreichen, um die Herausgabe zu erzwingen. Die Gesetze und Behörden im betreffenden Land würden dabei keine Rolle spielen. Ein "Umweg" über ein Rechtshilfeverfahren beziehungsweise eine Zusammenarbeit mit den Behörden im entsprechenden Land wäre damit unnötig.

Durchsuchung oder keine Durchsuchung?

Die US-Regierung stützt sich dabei auf den aus den Reagan-Jahren stammenden "Stored Communications Act". Microsoft argumentiert dagegen, dass dieses Gesetz nicht für das Ausland gelten könne. Eine solche Anordnung entspreche einem Durchsuchungsbefehl, und kein US-Gericht könne es US-Beamten befehlen, beispielsweise beim Microsoft-RZ in Dublin Türen aufzubrechen um Daten zu beschlagnahmen. Der Kongress habe dies kürzlich ausdrücklich so beschlossen.

Die US-Regierung wiederum empfindet dieses Argument als völlig irrelevant, da die Herausgabe von "online" gespeicherten Daten nichts mit einer physischen Durchsuchung zu tun habe.

Microsoft wird in seiner Argumentation von [anderen IT-Riesen wie Apple, AT&T, Cisco und Verizon](#) unterstützt. Für die amerikanischen Unternehmen geht es um viel Geld. Wenn sich die US-Regierung durchsetzt, dürfte das schon durch die Snowden-Affäre geschwächte Vertrauen ausländischer Kunden in ihre Cloud-Services weiter sinken. Zudem könnten Angestellte im Ausland ins juristische Dilemma geraten, wenn sie wählen sollen, ob sie die Anordnungen der US-Justiz oder die lokalen Gesetze befolgen wollen. Ausländische Niederlassungen von US-Unternehmen betonen bisher hartnäckig, dass sie selbstverständlich immer das letztere tun würden. (hjm)

Mehr zu diesem Thema:

[Microsoft liefert der US-Regierung \(noch\) keine Daten](#) **A165**

US-Behörden dürfen weiterhin auf Cloud-Daten im Ausland zugreifen
Obamas Expertengruppe verteidigt NSA-Praktiken

Kommentare:

Peter Zimmermann

15.07.2014 18:34 *Toll, wir könnten sicher eine Menge Geld und Personalressourcen sparen, wenn wir unseren Justizapparat gleich an die USA outsourcen. Brave new world!*

Peter Tobler

16.07.2014 12:33 *Diese Sache ist zweischneidig: Einerseits glaubt die US-Justiz tatsächlich siehe könne alles was zu ihrem Vorteil ist weltweit durchsetzen, egal was andere davon halten.*

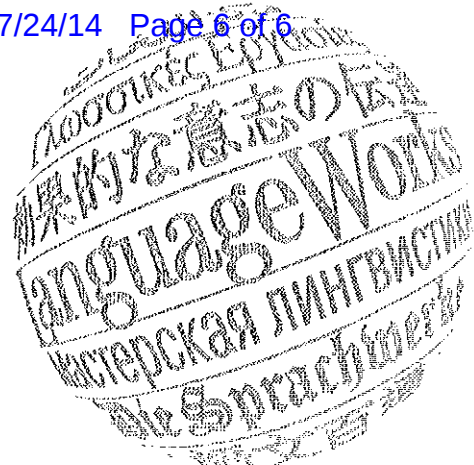
Andererseits können sich US-Unternehmen unter Umständen zu leicht hinter ausländischer Gesetzgebung verstecken - um vermutlich nicht immer nur legale Aktivitäten vor dem Zugriff von US-Gerichten zu schützen.

Gegen die zweite Variante gäbe es allerdings eine äusserst simple Vorgehensweise: Riesige Firmen wie Microsoft und Co müssten schlicht ihren rechtlichen Firmensitz in ein vorteilhafteres Land zügeln als die USA. Das dürfte die US-Regierung und -Justiz wohl äusserst schnell zum Einlenken zwingen. Schliesslich würde damit nicht nur die rechtliche Unterstellung sondern die viel relevantere Steuerliche auf den Tisch kommen.

Andreas Moser

21.07.2014 16:16 *Meines Erachtens tun amerikanische Firmen gut daran zu prüfen, ob sie in Europa nicht mit lokalen Partnern zusammenarbeiten möchten oder ob sie nicht in Europa Firmen gründen möchten, die ausschliesslich unserem Rechtsempfinden entsprechen. Ich finde es als äusserst stossend, wenn Regierungen die Souveränität von Drittstaaten im Bereich Recht nicht anerkennen wollen. Die Vereinigten Staaten von Amerika gehören leider dazu.*

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257




LanguageWorks

STATE OF NEW YORK)
) ss:
COUNTY OF NEW YORK)


CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "US-Regierung: Microsoft-Server unterstehen US-Gesetzen, egal in welchem Land" completed on 07/22/2014, originally written in German.



Kevin Hudson
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014



Notary Public

MARCEL HENRIQUE VOTLUCKA
Notary Public, State of New York
No. 01VO6154182
Certificate Filed in New York County
Qualified in Kings County
Commission Expires October 23, 2014

EXHIBIT 5

Neue Zürcher Zeitung

Tuesday, July 15, 2014, 2:22pm

Precedent

US Government Accessing Data on Foreign Servers

Henning Steier Tuesday, July 15, 2014, 2:22pm

[image caption: Who may access processing center data globally? (image: Imago/Symbolfoto)]

IT giants are not the only ones who are currently paying close attention to whether the largest software producer will prevail in its court case versus the US government. The decision will have far-reaching consequences for companies and users alike.

In the USA, Microsoft is taking legal action against having to provide US agencies with data stored in computer processing centers outside the United States. The line of argument by the American government in this court case, which will continue in late July, has now become public. In essence, it refers to the Stored Communications Act (SCA) of 1986 and [assumes](#) that online content is not protected under the Fourth Amendment. This Amendment concerns protection against federal searches and seizures.

At the end of April, a New York court argued that American companies must release data stored on servers abroad if there is a relevant request by a US government agency. Based on a search warrant in a drug smuggling case, Microsoft was asked to release client data stored on a server in Ireland. The company argued that the principle, according to which court-ordered search warrants are non-applicable abroad, would also have to be transferred to the online world. Judge James Francis however saw it differently and argued in his decision that the resulting burden would be major and criminal investigations would be gravely obstructed if US agencies first had to send requests for legal assistance to foreign governments.

Loss of trust as business risk

Following the [Snowden revelations](#), the largest software producer fears a [further reputational loss for US companies](#) and, as a result, an adverse impact on business in the rest of the world. Other large IT companies see it similarly. Verizon assumes that a decision in favor of the government could result in “conflicts with data protection laws in other countries.” Apple and Cisco also fear that the technology sector “runs the danger of being sanctioned by foreign governments.”

Microsoft opened its processing center in Ireland four years ago. By now, the company is running approximately 100 in 40 countries. In spring, the [Vereinigung der schweizerischen Datenschutzbeauftragten \(Privatim\)](#) prevailed against Microsoft

[Schweiz](#) by convincing the company to alter its contractual conditions as to permit the use of Office 365 in an academic context. To that end, a contract change specifically applying to the Swiss educational sector was developed, ensuring that usage in compliance with data privacy laws is guaranteed. Concretely, this also means: upon request, data may be stored only in Europe. The present court case in the USA should demonstrate how valuable this is.

Follow Digital editor Henning Steier in Social Networks:

You can order the daily Digital newsletter [here](#).

Dienstag, 15. Juli 2014, 14:22

Präzedenzfall

US-Regierung greift nach Daten in ausländischen Rechenzentren

Henning Steier Dienstag, 15. Juli 2014, 14:22



Wer darf global auf Daten in Rechenzentren zugreifen? (Bild: Imago/Symbolfoto)

Gespannt beobachten nicht nur IT-Riesen, ob der grösste Softwarehersteller im Prozess gegen die US-Regierung Erfolg hat. Das Urteil hat weitreichende Folgen für Unternehmen und Nutzer.

Microsoft wehrt sich in den USA gerichtlich dagegen, Daten an US-Behörden übergeben zu müssen, die in Rechenzentren ausserhalb der Vereinigten Staaten liegen. Im Prozess, der Ende Juli fortgesetzt wird, ist nun die Argumentationslinie der amerikanischen Regierung bekannt geworden. Im Kern beruft man sich auf den Stored Communications Act (SCA) von 1986 und geht davon aus, dass Online-Inhalte nicht vom Vierten Zusatzartikel geschützt sind. In diesem Artikel geht es um den Schutz vor staatlichen Übergriffen.

Ende April hatte ein New Yorker Gericht geurteilt, dass amerikanische Firmen Daten auf im Ausland befindlichen Servern herausgeben müssen, wenn eine entsprechende Anordnung einer US-Behörde vorliegt. Microsoft sollte gemäss einem Durchsuchungsbefehl in einen Drogenschmuggler-Fall Kundendaten aushändigen, die in einem Rechenzentrum in Irland gespeichert sind. Das Unternehmen argumentierte, der Grundsatz, nach dem gerichtlich angeordnete Hausdurchsuchungen im Ausland nicht durchsetzbar seien, müsse auch auf die virtuelle Welt übertragbar sein. Der Richter James Francis sah dies anders und

begründete sein Urteil damit, dass – müssten die US-Behörden erst Rechtshilfesuche an die ausländischen Regierungen stellen – die Belastung erheblich wäre und Strafverfolgungen ernsthaft behindert würden.

Vertrauensverlust als Geschäftsrisiko

Nach den **Snowden-Enthüllungen** befürchtet der grösste Softwarehersteller einen **weiteren Reputationsverlust für US-Unternehmen** und somit erschwerte Geschäfte im Rest der Welt. Andere grosse IT-Firmen sehen das ähnlich. Verizon geht davon aus, dass eine Entscheidung zugunsten der Regierung zu «Konflikten mit den Datenschutzgesetzen anderer Länder» führen könnte. Auch Apple und Cisco befürchten, dass der Technologiesektor «Gefahr läuft, von ausländischen Regierungen sanktioniert zu werden».

Microsoft eröffnete sein Rechenzentrum in Irland vor vier Jahren. Mittlerweile betreibt das Unternehmen rund 100 in 40 Ländern. Im Frühjahr hatte sich die **Vereinigung der schweizerischen Datenschutzbeauftragten (Privatim) gegen Microsoft Schweiz durchgesetzt** und das Unternehmen überzeugt, seine vertraglichen Bedingungen so anzupassen, dass im Schulbereich der Einsatz von Office 365 zulässig wird. Dafür wurde eine speziell für den Schweizer Bildungsbereich geltende Vertragsergänzung ausgearbeitet, die sicherstellt, dass eine datenschutzkonforme Nutzung gewährleistet ist. Konkret heisst das unter anderem: Daten lassen sich auf Wunsch nur in Europa speichern. Der Prozess in den USA dürfte zeigen, was das wert ist.

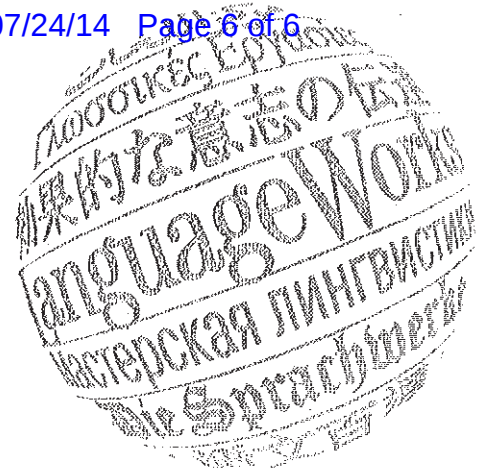
Digital-Redaktor Henning Steier in Social Networks folgen:

Follow [@henning_steier](#)



Hier können Sie den werktäglichen Digital-Newsletter bestellen.

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257




LanguageWorks

STATE OF NEW YORK)
) ss:
COUNTY OF NEW YORK)

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "US-Regierung greift nach Daten in ausländischen Rechenzentren" completed on 07/22/2014, originally written in German.



Kevin Hudson
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014



Notary Public

MARCEL HENRIQUE VOTLUCKA
Notary Public, State of New York
No. 01VO6154182
Certificate Filed in New York County
Qualified in Kings County
Commission Expires October 23, 2014

EXHIBIT 6

Obama also demands access to data stored outside US



(<http://datanews.knack.be/ict/service/contact/author-1194715612360.htm>)
Frederik Tibau (<http://datanews.knack.be/ict/service/contact/author-1194715612360.htm>)

July 15, 2014 – 10:00



The Obama administration is proposing that data stored on the servers of American companies outside the United States must be accessible to judicial authorities.

Technology companies such as Microsoft and Apple are screaming bloody murder and argue that upholding justice stops at the border.

According to the US government, global access to information is necessary to be better able to track scammers, hackers, and drug dealers. Obama & Co. also argue that any company with operations in the United States must comply with the data requirements of that country, even if the data have been stored on the other side of the world.

Tech giants like Microsoft and Apple do not agree on this and argue that confidence in American technology companies will take yet another blow that way, after the Snowden revelations.

And now one judge has subscribed to Obama's position. During a court case just last April involving a Microsoft customer, he put forward the idea that "an entity that is statutorily obligated to provide access to data must do so regardless of the location of those data."

Microsoft has already brought in a battery of lawyers to file an appeal. A ruling on the case is expected on July 31.

The US government is relying on the **Stored Communications Act** (<http://cdn.arstechnica.net/wp-content/uploads/2014/07/federalbrief-microsoftcase.pdf>) (SCA) to hit back, a rule that dates from the Reagan era. That rule states, "Overseas records must be disclosed domestically when a valid subpoena, order, or warrant compels their production."

Microsoft will again argue that the US Congress has never given the order to require information from outside the physical borders of the United States. "Furthermore, an American court cannot just require someone to break into the Microsoft's data center in Dublin," Redmond says. "The only thing that the government will achieve that way is American companies losing their leading position in IT."

Industry partners Apple, AT&T, Cisco, and Verizon **argue** (<http://cdn.arstechnica.net/wp-content/uploads/2014/07/applebriefinremicrosoft.pdf>) that a ruling in favor of the administration may cause "dramatic conflicts with foreign laws on data protection."

These companies argue that "there is a very great risk that foreign governments will penalize the tech industry and that it is better to work together with other nations."

[advertisement below]

Obama eist ook toegang tot data opgeslagen buiten de VS



(<http://datanews.knack.be/ict/service/contact/author-1194715612360.htm>)
 Frederik Tibau (<http://datanews.knack.be/ict/service/contact/author-1194715612360.htm>)

15/07/2014 - 10:0



De Obama-administratie oppert dat data die is opgeslagen op servers van Amerikaanse bedrijven buiten de VS, toegankelijk moet zijn voor het gerecht.

Technologiebedrijven als Microsoft en Apple schreeuwen moord en brand, en argumenteren dat de handhaving van het recht stopt aan de grens.

Volgens de Amerikaanse overheid is een wereldwijde toegang tot informatie nodig om fraudeurs, hackers en drugdealers beter te kunnen opsporen. Obama en co. stellen dan ook dat elk bedrijf met activiteiten in de VS moet voldoen aan de dataveren van dat land, zelfs als de data aan de andere kant van de wereld is opgeslagen.

Tech giganten als Microsoft en Apple zijn het hier niet mee eens, en opperen dat het vertrouwen in Amerikaanse technologiebedrijven op die manier nog maar eens een knauw krijgt, na de revelaties van Snowden.

Alvast één rechter volgt het standpunt van Obama. Hij wierp in april al op tijdens een rechtszaak waarin een klant van Microsoft betrokken was, dat 'een entiteit die wettelijk verplicht wordt om inzage te geven in data, dat moet doen ongeacht de locatie van die data.'

Microsoft heeft alvast een batterij advocaten ingeschakeld om in beroep te gaan. Op 31 juli wordt een uitspraak ten gronde verwacht in de zaak.

De Amerikaanse overheid beroept zich op de '**Stored Communications Act**' (<http://cdn.arstechnica.net/wp-content/uploads/2014/07/federalbrief-microsoftcase.pdf>) (SCA) om haar gram te halen, een regel die dateert uit de tijd van Ronald Reagan. "Overseas records must be disclosed domestically when a valid subpoena, order, or warrant compels their production", klinkt het in dat document.

Microsoft oppert dan weer dan het Amerikaanse Congres nog nooit het bevel heeft gegeven om informatie op te eisen buiten de fysieke grenzen van de VS. "Bovendien kan een Amerikaanse rechtbank zo maar niet eisen om in te breken in het datacenter van Microsoft in Dublin", klinkt het in Redmond. "Het enige wat de overheid hiermee bereikt is dat Amerikaanse bedrijven hun leidinggevende positie kunnen verliezen in ict."

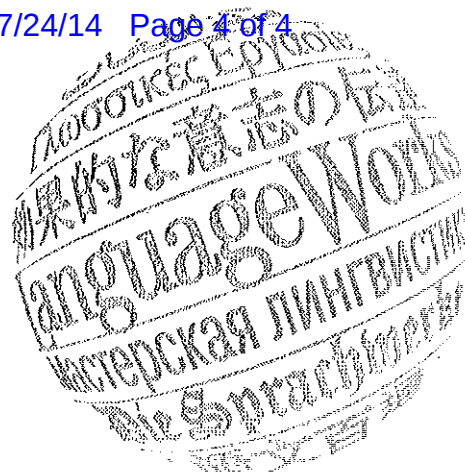
Ook sectorgenoten als Apple, AT & T, Cisco en Verizon **opperen** (<http://cdn.arstechnica.net/wp-content/uploads/2014/07/applebriefinremicrosoft.pdf>) dat een uitspraak ten gunste van de administratie "dramatische conflicten met buitenlandse wetgevingen inzake gegevensbescherming" kan veroorzaken.

Deze bedrijven stellen dat "het risico erg groot is dat buitenlandse regeringen de tech-sector zullen bestraffen, en dat het beter is om samen te werken met andere naties."

ONZE PARTNERS

<p>ALTEREGO DESIGN Design en deco</p>  <p>Koop uw meubelen online of in onze showrooms (Luik & Brussel).</p>	<p>GYMLISH Engelse lessen</p>  <p>7 dagen gratis cursus engels.</p>	<p>PARSHIP Dating met Parship</p>  <p>Vind de partner die echt bij je past.</p>	<p>CIAO Goedkoper kopen met Ciao</p>  <p>Vind, vergelijk en koop tegen de beste prijs.</p>	<p>GENERALI Omnium autoverzekering</p>  <p>Volledige bescherming vanaf 45€/maand!</p>
---	---	---	---	---

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257




LanguageWorks

STATE OF NEW YORK)
) ss:
COUNTY OF NEW YORK)

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "Obama eist ook toegang tot data opgeslagen buiten de VS" completed on 07/22/2014, originally written in Dutch.



Kevin Hudson
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014



Notary Public

MARCEL HENRIQUE VOTLUCKA
Notary Public, State of New York
No. 01VO6154182
Certificate Filed in New York County
Qualified in Kings County
Commission Expires October 23, 2014

EXHIBIT 7

Obama Also Requires Access to Data Stored Outside of the USA



(<http://datanews.levif.be/ict/service/contact/author-1104716134355.htm>)
Frederik Tibau (<http://datanews.levif.be/ict/service/contact/author-1104716134355.htm>)

15/07/2014 - 14:0



The Obama administration maintains that the data stored on American company servers outside of the United States should be accessible to the American justice system.

Technology companies such as Microsoft and Apple are loudly protesting by arguing that the law stops at the border.

According to the American authorities, worldwide access to information is necessary to better identify smugglers, pirates and other drug dealers. Obama & Co. also maintain that any enterprise doing business in the United States must conform to this country's requirements with regard to data, even if the data are stored on the other side of the planet.

Technology giants such as Microsoft and Apple do not share that opinion; they maintain that confidence in American technology companies will take a direct hit after the Snowden leaks.

A judge has already taken Obama's point of view. During proceedings involving a customer of Microsoft, he already affirmed in April that "an entity that is legally bound to provide access to data must do so regardless of the location of those data."

Microsoft has already resorted to a battery of lawyers to mount an appeal. A final ruling is expected on July 31.

The American authorities are using the Stored Communications Act (SCA) as justification. This is a rule that goes back to the time of Ronald Reagan: "Overseas records must be disclosed domestically when a valid subpoena, order or warrant compels their production," according to this document.

Microsoft, for its part, has asserted that the US Congress has never authorized demands for information from outside the physical boundaries of the United States. "Moreover, an American court cannot thus require access to the Microsoft data center in Dublin," is the response from Redmond. "The only thing that the authorities will gain by acting like this is American enterprises losing their leadership position in the ICT."

Other companies in the sector, such as Apple, AT&T, Cisco and Verizon, maintain that a judgment in favor of the administration would lead to "dramatic conflicts with foreign laws on the subject of data protection."

These businesses say that "there is a very great risk that foreign governments will penalize the technology sector; collaborating with the other nations is therefore the most appropriate thing to do."

[Advertisements unrelated to the text]

Obama réclame aussi l'accès aux données stockées en dehors des USA



(<http://datanews.levif.be/ict/service/contact/author-1194716134355.htm>)
Frederik Tibau (<http://datanews.levif.be/ict/service/contact/author-1194716134355.htm>)

15/07/2014 - 14:0



L'administration Obama affirme que les données qui sont stockées sur des serveurs de sociétés américaines en dehors des Etats-Unis doivent être accessibles pour la justice américaine.

Des entreprises technologiques comme Microsoft et Apple protestent à grands cris, en arguant que le maintien du droit s'arrête à la frontière.

Selon les autorités américaines, un accès mondial aux informations est nécessaire pour mieux repérer les fraudeurs, pirates et autres dealers de drogue. Obama et Cie affirment aussi que toute entreprise avec des activités aux Etats-Unis doit répondre aux exigences de ce pays en matière de données, même si les données sont stockées à l'autre bout de la planète.

Des géants des technologies comme Microsoft et Apple ne partagent pas cet avis, affirmant que la confiance dans les entreprises technologiques américaines va en prendre un solide coup, après les révélations de Snowden.

Un juge suit d'ores et déjà le point de vue d'Obama. Lors d'un procès impliquant un client de Microsoft, il a déjà affirmé en avril qu'"une entité qui est légalement tenue de donner l'accès à des données doit le faire indépendamment de l'emplacement de ces données."

Microsoft a déjà recouru à une batterie d'avocats pour aller en appel. Un jugement définitif est attendu dans cette affaire pour le 31 juillet.

Les autorités américaines se basent sur le « Stored Communications Act » (SCA) pour se justifier, une règle qui remonte au temps de Ronald Reagan. "Overseas records must be disclosed domestically when a valid subpoena, order, or warrant compels their production", peut-on lire dans ce document.

Microsoft fait valoir de son côté que le Congrès américain n'a jamais ordonné de réclamer des informations en dehors des frontières physiques des Etats-Unis. "En outre, un tribunal américain ne peut pas exiger ainsi d'avoir accès au centre de données de Microsoft à Dublin", dit-on à Redmond. "La seule chose que les autorités vont gagner en agissant de la sorte, c'est que les entreprises américaines vont perdre leur position de leader dans les TIC."

D'autres sociétés du secteur comme Apple, AT & T, Cisco et Verizon affirment qu'un jugement en faveur de l'administration peut entraîner "des conflits dramatiques avec les législations étrangères en matière de protection des données".

Ces entreprises indiquent que "le risque est très grand que des gouvernements étrangers pénalisent le secteur des technologies, et qu'il est plus opportun de collaborer avec les autres nations."

NOS PARTENAIRES

ALTEREGO DESIGN
Design & déco



Achetez vos meubles en ligne ou en showrooms (Liège & Bruxelles).

GYMGLISH
Cours d'anglais



Profitez d'un mois de cours d'anglais gratuit.

PARSHIP
Rencontre avec Parship



Rencontres sérieuses pour célibataires exigeants.

LEGUIDE.COM
Acheter moins cher



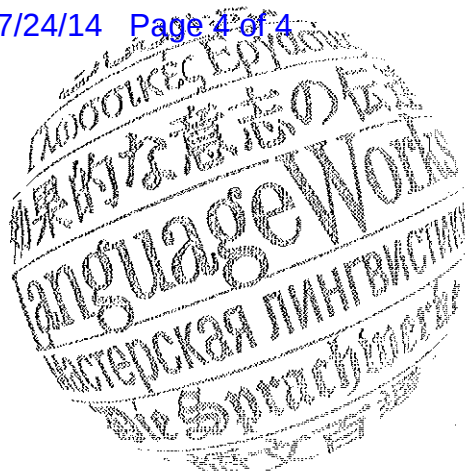
Trouvez, comparez et achetez au meilleur prix.

GENERALI
Assurance auto omnium



Protection complète à partir de 45€/mois!

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257




LanguageWorks

STATE OF NEW YORK)
) ss:
COUNTY OF NEW YORK)

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "Obama réclame aussi l'accès aux données stockées en dehors des USA" completed on 07/22/2014, originally written in French.



Kevin Hudson
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014



Notary Public

MARCEL HENRIQUE VOTLUCKA
Notary Public, State of New York
No. 01VO6154182
Certificate Filed in New York County
Qualified in Kings County
Commission Expires October 23, 20 14

EXHIBIT 8

derStandard.at > Web > Netzpolitik

US Government Requests Access to Data Held Abroad

July 15, 2014, 4:00pm

Microsoft and other US technology firms asked to release data stored on servers abroad

Microsoft is engaged in a legal dispute with the US Department of Justice. The company has been asked to release data not stored in the USA but on servers in Ireland. Microsoft, as well as other companies, are resisting the request and argue that the enforcement of US American laws would have to be limited to inside its borders.

US government refers to 1986 law

The government, however, refers to the Stored Communications Act of 1986 and argues that the Fourth Amendment on the protection against federal searches and seizures does not cover online content. Microsoft had no right to refer to the principles of extraterritoriality, according to the US government.

Loss of client trust

Microsoft fears that the trial could have far-reaching global consequences. Client confidence has already been low as a result of the exposure of the NSA's surveillance activities, says the company. According to Microsoft, the position of the government in this case would further erode trust, and ultimately also in the leadership of US technology companies in the global market.

Conflict with data privacy laws

Companies such as Apple, AT&T, Cisco and Verizon support Microsoft and foresee "grave conflicts with foreign data protection laws." Constitutional scholars in the USA think that the decision could result in a number of global legal disputes and that this is an important case (wen, derStandard.at, 7/15/2014).

Links

Heise

ArsTechnica

Microsoft

[image caption at left]: The US government wants access to all data of Microsoft, Apple & Co – irrespective of the country where they are stored.

US-Regierung fordert Zugriff auf Daten im Ausland

15. Juli 2014, 16:00



vergrößern (800x532)

foto: epa

Die US-Regierung will Zugriff auf allen Daten von Microsoft, Apple & Co. - egal in welchem Land sie gespeichert sind.

APPLE


USD 94,05

-0,41% 



CISCO

USD 25,90

-0,06% 



MICROSOFT

USD 45,00

+0,69% 



Microsoft und andere US-Technologiekonzerne sollen Daten herausgeben, die auf Servern im Ausland gespeichert sind

Microsoft befindet sich in einem Rechtsstreit mit dem US-Justizministerium. Von dem Konzern wird verlangt, Daten herauszugeben, die nicht in den USA sondern auf Servern in Irland gespeichert sind. Microsoft und auch andere Technologieunternehmen wehren sich dagegen und argumentieren, dass die Durchsetzung von US-amerikanischen Gesetzen an der Grenze halt mache.

US-Regierung beruft sich auf ein Gesetz aus 1986

Die Regierung hingegen beruft sich auf den Stored Communications Act aus dem Jahr 1986 und meint, dass Online-Inhalte nicht vom Vierten Zusatzartikel der Verfassung, der den Schutz vor staatlichen Übergriffen behandelt, geschützt seien. Microsoft liege mit seinem Vertrauen auf Prinzipien der Exterritorialität weit daneben, so die US-Regierung.

Vertrauensverlust der Kunden

Microsoft befürchtet, dass das Verfahren weitreichende globale Folgen haben könnte. Durch die Enthüllungen der Überwachungsmaßnahmen der NSA sei das Vertrauen der Kunden bereits niedrig, so das Unternehmen. Die Haltung der Regierung in diesem Fall würde das Vertrauen weiter aushöhlen und letztlich auch die Führung der US-amerikanischen Technologieunternehmen am globalen Markt gefährden.

Konflikt mit Datenschutzgesetzen

Unternehmen wie Apple, AT&T, Cisco und Verizon unterstützen Microsoft und sehen "schwere Konflikte mit ausländischen Datenschutzgesetzen". Verfassungsexperten in den USA meinen, dass eine Entscheidung zu einigen weltweiten Rechtsstreitigkeiten führen könne und es sich um ein wichtiges Verfahren handle. (wen, derStandard.at, 15.07.2014)

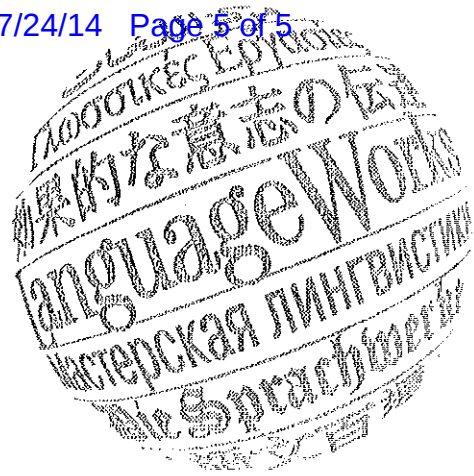
Links

Heise

ArsTechnica

Microsoft

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257



LanguageWorks

STATE OF NEW YORK)
) ss:
COUNTY OF NEW YORK)

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "US-Regierung fordert Zugriff auf Daten im Ausland" completed on 07/22/2014, originally written in German.

Kevin Hudson
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014

Notary Public

MARCEL HENRIQUE VOTLUCKA
Notary Public, State of New York
No. 01VO6154182
Certificate Filed in New York County
Qualified in Kings County
Commission Expires October 23, 2014

EXHIBIT 9

[advertisement]

Neue Osnabrücker Zeitung

[unrelated webpage buttons]

US Government: Access to Foreign Servers is Lawful

07/15/2014 1:16pm

(image caption: Microsoft fights against US agency access to data stored on foreign servers. Photo shows company headquarters in Redmond. Photo: dpa)

Osnabrück. The US-government is of the opinion that, following approval by the court, its agencies may also access data stored on servers in other countries. Washington has made this clear in a legal dispute with Microsoft. The US government has referred to a law from 1986, as reported by various Internet sources.

In the actual case, the matters concerned an order by an undisclosed US agency directing Microsoft to forward data stored on servers in Ireland to prosecutors in the USA. The case allegedly concerned all received and sent emails, access protocols and all credit card numbers and bank accounts of a certain account, which the agency eyed in the context of drug smuggling investigations.

Microsoft, however, rejected the US agency's request by pointing out that the client data was stored on a company server in Dublin, Ireland, and that US search warrants could not be extended abroad. "A US investigator also cannot simply search a house in a different country. [...] We think that this rule should also apply to the online world", the company argued.

The US government has now argued before the court tasked with making a decision during the appeals procedures, that online contents are not protected by the Fourth Amendment (Protection against federal searches and seizures). The English-language Internet site Ars Technica reported on the case by titling it "Obama government holds that the world's servers belong to him."

According to Ars Technica, Microsoft is warning against the global consequences of such a decision. The Internet company is worried about its non-American clients. Just a few months ago, Microsoft announced its intention to protect client data against monitoring by storing them outside the USA.

Apple, AT&T, Cisco and Verizon also spoke up. Apple and Cisco criticized that by releasing such data, US companies would in breach of the (data protection) laws of other countries.

[advertisements]

NEUE OSNABRÜCKER OZ ZEITUNG ^(/)

Suchbegriff eingeben

Anmelden | Registrieren (/login)



Zeitung | Lokalteil wählen

Lokales (/lokales) Deutschland & Welt (/deutschland-welt) Sport (/sport) Anzeigen (/anzeigen) Abo (/abo)

Startseite (/) Deutschland & Welt (/deutschland-welt) Gut zu wissen (/deutschland-welt/gut-zu-wissen)

Microsoft wehrt sich

US-Regierung: Zugriff auf Server im Ausland ist rechtens

Vom 15.07.2014, 13:16 Uhr

Nerviger Bauchspeck schmilzt wie Eis in der Sonne
12kg reines Fett in 2 Wochen verlieren durch diesen einfachen Trick. Trick erfahren? - Mehr...

weiterleiten (/weiterleiten/490495)

drucken



Microsoft wehrt sich gegen Zugriffe der US-Behörden auf Daten, die auf Servern im Ausland gespeichert sind. Im Bild die Firmenzentrale in Redmond. Foto:dpa

Osnabrück. Die US-Regierung vertritt den Standpunkt, dass ihre Behörden mit einem entsprechenden gerichtlichen Beschluss auch auf Daten, die auf Servern in anderen Ländern gespeichert sind, zugreifen dürfen. Das machte Washington in einem Rechtsstreit mit Microsoft klar. Die US-Regierung habe sich dabei auf ein Gesetz aus dem Jahr 1986 berufen, berichten verschiedene Internetportale.

Im konkreten Fall ging es um die Verfügung einer nicht näher genannten US-Behörde, mit der Microsoft angewiesen worden war, Daten, die auf einem Rechner in Irland gespeichert sind, an Strafverfolger aus den USA weiterzugeben. Dabei soll es sich um alle empfangenen und versendeten E-Mails, Zugriffsprotokolle und sämtliche Kreditkartennummern und Bankkonten eines bestimmten Kontos, das im Zusammenhang mit Ermittlungen zu Drogenschmuggel in Visier der Behörde geraten war, gehandelt haben.

Case 1:13-mj-02814-UA Document 71-9 Filed 07/24/14 Page 4 of 5

Microsoft hatte das Argument der US-Behörde abgelehnt mit dem Hinweis zurückgewiesen, dass die Daten des Kunden auf einem Server des Unternehmens in Dublin in Irland gespeichert seien. US-Durchsuchungsbefehle könnten nicht auf Übersee ausgeweitet werden. „Ein US-Ermittler kann auch nicht einfach ein Haus in einem anderen Land durchsuchen. [...] Wir denken, dass diese Regel auch in der Online-Welt Anwendung finden sollte“, hatte das Unternehmen argumentiert.

Vor dem Gericht, das über den Fall jetzt im Revisionsverfahren entscheiden soll, hat die US-Regierung nun argumentiert, Online-Inhalte seien ihrer Meinung nach nicht vom Vierten Zusatzartikel (Schutz vor staatlichen Übergriffen) geschützt. Die englischsprachige Internetseite Ars Technica berichtet über den Fall unter dem Titel „Obama-Regierung sagt, dass die Server der Welt ihr gehören“.

Nach Angaben von Ars Technica warnt Microsoft vor den weltweiten Folgen einer solchen Entscheidung. Der Internetkonzern fürchte um seine nicht-amerikanischen Kunden. Microsoft hatte erst vor wenigen Monaten angekündigt, Kundendaten durch die Speicherung außerhalb der USA vor der Überwachung schützen zu wollen.

Auch Apple, AT&T, Cisco und Verizon äußerten sich. US-Unternehmen würden durch die Herausgabe solcher Daten gegen die (Datenschutz-)Gesetze anderer Staaten verstoßen, kritisierten Apple und Cisco

Anzeige

0,75 % - Nichts für Zocker!
Sicherer Vermögensaufbau mit bis zu 0,75 % Zinsen p.a. Der ExtraZins-Sparbrief von mbs direkt.
www.mbsdirekt.de

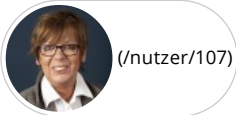
Warum verzichten Sie auf 15.000 Euro?
Privat vorsorgen und bis zu 15.000 Euro vom Staat kassieren. Riesterrente. JETZT ABSCHLIESSEN!
www.hannoversche.de

Die eigenen 4 Wände
Jetzt günstig verwirklichen. Mit einer Baufinanzierung der ING-DiBa.
[Bitte mehr Informationen ...](#)

1,05 % TAGESGELD-Zinsen und kein Postident!
Das schnelle und einfache Tagesgeld der Amsterdam Trade Bank.
[Das klingt gut. Bitte mehr Infos ...](#)

HUK-COBURG - Günstige Baufinanzierung nach Maß
Niedrige Zinsen, Einbindung von KfW-Programmen und Wohn-Riester Darlehen, Sondertilgungen.
[Das interessiert mich. Mehr ...](#)

Ein Artikel von



Waltraud Messmann » (/nutzer/107)
[E-Mail schreiben » \(mailto:w.messmann@noz.de\)](mailto:w.messmann@noz.de)

Waltraud Messmann ist stellvertretende Themenbereichsleiterin Kultur und Service, Jahrgang 1953. Die gebürtige Papenburgerin hat an der Westfälischen-Wilhelms-Universität in Münster das Lehramtsstudium in den Fächern Deutsch und Englisch mit dem Ersten Staatsexamen abgeschlossen.

– Oft gelesen in den letzten Tagen

1. [Wendler-Klatsche holt „Schlag den Star“ aus Quotenloch »](/deutschland-welt/medien/artikel/491766/wendler-klatsche-holt-schlag-den-star-aus-quotenloch)
(/deutschland-welt/medien/artikel/491766/wendler-klatsche-holt-schlag-den-star-aus-quotenloch)
2. [Stefan Raab lacht über den Wendler »](/deutschland-welt/medien/artikel/491722/stefan-raab-lacht-uber-den-wendler)
(/deutschland-welt/medien/artikel/491722/stefan-raab-lacht-uber-den-wendler)
3. [Zehn Tote bei Busunglück auf der Autobahn »](/deutschland-welt/politik/artikel/491701/zehn-tote-bei-busungluck-auf-der-autobahn)
(/deutschland-welt/politik/artikel/491701/zehn-tote-bei-busungluck-auf-der-autobahn)

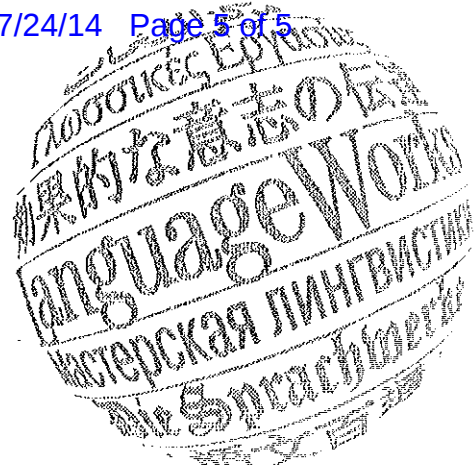
+ Meist kommentiert

+ Neueste Kommentare

Rubriken & Märkte



The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257




LanguageWorks

STATE OF NEW YORK)
) ss:
COUNTY OF NEW YORK)

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "US-Regierung: Zugriff auf Server im Ausland ist rechters" completed on 07/22/2014, originally written in German.



Kevin Hudson
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014



Notary Public

MARCEL HENRIQUE VOTLUCKA
Notary Public, State of New York
No. 01VO6154182
Certificate Filed in New York County
Qualified in Kings County
Commission Expires October 23, 2014

EXHIBIT 10

[unrelated buttons for webpage]

H Online > News > 2014 > KW 29 > US Government Requests Access to Data in EU Processing Centers

07/15/2014 10:49am

US Government Requests Access to Data in EU Processing Centers

Microsoft battles in court against having to release data in the USA that is not even stored inside the country. The US government has submitted its opinion, making reference to a law from before the Internet era.

The US government is referring to a decades-old law for justifying access to data stored by US services abroad. This bases on **a reply**

[<http://cdn.arstechnica.net/wp-content/uploads/2014/07/federalbrief-microsoftcase.pdf>] to a line of argument by Microsoft that the US company used against the release of emails stored in Ireland, as reported by **Ars Technica** [<http://arstechnica.com/tech-policy/2014/07/obama-administration-says-the-worlds-servers-are-ours/>]. Before the court charged with making a decision on the case, the US government referred to the Stored Communications Act from 1986 and argued that, in its opinion, online contents were not protected by the Fourth Amendment (protection against federal searches and seizures).

This process, with allegedly far-reaching consequences, concerns data stored at a processing center in Ireland. The US government made a request in court for their release in the context of investigations involving drug smugglers. **Microsoft is resisting.**

[photo caption] Can Microsoft protect European data from (legal) access by the US?

[advertisement]

Topthemen: **Netzneutralität** NSA TrueCrypt Windows 8.1 Android iPad iPhone Bitcoin

heise online > News > 2014 > KW 29 > US-Regierung fordert Zugriff auf Daten in EU-Rechenzentren

15.07.2014 10:49


US-Regierung fordert Zugriff auf Daten in EU-Rechenzentren

Microsoft kämpft vor Gericht dagegen, dass in den USA Daten herausgegeben werden müssen, die gar nicht in dem Land gespeichert sind. Nun hat die US-Regierung ihre Meinung vorgelegt und beruft sich auf ein Gesetz aus der Prä-Internet-Zeit.

Die US-Regierung beruft sich auf ein Jahrzehnte altes Gesetz, um den Zugriff auf Daten zu rechtfertigen, die US-Dienste im Ausland gespeichert haben. Das geht aus **einer Antwort** [<http://cdn.arstechnica.net/wp-content/uploads/2014/07/federalbrief-microsoftcase.pdf>] auf eine Argumentation von Microsoft hervor, mit dem sich der US-Konzern gegen die Herausgabe von in Irland gespeicherten E-Mails wehrt, **berichtet nun Ars Technica** [<http://arstechnica.com/tech-policy/2014/07/obama-administration-says-the-worlds-servers-are-ours/>]. Vor dem Gericht, das über den Fall entscheiden soll, hat die US-Regierung nun unter Berufung auf den Stored Communications Act von 1986 argumentiert, Online-Inhalte seien ihrer Meinung nach nicht vom Vierten Zusatzartikel (Schutz vor staatlichen Übergriffen) geschützt.

In dem Verfahren mit mutmaßlich weitreichenden Konsequenzen geht es um Daten, die in einem Rechenzentrum in Irland gespeichert sind. Im Zusammenhang mit Ermittlungen gegen Drogenschmuggler hat die US-Regierung vor Gericht deren Herausgabe verlangt. **Microsoft wehrt sich dagegen**



Kann Microsoft europäische Daten vor dem (legalen) US-Zugriff schützen? 
 [<http://www.heise.de/newsticker/meldung/US-Regierung-fordert-Zugriff-auf-Daten-in-EU-Rechenzentren-2260639.html?view=zoom;zoom=1>]
 Bild: dpa, Britta Pedersen

[<http://www.heise.de/newsticker/meldung/Microsoft-will-Zugriff-der-US-Regierung-auf-EU-Rechenzentrum-verhindern-2219295.html>], fürchtet das Unternehmen doch um seine nicht-amerikanischen Kunden. Außerdem würden US-Unternehmen durch die Herausgabe solcher Daten gegen die (Datenschutz-)Gesetze anderer Staaten verstoßen, **kritisierten Apple und Cisco**

[<http://www.heise.de/newsticker/meldung/Apple-und-Cisco-unterstuetzen-Microsoft-gegen-US-Zugriff-auf-EU-Rechenzentren-2224278.html>], die Microsoft unterstützen. (mho [<mailto:mho@heise.de>])

Kommentare lesen (168 Beiträge)

[<http://www.heise.de/newsticker/foren/S-US-Regierung-fordert-Zugriff-auf-Daten-in-EU-Rechenzentren/forum-282692/list/>]

Permalink: <http://heise.de/-2260639>

[<http://heise.de/-2260639>]



Artikel zum Thema



Apple und Cisco unterstützen Microsoft gegen US-Zugriff auf EU-Rechenzentren

Microsoft will den Zugriff von US-Behörden auf E-Mails verhindern, die auf Servern in Irland liegen. Apple und Cisco haben sich...

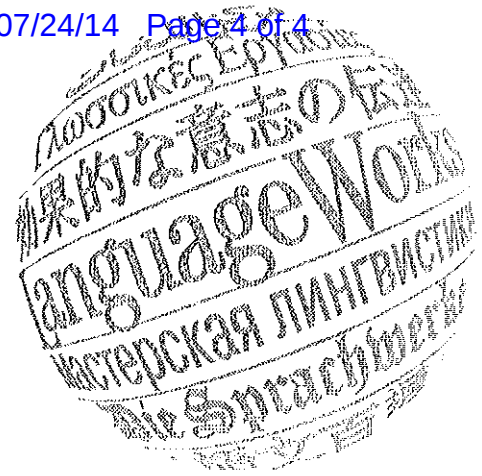


Microsoft will Zugriff der US-Regierung auf EU-Rechenzentrum verhindern

Die US-Regierung verlangt von Microsoft die Herausgabe von Nutzerdaten, die in einem Rechenzentrum in Irland liegen.

Deutsche bemängeln Datenschutz in sozialen Netzwerken

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257



LanguageWorks

STATE OF NEW YORK)
) ss:
COUNTY OF NEW YORK)

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "US-Regierung fordert Zugriff auf Daten in EURechenzentren" completed on 07/22/2014, originally written in German.

Kevin Hudson
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014

Notary Public
MARCEL HENRIQUE VOTLUCKA
Notary Public, State of New York
No. 01VO6154182
Certificate Filed in New York County
Qualified in Kings County
Commission Expires October 23, 2014

EXHIBIT 11

Data Protection

USA Also Wants Data from Foreign Servers

[image caption: Data are no longer secure anywhere – photo: Benjamin Haas, fotolia]

The US government is of the opinion that any company doing business in the USA must release data upon request, even if those are stored outside the USA.

USA, MICROSOFT, REPORT, DATA PROTECTION

This opinion is currently being put on trial. As reported by Ars Technica, the current case concerns Microsoft having to release emails stored on servers in Dublin, Ireland, to US agencies. In contrast, US companies such as Microsoft and Apple believe that US laws may only apply inside domestic borders. In the first instance back in April, a judge agreed with the government's arguments requesting the release of Microsoft data. The company has appealed and a federal judge will hear the case on July 31st.

In the context of submitting the case, the US government has declared that electronically stored information does not enjoy the same protection as physical documents in the real world. Microsoft, however, is asking the judge to take into account that the trust in US technology firms is already at an all-time low. That, in turn, would jeopardize the dominance of American technology. The US Justice Department claims, however, that global criminal prosecution is necessary since no borders exist online. The disputed emails should help to take out a drug smuggling operation.

(FUTUREZONE) ERSTELLT AM 15.07.2014, 13:24

[Text at left]

Data protection

USA Also Wants Data from Foreign Servers

COMMENTS (0)

MORE ON THIS TOPIC

DATENSCHUTZ

USA wollen auch Daten von auswärtigen Servern

15.07.14, 13:24

[Mail an die Redaktion](#)Suche 

[Netzpolitik](#) [B2B](#) [Produkte](#) [Digital Life](#) [Science](#) [Meinung](#) [Games](#) [Apps](#) [Community](#)



Daten sind nirgends mehr sicher - Foto: Benjamin Haas, fotolia

[f](#) Empfehlen 10 [t](#) Twittern 9 [g+](#) Senden [s](#) 19

DATENSCHUTZ

USA wollen auch Daten von auswärtigen Servern

KOMMENTARE (0)

[MEHR ZUM THEMA](#)

Die US-Regierung ist der Ansicht, dass jede Firma, die Geschäfte in den USA macht, Daten auf Anfrage herausgeben muss, auch wenn diese außerhalb der USA gespeichert sind.

USA, MICROSOFT, GERICHT, DATENSCHUTZ

Diese Ansicht steht derzeit vor Gericht auf dem Prüfstand. In dem konkreten Fall geht es darum, dass Microsoft E-Mails, die auf einem Server in Dublin, Irland, gespeichert sind, an US-Behörden ausliefern soll, wie arstechnica berichtet. US-Unternehmen wie Microsoft und Apple sind hingegen der Ansicht, dass US-Recht nur bis zur Staatsgrenze gelten kann. In erster Instanz ist ein Richter im April der Argumentation der Regierung gefolgt und die Herausgabe der Daten von Microsoft verlangt. Der Konzern hat Berufung eingelegt, ein Bundesrichter wird den Fall am 31. Juli anhören.

Im Rahmen der Einreichungen für den Fall hat die US-Regierung kundgetan, dass elektronisch gespeicherte Information nicht denselben Schutz genießt, wie in der realen Welt abgelegte Dokumente. Microsoft hingegen bittet den Richter zu berücksichtigen, dass das Vertrauen in US-Technologiefirmen auf einem Tiefstand ist. Das gefährde die Vorherrschaft amerikanischer Technik. Die US-Justiz hingegen sagt, globale Strafverfolgung sei eine Notwendigkeit, da es im Netz keine Grenzen gebe. Die umstrittenen E-Mails sollen helfen, einen Drogenschmuggler auszuheben.

(FUTUREZONE) ERSTELLT AM 15.07.2014, 13:24

A198



HI RES MP3 ade: Warum Musik wieder gut klingen soll

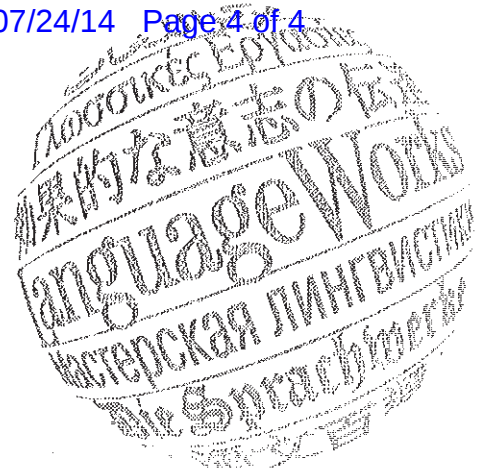


SINGULARITY UNIVERSITY
Wo aus Science Fiction Realität wird



DOTA 2
Profi-Gamern winkt höhere Prämie als Fußball-Weltmeistern

The LanguageWorks, Inc.
1123 Broadway
New York, NY 10010
Tel. 212 447 6060
Fax 212 447 6257




LanguageWorks

STATE OF NEW YORK)
) ss:
COUNTY OF NEW YORK)

CERTIFICATION

This is to certify that the accompanying, to the best of my knowledge and belief, is a true and accurate translation into English of "USA wollen auch Daten von auswärtigen Servern" completed on 07/22/2014, originally written in German.



Kevin Hudson
Director of Production
The LanguageWorks, Inc.

Sworn to and subscribed before me
This 22nd day of July 2014



Notary Public

MARCEL HENRIQUE VOTLUCKA
Notary Public, State of New York
No. 01VO6154182
Certificate Filed in New York County
Qualified in Kings County
Commission Expires October 23, 2014

EXHIBIT 12

By continuing to use this site you consent to the use of cookies on your device as described in our [cookie policy](#) unless you have disabled them. You can change your [cookie settings](#) at any time but parts of our site will not function correctly without them.

FINANCIAL TIMES

Home | World | Companies | Markets | Global Economy | Lex | Comment | Management | Life & Arts
 Energy | Financials | Health | Industrials | Luxury 360 | Media | Retail & Consumer | Tech | Telecoms | Transport | By Region | Tools

June 30, 2014 11:00 am

EU slams US over Microsoft privacy case

By Richard Waters in San Francisco



A US attempt to force [Microsoft](#) to hand over emails held on servers in Ireland has drawn a strong rebuke from Brussels in one of the first tests of cross-border privacy raised by cloud computing.

The US demand could contravene international law and should have been handled through the official channels normally used for law enforcement between different regions, according to Viviane Reding, vice-president of the European Commission.

The case comes as US technology is already caught up in a transatlantic privacy dispute over revelations about widespread US internet surveillance.

The demand for information held in a different location from the people it relates to could “hurt the competitiveness of US cloud providers in general”, Microsoft warned in a lawsuit challenging the order this year.

The software company added: “Microsoft and US technology companies have faced growing mistrust and concern about their ability to protect the privacy of personal information located outside the US.”

A magistrate in New York issued a search warrant late last year requiring Microsoft to give emails belonging to a user of its Outlook email service to US law enforcement agencies. The nature of the case and identity of the suspect were not disclosed.

Microsoft’s argument that the US enforcement order amounted to an illegal attempt to enforce a warrant beyond US borders has now won support in Europe, with Ms Reding weighing in on Microsoft’s side.

“The commission’s concern is that the extraterritorial application of foreign laws [and orders to companies based thereon] may be in breach of international law,” she wrote last week in a letter to Sophie in’t Veld, a Dutch member of the European Parliament.

She added that the US “may impede the attainment of the protection of individuals guaranteed in the [European] Union”.

Rather than trying to force Microsoft to surrender information, she said that the US should have relied on the mutual legal assistance treaties that create a framework for co-operation between law enforcement agencies.

Ms Reding’s rebuke came in the same week that the US Supreme Court put new limits on the power of law enforcement agencies to search suspects’ mobile devices. The judges ruled unanimously that searches could not be carried out without a warrant.

The mobile phone case marked a historic moment in which the court had recognised the need for greater privacy protection as technology advances, Brad Smith, Microsoft’s general counsel, wrote in a blog post on Saturday welcoming the decision. It also marked the first time the Supreme Court has considered privacy issues raised by cloud computing, he said.

RELATED TOPICS [United States of America](#) [European Commission](#) [Internet privacy](#) [Data protection](#)

Printed from: <http://www.ft.com/cms/s/0/1bfa7e90-ff6e-11e3-9a4a-00144feab7de.html>

Print a single copy of this article for personal use. Contact us if you wish to print more to distribute to others.

© THE FINANCIAL TIMES LTD 2014 FT and ‘Financial Times’ are trademarks of The Financial Times Ltd.

EXHIBIT 13

High Court refers Facebook privacy case to Europe

[Ruadhán Mac Cormaic](#)

Last Updated: Thursday, June 19, 2014, 01:04

The [High Court](#) has referred questions raised by a case taken by an Austrian privacy activist over the alleged mass transfer of personal data to US intelligence services to the European Court of Justice.

Privacy campaigner [Max Schrems](#) had argued that the Data Protection Commissioner, [Billy Hawkes](#), wrongly refused to investigate whistleblower Edward Snowden's claims that Dublin-based [Facebook](#) International had passed on its EU users' data to the US [National Security Agency](#) as part of its Prism surveillance programme.

While the judge did not find in Mr Schrems's favour today, he adjourned the case pending a reference to the European court.

Lawyers for Mr Schrems had told the court the Data Protection Commissioner was not entitled to "turn a blind eye" to the allegations by the former NSA contractor.

Mr Schrems, who is behind a data privacy campaign 'Europe v Facebook', claimed Mr Hawkes wrongly interpreted and applied the law governing the transfer of personal data from Europe to the US when he rejected Mr Schrems' complaint.

However counsel for Mr Hawkes, Paul Anthony McDermott BL, said the controversy was a result of Snowden allegations and was therefore a matter for the political level.

The transfer of data from firms in the EU to the US is subject to the transatlantic Safe Harbour arrangement dating back to 2000. The [European Commission](#) has previously expressed concern that Prism exposed a loophole in the Safe Harbour agreement. Mr Hawkes must await the outcome of "political negotiations" in Europe on the Safe Harbour law, Mr McDermott said.

Mr Schrems said he was not challenging the validity of Safe Harbour, rather the operation of it, and that the transfer of data to the NSA was not in accordance with any exceptions under the agreement. Safe Harbour rules are subject to rights contained in EU directives, under the European Convention on Human Rights and under national law, he said.

In court this morning, Mr Justice Gerard Hogan said the evidence suggested that personal data was "routinely accessed on a mass and undifferentiated basis by the US security authorities".

The judge said that Irish law had effectively been "pre-empted" by EU law, specifically the provisions of a 1995 directive and the 2000 decision establishing the Safe Harbour regime.

With the July 2000 decision the European Commission found that US data protection law and practice was sufficient to safeguard the rights of European data subjects and it was clear from Article 25(6) of the 1995 directive that national data protection authorities must comply with findings of this nature.

He said it followed that if the data protection commissioner cannot look beyond the Safe Harbour decision, "then it is clear that the present application for judicial review must fail."

[Mr Justice Hogan](#) said the commissioner had demonstrated "scrupulous steadfastness" to the letter of the 1995 directive and the 2000 decision.

"The applicant's objection is, in reality, to the terms of the Safe Harbour regime itself rather than to the manner in which the commissioner has actually applied the Safe Harbour regime, although neither the validity of the 1995 directive nor the validity of the commissioner's Safe Harbour decision have, as such, been challenged in these proceedings," the judge said.

In these circumstances, Mr Justice Hogan concluded, the "critical issue" which arose was whether the proper interpretation of the 1995 directive and the 2000 commission decision should be "re-evaluated" in light of the subsequent entry into force of Article 8 of the Charter and whether, as a consequence, the commissioner can look beyond or otherwise disregard this community finding."

Mr Hawkes has dismissed the six-page complaint by Mr Schrems as "frivolous or vexatious". Mr Schrems's barrister, Paul O'Shea, said there was "no lawful basis" for the finding. "Members of the public may think this is insulting," Mr McDermott said. "But in a legal sense it means there is not any realistic prospect of succeeding," he said.

The reason the Commissioner found the complaint was vexatious was because it was not possible for him to make an order stopping the flow of information between Ireland and the US. **A.203** counsel added.

Mr Schrems has asked Mr Justice Hogan to quash that decision and direct Mr Hawkes to reconsider the complaint. He also wanted a preliminary reference to the European Court of Justice of issues arising from the case.

The Commissioner, who found Facebook acted within the terms of Safe Harbour, opposed his action. Mr Hawkes found Facebook had no case to answer and was in compliance with the relevant regulations.

Mr Schrems contended that the Data Protection Commissioner didn't want to deal with the issue of Facebook because it is a "hot potato" which he does "not have the courage to take this on", Mr McDermott said. The commissioner's barrister rejected this and said Mr Hawkes was not afraid to take on big companies, noting that he was investigating 22 other similar complaints by Mr Schrems. Mr McDermott argued that Mr Schrems should seek remedy with the US authorities under Safe Harbour and if they would not deal with him he could then come back to the Data Commissioner .

© 2014 irishtimes.com

EXHIBIT 14

THE HIGH COURT

[2013 No. 765JR]

BETWEEN/

MAXIMILLIAN SCHREMS

APPLICANT

AND

DATA PROTECTION COMMISSIONER

RESPONDENTS

JUDGMENT of Mr. Justice Hogan delivered on the 18th June, 2014

I

1. In May, 2013 a computer systems administrator named Edward Snowden - who up to that point had been working for the international consulting firm Booz Allen Hamilton - caused a sensation following his arrival in Hong Kong. Mr. Snowden's firm had been contracted to work for the US National Security Agency ("NSA"). In the course of that employment Mr. Snowden unlawfully appropriated thousands of highly classified NSA files which, when disclosed by him following his arrival in Hong Kong to media outlets such as *The Guardian* (in the UK) and the *New York Times* and the *Washington Post* (in the US), revealed the interception and

surveillance of internet and telecommunications systems by the NSA on a massive, global scale.

2. These revelations form the backdrop to the present judicial review application. The applicant, Mr. Schrems, maintains that as the Snowden disclosures demonstrate that there is no effective data protection regime in the United States, the respondent Data Protection Commissioner (“the Commissioner”) should exercise his statutory powers to direct that the transfer of personal data from Facebook Ireland to its parent company in the United States should cease. The Commissioner for his part maintains that he is bound by the terms of a finding of the European Commission in July 2000 to hold that the data protection regime in the United States is adequate and effective where the companies which transfer or process the data to the United States self-certify that they comply with the principles set down in this Commission decision. The European Commission decision of July 2000 sets up a regime known as the Safe Harbour regime and one of the many issues which arise from these proceedings is whether the Safe Harbour principles are still effective and functional some fourteen years after that decision and finding.

3. Central to the entire case is the Commissioner’s conclusion that the applicant’s complaint is unsustainable in law, precisely because the Safe Harbour regime gives the *imprimatur* to such data transfers on the basis that the European Commission concluded that the US does, in fact, provide for adequate data protection. The applicant maintains in turn that this decision of the Commissioner is unlawful.

II

4. While it is true that the Snowden disclosures caused – and are still causing – a sensation, only the naïve or the credulous could really have been greatly surprised. The question of transnational data protection and state surveillance is admittedly

difficult and sensitive and, subject to fundamental legal protections, a satisfactory *via media* can in many respects be resolved only at the level of international diplomacy and *realpolitik*. While a court must naturally be aware of these underlying realities, in resolving issues such as arise in the present case it must nonetheless endeavour to apply neutrally the applicable legal materials.

5. Yet only the foolish would deny that the United States has, by virtue of its superpower status, either assumed – or, if you prefer, has had cast upon it – far-reaching global security responsibilities. It is probably the only the world power with a global reach which can effectively monitor the activities of rogue states, advanced terrorist groups and major organised crime, even if the support of allied states such as the United Kingdom is also of great assistance in the discharge of these tasks and responsibilities. The monitoring of global communications – subject, of course, to key safeguards - is accordingly regarded essential if the US is to discharge the mandate which it has thus assumed. These surveillance programmes have undoubtedly saved many lives and have helped to ensure a high level of security, both throughout the Western world and elsewhere. But there may also be a suspicion in some quarters that this type of surveillance has had collateral objects and effects, including the preservation and re-inforcing of American global political and economic power.

6. One may likewise fairly assume that the Snowden revelations have compromised these important national security programmes. This will certainly hamper entirely legitimate counter-terrorism operations and, by reason of the possibly inadvertent disclosure of personal information, perhaps even the lives of security operatives working overseas have been put at risk: see *Miranda v. Home Secretary* [2014] EWHC Admin 255 where these adverse effects of the Snowden revelations

were summarised by Laws L.J. for the English High Court in these terms by reference to evidence tendered in that case by security specialists and operatives.

7. It would, however, be equally naïve to believe that this sort of surveillance is the preserve of the superpowers. One may fairly assume that even those states – both big and small - who protested loudly in the wake of the Snowden revelations concerning the invasion of the data protection of their citizens would not themselves be above resorting to such irregular espionage (*i.e.*, surveillance and interception of communications which are not provided for by law) where it suited their interests. This might be especially so where these governments could conveniently turn a blind eye to such surveillance and interception activities on the part of their security forces, or, better still, where they could credibly deny that such espionage had ever been officially “sanctioned.”

8. On the other hand, the Snowden revelations demonstrate a massive overreach on the part of the security authorities, with an almost studied indifference to the privacy interests of ordinary citizens. Their data protection rights have been seriously compromised by mass and largely unsupervised surveillance programmes.

9. It is necessary now to say something briefly about the PRISM programme, the details of which were at the core of the Snowden revelations.

III

The Snowden revelations and the PRISM programme

10. According to a report in *The Washington Post* published on 6th June 2013, the NSA and the Federal Bureau of Investigation (“FBI”):

“are tapping directly into the central servers of nine leading US internet companies, extracting audio and video chats, photographs, e-mails, documents and connection logs that enable analysts to track foreign targets....”

11. According to the *Washington Post* the programme is code-named PRISM and it apparently enables the NSA to collect personal data such as emails, photographs and videos from major internet providers such Microsoft, Google and Facebook. This is done on a mass scale in accordance with orders made by the US Federal Intelligence Court sanctioning such activities.

12. In a report in *The Guardian* newspaper dated 31st July, 2013, it was claimed that a top secret NSA programme entitled “X Keyscore” enabled it to collect “nearly everything a user does on the internet”. The report further claimed that:

“A top secret NSA programme allows analysts to search with no prior authorisation through vast databases containing emails, online chats and the browsing history of millions of individuals, according to documents provided by whistleblower Edward Snowden.”

13. While there may be some dispute regarding the scope and extent of some of these programmes, it would nonetheless appear from the extensive exhibits contained in the affidavits filed in these proceedings that the accuracy of much of the Snowden revelations does not appear to be in dispute. The denials from official sources, such as they have been, were feeble and largely formulaic, often couched in carefully crafted and suitably ambiguous language designed to avoid giving diplomatic offence. I will therefore proceed on the basis that personal data transferred by companies such as Facebook Ireland to its parent company in the United States is thereafter capable of being accessed by the NSA in the course of a mass and indiscriminate surveillance of such data. Indeed, in the wake of the Snowden revelations, the available evidence presently admits of no other realistic conclusion.

IV

14. It is, however, appropriate to note that many of the activities of the NSA are subject to the supervision of the Foreign Intelligence Surveillance Court as provided for by the US federal statute, the Foreign Intelligence Surveillance Act 1978 (“the FISA Court”). The FISA Court is a specialist court consisting of federal judges enjoying standard constitutional guarantees in relation to tenure and independence. This Court entertains applications by the NSA for warrants in relation to foreign surveillance and interception of communications.

15. It would seem, however, that the FISA Court’s hearing are entirely conducted in secret, so that even the court orders and its jurisprudence remain a closed book. The US security authorities are, in effect, the only parties who are or who can be heard in respect of such applications before the FISA Court. One of the striking features of the Snowden revelations was the disclosure of (hitherto secret) orders of the FISA Court which effectively required major telecommunication companies to make disclosure of daily telephone call records on a vast and undifferentiated scale, while the company in question was itself prevented from disclosing the existence or the nature of the order. Yet the essentially secret and *ex parte* nature of the FISA Court’s activities makes an independent assessment of its orders and jurisprudence all but impossible. This is another factor which must – to some degree, at least - cast a shadow over the extent to which non-US data subjects enjoy effective data protection rights in that jurisdiction so far as generalised and mass State surveillance of interception of communications is concerned.

V

16. The applicant, Mr. Schrems, is an Austrian post-graduate law student at the University of Vienna who is plainly deeply concerned about data protection security

and data protection law. He is also since 2008, a user of the social network, Facebook. Although Facebook Inc. (“Facebook”) is a major US company based in California, all Facebook users in Europe are required to enter into an agreement with Facebook Ireland Ltd. (“Facebook Ireland”). To that extent, therefore, Facebook Ireland falls to be regulated by the respondent Data Protection Commissioner under the terms of the Data Protection Acts, 1988-2003.

17. The practical effect of this is that Facebook Ireland is designated as a “data controller” within the meaning of s. 2 of the Data Protection Act 1988 for personal data relating to Facebook subscribers resident in the member states of the European Economic Area (“EEA”). It is not in dispute that while Facebook Ireland is subject to regulation under the Data Protection Acts, some or all data relating to Facebook subscribers resident within the EEA is in fact transferred to and held on servers which are physically located in the United States.

18. Mr. Schrems has already made some 22 other complaints concerning Facebook Ireland to the Commissioner, but it is agreed none of these fall to be considered in the present judicial review proceedings. This case rather concerns the 23rd complaint which Mr. Schrems made concerning Facebook Ireland. This particular complaint was dated 25th June, 2013, and arose directly out of the Snowden revelations and, specifically, the PRISM programme.

VI

19. The office of the Data Protection Commissioner was established by s. 9 of the Data Protection Act 1988 (“the 1988 Act”). The 1988 Act itself has been subsequently amended in an extensive fashion, not only by the Data Protection (Amendment) Act 2003, but by a variety of other statutes and ministerial regulations which are designed to transpose EU legislation in this area.

20. Section 11(1) of the 1988 Act articulates a general prohibition on the transfer of personal data outside of the State, save where that foreign State “ensures an adequate level of protection for the privacy and the fundamental rights and freedoms of data subjects in relation to the processing of personal data having regard to all the circumstances surrounding that transfer.” The reference here to privacy and the fundamental rights and freedoms of data subjects must be gauged in the first instance by the protections afforded in this regard by the Constitution, a topic to which I will presently revert.

21. So far as these proceedings are concerned, however, the critical sub-section is that contained in s. 11(2) of the 1988 Act, a sub-section which allows for the pre-emption of Irish law by EU law where a “Community finding” as to the adequacy of data protection in the third country has been made by the European Commission.

Section 11(2)(a) accordingly provides:

“Where in any proceedings under this Act a question arises –

- (i) whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area to which personal data are to be transferred, and
- (ii) a Community finding has been made in relation to transfers of the kind in question,

the question shall be determined in accordance with that finding.”

22. The term “Community finding” is defined by s. 11(2)(b) as meaning:

“...a finding of the European Commission made for the purposes of paragraph (4) or (6) of Article 25 of the Directive under the procedure provided for in Article 31(2) of the Directive in relation to whether the adequate level of

protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area.”

23. The Directive is defined by s. 1(1) as meaning the Data Protection Directive, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (O.J. L281/38)(“the 1995 Directive”). Article 25(6) of the 1995 Directive provides that:

“The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitment it has entered into, particularly upon conclusions of the negotiations referred to in paragraph 5, for the protection of private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission’s decision.”

24. The European Commission did adopt such a decision on 26th July, 2000 (2000/520/EC)(O.J. L 215, 25th August, 2000), citing Article 25(6) of the 1995 Directive as the legal basis for this decision. The date of this decision is, perhaps, of some significance, given that it was taken some months before the EU Charter of Fundamental Rights was adopted at Nice in December 2000 and it ante-dated by several years the coming into force of the Lisbon Treaty on 1 December 2009, which is the date on which the Charter itself was first given legally justiciable status.

25. As the recitals to that Commission decision make clear, however, an adequate level of protection:

“for the transfer of data from the Community to the United States recognised by this Decision, should be attained if organisations comply with the safe

harbour privacy principles for the protection of personal data transferred from a Member State to the United States...and the frequently asked questions [“FAQs”]...providing guidance for the implementation of the Principles issued by the Government of the United States on 21st July 2000. Furthermore, the organisations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission under section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce, or that of another statutory body that will effectively ensure compliance with the Principles implemented in accordance with the FAQs.”

26. Article 1(2) of the decision then provides that:

“In relation to each transfer of data the following conditions shall be met:

- (a) the organisation receiving the data has unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs;
- (b) the organisation is subject to the statutory powers of a government body in the United States listed in Annex VII to this Decision which is empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in the case of non-compliance with the Principles implemented in accordance with the FAQs.”

27. Article 1(3) then provides for a self-certification procedure:

“The conditions set out in paragraph 2 are considered to be met for each organisation that self-certifies its adherence to the Principles implemented in

accordance with the FAQs from the date on which the organisation notifies to the US Department of Commerce (or its designee) the public disclosure of the commitment referred to in paragraph 2(a) and the identity of the government body referred to in paragraph 2(b).”

28. In terms of potential enforcement of these principles, Article 3 of the Decision is perhaps the most critical provision of all:

“Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data in cases where:

- (a) the government body in the United States referred to in Annex VII to this Decision or an independent recourse mechanism within the meaning of letter (a) of the Enforcement Principle set out in Annex I to this Decision has determined that the organisation is violating the Principles implemented in accordance with the FAQs; or
- (b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an

imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

The suspension shall cease as soon as compliance with the Principles implemented in accordance with the FAQs is assured and the competent authorities concerned in the Community are notified thereof.”

VII

The complaints made by Mr.Schrems of 25th June, 2013

29. The complaint made by Mr. Schrems on 25th June, 2013, was, in essence, that by transferring user data to the United States, Facebook Ireland was facilitating the processing of such data by Facebook itself. While Facebook has self-certified by reference to the Safe Harbour principles, Mr. Schrems contended that the Snowden revelations regarding the Prism programme demonstrated that there was no meaningful protection in US law or practice in respect of data so transferred so far as State surveillance was concerned. Specifically, Mr. Schrems maintained that this was especially so given that the US law enforcement agencies could obtain access to such data without the need for a court order, or, at least, a court order showing probable cause that a particular data subject had engaged in illegal activities or stood possessed of information which would be of genuine interest to law enforcement bodies.

30. The response of the Commissioner to this complaint can probably be best summed up in a letter dated 26th July, 2013:

“...we would reiterate that the ‘Safe Harbour’ agreement stands as a formal decision of the EU Commission...under Article 25(6) of the Data Protection

Directive 95/46/EC that the agreement provides adequate protection for personal data transferred from the EU to the USA. Section 11(2) of the (Irish) Data Protection Acts which we consider faithfully reflects our obligation to accept ‘adequacy’ decisions provides that

‘Where in any proceedings under this Act a question arises:

- (i) whether the adequate level of protection specified in sub-section (1) of this section is ensured by a country or territory outside the European Economic Area to which personal data are to be transferred, and
- (ii) a Community finding has been made in relation to transfers of this kind, the question shall be determined in accordance with that finding.’

The Commissioner has concluded that, as Facebook-Ireland is registered under the Safe Harbour arrangement and as this provides for US law enforcement access, there is nothing for this Office to investigate.”

31. On the previous day, 25th July, 2013, the Commissioner had further explained by letter the approach which he was taking:

“Section 10(1)(a) of the Data Protection Acts provides that the Commissioner “*may* investigate whether any of the provisions of [the] Act...have, are being or are likely to be contravened in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he is otherwise of opinion that there may be such a contravention.” As the Commissioner is satisfied that there is no evidence of a contravention in this case, he has exercised his discretion not to proceed to a formal investigation under s. 10(1)(b) of the Acts. In making this assessment the Commissioner is

also mindful of the fact that there is no evidence – and you have not asserted – that your personal data has been disclosed to the US authorities. The situation in this respect is quite different to that in relation to the 22 complaints you submitted earlier which related to terms and conditions of Facebook-Ireland which clearly apply to you as user.”

32. In essence, therefore, it is clear that the Commissioner formed the view that as Facebook had self-certified under the Safe Harbour regime and as there was a Community finding that the Safe Harbour regime provided adequate data protection, there was nothing left for him to investigate. The Commissioner accordingly exercised his power not to investigate the matter further under s. 10(1)(b) of the 1988 Act on the basis that the complaint was “frivolous and vexatious”.

33. It should also be pointed out that the Commissioner had, in any event, raised the question of the PRISM allegations with Facebook Ireland *in advance* of receiving Mr. Schrem’s complaint. In the course of those discussions, Facebook Ireland confirmed that its parent, Facebook, did not provide access to US security agencies to subscriber data, save by means of targeted requests which were properly and lawfully made. The Commissioner had satisfied himself on the basis of an audit which he had carried out of Facebook Ireland that it had appropriate procedures in place for the handing of access requests received from security agencies generally.

VIII

Whether the complaint was “frivolous and vexatious”

34. Section 10(1) of the 1988 Act provides as follows:-

“(a) The Commissioner may investigate, or cause to be investigated, whether any of the provisions of this Act, have been, are being or are likely to be contravened in relation to an individual either where the

individual complains to him of a contravention of any of those provisions or he is otherwise of opinion that there may be such a contravention.

(b) Where a complaint is made to the Commissioner under *paragraph (a)* of this subsection, the Commissioner shall -

- (i) investigate the complaint or cause it to be investigated, unless he is of opinion that it is frivolous or vexatious, and
- (ii) if he or she is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the matter, the subject of the complaint notify in writing the individual who made the complaint of his or her decision in relation to it and that the individual may, if aggrieved by the decision, appeal against it, to the Court under section 26 of this Act within 21 days from the receipt by him or her of the notification.”

35. The jurisdiction of the Commissioner not to investigate complaints further under s. 10(1)(b) has been very helpfully examined by Birmingham J. in his judgment in *Novak v. Data Protection Commissioner* [2012] IEHC 449, [2013] 1 I.L.R.M. 207. Where the Commissioner has proceeded to the investigation stage, then an appeal will lie from that decision to the Circuit Court: see s. 26(1)(d) of the 1988 Act. It is common case, however, that no such appeal lies where the complaint is deemed to be frivolous and vexatious. In essence, therefore, the only remaining remedy which is available to Mr. Schrems is that of judicial review: can it be said that the

Commissioner erred in law that in concluding that the complaint was “frivolous and vexatious”?

36. In *Novak* the issue was whether a candidate’s answer paper in a professional examination constituted “personal data” within the meaning of the Data Protection Acts. The Commissioner concluded that the examination answer did not so constitute personal data and he declined to investigate the matter further. The student appealed to the Circuit Court, but in her judgment delivered on 16th November, 2010, Her Honour Judge Linnane concluded that absent a decision to proceed to investigate no such appeal lay. This decision was subsequently upheld by the decision of Birmingham J. for this Court.

37. So far as the jurisdictional issue is concerned, Birmingham J. concluded:

“Section 10(1) seems to envisage that the following sequence of events will occur:-

- (1) The Commissioner has to decide whether the matter submitted to him is frivolous or vexatious.
- (2) If the Commissioner is of the view that the matter was not frivolous or vexatious, then, unless an amicable resolution can be arranged within a reasonable time, he considers the matter and reaches a decision in relation to it and then informs the complainant of the decision that has been reached and that the decision may be appealed.
- (3) However, if the view is formed that the matter that has been submitted is frivolous or vexatious, then the Commissioner

does not investigate the complaint or cause it to be investigated.

In that event the procedure comes to a halt.

I find myself in respectful agreement with Judge Linnane that the jurisdiction of the Circuit Court is to hear an appeal against a decision that has been arrived at after there has been an investigation. I share her view that absent investigation of the complaint and a decision in relation to the investigation, that the Circuit Court has no jurisdiction. The entitlement of an aggrieved party in the first place to submit an appeal and then of the Court to hear and determine an appeal arises only where there has been a decision of the Commissioner in relation to a complaint under section 10(1)(a). However, the Commissioner reaches a decision in relation to a complaint only if, not having decided that the matter is frivolous and vexatious, he proceeds to investigate the complaint and reaches a decision in relation thereto.”

38. Birmingham J. then turned to the question of whether the Commissioner was correct on the merits of the complaint, saying:

“Once the Commissioner had formed the view that the examination script did not constitute personal data, it followed that he was being asked to proceed with an investigation where no breach of the Data Protection Acts could be identified. It was in those circumstances he had resort to s. 10(1)(b)(i). That section refers to complaints that are frivolous or vexatious. However, I do not understand these terms to be necessarily pejorative. Frivolous, in this context does not mean only foolish or silly, but rather a complaint that was futile, or misconceived or hopeless in the sense that it was incapable of achieving the desired outcome... Having regard to the view the Commissioner had formed

that examination scripts did not constitute personal data, he was entitled to conclude that the complaint was futile, misconceived or hopeless in the sense that I have described, indeed such a conclusion was inevitable.”

39. It is against this background that the present complaint falls to be evaluated. It is certainly true that in the ordinary sense of these words the present complaint – raising as it does weighty issues of transcendent importance in relation to data protection – is neither “frivolous” nor “vexatious”. While in this respect the actual language of s. 10(1)(b) of the 1988 Act is somewhat unfortunate and perhaps even unhelpful, nevertheless, as Birmingham J. pointed out in *Novak*, in this particular statutory context these words also apply to a case where the claim is considered to be unsustainable in law. In fairness, the Commissioner has also been most anxious to stress – both in correspondence and in submissions advanced by his counsel, Mr. McDermott – that it is in this particular sense that the terms have been used in the present case and that they described the Commissioner’s conclusion that the complaint cannot succeed.

40. We can now proceed to examine the merits of these judicial review proceedings. Before doing so, however, it is necessary to consider a preliminary point raised as an objection by the Commissioner, namely, that of *locus standi* of the complainant.

IX

The *locus standi* of the complainant

41. The Commissioner contends that as there is no evidence by which he could have concluded that the Safe Harbour Principles were in fact being violated in the case of data transfers between Facebook Ireland and Facebook, it was submitted that these complaints were essentially hypothetical and speculative in nature. Nor, it was

further submitted, was any evidence ever adduced to suggest that there was an imminent risk of grave harm to him or that any of his data had been or was likely to be accessed by the NSA.

42. For my part, I do not think that this objection is well founded. The Snowden revelations demonstrate - almost beyond peradventure - that the US security services can routinely access the personal data of European citizens which has been so transferred to the United States and, in these circumstances, one may fairly question whether US law and practice in relation to data protection and State security provides for meaningful or effective judicial or legal control. It is true that Mr. Schrems cannot show any evidence that his data has been accessed in this fashion, but this is not really the gist of the objection.

43. The essence of the right to data privacy is that, so far as national law is concerned and by analogy with the protection afforded by Article 40.5 of the Constitution, that privacy should remain inviolate and not be interfered with save in the manner provided for by law, *i.e.*, by means of a probable cause warrant issued under s. 6 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, on the basis that the interception of such communications involving a named individual is necessary in the interests of either the suppression of serious crime or the protection of national security.

44. This is also clearly the position under EU law as well, a point recently confirmed by the Court of Justice in Case C-293/12 *Digital Rights Ireland* in a case where the Data Retention Directive, Directive 2006/24/EC was held to be invalid by reason of the absence of sufficient safeguards in respect of the accessing of such data by national authorities:

“By requiring the retention of the data listed in Article 5(1) of Directive 2006/24 and by allowing the competent national authorities to access those data, Directive 2006/24, ...derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector, directives which provided for the confidentiality of communications and of traffic data as well as the obligation to erase or make those data anonymous where they are no longer needed for the purpose of the transmission of a communication, unless they are necessary for billing purposes and only for as long as so necessary.

To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way (see, to that effect, Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 75).

As a result, the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person’s private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.

Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right....Accordingly,

Articles 4 and 8 of Directive 2006/24 laying down rules relating to the access of the competent national authorities to the data also constitute an interference with the rights guaranteed by Article 7 of the Charter.

Likewise, Directive 2006/24 constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data.

It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is... and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.”

45. The same reasoning applies here. Quite obviously, Mr. Schrems cannot say whether his own personal data has ever been accessed or whether it would ever be accessed by the US authorities. But even if this were considered to be unlikely, he is nonetheless certainly entitled to object to a state of affairs where his data are transferred to a jurisdiction which, to all intents and purposes, appears to provide only a limited protection against any interference with that private data by the US security authorities.

46. It is manifestly obvious that the present case raises issues of both national and EU law, although in the event the issue is largely governed by EU law given the central importance of the Commission decision of July 2000. It may nevertheless be

convenient to consider the position both from the perspective of national law and EU law.

X

The position under national law

47. As far as Irish law is concerned, the accessing of private communications by the State authorities through interception or surveillance directly engages the constitutional right to privacy: see, e.g., *Kennedy v. Ireland* [1987] I.R. 587; *People v. Dillon* [2003] 1 I.L.R.M. 531 and *People v. Idah* [2014] IECCA 3. As Hamilton P. noted in *Kennedy*, this constitutional right is underscored by the Preamble’s commitment to the protection of the “dignity and freedom of the individual” and the guarantee of a democratic society contained in Article 5 of the Constitution.

48. One might add that the accessing by State authorities of private communications generated within the home – whether this involves the accessing of telephone calls, internet use or private mail – also directly engages the inviolability of the dwelling as guaranteed by Article 40.5 of the Constitution. As it happens, by one of those accidents of legal history, these very same words are also contained in Article 13(1) of the German Basic Law (“inviolability of the dwelling”) (“unverletzlichkeit der Wohnung”). It is accordingly of interest that the German Constitutional Court has held that the accessing by state authorities of otherwise private communications within the home also engages that more or less identically worded guarantee of inviolability of the dwelling which is contained in Article 13(1) of the Basic Law. Indeed that Court went further and found that legislation providing for the interception and surveillance of communications partly unconstitutional because it provided for a disproportionate interference without adequate safeguards with that very guarantee of inviolability of the dwelling in Article 13(1) of the Basic Law: see

Anti-Terrorism Database Law decision (I B v R 1215/07)(April 24, 2013) at paras. 93 *et seq.*

49. Naturally, the mere fact that these rights are thus engaged does not necessarily mean that the interception of communications by State authorities is necessarily or always unlawful. The Preamble to the Constitution envisages a “true social order” where the “dignity and freedom of the individual may be assured”, so that both liberty and security are valued. Provided appropriate safeguards are in place, it would have to be acknowledged that in a modern society electronic surveillance and interception of communications is indispensable to the preservation of State security. It is accordingly plain that legislation of this general kind serves important – indeed, vital and indispensable - State goals and interests: *cf.* by analogy the decision of the German Constitutional Court in the *Anti-Terrorism Database* case (at paras. 106, 131 and 133, *passim*) and the comments of the Court of Justice in Case C-293/12 *Digital Rights Ireland Ltd.* [2014] E.C.R. I-000 at paras. 42-44.

50. The importance of these rights is such nonetheless that the interference with these privacy interests must be in a manner provided for by law and any such interference must also be proportionate. This is especially the case in respect of the interception and surveillance of communications within the home. While the use of the term “inviolable” in respect of the dwelling in Article 40.5 does not literally mean what it says, the reference to inviolability in this context nonetheless conveys that the home enjoys the highest level of protection which might reasonably be afforded in a democratic society: see, e.g., *Wicklow County Council v. Fortune (No.1)* [2012] IEHC 406.

51. By safeguarding the inviolability of the dwelling, Article 40.5 provides yet a further example of a *leitmotif* which suffuses the entire constitutional order, namely, that the State exists to serve the individual and society and not the other way around.

52. In this regard, it is very difficult to see how the mass and undifferentiated accessing by State authorities of personal data generated perhaps especially within the home – such as e-mails, text messages, internet usage and telephone calls – would pass any proportionality test or could survive constitutional scrutiny on this ground alone. The potential for abuse in such cases would be enormous and might even give rise to the possibility that no facet of private or domestic life within the home would be immune from potential State scrutiny and observation.

53. Such a state of affairs – with its gloomy echoes of the mass state surveillance programmes conducted in totalitarian states such as the German Democratic Republic of Ulbricht and Honecker - would be totally at odds with the basic premises and fundamental values of the Constitution: respect for human dignity and freedom of the individual (as per the Preamble); personal autonomy (Article 40.3.1 and Article 40.3.2); the inviolability of the dwelling (Article 40.5) and protection of family life (Article 41). As Hardiman J. observed in *The People v. O'Brien* [2012] IECCA 68, Article 40.5

“...presupposes that in a free society the dwelling is set apart as a place of repose from the cares of the world. In so doing, Article 40.5 complements and re-inforces other constitutional guarantees and values, such as assuring the dignity of the individual (as per the Preamble to the Constitution), the protection of the person (Article 40.3.2), the protection of family life (Article 41) and the education and protection of children (Article 42). Article 40.5 thereby assures the citizen that his or her privacy, person and security will be

protected against all comers, save in the exceptional circumstances presupposed by the saver to this guarantee.”

54. One might accordingly ask how the dwelling could in truth be a “place of repose from the cares of the world” if, for example, the occupants of the dwelling could not send an email or write a letter or even conduct a telephone conversation if they could not be assured that they would not be subjected to the prospect of general or casual State surveillance of such communications on a mass and undifferentiated basis.

55. That general protection for privacy, person and security in Article 40.5 would thus be entirely compromised by the mass and undifferentiated surveillance by State authorities of conversations and communications which take place within the home. For such interception of communications of this nature to be constitutionally valid, it would, accordingly, be necessary to demonstrate that this interception of communications and the surveillance of individuals or groups of individuals was objectively justified in the interests of the suppression of crime and national security and, further, that any such interception was attended by appropriate and verifiable safeguards.

56. If this matter were entirely governed by Irish law, then, measured by these constitutional standards, a significant issue would arise as to whether the United States “ensures an adequate level of protection for the privacy and the fundamental rights and freedoms”, such as would permit data transfers to that country having regard to the general prohibition contained in s. 11(1) of the 1988 Act and the constitutional principles I have just set out. Certainly, given what I have already described as the (apparently) limited protection given to data subjects by contemporary US law and practice so far as State surveillance is concerned, this

would indeed have been a matter which the Commissioner would have been obliged further to investigate.

57. It is, however, agreed, that the matter is only partially governed by Irish law and that, in reality, on this key issue Irish law has been pre-empted by general EU law in this area. This is because s. 11(2)(a) of the 1988 Act (as substituted by s. 12 of the Data Protection (Amendment) Act 2003) effects a *renvoi* of this wider question in favour of EU law. Specifically, s. 11(2)(b) of the 1988 Act provides that the Commissioner must determine the question of the adequacy of protection in the third State “in accordance” with a Community finding made by the European Commission pursuant to Article 25 of the 1995 Directive. It is accordingly for this reason that we must therefore turn to a consideration of the position at EU law.

XI

The position under EU law

58. The position under EU law is equally clear and, indeed, parallels the position under Irish law, albeit perhaps that the safeguards for data protection under the EU Charter of Fundamental Rights thereby afforded are perhaps even more explicit than under our national law. These fundamental protections are contained in Article 7 and Article 8 of the EU Charter of Fundamental Rights. Article 7 provides:

“Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.”

59. Article 8 provides:

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.”

60. Given that the validity of the administrative decision taken by the Commissioner is contingent on the proper interpretation and application of a Directive and, indeed, a Commission Decision taken pursuant to that Directive, it is plain that this is a case concerning the implementation of the EU law by a Member State within the meaning of Article 51(1) of the Charter, sufficient – at least so far as this part of the case is concerned – to trigger the application of the Charter: see, *e.g.*, Cases C-411/10 and C-493/10 *N.S.* [2011] E.C.R. I – 13991, paras. 64-69.

61. In *Digital Rights Ireland* the Court of Justice held that the Data Retention Directive was invalid, precisely because not only did it not contain appropriate safeguards, but it failed to provide for the retention of the data within the European Union with supervisions by an independent authority in the manner required by Article 8(3) of the Charter. As the Court observed (at paras. 65-69):

“It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.

In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data...

Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.”

62. Judged by these standards, it is not immediately apparent how the present operation of the Safe Harbour Regime can in practice satisfy the requirements of Article 8(1) and Article 8(3) of the Charter, especially having regard to the principles articulated by the Court of Justice in *Digital Rights Ireland*. Under this self-certification regime, personal data is transferred to the United States where, as we have seen, it can be accessed on a mass and undifferentiated basis by the security authorities. While the FISA Court doubtless does good work, the FISA system can at best be described as a form of oversight by judicial personages in respect of applications for surveillance by the US security authorities. Yet the very fact that this oversight is not carried out on European soil and in circumstances where the data subject has no effective possibility of being heard or making submissions and, further, where any such review is not carried out by reference to EU law are all considerations

which would seem to pose considerable legal difficulties. It must be stressed, however, that neither the validity of the 1995 Directive nor the Commission Decision providing for the Safe Harbour Regime are, as such, under challenge in these judicial review proceedings.

63. The Safe Harbour Regime was, of course, not only drafted before the Charter came into force, but its terms may also reflect a somewhat more innocent age in terms of data protection. This Regime also came into force prior to the advent of social media and, of course, before the massive terrorist attacks on American soil which took place on September 11th, 2001. Outrages of this kind – sadly duplicated afterwards in Madrid, London and elsewhere - highlighted to many why, subject to the appropriate and necessary safeguards, intelligence services needed as a matter of practical necessity to have access to global telecommunications systems in order to disrupt the planning of such attacks

XII

Conclusions

64. This brings us to the nub of the issue for the Commissioner. He is naturally bound by the terms of the 1995 Directive and by the 2000 Commission Decision. Furthermore, as the 2000 Decision amounts to a “Community finding” regarding the adequacy of data protection in the country to which the data is to be transferred, s. 11(2)(a) of the 1988 Act (as amended) requires that the question of the adequacy of data protection in the country where the data is to be so transferred “shall be determined in accordance with that finding.” In this respect, s. 11(2)(a) of the 1988 Act faithfully follows the provisions of Article 25(6) of the 1995 Directive.

65. All of this means that the Commissioner cannot arrive at a finding inconsistent with that Community finding, so that if, for example, the Community finding is to the effect that a particular third party state has adequate and effective data protection laws, the Commissioner cannot conclude to the contrary. The Community finding in question was, as we have already seen, to the effect that the US does provide adequate data protection for data subjects in respect of data handled or processed by firms (such as Facebook Ireland and Facebook) which operate the Safe Harbour regime.

66. It follows, therefore, that if the Commissioner cannot look beyond the European Commission's Safe Harbour Decision of July 2000, then it is clear that the present application for judicial review must fail. This is because, at the risk of repetition, the Commission *has* decided that the US provides an adequate level of data protection and, as we have just seen, s. 11(2)(a) of the 1998 Act (which in turn follows the provisions of Article 25(6) of the 1995 Directive) ties the Commissioner to the Commission's finding. In those circumstances, any complaint to the Commissioner concerning the transfer of personal data by Facebook Ireland (or, indeed, Facebook) to the US on the ground that US data protection was inadequate would be doomed to fail.

67. This finding of the Commission is doubtless still true at the level of consumer protection, but, as we have just seen, much has happened in the interval since July 2000. The developments include the enhanced threat to national and international security posed by rogue States, terrorist groupings and organised crime, disclosures regarding mass and undifferentiated surveillance of personal data by the US security authorities, the advent of social media and, not least from a legal perspective, the enhanced protection for personal data now contained in Article 8 of the Charter.

68. While the applicant maintains that the Commissioner has not adhered to the requirements of EU law in holding that the complaint was unsustainable in law, the opposite is in truth the case. The Commissioner has rather demonstrated scrupulous steadfastness to the letter of the 1995 Directive and the 2000 Decision.

69. The applicant's objection is, in reality, to the terms of the Safe Harbour Regime itself rather than to the manner in which the Commissioner has actually applied the Safe Harbour Regime. There is, perhaps, much to be said for the argument that the Safe Harbour Regime has been overtaken by events. The Snowden revelations may be thought to have exposed gaping holes in contemporary US data protection practice and the subsequent entry into force of Article 8 of the Charter suggests that a re-evaluation of how the 1995 Directive and 2000 Decision should be interpreted in practice may be necessary. It must be again stressed, however, that neither the validity of the 1995 Directive nor the validity of the Commission's Safe Harbour decision have, as such, been challenged in these proceedings

70. Although the validity of the 2000 Decision has not been directly challenged, the essential question which arises for consideration is whether, *as a matter of European Union law*, the Commissioner is nonetheless absolutely bound by that finding of the European Commission as manifested in the 2000 Decision in relation to the adequacy of data protection in the law and practice of the United States having regard in particular *to the subsequent entry into force of Article 8 of the Charter*, the provisions of Article 25(6) of the 1995 Directive notwithstanding. For the reasons which I have already stated, it seems to me that unless this question is answered in a manner which enables the Commissioner either to look behind that Community finding or otherwise disregard it, the applicant's complaint both before the Commissioner and in these judicial review proceedings must accordingly fail.

71. Given the general novelty and practical importance of these issues which have considerable practical implications for all 28 Member States of the European Union, it is appropriate that this question should be determined by the Court of Justice. In these circumstances, I propose to refer the following questions to that Court in accordance with Article 267 TFEU:

“Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC) having regard to Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union (2000/C 364/01), the provisions of Article 25(6) of Directive 95/46/EC notwithstanding? Or, alternatively, may the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?”

72. In these circumstances, the present proceedings must stand adjourned pending the outcome of the Article 267 reference.

XIII

Summary of overall conclusions

73. It remains only to summarise my principal conclusions:

74. First, while it is clear that Mr. Schrems’ complaints are not “frivolous or vexatious” in the ordinary sense of these words, these words bear a different

connotation in the context of s. 10(1)(b)(i) of the 1988 Act, at least so far as the present complaint is concerned. Used in this fashion and in this context, these term mean no more than that the Commissioner had concluded that this complaint was unsustainable in law.

75. Second, Mr. Schrems enjoys *locus standi* to bring this complaint and to bring these proceedings. It is irrelevant that Mr. Schrems cannot show that his own personal data was accessed in this fashion by the NSA, since what matters is the essential inviolability of the personal data itself. The essence of that right would be compromised if the data subject had reason to believe that it could be routinely accessed by security authorities on a mass and undifferentiated basis.

76. Third, the evidence suggests that personal data of data subjects is routinely accessed on a mass and undifferentiated basis by the US security authorities.

77. Fourth, so far as Irish law is concerned, s. 11(1)(a) of the 1988 Act forbids the transfer of personal data to a third country unless it is clear that that jurisdiction sufficiently respects and protects the privacy and fundamental freedoms of the data subjects. In this particular context of national law, the standards in question are those contained in the Constitution.

78. Fifth, the chief constitutional protections are those relating to personal privacy and the inviolability of the dwelling. The general protection for privacy, person and security which is embraced by the “inviolability” of the dwelling in Article 40.5 of the Constitution would be entirely compromised by the mass and undifferentiated surveillance by State authorities of conversations and communications which take place within the home. For such interception of communications to be constitutionally valid, it would, accordingly, be necessary to demonstrate that this interception and surveillance of individuals or groups of individuals was objectively justified in the

interests of the suppression of crime and national security and, further, that any such interception was attended by appropriate and verifiable safeguards.

79. Sixth, if the matter were to be measured solely by Irish law and Irish constitutional standards, then a serious issue would arise which the Commissioner would then have been required to investigate as to whether US law and practice in relation to data privacy, interception and surveillance matched these constitutional standards.

80. Seventh, in this regard, however, Irish law has been effectively pre-empted by EU law and specifically by the provisions of the 1995 Directive and the 2000 Decision establishing the Safe Harbour regime. With the July 2000 Decision the European Commission found that US data protection law and practice was sufficient to safeguard the rights of European data subjects and it is clear from Article 25(6) of the 1995 Directive that national data protection authorities must comply with findings of this nature.

81. Eight, it follows, therefore, that if the Commissioner cannot look beyond the European Commission's Safe Harbour Decision of July 2000, then it is clear that the present application for judicial review must fail. This is because the Commission *has* already decided that the US provides an adequate level of data protection and, as we have just seen, s. 11(2)(a) of the 1998 Act (which in turn follows the provisions of Article 25(6) of the 1995 Directive) ties the Commissioner to the Commission's finding. In those circumstances, any complaint to the Commissioner concerning the transfer of personal data by Facebook Ireland (or, indeed, Facebook) to the US on the ground that US data protection was inadequate would be doomed to fail.

82. Ninth, while the applicant maintains that the Commissioner has not adhered to the requirements of EU law in holding that the complaint was unsustainable in law,

the opposite is, in fact, in truth the case. The Commissioner has rather demonstrated scrupulous steadfastness to the letter of the 1995 Directive and the 2000 Decision.

83. Tenth, the applicant's objection is, in reality, to the terms of the Safe Harbour Regime itself rather than to the manner in which the Commissioner has actually applied the Safe Harbour Regime, although neither the validity of the 1995 Directive nor the validity of the Commission's Safe Harbour decision have, as such, been challenged in these proceedings.

84. Eleventh, in these circumstances the critical issue which arises is whether the proper interpretation of the 1995 Directive and the 2000 Commission decision should be re-evaluated in the light of the subsequent entry into force of Article 8 of the Charter and whether, as a consequence, the Commissioner can look beyond or otherwise disregard this Community finding. It is for these reasons accordingly that I have decided to refer this question (and other linked questions) to the Court of Justice pursuant to Article 267 TFEU.

EXHIBIT 15



Data Retention and Investigatory Powers Act 2014

CHAPTER 27

Explanatory Notes have been produced to assist in the
understanding of this Act and are available separately

£6.00



Data Retention and Investigatory Powers Act 2014

CHAPTER 27

CONTENTS

Retention of relevant communications data

- 1 Powers for retention of relevant communications data subject to safeguards
- 2 Section 1: supplementary

Investigatory powers

- 3 Grounds for issuing warrants and obtaining data
- 4 Extra-territoriality in Part 1 of RIPA
- 5 Meaning of “telecommunications service”
- 6 Half-yearly reports by the Interception of Communications Commissioner
- 7 Review of investigatory powers and their regulation

Final provisions

- 8 Commencement, duration, extent and short title

ELIZABETH II

c. 27



Data Retention and Investigatory Powers Act 2014

2014 CHAPTER 27

An Act to make provision, in consequence of a declaration of invalidity made by the Court of Justice of the European Union in relation to Directive 2006/24/EC, about the retention of certain communications data; to amend the grounds for issuing interception warrants, or granting or giving certain authorisations or notices, under Part 1 of the Regulation of Investigatory Powers Act 2000; to make provision about the extra-territorial application of that Part and about the meaning of “telecommunications service” for the purposes of that Act; to make provision about additional reports by the Interception of Communications Commissioner; to make provision about a review of the operation and regulation of investigatory powers; and for connected purposes. [17th July 2014]

BE IT ENACTED by the Queen’s most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

Retention of relevant communications data

1 Powers for retention of relevant communications data subject to safeguards

- (1) The Secretary of State may by notice (a “retention notice”) require a public telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2) of the Regulation of Investigatory Powers Act 2000 (purposes for which communications data may be obtained).
- (2) A retention notice may –
 - (a) relate to a particular operator or any description of operators,

- (b) require the retention of all data or any description of data,
 - (c) specify the period or periods for which data is to be retained,
 - (d) contain other requirements, or restrictions, in relation to the retention of data,
 - (e) make different provision for different purposes,
 - (f) relate to data whether or not in existence at the time of the giving, or coming into force, of the notice.
- (3) The Secretary of State may by regulations make further provision about the retention of relevant communications data.
- (4) Such provision may, in particular, include provision about—
- (a) requirements before giving a retention notice,
 - (b) the maximum period for which data is to be retained under a retention notice,
 - (c) the content, giving, coming into force, review, variation or revocation of a retention notice,
 - (d) the integrity, security or protection of, access to, or the disclosure or destruction of, data retained by virtue of this section,
 - (e) the enforcement of, or auditing compliance with, relevant requirements or restrictions,
 - (f) a code of practice in relation to relevant requirements or restrictions or relevant powers,
 - (g) the reimbursement by the Secretary of State (with or without conditions) of expenses incurred by public telecommunications operators in complying with relevant requirements or restrictions,
 - (h) the 2009 Regulations ceasing to have effect and the transition to the retention of data by virtue of this section.
- (5) The maximum period provided for by virtue of subsection (4)(b) must not exceed 12 months beginning with such day as is specified in relation to the data concerned by regulations under subsection (3).
- (6) A public telecommunications operator who retains relevant communications data by virtue of this section must not disclose the data except—
- (a) in accordance with—
 - (i) Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act 2000 (acquisition and disclosure of communications data), or
 - (ii) a court order or other judicial authorisation or warrant, or
 - (b) as provided by regulations under subsection (3).
- (7) The Secretary of State may by regulations make provision, which corresponds to any provision made (or capable of being made) by virtue of subsection (4)(d) to (g) or (6), in relation to communications data which is retained by telecommunications service providers by virtue of a code of practice under section 102 of the Anti-terrorism, Crime and Security Act 2001.

2 Section 1: supplementary

- (1) In this section and section 1—
- “communications data” has the meaning given by section 21(4) of the Regulation of Investigatory Powers Act 2000 so far as that meaning

- applies in relation to telecommunications services and telecommunication systems;
- “functions” includes powers and duties;
- “notice” means notice in writing;
- “public telecommunications operator” means a person who—
- (a) controls or provides a public telecommunication system, or
 - (b) provides a public telecommunications service;
- “public telecommunications service” and “public telecommunication system” have the meanings given by section 2(1) of the Regulation of Investigatory Powers Act 2000;
- “relevant communications data” means communications data of the kind mentioned in the Schedule to the 2009 Regulations so far as such data is generated or processed in the United Kingdom by public telecommunications operators in the process of supplying the telecommunications services concerned;
- “relevant powers” means any powers conferred by virtue of section 1(1) to (6);
- “relevant requirements or restrictions” means any requirements or restrictions imposed by virtue of section 1(1) to (6);
- “retention notice” has the meaning given by section 1(1);
- “specify” means specify or describe (and “specified” is to be read accordingly);
- “telecommunications service” and “telecommunication system” have the meanings given by section 2(1) of the Regulation of Investigatory Powers Act 2000;
- “telecommunications service provider” means a person who provides a telecommunications service;
- “unsuccessful call attempt” means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention;
- “the 2009 Regulations” means the provisions known as the Data Retention (EC Directive) Regulations 2009 (S.I. 2009/859).
- (2) “Relevant communications data” includes (so far as it otherwise falls within the definition) communications data relating to unsuccessful call attempts that—
 - (a) in the case of telephony data, is stored in the United Kingdom, or
 - (b) in the case of internet data, is logged in the United Kingdom,
 but does not include data relating to unconnected calls or data revealing the content of a communication.
 - (3) Regulations under section 1(3) may specify the communications data that is of the kind mentioned in the Schedule to the 2009 Regulations and, where they do so, the reference in the definition of “relevant communications data” to communications data of that kind is to be read as a reference to communications data so specified.
 - (4) Any power to make regulations under section 1—
 - (a) is exercisable by statutory instrument,
 - (b) includes power to—
 - (i) confer or impose functions (including those involving the exercise of a discretion) on any person (including the Secretary of State),

- (ii) make supplementary, incidental, consequential, transitional, transitory or saving provision,
 - (iii) make different provision for different purposes,
 - (c) may, so far as relating to provision about codes of practice, be exercised in particular by modifying the effect of sections 71 and 72 of the Regulation of Investigatory Powers Act 2000 (codes of practice in relation to certain powers and duties).
- (5) A statutory instrument containing regulations under section 1 is not to be made unless a draft of the instrument has been laid before, and approved by a resolution of, each House of Parliament.

*Investigatory powers***3 Grounds for issuing warrants and obtaining data**

- (1) Section 5 of the Regulation of Investigatory Powers Act 2000 (power to issue necessary and proportionate interception warrants in interests of national security, to prevent or detect serious crime or to safeguard the UK's economic well-being) is amended as set out in subsection (2).
- (2) In subsection (3)(c) (economic well-being of the UK), after "purpose" insert " , in circumstances appearing to the Secretary of State to be relevant to the interests of national security,".
- (3) Section 22 of that Act (power to obtain communications data in interests of national security, to prevent or detect serious crime, in interests of the UK's economic well-being and for other specified purposes) is amended as set out in subsection (4).
- (4) In subsection (2)(c) (economic well-being of the UK), after "United Kingdom" insert "so far as those interests are also relevant to the interests of national security".

4 Extra-territoriality in Part 1 of RIPA

- (1) Part 1 of the Regulation of Investigatory Powers Act 2000 (communications) is amended as follows.
- (2) In section 11 (implementation of interception warrants), after subsection (2) insert—
 - “(2A) A copy of a warrant may be served under subsection (2) on a person outside the United Kingdom (and may relate to conduct outside the United Kingdom).
 - (2B) Service under subsection (2) of a copy of a warrant on a person outside the United Kingdom may (in addition to electronic or other means of service) be effected in any of the following ways—
 - (a) by serving it at the person's principal office within the United Kingdom or, if the person has no such office in the United Kingdom, at any place in the United Kingdom where the person carries on business or conducts activities;
 - (b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person's behalf, will

accept service of documents of the same description as a copy of a warrant, by serving it at that address;

- (c) by making it available for inspection (whether to the person or to someone acting on the person's behalf) at a place in the United Kingdom (but this is subject to subsection (2C)).
- (2C) Service under subsection (2) of a copy of a warrant on a person outside the United Kingdom may be effected in the way mentioned in paragraph (c) of subsection (2B) only if—
 - (a) it is not reasonably practicable for service to be effected by any other means (whether as mentioned in subsection (2B)(a) or (b) or otherwise), and
 - (b) the person to whom the warrant is addressed takes such steps as the person thinks appropriate for the purpose of bringing the contents of the warrant, and the availability of a copy for inspection, to the attention of the person outside the United Kingdom.

The steps mentioned in paragraph (b) must be taken as soon as reasonably practicable after the copy of the warrant is made available for inspection.”

- (3) In subsection (4) of that section, after “that person” insert “(whether or not the person is in the United Kingdom)”.
- (4) After subsection (5) of that section insert—
 - “(5A) Where a person outside the United Kingdom is under a duty by virtue of subsection (4) to take any steps in a country or territory outside the United Kingdom for giving effect to a warrant, in determining for the purposes of subsection (5) whether the steps are reasonably practicable for the person to take, regard is to be had (amongst other matters) to—
 - (a) any requirements or restrictions under the law of that country or territory relevant to the taking of those steps, and
 - (b) the extent to which it is reasonably practicable to give effect to the warrant in a way that does not breach any such requirements or restrictions.”
- (5) In subsection (8) of that section, after “enforceable” insert “(including in the case of a person outside the United Kingdom)”.
- (6) In section 12 (maintenance of interception capability), after subsection (3) insert—
 - “(3A) An obligation may be imposed in accordance with an order under this section on, and a notice under subsection (2) given to, persons outside the United Kingdom (and may be so imposed or given in relation to conduct outside the United Kingdom).
 - (3B) Where a notice under subsection (2) is to be given to a person outside the United Kingdom, the notice may (in addition to electronic or other means of giving a notice) be given to the person—
 - (a) by delivering it to the person's principal office within the United Kingdom or, if the person has no such office in the United Kingdom, to any place in the United Kingdom where the person carries on business or conducts activities, or

- (b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person's behalf, will accept documents of the same description as a notice, by delivering it to that address."
- (7) In subsection (7) of that section –
- (a) after "person" insert "(whether or not the person is in the United Kingdom)", and
- (b) after "enforceable" insert "(including in the case of a person outside the United Kingdom)".
- (8) In section 22 (obtaining and disclosing communications data), after subsection (5) insert –
- “(5A) An authorisation under subsection (3) or (3B), or a requirement imposed in accordance with a notice under subsection (4), may relate to conduct outside the United Kingdom (and any such notice may be given to a person outside the United Kingdom).
- (5B) Where a notice under subsection (4) is to be given to a person outside the United Kingdom, the notice may (in addition to electronic or other means of giving a notice) be given to the person in any of the following ways –
- (a) by delivering it to the person's principal office within the United Kingdom or, if the person has no such office in the United Kingdom, to any place in the United Kingdom where the person carries on business or conducts activities;
- (b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person's behalf, will accept documents of the same description as a notice, by delivering it to that address;
- (c) by notifying the person of the requirements imposed by the notice by such other means as the person giving the notice thinks appropriate (which may include notifying the person orally, except where the notice is one to which section 23A applies).”
- (9) In subsection (6) of that section, after "operator" insert "(whether or not the operator is in the United Kingdom)".
- (10) In subsection (8) of that section, after "enforceable" insert "(including in the case of a person outside the United Kingdom)".

5 Meaning of "telecommunications service"

In section 2 of the Regulation of Investigatory Powers Act 2000 (meaning of "interception" etc), after subsection (8) insert –

- “(8A) For the purposes of the definition of "telecommunications service" in subsection (1), the cases in which a service is to be taken to consist in the provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system.”

6 Half-yearly reports by the Interception of Communications Commissioner

- (1) Section 58 of the Regulation of Investigatory Powers Act 2000 (reports by the Interception of Communications Commissioner) is amended as follows.
- (2) In subsection (4) (annual reports), after “calendar year” insert “and after the end of the period of six months beginning with the end of each calendar year”.
- (3) In subsection (6) (duty to lay annual reports before Parliament), after “annual report” insert “, and every half-yearly report,”.
- (4) In subsection (6A) (duty to send annual reports to the First Minister), after “annual report” insert “, and every half-yearly report,”.
- (5) In subsection (7) (power to exclude matter from annual reports), after “annual report” insert “, or half-yearly report,”.

7 Review of investigatory powers and their regulation

- (1) The Secretary of State must appoint the independent reviewer of terrorism legislation to review the operation and regulation of investigatory powers.
- (2) The independent reviewer must, in particular, consider –
 - (a) current and future threats to the United Kingdom,
 - (b) the capabilities needed to combat those threats,
 - (c) safeguards to protect privacy,
 - (d) the challenges of changing technologies,
 - (e) issues relating to transparency and oversight,
 - (f) the effectiveness of existing legislation (including its proportionality) and the case for new or amending legislation.
- (3) The independent reviewer must, so far as reasonably practicable, complete the review before 1 May 2015.
- (4) The independent reviewer must send to the Prime Minister a report on the outcome of the review as soon as reasonably practicable after completing the review.
- (5) On receiving a report under subsection (4), the Prime Minister must lay a copy of it before Parliament together with a statement as to whether any matter has been excluded from that copy under subsection (6).
- (6) If it appears to the Prime Minister that the publication of any matter in a report under subsection (4) would be contrary to the public interest or prejudicial to national security, the Prime Minister may exclude the matter from the copy of the report laid before Parliament.
- (7) The Secretary of State may pay to the independent reviewer –
 - (a) expenses incurred in carrying out the functions of the independent reviewer under this section, and
 - (b) such allowances as the Secretary of State determines.
- (8) In this section “the independent reviewer of terrorism legislation” means the person appointed under section 36(1) of the Terrorism Act 2006 (and “independent reviewer” is to be read accordingly).

Final provisions

8 Commencement, duration, extent and short title

- (1) Subject to subsection (2), this Act comes into force on the day on which it is passed.
- (2) Section 1(6) comes into force on such day as the Secretary of State may by order made by statutory instrument appoint; and different days may be appointed for different purposes.
- (3) Sections 1 to 7 (and the provisions inserted into the Regulation of Investigatory Powers Act 2000 by sections 3 to 6) are repealed on 31 December 2016.
- (4) This Act extends to England and Wales, Scotland and Northern Ireland.
- (5) This Act may be cited as the Data Retention and Investigatory Powers Act 2014.

© Crown copyright 2014

Printed in the UK by The Stationery Office Limited under the authority and superintendence of Carol Tullo, Controller of Her Majesty's Stationery Office and Queen's Printer of Acts of Parliament

07/2014 42350 19585



Published by TSO (The Stationery Office) and available from:

Online

www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail

TSO

PO Box 29, Norwich, NR3 1GN

Telephone orders/General enquiries: 0870 600 5522

Fax orders: 0870 600 5533

E-mail: customer.services@tso.co.uk

Textphone 0870 240 3701

TSO@Blackwell and other Accredited Agents

ISBN 978-0-10-542714-8



9 780105 427148

A253

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain E-
Mail Account Controlled and Maintained by
Microsoft Corporation

Action Nos. 13-MAG-2814, M9-150

DECLARATION OF JOSEPH V. DEMARCO

I, **JOSEPH V. DEMARCO, ESQ.**, pursuant to Title 28, United States Code,
Section 1746, declare as follows:

1. I am a partner in the law firm of DeVore & DeMarco LLP, an attorney in good standing to practice law in the State of New York, and am admitted to practice in the United States District Court for the Southern District of New York.

2. At the request of Microsoft Corporation (“Microsoft”), I have prepared this Declaration in connection with the above-captioned litigation. Specifically, in order to aid this Court in a proper resolution of the issues in controversy, Microsoft has requested that I provide my insight and analysis concerning certain practices and procedures related to the preservation of electronic evidence held by electronic communications service providers located outside the United States pending the fulfillment of requests made under Mutual Legal Assistance treaties (“MLATs”) and Letters Rogatory for such evidence by the U.S Department of Justice (the “DOJ”).

I. SUMMARY

3. I have reviewed the April 25, 2014, Memorandum and Order of U.S. Magistrate Judge James C. Francis IV (1:13-mj-02814-UA, No. 5), Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion dated June 6, 2014 (1:13-mj-02814-UA, No. 15), the Government's Brief in Support of the Magistrate Judge's Opinion filed on July 9, 2014 (1:13-mj-02814-UA, No. 60), the Council of Europe's Convention on Cybercrime, and the related supporting materials cited herein. Based on my experience and expertise in the field of electronic evidence preservation and collection, as described below, and my review of the aforementioned documents, I am aware that there are several methods of evidence preservation that are used by the DOJ for the purpose of quickly, effectively, and efficiently ensuring that electronic communications and other digital evidence located abroad are preserved pending the execution of formal legal process to obtain such evidence.

II. QUALIFICATIONS

4. I am a founding partner at the law firm of DeVore & DeMarco LLP, where I specialize in counseling clients on complex issues involving information privacy and security, computer intrusions, theft of intellectual property, on-line fraud, and the preservation and collection of digital evidence. From 1997 to 2007, I served as an Assistant United States Attorney for the Southern District of New York, where I founded and headed the Computer Hacking and Intellectual Property ("CHIPs") program, a group of prosecutors dedicated to investigating and prosecuting violations of federal cybercrime laws. From January, 2001, until July, 2001, I served as a visiting Trial Attorney at the Computer Crime and Intellectual Property Section of DOJ in Washington, D.C. ("CCIPS"). At CCIPS, among other things, I was responsible for assisting federal and state prosecutors throughout the United States as well as

foreign prosecutors and other law enforcement officials in the preservation and collection of electronic evidence from, among other entities, Internet Service Providers (“ISPs”) located inside and outside the United States. In these roles, I personally prepared and facilitated, and was aware of the preparation and facilitation by other law enforcement officials, of emergency requests for electronic evidence, including requests for the preservation and collection of electronic evidence from ISPs and providers of electronic communications services. In addition, I was also responsible for working on CCIPS’ policy-related efforts concerning the Council of Europe’s (then draft, now final) Convention on Cybercrime (the “Budapest Convention”).

5. Since 2007, in my private practice, I have regularly counseled clients on the preservation and collection of electronic evidence in criminal and civil litigations and investigations both domestically and internationally. This has included requests for the emergency preservation of electronic evidence from electronic communications service providers.

6. Since 2002, I have served as an Adjunct Professor at Columbia Law School, where I teach the upper-class Internet and Computer Crimes seminar. I have spoken throughout the world on a range of cybercrime, digital evidence collection and preservation, cloud computing, e-commerce law, and IP rights enforcement issues. Domestically, I have lectured on the subject of cybercrime and electronic evidence gathering at Harvard Law School, the Practising Law Institute (“PLI”), the National Advocacy Center, and at the FBI Academy in Quantico, Virginia. Internationally, I have lectured on these subjects to law enforcement officials and lawyers in Europe, Asia, and the Middle East. I am on the Board of Advisors of the *Center for Law and Information Policy* at Fordham University School of Law, and am a member of the Professional Editorial Board of the *Computer Law and Security Review* published by

Elsevier. I am also listed in *Chambers USA: America's Leading Lawyers for Business* guide as a leading lawyer nationwide in Privacy and Data Security, and am a *Martindale-Hubbell* AV-rated lawyer in the areas of Computers and Software, Litigation and Internet Law.

7. As a former federal prosecutor and as an attorney in private practice, I have had extensive experience throughout my career with complex issues relating to electronic evidence preservation, collection, and spoliation. For example, as the head of the CHIPs program in the Southern District of New York, I was responsible for supervising and advising Assistant United States Attorneys in the District in a broad variety of criminal cases on how to find and collect electronic evidence -- such as the content of e-mails and associated account transmission and subscriber records -- from a wide range of sources, both domestically and internationally. In particular, I regularly reviewed applications for search warrants, court orders, MLAT requests, as well as grand jury subpoenas and administrative subpoenas which called for the production of various forms of electronic evidence. In addition, while at CCIPS, I was responsible for advising foreign law enforcement officials from numerous countries regarding evidence preservation techniques and strategies as they related to U.S. law, as well as with applicable evidence retention, preservation, and access policies and practices of ISPs based in the United States. I provided this advice and assistance in cases involving routine requests for electronic evidence as well as in exigent circumstances where the need for very rapid and efficient action was frequently of paramount importance.

8. In addition to my experience in government, in private practice I have continued to be frequently called upon to provide advice on the preservation and collection of digital evidence. The need for this assistance arises in cases implicating both criminal statutes as well as civil causes of action; not infrequently, these requests are either extremely time-sensitive

and/or involve high-stakes digital evidence preservation and collection issues. For example, I have provided advice related to the preservation and collection of e-mail communications and other electronic evidence in cases involving extortion, computer hacking, theft of trade secrets, illegal password trafficking, copyright infringement, and harassment and cyber-stalking, among others. I have also frequently been involved in representing clients who have been asked to provide digital evidence and other assistance to the government in criminal as well as intelligence-related investigations.

9. Based on the above experience, I am familiar with requests to seek evidence preservation and collection from ISPs and similar entities, including through the assistance of foreign law enforcement officials. I am also aware that law enforcement officials outside the United States regularly cooperate with federal and state criminal investigators in the United States to achieve the preservation of electronic evidence for use in investigations and prosecutions. This cooperation both complements and reinforces the MLAT and Letters Rogatory framework and includes (a) direct law-enforcement-to-law-enforcement informal cooperation, (b) a more formal “24/7” network, and (c) the Budapest Convention discussed below.

III. INTERNATIONAL EVIDENCE PRESERVATION IN CRIMINAL INVESTIGATIONS

10. Because of its nature, electronic evidence often can be lost if it is not secured in a timely and efficient manner. Partly as a result of this, in my experience, law enforcement officials in various countries communicate with each other directly in cases involving electronic evidence in order to locate, preserve, and collect such evidence. Based on my experience, such direct cooperation is particularly close between United States and Western

European law enforcement officials, as well as between law enforcement officials in the United States and those of English-speaking nations throughout the world.

11. In addition to the direct law-enforcement-to-law-enforcement cooperation noted above, since at least 2001, the DOJ has maintained a “24/7 Network” list of emergency law enforcement contacts committed to assist in the preservation of digital evidence across international borders consistent with national legislation. As its name suggests, this list allows for around-the-clock contact among participants to achieve electronic evidence preservation. The list consists of representatives from dozens of countries around the world.

12. Moreover, on December 29, 2006, the United States ratified the Budapest Convention. Notably, Article 29 of the Convention requires that signatory countries implement laws so that foreign governments can request the preservation of electronic data inside their borders and thus ensure that requested data is “not [] altered, removed or deleted during the period of time required to prepare, transmit and execute a request for mutual assistance to obtain the data.”¹ The Convention contemplates that, following preservation pursuant to its mandate, access to data by a foreign nation shall proceed according to established international legal process. Notably, international preservation requests as contemplated by the drafters are quite common.² Noteworthy too is that the Convention affirms and supports the 24/7 Network

¹ See Council of Europe, *Explanatory Report to the Convention on Cybercrime*, available at <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm> (last visited July 22, 2014).

² See Cybercrime Convention Committee, *Assessment Report: Implementation of the Preservation Provisions of the Budapest Convention on Cybercrime*, at 17, 49 (January 25, 2013), available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.pdf (last visited July 22, 2014), (noting that as of 2012 the “U.S. sends and receives hundreds of preservation requests per year”).

discussed above.³ To be clear, these mechanisms supplement the direct law-enforcement-to-law-enforcement communications which I describe in paragraphs 10 and 11, above.

13. Through law-enforcement-to-law-enforcement cooperation, the 24/7 Network, and the Budapest Convention, U.S. law enforcement officials and their foreign counterparts regularly preserve electronic evidence on behalf of one another, including evidence at ISPs, across international borders.

14. The government states in its brief that MLATs “typically take[] months to process.” Gov’t Br. 25. Based on my knowledge and experience, there is no “one size fits all” period of time in which MLATs are executed. Rather, the speed at which an MLAT is acted upon is a function of the urgency and priority of that request to law enforcement officials. Many MLATs submitted by United States officials to foreign counterparts are not especially time sensitive or urgent, and part of the period associated with receiving evidence via an MLAT consists of the time that DOJ takes to prepare and transmit the MLAT to foreign counterparts. This involves work at the local United States Attorney’s office and/or prosecuting unit at DOJ and, subsequently, at the Office of International Affairs, which is the central office at DOJ to which draft MALTs are regularly forwarded for review, comment, approval, and ultimate transmittal abroad. Importantly, however, in my experience, DOJ officials and relevant foreign

³ *Id.* at 4, 12.

executing officials can, and regularly do, move with great alacrity and efficiency in processing, transmitting, and responding to high-priority MLATs.

15. I declare under penalty of perjury that the foregoing is true and correct.

Dated: New York, New York
July 24, 2014


Joseph V. DeMarco

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain
E-Mail Account Controlled and Maintained by
Microsoft Corporation

Action Nos. 13-MAG-2814, M9-150

SUPPLEMENTAL DECLARATION OF MICHAEL MCDOWELL

I, **MICHAEL MCDOWELL**, declare as follows:

1. I am a Senior Counsel at the Bar of Ireland, having been called to the Bar in 1974 and to the Inner Bar in 1987. I was Attorney General of Ireland from 1999 to 2002, Minister of Justice, Equality and Law Reform from 2002 to 2007, and Deputy Prime Minister from 2006 to 2007. I left government service in 2007, and I am now in practice as a Senior Counsel in the Irish High and Supreme Courts.

2. I have been engaged by Microsoft as an independent expert to opine on the issues raised in this case. This declaration supplements my declaration of 5 June 2014, and provides additional information in respect of certain statements made by the U.S. Government in its submission of 9 July 2014.

3. Specifically, on page 25 of its submission, the U.S. Government states that an “MLAT request typically takes months to process.” This statement is not accurate with respect to MLAT requests processed by the Irish government.

4. The amount of time the Irish government requires to process an MLAT request (*i.e.*, the time from when the request is made until the evidence is received by the foreign MLAT party) depends upon the type and urgency of the request. Some requests, such as a request for a deposition, can take months from start to finish. Other requests, such as requests

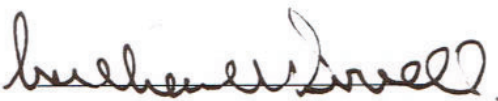
for digital evidence, are generally fulfilled within a matter of weeks. Furthermore, if a request is urgent, the Irish government will process the request more quickly than if it is not urgent. If necessary, urgent requests can be processed in a matter of days.

5. In addition, the Criminal Justice (Mutual Assistance) Act, 2008, mandates procedures to ensure that evidence (most often bank accounts but also digital evidence) sought by an MLAT request is not destroyed or altered while the request is being processed. Where a foreign government requests that Ireland preserve (or “freeze”) digital evidence located in Ireland, the Irish Department of Justice and Equality (acting as Ireland’s Central Authority) can apply to the Irish High Court for a freezing cooperation order. This freezing cooperation order prohibits any person with possession of the evidence from altering or destroying it, and may also authorize the An Garda Síochána — Ireland’s national police service — to seize property subject to the order to prevent it from being removed, altered, or destroyed. Ireland generally processes requests for freezing cooperation orders within 24 hours from when they are made.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on 23rd July 2014.

Signed: 
Michael McDowell

E7V3MICC

1 UNITED STATES DISTRICT COURT
1 SOUTHERN DISTRICT OF NEW YORK

2 -----x

2
3 IN THE MATTER OF A WARRANT
3 TO SEARCH A CERTAIN
4 E-MAIL ACCOUNT 13 MJ 2814
4 CONTROLLED AND MAINTAINED
5 BY MICROSOFT CORPORATION

6 -----x

7 New York, N.Y.
7 July 31, 2014
8 10:45 a.m.
8
9

9 Before:

10 HON. LORETTA A. PRESKA,

11 District Judge

12
13 APPEARANCES

14 PREET BHARARA
14 United States Attorney for the
15 Southern District of New York
15 JUSTIN ANDERSON
16 SERRIN TURNER
16 Assistant United States Attorneys

17 ORRICK, HERRINGTON & SUTCLIFFE
18 Attorneys for Microsoft
18 E. JOSHUA ROSENKRANZ
19 ROBERT E. LOEB
19 BRIAN P. GOLDMAN

20 PETRILLO KLEIN & BOXER
21 Attorneys for Microsoft
21 GUY PETRILLO

22 COVINGTON & BURLING
23 Attorneys for Microsoft
23 JAMES GARLAND
24 NANCY KESTENBAUM

24
25 SOUTHERN DISTRICT REPORTERS, P.C.
(212) 805-0300

E7V3MICC

1 Appearances Continued
2 ZWILLGEN
2 Attorneys for Apple, Inc. and Cisco
3 MARC J. ZWILLINGER
3
4 STEPTOE & JOHNSON
4 Attorneys for Verizon Communications Inc.
5 MICHAEL A. VASTIS
5
6 SIDLEY AUSTIN
6 Attorneys for AT&T CORP.
7 ALAN C. RAUL

8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

SOUTHERN DISTRICT REPORTERS, P.C.
(212) 805-0300

E7V3MICC

1 THE COURT: Mr. Turner, Mr. Anderson.

2 MR. TURNER: Yes, good morning.

3 THE COURT: Mr. Rosenkranz.

4 MR. ROSENKRANZ: Yes.

5 THE COURT: Good morning. Mr. Garland, Mr. Petrillo.

6 And where are the amici? Good morning, nice to see

7 you all. Thank you for your excellent papers, counsel, from

8 everyone.

9 Could I ask the government to start, please. What

10 exactly is the government's position on whether or not SCA

11 warrants are or are not searches? And in the context we're

12 speaking, where do these searches take place, please.

13 MR. TURNER: Your Honor, the government's view is

14 those terms in this context tend to confuse, really, more than

15 they clarify.

16 I know that Microsoft wants to invoke those terms

17 because they want to shoehorn SCA warrants into the terminology

18 of a physical search warrant. But that shoe doesn't fit, and

19 what the statute talks about is required disclosure. That's

20 what we're seeking through the warrant. That's what the

21 warrant authorizes.

22 In terms of when a search occurs, when a seizure

23 occurs, those terms can be used in all sorts of different ways,

24 but certainly, I think if Microsoft's position is accepted, it

25 would imply that every subpoena the government has ever issued

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 would entail a Fourth Amendment search. Because their position
2 is basically their mere gathering of records in response to the
3 compulsory process that an SCA warrant constitutes is a search
4 and a seizure.

5 If that's the case, then that would also be the case
6 for every production of records for a subpoena, because
7 functionally it is really no different.

8 In terms of the Fourth Amendment interest in play,
9 there is an issue as to whether the Fourth Amendment applies to
10 e-mails held in the hands of a third-party provider.

11 As to that issue, the government does not concede that
12 the Fourth Amendment applies and --

13 THE COURT: Doesn't concede?

14 MR. TURNER: Doesn't concede Warshak, the Sixth
15 Circuit holding that the Fourth Amendment applies to e-mail
16 held by a third-party provider.

17 But the Court really doesn't need to reach that issue
18 here because the government got a warrant. So whatever Fourth
19 Amendment rights do attach to these e-mails, they have been
20 attended to through the government's obtaining of a warrant,
21 with all the privacy safeguards that are attendant to a
22 warrant. This warrant was issued by a neutral magistrate
23 judge.

24 THE COURT: Right. But you have materials in your
25 papers talking about the search doesn't take place until the

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 government agent has opened, essentially, the content and read
2 the content. Your position, I thought, was that any search did
3 not take place where the content is stored. That is in this
4 case in Dublin.

5 MR. TURNER: Any review or search, whatever the term
6 is, does not take place until we've actually gotten the
7 documents. I think that's really what the Fourth Amendment
8 would be concerned about here. That the government shouldn't
9 have a right to access and review these materials until it's
10 gone through the hoops of getting a warrant and approval from a
11 judge.

12 So, certainly we would not agree that there is any
13 search or seizure until the government actually obtains the
14 records from Microsoft. Even then, I think these terms are not
15 really useful in this context. It is better to stick to the
16 terms of the statute of required disclosure.

17 THE COURT: What do you say to Microsoft's argument
18 that compelling Microsoft to be the agent of the government is
19 the same as the government's searching or opening or reading
20 that content?

21 MR. TURNER: Again, if that were the case, then every
22 subpoena ever issued would constitute compelling someone to
23 execute a search on the government's behalf. That is not the
24 law. I can point your Honor to cases if you'd like.

25 THE COURT: That's okay.

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 Let me ask Microsoft this. Isn't the magistrate
2 judge's holding consistent with the Fourth Amendment because,
3 unlike a subpoena, an SCA warrant requires a finding of
4 probable cause by a neutral magistrate judge?

5 Or put a different way, aren't the Fourth Amendment
6 concerns addressed here by an SCA warrant issued by a
7 magistrate judge?

8 MR. ROSENKRANZ: Your Honor, the Fourth Amendment
9 concerns are addressed. We are not making in our ECPA piece of
10 the argument a Fourth Amendment challenge. There is a separate
11 particularity point.

12 But, let me just back up before embellishing that by
13 just commenting on the two questions that you asked Mr. Turner,
14 and then it will be much clearer why the Fourth Amendment is
15 relevant to our argument, but it is not a Fourth Amendment
16 argument.

17 So, your Honor was exactly right. You asked two
18 questions. There are three questions in this case. Question
19 number one is what is the conduct that the government by
20 Congressional statute, they claim, is requiring Microsoft to
21 do. That conduct is a search and a seizure. And one of the
22 reasons that we know it is a search and a seizure is because
23 here in the United States, if they did it, we would call it a
24 search and a seizure and you would require a warrant. It is a
25 violation of or it is an infringement on reasonable

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 expectations of privacy. The same is true abroad, even though
2 we don't need a warrant.

3 So the fact that it is a warrant that in this country
4 we would view as something that justifies a search and a
5 seizure is relevant as an evidentiary matter to the answer to
6 that first question.

7 THE COURT: I didn't understand that.

8 MR. ROSENKRANZ: I apologize. Let me say what the
9 three questions are. So the first question is, what is the
10 conduct that this statute requires Microsoft to engage in. Our
11 answer is, for reasons that I'll explain in a moment, it is a
12 search and a seizure.

13 The second question which you correctly asked, your
14 Honor, of the government, is where do the search and seizure
15 occur? Our answer is that the search and seizure occurred in
16 Ireland.

17 Then a third question, which you haven't asked yet is,
18 if so, under Morrison, if the search and seizure that is
19 commanded here occurs in Ireland, then, did Congress express a
20 clear intention to authorize searches and seizures in Ireland.

21 And the question your Honor asked me about the Fourth
22 Amendment is relevant to that first question. So if I may
23 embellish a bit, and you'll see contextually where the Fourth
24 Amendment values play in.

25 THE COURT: All right. But I really wanted to hear
SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 the answer. I guess you've already said and you've already
2 conceded that the Fourth Amendment concerns are addressed by
3 the requirement for an SCA warrant, that a neutral magistrate
4 judge issue it upon a finding of probable cause. So, I think
5 that's off the table. Isn't it?

6 MR. ROSENKRANZ: That is -- yes, that is correct. If
7 this warrant were served in the United States, the Fourth
8 Amendment concerns would be satisfied. If --

9 THE COURT: It was served in the United States.

10 MR. ROSENKRANZ: I'm sorry. If the warrant related to
11 property to correspondence that resides in the United States,
12 the Fourth Amendment interests would be satisfied.

13 The Fourth Amendment interests are -- the Fourth
14 Amendment or at least the warrant clause is not applicable
15 abroad. But the answer to the question whether this is a
16 search resolves around the question what is this conduct, what
17 does it require. And what it requires is, an invasion of
18 privacy of the individual, with a warrant or without, it still
19 is an invasion of privacy.

20 THE COURT: We've decided that the Fourth Amendment
21 concerns about at least privacy are addressed because a neutral
22 magistrate judge issued the warrant.

23 MR. ROSENKRANZ: So our --

24 THE COURT: That doesn't help us.

25 MR. ROSENKRANZ: Yes. Our concerns in the United

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 States about an invasion of privacy are addressed. But this
2 case is about a power that the government claims, which is an
3 extraordinary power, which is to conscript Microsoft here in
4 the United States to search files abroad.

5 Now, if a foreign government did that to us, in other
6 words, if a foreign government went to Microsoft and said we
7 are interested in the e-mails of your customers, we are
8 interested in getting them in the United States, so why don't
9 you just connect to servers in the United States, we would
10 consider that an astounding infringement of our sovereignty.

11 So the question for this Court, ultimately, the third
12 question will end up being, did Congress authorize that
13 infringement on sovereignty.

14 THE COURT: Two things. I think we have to agree that
15 Congress certainly intended these SCA warrants to be different
16 in some respects from Rule 41 warrants. We've talked about who
17 may issue them and under what jurisdiction and this and that
18 and the other thing. So for that reason, we have to see what
19 Congress intended.

20 Also, we know that one of the differences that
21 Congress prescribed with respect to these SCA warrants was that
22 a law enforcement officer didn't have to be present anywhere.
23 So these are clearly different.

24 Secondly, don't we have to presume that Congress was
25 aware of the Bank of Nova Scotia doctrine where banks for

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 decades have been required to do precisely what Microsoft is
2 being required to do here? And that is, to access their
3 documents abroad, bring them back, documents they have
4 possession, custody and control over, bring them back and
5 produce them to the government here.

6 So why wouldn't we think that in using the language
7 Congress used, which I think Mr. Turner was referring to,
8 disclosure of records, why wouldn't we assume Congress knew
9 about the Bank of Nova Scotia doctrine and intended that to be
10 applicable here?

11 MR. ROSENKRANZ: Well, so, my answer begins with the
12 premise that this is a search. What the statute requires is a
13 search. It is Microsoft doing the search, or as your Honor
14 said, the government doesn't have to be present under 2703(g),
15 but the government could do the search in Microsoft's place.
16 So what this authorizes is a search.

17 Now, I hear the government, and sort of embedded in
18 one of your questions is the government's point, well, it is
19 not the government doing the search, it is the government
20 requiring Microsoft to do the search. Well, that's just wrong.
21 The Supreme Court said it was wrong in 1925. A search is a
22 search. The government cannot compel us to do a search by
23 operation of law and then disclaim responsibility for the
24 search that it is requiring us to do.

25 THE COURT: Where are all the bank cases in the
SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 decades since Nova Scotia?

2 MR. ROSENKRANZ: So the bank cases are, at least for
3 now, certainly still good law. But, plainly different from
4 what's going on here, precisely because what the government is
5 commanding here is a search of other people's property, effects
6 and correspondence, rather than --

7 THE COURT: Which other people have freely handed over
8 to the ISP.

9 MR. ROSENKRANZ: Yes, your Honor, that is a critical
10 distinction. A critical point that I want to make sure to
11 address.

12 So the government's point is no big deal, this is a
13 disclosure. Now, the disclosure point in the statute, I just
14 want to be clear what it says. The statute says the
15 government, "may require the disclosure by a provider of e-mail
16 contents only pursuant to a warrant."

17 So step one is Congress is recognizing that the first
18 thing that is happening is a search and seizure that is
19 authorized by this piece of paper called a search and seizure
20 warrant. The next thing is once we have it --

21 THE COURT: Let me just interrupt you. The statute
22 uses precisely the same terminology when talking about a
23 subpoena and a court order. So all of the various gradations
24 of disclosures that are authorized in the act are couched in
25 the same terms of disclosure of documents by the ISP.

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 MR. ROSENKRANZ: So, yes. At the front of each
2 sentence the government -- the Congress says that the
3 government can order us to disclose.

4 At the back of this particular sentence is disclose
5 only pursuant to a warrant. The warrant is evidence that
6 Congress understood that what we were being required to do was
7 a search and a seizure. It is something that we would view as
8 a search and a seizure if another country did it to us, and the
9 other country would view as a search and seizure when we do it
10 to them.

11 THE COURT: I'm not sure what the import of that is,
12 given that a neutral magistrate has found probable cause in the
13 same way he or she would in any other kind of warrant.

14 MR. ROSENKRANZ: The import, your Honor, is it is
15 perfectly fine in this country for magistrates to issue search
16 and seizure warrants against our citizens for property that is
17 here. When we do that in another country, that is an invasion
18 of that country's --

19 THE COURT: Now we're back to my question, which is,
20 isn't the language used by Congress, which is the disclose
21 language, doesn't that lead us to the Bank of Nova Scotia
22 result? That is, that the company that is here in the United
23 States may be required to disclose records it keeps overseas.

24 MR. ROSENKRANZ: The answer, your Honor, is no. For
25 two reasons. First, just because Congress calls it "disclose"

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 doesn't change the fundamental nature of what it is. The
2 fundamental nature of what it is, is a search and a seizure.
3 Congress's use of the word "warrant" and all sorts of other
4 indications and evidence demonstrates it is in fact a search
5 and a seizure.

6 So calling it a "disclosure" doesn't change what it
7 is. If Congress passed a statute that says that Chase Bank
8 must disclose the contents of a safe deposit box when the safe
9 deposit box is filled with private correspondence, the answer
10 would be Congress can't just call it a disclosure and avoid the
11 fact that what it really is, is a search and a seizure.

12 THE COURT: There is no history of the use of
13 disclosure in that context. Whereas here, there is a history
14 from I think the mid '80s at least of disclosure of records.

15 MR. ROSENKRANZ: Agreed, your Honor. So let's talk
16 about the backdrop. So the backdrop is the subpoena power.
17 And the use of the word disclosure.

18 Now, the subpoena power would never authorize the
19 government to seek a subpoena for the records sitting in a safe
20 deposit box in Chase. They couldn't subpoena those documents
21 of a private customer. They would need a warrant. Why?
22 Because it is a search and a seizure. BNS says that when the
23 government goes to a target and says give us your documents,
24 then that is not a search. That is rather the disclosure of a
25 witness's own information.

SOUTHERN DISTRICT REPORTERS, P.C.
(212) 805-0300

E7V3MICC

1 When the government goes to a bank and says give us
2 your records describing al Qaeda's financial transactions, that
3 is not a search. That is simply a disclosure of information.
4 That is the company's own business records.

5 But there is a world of difference between what BNS
6 justifies, which is a disclosure of information that is the
7 company's own business records on one hand, versus on the other
8 hand, the government going to a private actor and saying we
9 don't want your records, we want the records of your customers
10 who entrust those records to you surrounded by a safeguard. It
11 is the digital lockbox --

12 THE COURT: Let me ask you this then. Why is that not
13 equally applicable to content stored on Microsoft's servers in
14 this country? Why does Microsoft not take the position in
15 response to a subpoena, sorry, it is not my information, I'm
16 not turning that over.

17 MR. ROSENKRANZ: We do, your Honor. If the government
18 tried to subpoena us for the records of our customers that are
19 imbued with expectations of privacy on which we promise them
20 privacy, we would say you can't do that by subpoena. Warshak
21 says --

22 THE COURT: You need a warrant.

23 MR. ROSENKRANZ: Warshak says you need a warrant.

24 Why? Because it's a search and seizure.

25 THE COURT: Because the neutral magistrate judge signs
SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 off on probable cause.

2 MR. ROSENKRANZ: That is the next legal act that
3 occurs, but the predicate for why you need a search warrant is
4 because it is indeed a search. And if it is a search when it
5 happens here in the United States, it is a search when it
6 happens abroad.

7 The critical question when it happens abroad, the
8 privacy interests are relevant to that first question, is it a
9 search and seizure. Once the answer is yes, the question is
10 where does it happen. It happens in Ireland.

11 The critical question once we acknowledge that it is a
12 search and a seizure and it happens in Ireland, is, is that an
13 invasion of Irish sovereignty? Of course it is. We would
14 consider it an invasion of our sovereignty. Then you get to
15 the question -- so it is perfectly fine that U.S. privacy
16 interests are satisfied. But international law says that we
17 are not allowed to engage in police searches and seizures in
18 foreign lands without the consent and knowledge of the foreign
19 government.

20 And that invokes not just the Morrison principle of
21 extraterritoriality, but the Charming Betsy principle. The
22 question has to be has Congress clearly authorized this
23 incursion into foreign sovereignty?

24 Not only has it not clearly authorized it, all
25 indications are that the thought never occurred to Congress.

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 THE COURT: All the indications are that Congress
2 understood how content was to be compelled from Internet
3 service providers as opposed to searches of physical locations.
4 And the structure of the statute, the language of the statute,
5 I believe we've already talked about the use of "disclosure" in
6 each of the prongs. All of it indicates Congress was talking
7 in those terms and not in physical search terms, including the
8 differences between an SCA warrant and Rule 41 warrant. An
9 officer has to be there, issued by a judge in the district in
10 which the investigation is ongoing, etc.

11 MR. ROSENKRANZ: Right. So now, your Honor, we're
12 talking about the third question, which is, did Congress
13 clearly authorize that when you used one of these warrants, it
14 was okay to use one of these warrants to search correspondence
15 that is purely overseas.

16 THE COURT: Right. Go back to my question about the
17 Bank of Nova Scotia doctrine. Don't we have to presume
18 Congress knew about that?

19 MR. ROSENKRANZ: We have to presume Congress knew the
20 backdrop law. The backdrop law was, when you went after
21 Microsoft, when the government went after Microsoft for
22 Microsoft's own documents, the backdrop law was, sure, we're a
23 witness, we have to draw our documents from wherever they are.

24 The backdrop law, and in a case from the Second
25 Circuit says this explicitly, that when you're going after

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 other people's documents that you are safeguarding for them in
2 that case, it was --

3 THE COURT: It was a search. You need a warrant.

4 MR. ROSENKRANZ: Well, you need a warrant but why?
5 Because it's a search.

6 THE COURT: Okay, we have a warrant here.

7 MR. ROSENKRANZ: We have a warrant that is perfectly
8 good when it operates within the United States. The question
9 here is --

10 THE COURT: You haven't answered why Congress should
11 not be presumed under the Bank of Nova Scotia doctrine to
12 understand that's what it meant. That the government could be
13 asking for documents resident overseas.

14 MR. ROSENKRANZ: Because, your Honor, the law here
15 long before Congress passed ECPA and actually even long before
16 this Bank of Nova Scotia -- contemporaneous with the existence
17 of the Bank of Nova Scotia principles, was there is a
18 fundamental difference between, on the one hand asking a
19 company for its own documents, which is not considered a
20 search, it is considered a witness coming forward with
21 information, versus the Second Circuit held in this case that I
22 mentioned called Guterma, versus when you are going after
23 someone else's documents, you cannot get the documents -- the
24 government cannot get the documents that are entrusted to us on
25 behalf of our clients with promise -- our customers with

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 clients of -- with promises of confidentiality.

2 THE COURT: I got it.

3 MR. ROSENKRANZ: You can't get them without a warrant.
4 Which, and the reason is, that it is a search and a seizure.

5 THE COURT: Let me ask Mr. Turner his view. Counsel
6 says that there is a difference between asking Microsoft for
7 its documents and its customers' documents. What do you say to
8 that?

9 MR. TURNER: I think there are a number of things
10 wrong with that position, your Honor. To start with, Microsoft
11 conflates the question of ownership versus control. I don't
12 know what it means to own an e-mail. But clearly, Microsoft
13 controls these e-mails. And that's the only issue under the
14 BNS doctrine, the control of the records. There is no dispute
15 that Microsoft controls these records.

16 I think what Microsoft is trying get at is they're
17 arguing these e-mails are protected by the Fourth Amendment
18 because people have a reasonable expectation of privacy.
19 That's their position. Again, we don't concede that, but even
20 assuming that it is true, they argue that that means you can't
21 get it with a subpoena. That premise is just wrong at the
22 outset.

23 There are a couple of cases I'd like to point your
24 Honor to that provide very useful examples of the use of
25 subpoenas to get private records held in the hands of a third

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 party, some of which can be protected by the Fourth Amendment
2 U.S. v. Horowitz, 482 F.2d 72, a 1973 case in the Second
3 Circuit, a Judge Friendly case. In that case it was a subpoena
4 used to obtain a defendant's file cabinet with his private
5 records that was held by his accountant.

6 The Court goes into an extended discussion of why this
7 is not a search or seizure. It is simply a subpoena and it is
8 something the government is allowed to do.

9 I think a case even more on point here is U.S. v.
10 Barr, 605 F.Supp. 114. An S.D.N.Y. case from 1985. In that
11 case, the government issued a subpoena to get the defendant's
12 mail. The mail was held by an answering service that he used
13 to get his mail for him. Very similar to what we have here.
14 What it did, it got a subpoena to get the unopened mail, and it
15 got a search warrant to open the mail and review its contents.
16 And the Court held that was valid, the subpoena and search
17 warrant combo is valid.

18 U.S. v. Triumph Capital Group, 211 F.R.D. 31. In that
19 case it was a similar combination of a subpoena and search
20 warrant that was used to get a defendant's private computer
21 that was held in a locked cabinet at his employer's premises
22 with a subpoena to the employer and a search warrant to review
23 its contents.

24 That combination of process, of a subpoena to obtain
25 custody and a search warrant to substantively review, is

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 essentially what we have in the SCA. I think Judge Francis
2 recognized it is a hybrid instrument. It is executed like a
3 subpoena, but it gives the authority to the government to
4 review the contents of potentially Fourth Amendment protected
5 material.

6 And that I think is why Microsoft's argument is so off
7 base. Because, we did not just get a subpoena, as your Honor
8 recognized, to get these records. We got a warrant.
9 Microsoft's position seems to be it is not the type of warrant
10 that's good enough. But, why not? It contains all of the
11 privacy safeguards of an ordinary warrant. And, as your Honor
12 recognized, that is sufficient to address the Fourth Amendment
13 issues.

14 It is not executed the same way as an ordinary
15 physical search warrant. But why would it be? This is a
16 completely different context. The Supreme Court has made clear
17 repeatedly the Fourth Amendment is not a rigid principle. It
18 is adaptable to different technological contexts.

19 In this context, it makes absolutely no sense to focus
20 on the physical location of data. Data can be stored at any
21 place, at any time. As we pointed out in our briefs, today
22 with cloud services, it has become increasingly common for the
23 location of data to change from day to day, or hour to hour.
24 You can have the contents of a single account distributed
25 across multiple servers.

SOUTHERN DISTRICT REPORTERS, P.C.
(212) 805-0300

E7V3MICC

1 It makes no sense for Congress to require the
2 government to go on a wild goose chase to track down the
3 physical location of data every time it wants to get an e-mail
4 account when the provider is sitting right here in this
5 country, and can get it at the touch of a button.

6 And that's why, unsurprisingly, in the SCA Congress
7 did not require the government to execute physical search
8 warrants. It created a form of compelled process. And there
9 is no reason that that form of compelled process should work
10 any differently from every other form of compulsory process
11 we're familiar with.

12 Under the BNS doctrine, with compulsory process, the
13 test is control. Not location. So it doesn't matter if
14 Microsoft stores it in this state, in Washington, or in some
15 foreign state. The point is that they have total control over
16 those records from here, can produce them from here, and that's
17 all that matters.

18 THE COURT: Mr. Rosenkranz, what do you say to
19 counsel's suggestion that it is the control that controls here?

20 MR. ROSENKRANZ: Your Honor, it is the control that
21 controls here, only if what we are talking about are our own
22 documents. And that's what BNS talks about. That's what Marc
23 Rich talks about.

24 The test is not control when the control is we
25 happen -- we have physical possession of other people's

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 documents, so the government can just subpoena it. If one of
2 our customers printed out all of his e-mails and put them in a
3 safe deposit box at Chase, Chase would have control --

4 THE COURT: What do you say to counsel's examples of
5 the combination of subpoenas and search warrants?

6 MR. ROSENKRANZ: Your Honor, the examples that he
7 gave, actually most of them I think were not cited in his
8 brief. But --

9 THE COURT: I knew that, counsel. You didn't have to
10 tell me.

11 MR. ROSENKRANZ: Okay. But the examples he gave were
12 all examples of people sharing documents with a business,
13 thereby exposing those documents to the prying eyes of a
14 third --

15 THE COURT: The accountant had them locked up in the
16 file cabinet.

17 MR. ROSENKRANZ: To be safe from other people. But
18 the accountant perused them. Microsoft does not peruse --

19 THE COURT: That wasn't necessary to the holding of
20 the case.

21 MR. ROSENKRANZ: It was indeed. It was central to the
22 holding of the case.

23 THE COURT: No, no. The fact that they were in the
24 accountant's control was central. That's why they were able to
25 be reached by the subpoena. But then when the government

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 wanted to know the content, the government had to do what the
2 government's done here, and get a neutral magistrate to find
3 probable cause.

4 MR. ROSENKRANZ: No, your Honor. The reason it was
5 okay to seize them in the first place was that they were the
6 accountant's documents -- documents that had been shared with
7 the accountant, and therefore it was permissible to tell him
8 you've got to turn them over. But here --

9 THE COURT: They were in the accountant's control.
10 That's why they could be subpoenaed.

11 MR. ROSENKRANZ: But they were shared with the
12 accountant -- shared for that --

13 THE COURT: What does that mean?

14 MR. ROSENKRANZ: Shared for his eyes to review, and
15 because of that, the expectation of privacy was diminished.

16 THE COURT: What about the mail example? That wasn't
17 shared with respect to content.

18 MR. ROSENKRANZ: So, I mean, counsel's referring to a
19 case that wasn't cited so I don't know the mail example.

20 But I can tell you that if UPS has an envelope that
21 the government wants to know the contents of, the government
22 can't just -- and it is in some other country, the government
23 can't subpoena that document and say import it to the United
24 States. If the government wants it, it's got to go through --

25 THE COURT: The banks have to do that. Banks have to
SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 bring their documents in from overseas.

2 MR. ROSENKRANZ: Their documents, yes.

3 THE COURT: Some of them are customer documents.

4 MR. ROSENKRANZ: No.

5 THE COURT: In that they relate to the account
6 transactions that the customer undertook.

7 MR. ROSENKRANZ: Sure. So if the government wants a
8 bank's record of the bank's transactions with al Qaeda, the
9 government can get them. Al Qaeda may want it to be private,
10 but al Qaeda has no expectation of privacy in the transactions
11 that it is engaging in with a bank. That's what BNS says.

12 BNS doesn't stand for the proposition, or Marc Rich
13 does not stand for the proposition that Guterma, the Second
14 Circuit case, is overruled. That as long as you have
15 possession and control of someone else's documents that you
16 have promised to keep under a lock and key, and that you've
17 promised not to access even yourself, that the government gets
18 to say because the service provider is controlling them,
19 therefore, we can get them by subpoena.

20 THE COURT: But that's not what the government is
21 saying. The government is saying, we may compel you to produce
22 those documents to us. And this is not obviously in an SCA
23 context, but the cases that counsel just gave us seem to stand
24 for the proposition that the production may be compelled by a
25 subpoena. But the government's access to the content must be

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 compelled by a warrant, which we have here.

2 MR. ROSENKRANZ: And --

3 THE COURT: Let me ask it a different way. May I
4 please.

5 MR. ROSENKRANZ: Yes, of course.

6 THE COURT: We've agreed that the Fourth Amendment
7 concerns have been addressed by the finding by the magistrate
8 judge that there is probable cause here. And I take it that
9 your objections are not that your customers' expectation of
10 privacy has been breached, because that's all taken care of
11 under the Fourth Amendment.

12 Your objections seem to be relatively formal ones
13 relating to the strict Rule 41 warrant, and not necessarily to
14 the warrant that is authorized by the SCA.

15 MR. ROSENKRANZ: So --

16 THE COURT: For example, you are worried about the
17 particularity of the description of the items to be seized.
18 You say that the location of the server should be disclosed.
19 And obviously there are technical reasons that that doesn't
20 seem to be appropriate here. This cloud stuff which you people
21 understand. You have also analogized it to breaking down a
22 door and going into a physical facility.

23 I think your arguments are related to the more normal
24 warrant for physical objects under Rule 41, rather than the
25 type of warrant that is authorized by the statute.

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 MR. ROSENKRANZ: Your Honor, I disagree. Our
2 fundamental objection here under ECPA is not at all formal.
3 Our fundamental objection here is that Congress never
4 authorized the government to issue a search warrant of any
5 sort, any document, that authorizes it to conscript us into
6 conducting a search that is in Ireland. If so, that is not at
7 all the formal objection.

8 If another country did that to us, even if we really
9 like their Fourth Amendment equivalent and we really believe
10 that they tried to protect privacy, or, if a country did that
11 without with bothering to protect privacy, either way, we would
12 be outraged at the notion that a foreign country could issue
13 something that they call a warrant and they think is really
14 special and full of protections for our citizens, and which
15 allows them to descend on Microsoft or Google and say execute
16 this, take information that is stored in the United States,
17 private correspondence of U.S. citizens, stored in the United
18 States, and search it.

19 The reason we would be outraged is because it is a
20 violation of our sovereignty. And the Morrison principles are
21 about reciprocity, about making sure that we don't violate
22 other sovereigns' sovereignty, at least not without a clear
23 Congressional command.

24 I do want to address your Honor's point about the
25 obviousness that Congress understood this. Congress back in

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 1986, most members couldn't even have conceived of the
2 possibility that Microsoft would have in one country, Ireland,
3 people's personal correspondence that could be accessed from
4 the United States.

5 THE COURT: Isn't that Congress's problem? We know
6 that technology has changed and very rapidly and in lots of
7 areas. But it is not the job of you and me standing here to
8 change the statute to comply with the technology.

9 MR. ROSENKRANZ: Agreed, your Honor, with this caveat:
10 It will be the Congress's problem to solve the ways in which
11 technology has completely bypassed the structure that Congress
12 set up.

13 When we are talking about extraterritoriality, the
14 presumption runs the other way. If we want to apply a statute
15 that purports to authorize the government to conscript
16 Microsoft into conducting searches and seizures in other
17 countries, Congress has to be really clear about that. And
18 Congress never was because it never thought of the possibility.

19 I mean, think about all of the other places where the
20 extraterritoriality principle has applied. They're all broadly
21 worded statutes that seem to apply abroad, but the Chief
22 Justice said in Bond that when Congress doesn't say it
23 explicitly, then you don't presume it. That certain things in
24 legislation, as in life, do go unsaid.

25 Congress also provides several textual hooks that

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 indicate that Congress thought it was local. So the first
2 version of ECPA incorporated Rule 41 hook, line, and sinker.
3 Rule 41 in almost every sentence says "in this district."
4 "Property in this district." It says it over and over again.
5 That changed in 2001 with a statute that was called National
6 Service of Process, that the legislative history described as a
7 statute that was designed to break down district geographic
8 boundaries and instead allow for service, "anywhere in the
9 United States."

10 It is inconceivable that the Congress that first
11 adopted the Rule 41 territorial limitations, and then expanded
12 it to the nation, without ever saying it, was actually
13 expanding the power of the government to conscript a private
14 party to conduct a search that is outside the United States.

15 THE COURT: But they had done it for years under the
16 Bank of Nova Scotia doctrine, using words just like the words
17 that were used in the statute when it was passed about
18 disclosure.

19 MR. ROSENKRANZ: Under the Bank of Nova Scotia
20 doctrine, yes. But only as to documents that are the company's
21 own records. I mean, Bank of Nova Scotia and Marc Rich did not
22 overrule the preexisting law that says that when you are
23 talking about records of other people, the government needs a
24 search warrant, which I grant you they got, but the reason they
25 got it is because this is a search and seizure. The warrant

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 protects U.S. citizens. But when you do the search and seizure
2 in another country, it is fine for us to say that those
3 people's privacy is protected. But Morrison says we ask
4 whether the other country would be offended by the extension of
5 U.S. law enforcement authority in the incursion on their
6 sovereignty. And the answer is yes, they would be. Just like
7 we would be if China or Russia or the United Arab Emirates did
8 it to us.

9 THE COURT: Thank you.

10 Mr. Turner, counsel says that essentially that you
11 should be using the MLAT procedure rather than doing this. So
12 essentially what is your response to the offense that the
13 foreign sovereign would take at this sort of disclosure?

14 MR. TURNER: Your Honor, we don't need to go to a
15 foreign country to get the records. The provider is right
16 here. The provider is 10 feet away from me. The provider has
17 control over the records. We can get them easily with domestic
18 process. In that sort of circumstance, why would we go through
19 all the extra hoops that are entailed in an MLAT? There is no
20 reason to deal with the delays and complications that can
21 certainly accompany an MLAT. I know Microsoft wants to push
22 back and make it out as if the government can easily get
23 records under an MLAT, but life is not that simple.

24 THE COURT: Of course Mr. DeMarco's affidavit is
25 nothing other than fabulous.

SOUTHERN DISTRICT REPORTERS, P.C.
(212) 805-0300

E7V3MICC

1 MR. TURNER: Even Mr. DeMarco admits that foreign law
2 enforcement authorities have their own priorities and they have
3 to fit MLATs in with those priorities. It totally depends on
4 the country you're dealing with. And of course, many countries
5 don't even have MLATs to start with, and Microsoft has never
6 answered that problem. What do we do if there is no MLAT? I
7 guess we're just out of luck and can't get these records, even
8 though there is an employee of Microsoft right here in the
9 United States who can access those records on a keyboard just
10 as if they were on a server under his desk and produce those
11 records to us.

12 It is absurd. The potentials for abuse under that
13 sort of system are enormous.

14 THE COURT: The practicalities aren't really the
15 province here either. Isn't that something for Congress?

16 MR. TURNER: I think they are, your Honor. It is
17 inconceivable that Congress would have intended these sorts of
18 practical problems to result.

19 THE COURT: Counsel says that Congress could not have
20 foreseen cloud computing, which is probably true.

21 MR. TURNER: I think, for example, the 2001 amendment
22 showed that it was already aware of the issue of data location
23 not being relevant.

24 The statute says that the government can get one of
25 these orders from a judge who either is in the same district

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 that the data is located in or that the ISP is located in or
2 that just has jurisdiction over the offense.

3 That in itself is good evidence that Congress
4 understood that the government's need for this data should not
5 be limited by sort of physical issues about where the data is
6 stored.

7 It didn't want the government to have to go to another
8 district to get the records. Why would it want to force the
9 government to go to another country to get the records when all
10 it has to do is obtain a warrant from a judge in the district
11 where the offense is being investigated? And that warrant can
12 be faxed, e-mailed, transmitted to the provider. They send
13 back the records just like with a subpoena. This is nothing
14 new. This is how the statute has worked for the past 30 years.

15 So, just going back to the MLAT point and this issue
16 about retaliation by other countries. Microsoft can't point to
17 any abuses of privacy here, and they've admitted here today
18 they don't have an issue with privacy, that the warrant takes
19 care of any privacy interests.

20 So what they do is they conjure up speculative abuses
21 by other countries. Now you are going to have other countries
22 getting warrants to search members of Congress e-mail accounts,
23 and New York Times reporter accounts. Completely speculative.

24 At the end of the day what other countries can do or
25 will do under their legal systems is not at issue. What is at

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 issue are the rules of our legal system. The test is control,
2 not location, and this has been the rule for decades. And the
3 possibility of retaliation, I suppose, has been a possibility
4 for decades.

5 You can say the same with bank records under BNS. Now
6 other countries are going to get into members of Congress bank
7 records. That possibility, to the extent it is a significant
8 possibility, is a diplomatic issue for the political branches
9 to deal with. It is not a valid basis for Microsoft to contest
10 the warrant.

11 THE COURT: What do you say to counsel's suggestion
12 about the cases you just mentioned to us, that in those cases,
13 the customer, if you will, had not entrusted the content,
14 essentially, to the holder, the possessor of the documents.

15 MR. TURNER: First of all, your Honor, I just say in
16 terms of not citing cases before, it is because Microsoft has
17 raised this argument anew in its reply brief. Their position
18 has been in search of a theory throughout and the theory keeps
19 changing.

20 As to your Honor's question, it is wrong. For
21 example, just another case, U.S. v. Re, 313 F.Supp. 442.
22 Another accountant case where it was the correspondence and
23 other papers turned over to the accountant. The Court found,
24 quote, that these papers were clearly the property of the
25 clients. Nonetheless, it found it was proper to get them with

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 a subpoena.

2 Again, the issue is not some sense of ownership. The
3 only issue is control. If somebody leaves a murder weapon
4 behind in somebody else's home, okay, it doesn't matter that
5 the knife was owned by the other person. We can issue a
6 subpoena to the third party and get it from the third party.
7 So, there is no authority in the law for Microsoft's position.
8 They're just asserting it without any support.

9 THE COURT: All right. Counsel.

10 MR. ROSENKRANZ: Yes, your Honor. So first on the
11 last point Mr. Turner raised. Our theory has been consistent.
12 We've been saying it all along. And if the Court's decision
13 turns on this distinction, as it ought to turn on this
14 distinction between subpoenaing our own business records versus
15 other people's records, I just ask the Court for an opportunity
16 to brief this issue as to those other cases, because I
17 guarantee you --

18 THE COURT: I don't recall seeing anything about that
19 in Magistrate Judge Francis' opinion. So I confess I didn't go
20 back and read your briefs.

21 MR. ROSENKRANZ: Your Honor, our position all along
22 has been exactly same. The reason that the government cannot
23 conscript us to do this in a foreign country is because this is
24 a search, and we distinguish the BNS cases on exactly the
25 grounds we've been distinguishing them. So, it is in your

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 discretion, your Honor, to grant it or not but the --

2 THE COURT: Let me just ask you again. Was that
3 argued below?

4 MR. ROSENKRANZ: That there is a big difference
5 between a BNS subpoena --

6 THE COURT: I'm looking through the opinion, I don't
7 see anything.

8 MR. ROSENKRANZ: We definitely argued, we definitely
9 distinguished BNS on exactly this ground. On the ground that
10 BNS does not justify what we would always call searches of
11 other people's property. It justifies only subpoenas for our
12 own records.

13 By the way, I would add the government focused on this
14 business record concept, the government's concept that the
15 reason this is different is because these are our business
16 records actually for the first time in this court. But I do
17 want to address the substance --

18 THE COURT: Let me ask the government to comment on
19 that. Is that your recollection of what went on before Judge
20 Francis?

21 MR. TURNER: This argument was not raised below, your
22 Honor.

23 THE COURT: Go ahead.

24 MR. ROSENKRANZ: So Mr. Turner makes the observation
25 that Congress wanted to erase the difficulties, the

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 inefficiencies that occurred district to district, so why would
2 it not have wanted to erase the inefficiencies that occur when
3 you go from one country to the other. And the answer to that
4 question is sovereignty. When you cross the borders into
5 another country, the Supreme Court has told us that you have to
6 focus very carefully on whether what you are doing is invading
7 foreign sovereignty, supplanting foreign law for U.S. law. And
8 when you're talking about conducting a search and a seizure in
9 a foreign country, those sovereignty interests are at their
10 foremost.

11 So, if this were a case of physical correspondence,
12 there is no question that the government would have to use the
13 MLAT or some other bilateral negotiation with another
14 government which exists even in non-MLAT countries. It would
15 have to go through the much more --

16 THE COURT: It isn't. Congress knew it wasn't.

17 MR. ROSENKRANZ: It isn't and Congress made it a point
18 to say that what we are trying to do with this statute called
19 the Electronic Communications Privacy Act, is to apply the same
20 principles to physical letters and private papers, to apply
21 those principles to digital correspondence.

22 So, Congress over and over again kept trying to make
23 the same principles apply. And so, for example, if Chase had
24 documents in a safe deposit box in a branch in Ireland.

25 THE COURT: We've done this. Right?

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 MR. ROSENKRANZ: Well, but when we're talking about
2 international principles we have, they couldn't just say,
3 Chase, go and search that safe deposit box in Ireland, take a
4 photograph --

5 THE COURT: But they could make them bring them back
6 and then they would get a warrant for contents. Right?

7 MR. ROSENKRANZ: No. And that is the crux, truly the
8 nub of this disagreement is over exactly how far BNS extends.
9 There are no cases that say that BNS -- it would be a startling
10 proposition to Congress and our international partners to say
11 that BNS extends to require a business or an individual to go
12 and conduct a search and seizure abroad, and bring that
13 information into the United States.

14 THE COURT: The difference, isn't it, that Congress
15 well knew that Bank of Nova Scotia required U.S. companies to
16 retrieve records in their control, even if located abroad, and
17 to produce them here. That's the difference.

18 MR. ROSENKRANZ: I understand the point, your Honor.
19 And that's one of the reasons I think it might be useful to do
20 another brief. That is not the line the cases draw. The line
21 the cases draw is about a company being required by subpoena to
22 produce its own records, or, I will grant to Mr. Turner, other
23 people's records that have been shared with that company and
24 that therefore have already been exposed. Bring those.

25 But never there, is no case that says that Congress --

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 that the subpoena power extends to being able to require a
2 business to produce by subpoena private correspondence and
3 bring it into this country. That is, the location of those
4 documents, searching for them, is a search. The taking
5 possession of other people's correspondence is a seizure. The
6 importation over to the United States is an additional element
7 of the seizure.

8 So there are multiple events that each involve an
9 incursion into privacy, and most importantly, an invasion of
10 the sovereign's prerogatives to be the one that decides in a
11 multilateral conversation or bilateral conversation, whether to
12 assist U.S. law enforcement. And the MLAT process does work.
13 Is it clunkier --

14 THE COURT: That it works is of no moment. The
15 government says it's clunky. Maybe it is, maybe it isn't. Who
16 cares.

17 MR. ROSENKRANZ: Agreed.

18 THE COURT: The question is what does the statute
19 authorize, right?

20 MR. ROSENKRANZ: Well, the question under Morrison is
21 what does the statute clearly authorize. If this is in fact a
22 search and seizure in another country, which we strongly
23 believe it is, and so if it is in fact a search and seizure in
24 another country, then that is an extension of law enforcement
25 authority into that other country. And when you do that, you

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 need the consent and knowledge of that other country.

2 THE COURT: Why isn't the disclosure of bank records
3 under Bank of Nova Scotia just as offensive to the foreign
4 sovereign?

5 MR. ROSENKRANZ: Well, it is -- I would say less
6 offensive to the foreign sovereign, because there is a big
7 difference from the perspective of the foreign sovereign
8 between on the one hand the police requiring -- so foreign
9 police -- and by the way, it could be a state or local
10 government as well requiring this.

11 So requiring a search and seizure on foreign lands
12 within their own sovereign territory, big difference between
13 that on the one hand, and on the other hand a principle that
14 sovereigns all accept that when you are asking someone for
15 their own documents, or documents in which there is no
16 expectation of privacy, that is tantamount to treating that
17 person as a witness, a witness of things to which they are
18 knowledgeable, about which they are knowledgeable. And that
19 occurs in the United States. In other words --

20 THE COURT: I don't get it. My question was why don't
21 the foreign sovereigns consider the production of bank records
22 by a bank in the U.S., records resident overseas, why does the
23 foreign sovereign not become just as offended at that which has
24 been going on for decades, as with the situation we have here
25 today?

SOUTHERN DISTRICT REPORTERS, P.C.
(212) 805-0300

E7V3MICC

1 MR. ROSENKRANZ: Well, they might.

2 THE COURT: Then what is the difference? Congress
3 knew that.

4 MR. ROSENKRANZ: BNS has never been analyzed through
5 the lens of Morrison. But my more direct -- so in other words,
6 we don't know what Morrison would have to say about that
7 extension of authority. There is a big difference to a
8 sovereign, I think there would be a big difference to us,
9 between a sovereign that is requiring a third party to execute
10 a search and a seizure in the United States versus going to
11 someone who is a subject of their own country and saying these
12 are your documents, you know about them, you own them, you are
13 a witness, and we want you to bring those documents.

14 THE COURT: The only difference is that you're calling
15 it search and seizure, and under Bank of Nova Scotia it is mere
16 disclosure. Disclosure by Microsoft of its documents.
17 Documents that have been put on its system voluntarily.

18 MR. ROSENKRANZ: That is a key difference. And not --

19 THE COURT: Is it not just a label?

20 MR. ROSENKRANZ: No, your Honor. That's what I was
21 going to say. It is a difference that, yes, I'm calling it a
22 search and seizure because it is a search and seizure.

23 THE COURT: Even if it is, haven't we already agreed
24 the Fourth Amendment privacy concerns have been addressed by
25 the neutral magistrate?

SOUTHERN DISTRICT REPORTERS, P.C.
(212) 805-0300

E7V3MICC

1 MR. ROSENKRANZ: Our U.S. Fourth Amendment privacy
2 concerns have been addressed. What has not been addressed is
3 the sovereign interests of another country that does not want
4 the U.S. to conscript other parties to conduct searches and
5 seizures of correspondence stored in their sovereign territory.

6 THE COURT: We're speculating, and we're speculating
7 against the background of banks having been doing this for
8 decades. No squawking from anybody about it.

9 MR. ROSENKRANZ: No, your Honor, banks have not been
10 doing this for decades.

11 THE COURT: Bank of Nova Scotia was a mid '80s case,
12 wasn't it?

13 MR. ROSENKRANZ: Banks have been producing their own
14 records, records of transactions to which they were a party for
15 decades. When a bank produces its own records, it is just
16 fundamentally different from a bank going into a safe deposit
17 box or Microsoft going into its digital safe deposit box, and
18 revealing someone else's private information.

19 A foreign country and the U.S. certainly would view
20 the search and seizure that occurs there to be far more an
21 invasion of sovereign rights than simply asking someone who is
22 a witness to gather his own documents to which he is a witness.

23 THE COURT: Mr. Turner, what do you say?

24 MR. TURNER: It might be useful to look at the
25 Restatement Third for Foreign Relations Law which we cited in

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 our brief. That basically reflects the BNS principle. It
2 states: A court or agency in the United States may order a
3 person subject to its jurisdiction to produce documents,
4 objects, or other information relevant to an action or
5 investigation, even if the information or the person in
6 possession of the information is outside the United States.

7 There is no issue of the documents, do they belong to
8 the person or not. It is just whether they're relevant.
9 That's what the subpoena is determined by.

10 Under BNS the issue is not ownership. It is control.

11 The issue is whether Microsoft, which is subject to
12 this court's personal jurisdiction, has evidence that the
13 federal government needs, legitimately, to investigate a
14 violation of U.S. law. They do. They have control over that
15 evidence. They can produce it. That's what matters under the
16 BNS doctrine.

17 All this other stuff Microsoft is just an invention.
18 What drives BNS is the nature of compulsory process. How does
19 compulsory process work? It works on a person. And so the
20 issue is does that person, is he subject to the court's
21 personal jurisdiction, and does he have control over the
22 evidence the government needs. The answer here to both is yes.
23 That's all that matters.

24 So, again, these issues of "they aren't our records,
25 under our terms of service, etc., etc.," it doesn't matter.

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 All that matters is Microsoft controls the records. And I
2 think the cases we cited are actually perfectly on point.

3 I know Microsoft several times cited to the case they
4 put in their reply brief, Guterma. Very different
5 circumstances. That was a safe that only a defendant had
6 access to. Only he had the combination. The third party
7 didn't have the combination. What the Court emphasized was
8 there was no control by the third party. The third party
9 didn't have control to produce the records in the safe. And to
10 force the defendant to produce them would raise Fifth Amendment
11 privileges. Nothing analogous here. Microsoft has the
12 combination. They can turn over the contents of these records
13 to the government.

14 So the one cite that they push on the Court really is
15 very clearly distinguishable.

16 THE COURT: Mr. Rosenkranz, doesn't the restatement
17 situation about requiring production of documents really kill
18 the comity argument?

19 MR. ROSENKRANZ: No. The restatement recognizes
20 exactly the distinction I am drawing. On the one hand, there
21 is the portion of the restatement that addresses the subpoena
22 power as to one's own documents. On the other hand,
23 restatement Section 432(2), and I'll quote: A state's law
24 enforcement officers may exercise their functions in the
25 territory of another state only with the consent of the other

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 state.

2 And that's why a search and seizure of other people's
3 information that is protected and private is just different
4 from a bank producing its own records to --

5 THE COURT: What do you say to the issue that control
6 is the question here? It is the control. Your company has
7 control.

8 MR. ROSENKRANZ: We have --

9 THE COURT: You are being required to produce.

10 MR. ROSENKRANZ: And again, I will say, just because a
11 custodian has control and possession of someone else's private
12 information, does not mean the government can get it by
13 subpoena. I mean when --

14 THE COURT: Nobody disagrees with that. This is not a
15 subpoena. This is a warrant.

16 MR. ROSENKRANZ: But the government is saying this is
17 simply us producing our own business records, and it isn't a
18 search and a seizure. And that distinction that I'm drawing is
19 critical to recognizing what this act is. The act in a foreign
20 land. We are talking about --

21 THE COURT: It is an act by a Microsoft employee
22 sitting in California bringing that information back.

23 MR. ROSENKRANZ: It is --

24 THE COURT: Because Microsoft has control of it.

25 MR. ROSENKRANZ: We, yes, so I grant you, we have

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 control. But we have control of other people's information
2 that is imbued with an expectation of privacy that --

3 THE COURT: Which is taken care of by the magistrate
4 judge's warrant.

5 MR. ROSENKRANZ: Agreed, for a search in the United
6 States. If this is in fact a search in another country, that
7 country wants to --

8 THE COURT: You just said it is a search in the United
9 States.

10 MR. ROSENKRANZ: No, I did not. If I did, I'm
11 mistaken. I've been saying all along this is a search in
12 Ireland. What is going on is a person sitting in the United
13 States is locating these documents which sit in Ireland --

14 THE COURT: Over which the company has control.

15 MR. ROSENKRANZ: Agreed. So the company has control
16 of these documents, just like a bank has control of records in
17 a safe deposit box. Just like my firm entrusts documents to
18 Iron Mountain, but not to turn over to the government just
19 because the government subpoenas them. But again, that first
20 question that I posed --

21 THE COURT: I'm sorry. Turns over documents to Iron
22 Mountain. Why can't the government subpoena Iron Mountain to
23 get those documents? Iron Mountains has control over them.

24 MR. ROSENKRANZ: Because that is a seizure.

25 THE COURT: You can subpoena them for the documents.

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 MR. ROSENKRANZ: No, never. No. I don't think that
2 there is any case that says that when the government wants to
3 reach out and grab some documents, it is allowed to do that by
4 subpoena.

5 What the government is doing when it takes those
6 documents is seizing the documents. And the Second Circuit
7 just a couple of weeks ago decided a case that was actually
8 about that question. That case is Ganas. In Ganas it
9 actually involved digital information. In Ganas what happened
10 was the government put a freeze on, sort of a preservation of
11 someone else's e-mail account.

12 That was a seizure because the government was at that
13 point infringing on the individual's exclusive possession. The
14 moment the government takes possession of someone else's
15 effects, even if it is not perusing through them, that's a
16 seizure. When it imports them into the United States, it is
17 exercising even more of this seizure conduct.

18 So as I was saying before, the copying occurs in
19 Ireland. The documents are in Ireland. The copying occurs in
20 Ireland. They are then imported into the United States. So
21 Supreme Court law says that just because you can do something
22 remotely doesn't mean that it is happening where you're
23 sitting. In Kyllo, for example, when a government agent is
24 across the street directing a heat sensor at the home, the
25 search is in the home. Not where the agent is standing. If

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 the government --

2 THE COURT: The agent at that point doesn't have
3 control over what's in the home. The difference here is that
4 Microsoft has control over the documents.

5 MR. ROSENKRANZ: So, a landlord has control over the
6 premises that he promises to keep private. That doesn't mean
7 that when the government conscripts him to open the door and
8 show them around, or to go in himself as --

9 THE COURT: We've already agreed, I thought, that the
10 physical construct is not applicable here to this type of
11 information. It certainly seems that Congress understood that.
12 Especially with the changes in jurisdiction, the fact that the
13 officer did not have to be present, and the like.

14 MR. ROSENKRANZ: So I've heard your Honor say it, but
15 I haven't agreed with it. What Congress was trying to do was
16 apply the same principles that apply to letters and private
17 papers to --

18 THE COURT: The same privacy principles, but not
19 necessarily to some of the other Rule 41 requirements such as a
20 physical description of where on the planet something is.

21 Why is it sufficient in wiretaps for the government to
22 designate the telephone number but not to designate where that
23 information might be resident?

24 MR. ROSENKRANZ: Your Honor, again, our particularity
25 argument is a separate argument. What we've been talking about

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 all morning is whether Congress has clearly indicated an
2 intention to allow the government to require Microsoft to
3 conduct the search outside the United States.

4 THE COURT: Yes. But my point is Congress clearly
5 understood that these subpoenas, warrants, court orders that
6 require ISPs to produce information, are of a different breed
7 from subpoenas or warrants that relate to physical objects.
8 That's my point.

9 MR. ROSENKRANZ: Yes, your Honor. Understood. So
10 Congress -- yes. Congress did understand that.

11 The question before the Court is whether Congress
12 clearly expressed an intention to allow what we clearly know
13 Congress wanted to happen in the United States. To allow that
14 to happen in a foreign government.

15 THE COURT: I'm with you. That's a question.

16 MR. ROSENKRANZ: Right. And that question can't be
17 answered by saying Congress knew the data was different or that
18 digital correspondence was different. The only way to answer
19 that question, the only way for Congress to satisfy that
20 standard, is to say something in the statute that says, okay,
21 this is not just for the United States, where Congress was
22 thinking only about data that was in the United States. It is
23 also for what happens in other countries.

24 There is no such indication, the indications are all
25 to the contrary, including territorial limits within Rule 41.

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 THE COURT: All right. Mr. Turner, does Congress have
2 to have said explicitly "information may be compelled from
3 companies in this country who have control over that
4 information abroad"?

5 MR. TURNER: No, your Honor.

6 THE COURT: Why not?

7 MR. TURNER: For one thing, Microsoft is just wrong at
8 the outset. We're not talking about an extraterritorial
9 application of law here. The law is being applied here. The
10 legal duty is applied here. Microsoft must produce the records
11 here. If it doesn't, it is subject to sanctions here.

12 The rule is not -- the presumption is not, that
13 Congress doesn't want a law to have any extraterritorial
14 effects whatsoever. The issue is whether Congress is applying
15 law to acts occurring outside the United States or acts that
16 don't have any connection to the United States.

17 That's not what is going on here. And the whole
18 argument also is just precluded by the BNS doctrine. You can
19 say the same thing about BNS subpoenas. That the rules
20 authorizing the issuance of subpoenas don't expressly say this
21 can be used to obtain records that are held abroad.

22 Microsoft's notion as we pointed out in our brief
23 would imply that the tax laws would be extraterritorial if they
24 require somebody to move their money from a foreign bank
25 account to a bank account here in order to pay their tax bill.

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 That's not the sort of extraterritorial application that the
2 presumption against extraterritoriality concerns.

3 Just at the outset, in terms of some sort of clear
4 statement rule, it doesn't apply here because we're not talking
5 about extraterritorial of law in the first instance.

6 You also have the fact that Congress is presumed to
7 know the law, as your Honor pointed out. And the BNS doctrine
8 has been around for a long time, well before the '80s. The BNS
9 case is from the '80s. But before that there are Supreme Court
10 cases on point. Societe Internationale v. Rogers I think is
11 from the '50s or '60s from the Supreme Court. The doctrine
12 starts as far back as that.

13 So, no clear statement required in the first instance.
14 And in any event, I think Congress' intent to incorporate that
15 existing law can be assumed based on its assumed familiarity
16 with background and legal principles.

17 MR. ROSENKRANZ: Your Honor, if I may, just a couple
18 of things. First a housekeeping thing. On the BNS doctrine,
19 we did brief it before the magistrate judge at pages seven to
20 eight of our reply brief.

21 THE COURT: I'm not talking about the BNS doctrine
22 when I asked you that question of whether it was argued below.
23 I was talking about your suggestion, your argument here that
24 the documents were not Microsoft's documents, but rather were
25 the customer's documents and thus it made a big difference.

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 MR. ROSENKRANZ: We will go back and check, but I'm
2 pretty confident that we did make that argument.

3 THE COURT: Mr. Turner, what do you say to that?

4 MR. TURNER: That is not correct. That argument was
5 not made below.

6 THE COURT: Whatever it is, you people will figure it
7 out.

8 MR. ROSENKRANZ: So on the question of where does this
9 search occur, Gorshkov is about digital information as well.
10 The government in that case took the position, which is right,
11 that when you are sitting at a terminal in the United States,
12 and searching a server that is sitting in Russia, that search
13 occurs in Russia. And the government has to take that
14 position, because it wants the ability to perform those
15 searches without a warrant.

16 THE COURT: That's not the position here. There is a
17 warrant, as we've discussed 40 times.

18 MR. ROSENKRANZ: Yes. I grant that there is a
19 warrant. That protects U.S. privacy interests but it
20 doesn't -- it is not a document that is recognized by foreign
21 countries who are worried about searches and seizures of
22 information that people store on their own lands. We would not
23 accept, if China served --

24 THE COURT: I know. I know.

25 MR. ROSENKRANZ: Okay. A second point on that as to
SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 the difference between digital data and -- excuse me.

2 The difference between Microsoft doing it versus the
3 government's doing it. ECPA I believe authorizes the
4 government to do it in our place. To sit at the point of where
5 the Microsoft employee is sitting. 2703(g) says that the
6 government official need not be there. I think the government
7 would agree that if a DEA agent is sitting at that terminal,
8 then it is the government doing the search. And the government
9 can't just substitute a private party under legal compulsion to
10 perform that search. The government doesn't get to say just
11 because we got someone else to do it, we're sort of scot-free
12 and have no responsibility for the search.

13 And then the final point on the government's argument
14 that it is just speculation as to whether foreign governments
15 will be up in arms about the incursion on their sovereignty.
16 It isn't speculation. The European Commissioner of Justice,
17 Reding, we submitted a letter from her expressing outrage at
18 the incursion on their sovereignty.

19 And I would, in terms of speculation, I would just
20 punctuate the point by mentioning to the Court that just this
21 week, China served on Microsoft -- excuse me. China appeared
22 in Microsoft's offices in four locations in China to conduct a
23 law enforcement search and seizure. They took our servers,
24 okay, that's within their domain. They then demanded a
25 password to seek e-mail information in the United States. Now,

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 the e-mail information was information of our own employees.
2 But the government's point that there is no difference between
3 correspondence that is simply our own documents versus
4 correspondence that we are protecting on behalf of others means
5 that tomorrow, China can do the same thing, and seize e-mail
6 content from a server in China in the United States, and the
7 government is saying -- we know they would be outraged if China
8 did it. The government's position means when China or Russia
9 or one of these other countries does that next week, we have no
10 claim that this infringes on our sovereignty. We have no
11 argument that this was a search and seizure that occurs here.
12 Because everything occurred in China and they just got a
13 Microsoft employee in China to search its own business records
14 over which it had possession and control.

15 That is a very, very dangerous principle that the
16 government is articulating. It is dangerous -- other countries
17 view it as dangerous when they're talking about the United
18 States. We view it as dangerous for sure when we're talking
19 about our countries.

20 And an opinion from this Court saying that what the
21 government did here is just fine because it is not an incursion
22 on foreign sovereignty will be used by the countries that do
23 this as Exhibit A that the government cannot possibly complain
24 because one of the most respected judges in the United States
25 says it is perfectly fine.

SOUTHERN DISTRICT REPORTERS, P.C.
(212) 805-0300

E7V3MICC

1 THE COURT: Oh, counsel, you say that to all the
2 girls.

3 MR. ROSENKRANZ: I meant to say "the most respected."

4 THE COURT: Mr. Turner, what do you say to that? It's
5 pretty scary.

6 MR. TURNER: First of all, your Honor, it sounds like
7 a diplomatic issue to me. Again, it is not a basis for
8 resisting a Congressionally authorized warrant directing
9 Microsoft here. Other countries are going to do what other
10 countries are going to do. We already have, like the
11 government pointed to before, the Restatement, which already
12 announces that this is recognized law in the U.S. That we can
13 issue compulsory process to persons, companies here, and if
14 they have the responsive records abroad, they have to produce
15 them. So that's already embedded in the law. Again, it is
16 nothing new. As I pointed before, the possibility of
17 retaliation of some sort has been latent in that as well.

18 But again, to the extent that there are concerns about
19 what other countries do in this area, obviously this is an
20 emerging area of the law. That is something for the Executive
21 to pursue through political and diplomatic channels. But it is
22 not a valid basis for Microsoft to ask this Court to ignore the
23 plain terms of the statute here, which say that we can get an
24 order and a warrant requiring them to disclose records based on
25 probable cause. That's what we did. That's what any civil

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 libertarian would want to us do when the government needs
2 communications like this.

3 We did it. The statute says the next step is
4 Microsoft has to produce the records.

5 Microsoft has raised the issue of what about Ireland's
6 concern here. First of all, I would just point out we are not
7 talking necessarily about an Irish user. We are talking about
8 data on an Irish server. The location of data is by no means a
9 reliable proxy for the location of the user.

10 Under BNS, the only time you get into that kind of
11 analysis, what about Ireland's concerns, is if there is a
12 genuine conflict of law between the two countries. And here
13 Microsoft has had every opportunity to assert that here, and
14 has not been able to point to any specific provision of Irish
15 law that in any way forbids it from handing the data over.

16 So, the sort of interest that Microsoft points to, the
17 Court could in some other case, perhaps, take into account.
18 But there is no need to do so here. Because there is no
19 genuine conflict of law.

20 THE COURT: Thank you. Mr. Rosenkranz, did you want
21 to end with anything?

22 MR. ROSENKRANZ: Yes. Please, your Honor. So, first,
23 this is a diplomatic problem, to be sure. It is especially a
24 diplomatic problem when you take the Executive out of the
25 picture, and posit that Congress authorized a sheriff's deputy

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 in Dublin, Mississippi, to seek a search that occurs in Dublin,
2 Ireland. It isn't just a diplomatic problem. What Morrison
3 stands for is the proposition that when the U.S. is extending
4 its authority, and here in particular, its police power into
5 other states, it is a Congressional problem. It is a problem
6 that if you are using a Congressional statute to authorize that
7 incursion, you've got to look to Congress and ask did Congress
8 clearly say that this is what should happen.

9 Congress not only didn't it clearly say, as I've said
10 several times, it said the opposite. Congress does need to
11 step in to this question. The explosion of digital media has
12 been something that Congress could never have contemplated.
13 When Congress steps into it, it will have any number of
14 options. It can draw the line that the government says should
15 be drawn. It can draw the line that we say should be drawn.
16 It could say perhaps we allow the extraterritorial search, but
17 only for U.S. citizens and not for others. Perhaps only for
18 data -- perhaps only for countries that don't part --

19 THE COURT: I got it. Isn't the point, and following
20 on your point, whether it is an incursion on the sovereignty of
21 a foreign nation or not, the concerns of foreign nations and
22 the specter of what China might do is of no influence in
23 deciding the question you told me we had to decide, which is
24 whether Congress intended, etc., etc., right?

25 MR. ROSENKRANZ: No, your Honor.

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 THE COURT: You're just telling me practical
2 considerations.

3 MR. ROSENKRANZ: No, your Honor. The way Morrison
4 describes the inquiry, Morrison asks what is this conduct, is
5 this conduct an intrusion on foreign sovereignty.

6 All of the evidence and all of the parade of horrors
7 that are very real, are examples of situations that could arise
8 that could lead Congress -- that the Court had in mind when it
9 adopted this principle. That you do not allow an incursion
10 into foreign sovereignty without a clear statement from
11 Congress. So the Congress is the one weighing these parades of
12 horrors against law enforcement, for example.

13 THE COURT: Right. But the parade of horrors has no
14 impact here. I'm trying to read what Congress had in mind.
15 That I might think it is horrible and that I might have made
16 the balance come out differently, is of no moment. It is what
17 Congress intended, right?

18 MR. ROSENKRANZ: It is what Congress clearly intended.
19 But your Honor's question was, what is the relevance of the
20 possibility that foreign countries will be upset.

21 THE COURT: On me, nothing. Congress was supposed to
22 have weighed all of that in deciding what the statute should
23 say.

24 MR. ROSENKRANZ: Agreed. But it was relevant to the
25 Supreme Court in Morrison and Bond and in Kiobel to ask the

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 question if we allow this, what would the response of foreign
2 sovereigns be? If the Supreme Court thinks the response of
3 foreign sovereigns would be to shrug because it actually isn't
4 much of an infringement on foreign sovereignty, it is
5 incidental, a word the Supreme Court has used before, then it
6 would conclude that there is no extraterritorial effect.

7 But as long as one can posit -- and actually we
8 presented proof of the proposition -- that foreign sovereigns
9 will be deeply offended by this action, just as we would be if
10 they did it to us, the rule requiring the presumption of
11 extraterritoriality is in play, and you have to ask the
12 question did Congress clearly indicate --

13 THE COURT: That's the question.

14 MR. ROSENKRANZ: Agreed.

15 THE COURT: Okay. Did you want to end with anything,
16 Mr. Turner?

17 MR. TURNER: Just a few thoughts, your Honor. The
18 rule is not that the possibility that other nations might take
19 offense triggers some presumption against extraterritoriality.
20 That's not what the rule is.

21 If you look at Morrison, what was at issue was the
22 Securities and Exchange Act and whether it regulated frauds
23 concerning foreign exchanges. And the Court said no, no, no,
24 Congress's focus was on domestic exchanges, domestic stock
25 exchanges. No reason to think they wanted to get in the

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 business of regulating foreign exchanges.

2 We have nothing analogous to that circumstance here.
3 Here we're talking about domestic law enforcement. We're
4 talking about enabling law enforcement to obtain records from
5 U.S. providers relevant to U.S. investigations. That's
6 domestic. That is a domestic Congressional focus of concern.

7 So there is no issue of extending a statute here to
8 some other foreign-based focus of concern that didn't line up
9 with Congress's intention.

10 So, basically, Microsoft's position seems to come down
11 to Morrison, the idea that Morrison reversed or overruled the
12 BNS doctrine. It didn't. There is no law holding that. It
13 certainly is not for this Court to decide that anyway, since it
14 is a valid Second Circuit holding.

15 But the bottom line is, this is an enforcement of a
16 domestic law enforcement statute. It is a domestic law
17 enforcement investigation. And these principles of
18 extraterritoriality Microsoft is trying to draw in really are
19 just out of place here.

20 THE COURT: Thank you. Do any of the amici wish to
21 add anything different? Not repeat the topics my friends here
22 have talked about.

23 Yes, counsel.

24 MR. VATIS: Michael Vatis for Verizon. As your Honor
25 pointed out, the key question here is what did Congress intend

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 with regard to the ability of the government to get information
2 located abroad.

3 THE COURT: Yes.

4 MR. VATIS: We have to start with the presumption of
5 extraterritoriality. We cannot assume, as the government does,
6 that Congress intended that the statute apply
7 extraterritorially. Morrison requires that the Court presume
8 the opposite. That Congress did not intend to authorize
9 searches abroad.

10 Your Honor's pointed out that we should presume that
11 Congress was aware of the BNS line of cases. That may be true.
12 I am not sure that overcomes the presumption of
13 extraterritoriality. I think if we're dealing with a subpoena
14 for Microsoft's own business records, that would be a close
15 question. But here, we also have to understand that Congress
16 was aware of Rule 41. And its explicit limitations on the
17 territoriality of search warrants, that they're limited to
18 application within the United States. That's a very big
19 difference.

20 In ECPA, Congress decided to require a search warrant
21 for e-mails, for content of communications. So the relevant
22 thing there is Rule 41. That's what Congress had in mind. Not
23 the BNS line of cases.

24 THE COURT: Would you do that again? That last
25 sentence, that's where I missed you. You told me that we have

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 to presume that Congress was aware of the BNS doctrine.

2 MR. VATIS: Congress may have been aware.

3 THE COURT: We must presume Congress was, right?

4 MR. VATIS: We can presume that. But we also must
5 presume that Congress was aware of Rule 41, and its explicit
6 limitations on the service of search warrants and their
7 application to property in the United States. Rule 41 is the
8 model that Congress decided to go with when it comes to
9 e-mails. So we have to presume that Congress intended the
10 territorial limitations of Rule 41 to apply to search warrants
11 issued under the SCA.

12 There is certainly no indication in the statute or in
13 the legislative history that Congress intended otherwise.

14 When you bring in, again, the presumption against
15 extraterritoriality, I think the answer is clear. There is no
16 indication whatsoever.

17 There are policy issues here. Very significant policy
18 issues. There is the interest of law enforcement in getting
19 data without having to go through an MLAT. There is also the
20 interest of companies in not losing billions of dollars in
21 foreign business because of the impact overseas, because of
22 foreign customers wanting to go to a German provider instead of
23 an American one. These are precisely the sorts of policy
24 considerations that need to be left to Congress. Not to a
25 prosecutor in New York, not to a Court. And that's what the

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 presumption of extraterritoriality is all about. That's what
2 the Charming Betsy doctrine is all about.

3 At rock bottom, these are separation of powers issues.
4 Who is to decide which policy consideration is more --

5 THE COURT: I don't disagree with you. I think we all
6 agree about that. I think my last question to or next-to-last
7 question to counsel was whether or not these practical
8 considerations are something to make a difference in my
9 determination. Or rather, wasn't it not something that
10 Congress was supposed to consider when deciding on the statute?
11 I think we all agree on that.

12 MR. VATIS: We all agree.

13 THE COURT: The question is more what did Congress
14 intend.

15 MR. VATIS: It did not consider these issues at all in
16 1986 because it simply wasn't an issue. Congress could well
17 decide now that it needs to address this issue. It could well
18 decide that the interest in law enforcement and its ability to
19 get information abroad is more important than the effect on
20 providers or the effect on diplomatic relations. That is an
21 issue for Congress. But it would have to do that through an
22 amendment to ECPA. Because it never expressed such an
23 intention in 1986, because it never considered the question.

24 THE COURT: Counsel and I have beaten this horse dead,
25 I think, but the language used in the SCA is language which

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 mirrors the subpoenaing of information from banks and the like.
2 And thus, we have to assume that that's what Congress had in
3 mind, and it tweaked some of the requirements of Rule 41.

4 MR. VATIS: The only requirement it tweaked was who
5 would do the searching and the seizing in the first instance.

6 THE COURT: And the jurisdiction of the judge issuing.

7 MR. VATIS: Later on they did do that as well. But
8 they never indicated an intention or even an understanding that
9 the government might seek to get information stored abroad.

10 The reason it used the disclosure language in
11 significant part was to ease the burden on the providers.
12 Because there was no reason to have the government go in and do
13 a search on the provider's servers. It wasn't because they
14 thought there was any less infringement on privacy or that
15 somehow electronic information should be treated differently
16 from physical information. It was --

17 THE COURT: I think I have to disagree with you on
18 that, counsel. Even back in the dim ages of the '80s when we
19 were talking about electronic information, Congress certainly
20 had to understand that it was different from physical
21 information, and had to have been aware of the use of subpoenas
22 to require U.S. companies to retrieve data it had, they had
23 control over overseas, and produce it to the government in the
24 U.S.

25 MR. VATIS: The companies' own records. And the cases
SOUTHERN DISTRICT REPORTERS, P.C.
(212) 805-0300

E7V3MICC

1 are very much focused exclusively on the companies' own
2 records, not the property of a third party. Again, Congress
3 decided to treat e-mails, the content of electronic
4 communications, differently from a company's own records about
5 its subscribers. That's why it required a search warrant.

6 The attorney general earlier this year and a deputy
7 assistant attorney general have both conceded that a search
8 warrant is required for the reason that there is a legitimate
9 expectation of privacy.

10 THE COURT: We all agree to that. We all agree.
11 Counsel agreed with me that Fourth Amendment concerns are met
12 here.

13 MR. VATIS: Correct, your Honor. But the import of
14 the government's position in this case, that we need to just
15 look at BNS, the import of that is that there really is no
16 difference between Microsoft's own records about its billing
17 practices or what have you, and the e-mails of its subscribers.
18 That's the end result of the government's argument.

19 THE COURT: Anybody else?

20 Yes, sir.

21 MR. ZWILLINGER: Marc Zwillinger for Apple and Cisco.

22 When we're thinking of what Congress was aware of when
23 it passed ECPA, we also have to think about Congress being
24 aware of the ability of the U.S. government to use the MLAT
25 process to get evidence in foreign countries. I think we've

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 had a complicated argument, but we recommend a simple rule.
2 When the U.S. government wants to get information about a
3 foreign user, in a foreign country, stored in a foreign data
4 center, by a foreign subsidiary, the fact that the U.S. parent
5 company can technically access the data and bring it back is
6 not enough. That is, Congress has to speak more clearly that
7 ECPA is designed to operate in an extraterritorial way. And if
8 the BNS principles were baked into ECPA in 1986, Congress
9 wouldn't have needed to make the tweaks it did in 2001.
10 Because it wouldn't have mattered what district the order came
11 from, it wouldn't have mattered where the evidence resided.
12 The provider could have pulled the data on any warrant.

13 The fact that Congress tweaked the statute but said
14 nothing to indicate that the statute should operate overseas is
15 all the indication the Court needs to say this is Congress's
16 problem to act now. But they have given no indication that
17 this statute, the SCA, should reach overseas and grab foreign
18 data for a foreign user stored in a foreign data center.

19 THE COURT: Okay. Mr. Turner, do you have anything
20 different to say about that?

21 MR. TURNER: Very briefly, on the Rule 41 point. What
22 the statute says is warrants need to be issued using the
23 procedures of Rule 41. Not executed under Rule 41. It is
24 issued. And of course there is nothing particular about Rule
25 41. Congress referred to state procedures as well. Basically

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 the idea is however you get a warrant, in your district or your
2 office, that's how you get a warrant issued for purposes of the
3 SCA. But it is still executed like a subpoena. That's really
4 the only -- that's the part of the warrant that's really in
5 play here. I'll stop with that.

6 THE COURT: Counsel.

7 MR. RAUL: Alan Raul, Sidley Austin, on behalf of
8 amici AT&T Corp.

9 I think it is important to emphasize that Bank of Nova
10 Scotia case was not a search warrant case. It was not a
11 communication service provider case. It was a bank records
12 case. And that's relevant to the distinctions here. And I
13 think we need to understand that this is really about the
14 so-called third-party doctrine that's evolved since the U.S. v.
15 Miller and Smith v. Maryland cases. U.S. v. Miller was a bank
16 records case, and the Supreme Court held it was not a
17 reasonable expectation of privacy in records voluntarily turned
18 over to a bank. But that are essentially transactional records
19 of the company itself.

20 Really that goes, Mr. Rosenkranz said, to the nub of
21 the issue here. Which is how far to extend the BNS doctrine
22 and the distinction between business records of the company
23 itself and the confidential personal private communications of
24 the customer.

25 So Congress decided in ECPA in 1986 in which the
SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 Stored Communications Act is a part, that the records held by a
2 communications service provider would be treated differently.

3 So the cases that Mr. Turner cited, I believe none of
4 which -- was cited today, none of which was a communications
5 service provider case under ECPA, so may have little relevance
6 here.

7 Congress recognized in ECPA, and under the Stored
8 Communications Act, the various tiers of contents of
9 communications of the customers, versus records about the
10 subscriber or customer, and treated them differently. In some
11 cases a search warrant was required for content. In other
12 cases if they were transactional records perhaps, a court order
13 under 2703(d) or a subpoena.

14 In those cases, by the way, notification to the
15 customer was provided. So a very different regime of privacy
16 was established in the Electronic Communication Privacy Act.

17 That's relevant here because the government's position
18 is that the BNS doctrine really explains it all. That's
19 clearly a bank records case, clearly not a search warrant case,
20 and clearly isn't coming under the SCA and the ECPA.

21 Mr. Turner also said this is not a case where there is
22 no connection with the United States. So, he asked us to draw
23 from that proposition that there is no extraterritorial impact.
24 But clearly, we have to view this case as having significant
25 extraterritorial impact.

SOUTHERN DISTRICT REPORTERS, P.C.
(212) 805-0300

E7V3MICC

1 Microsoft has cited in its brief and attached
2 declarations and discussed here the impacts that other
3 countries have in reacting to this. That, I would submit, your
4 Honor, is essential to the Court's judgment about whether there
5 is extraterritorial impact here and one that Congress intended.

6 So in AT&T's brief for the Court, we proposed
7 consideration of a substantial nexus test. That is to say,
8 what is the connection with the United States, what is the
9 connection with the foreign government. And to use that as a
10 prism through which to judge the extent to which there is an
11 extraterritorial impact that Congress would not have been
12 comfortable with.

13 And that would go to where the records are located, of
14 course, is the predominant factor there, but also the nature of
15 the business relationship. Can it really be that a U.S.
16 communication service provider cannot have a primarily foreign
17 business relationship with customers located out of the United
18 States, simply because, as a technical matter, Mr. Turner could
19 show up with a document, serve process in the United States,
20 and technically, because as your Honor noted at the outset, it
21 can be moved around and this is the digital world we live in.
22 So, if in fact it is sufficient that the U.S. service provider
23 can access the documents technically because it has the
24 computer power to do so, that that's a sufficient U.S.
25 connection to overcome the presumption against

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 extraterritoriality. We don't think that's enough. A
2 substantial nexus with the United States should be established
3 instead. Thank you.

4 THE COURT: All right. Anyone else?

5 MR. ROSENKRANZ: May I just say literally 15 seconds'
6 worth?

7 THE COURT: All right.

8 MR. ROSENKRANZ: It is new.

9 THE COURT: I can't wait.

10 MR. ROSENKRANZ: I keep hearing you saying Congress
11 used the word "disclose," so doesn't that reveal Congress's
12 intention, and some of these remarks I think underscore this.
13 Congress used the word "disclose" and I grant you that points
14 one way. But Congress also used the word "warrant," with all
15 of the territorial limitations that were referred to. That
16 points the other way. And how do you break the tie? The
17 presumption against extraterritoriality.

18 Thank you very much for your attention, your Honor.

19 THE COURT: Excellent. Give me two seconds, counsel.

20 I'm well aware of the requirement here of conducting a
21 de novo review of the memorandum and order issued by Judge
22 Francis. I have done that with the assistance of your very
23 excellent briefing and arguments.

24 Having done that, I adopt the memorandum and order of
25 Judge Francis. Today with your assistance, we have uncovered,

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 in my view, additional examples of why the structure, language,
2 legislative history, Congressional knowledge of precedent,
3 including the Bank of Nova Scotia doctrine, all lead to the
4 conclusion that Congress intended in this statute for ISPs to
5 produce information under their control, albeit stored abroad,
6 to law enforcement in the United States. As Judge Francis
7 found, it is a question of control, not a question of the
8 location of that information.

9 The result of that finding is that the production of
10 that information is not an intrusion on the foreign sovereign.
11 It is incidental at best.

12 To the issue of the concerns of the foreign sovereign,
13 in my view, the restatement Section 442(1)(a) is dispositive in
14 that it states "A court or agency in the United States, when
15 authorized by statute or rule of court" is empowered to "order
16 a person subject to its jurisdiction to produce documents,
17 objects, or other information relevant to an action or
18 investigation, even if the information or the person in
19 possession of the information is outside the United States."

20 That's precisely what is required here. And
21 accordingly, I agree with Judge Francis that this is not an
22 extraterritorial application of United States law.

23 In my view, also, the argument that the documents are
24 not Microsoft's documents but the documents of its customers
25 has been waived because it was not argued below.

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

E7V3MICC

1 In sum, the magistrate judge's memorandum and order is
2 affirmed.

3 Counsel, thank you again for your excellent briefing
4 and quite enjoyable arguments.

5 MR. ROSENKRANZ: Thank you. May I just ask just a
6 housekeeping matter.

7 THE COURT: Sir.

8 MR. ROSENKRANZ: The magistrate judge stayed the order
9 in order to provide for appellate review. I believe it was
10 with the government's consent.

11 THE COURT: Mr. Turner?

12 MR. TURNER: We'd like to deliberate on that briefly.
13 We can get back to the Court later today whether we consent.

14 MR. ROSENKRANZ: We ask the Court to stay it without
15 regard to what the government's decision is.

16 THE COURT: In any event, I will stay it for however
17 long it takes you to file your notice of appeal. Ask for
18 expedited treatment and ask to be heard on a stay.

19 MR. ROSENKRANZ: Thank you.

20 THE COURT: If the government consents later in the
21 day, let me know.

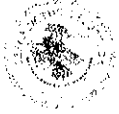
22 MR. TURNER: We will.

23 THE COURT: Thank you, counsel.

24 o0o

25

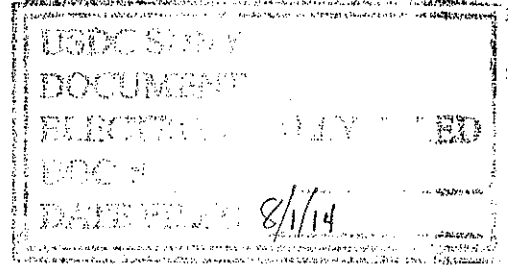
SOUTHERN DISTRICT REPORTERS, P.C.
(212) 805-0300



United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

July 31, 2014



BY ECF

The Honorable Loretta A. Preska
Chief United States District Judge
Daniel Patrick Moynihan U.S. Courthouse
500 Pearl Street
New York, New York 10007

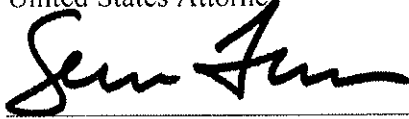
**Re: In re Search Warrant,
No. 13 Mag. 2814, M9-150**

Dear Chief Judge Preska:

The Government respectfully submits this letter to inform the Court that the Government consents to a stay of the Court's decision in this matter pending appeal.

Respectfully submitted,

PREET BHARARA
United States Attorney

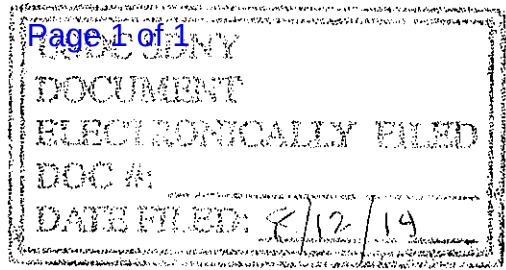
By: 
SERRIN TURNER
JUSTIN ANDERSON
Assistant United States Attorneys
(212) 637-1946/-1035

cc: Counsel for Microsoft (by ECF)

The stay shall extend only for such period as will permit Microsoft to file its notice of appeal, request for a stay and request for an expedited appeal.

August 1, 2014

*So ordered
Loretta A. Preska
USDC*



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK


-----X
IN THE MATTER OF A WARRANT TO : M9-150/ 13-MJ-2814
SEARCH A CERTAIN E-MAIL ACCOUNT :
CONTROLLED AND MAINTAINED BY : ORDER
MICROSOFT CORPORATION :
-----X

LORETTA A. PRESKA, Chief United States District Judge:

This order confirms that immediately following oral argument on July 31, 2014, for the reasons set forth on the record, the Court affirmed the decision of Magistrate Judge James C. Francis IV dated April 25, 2014 [dkt. no. 5].

SO ORDERED.

Dated: New York, New York
August 11, 2014


LORETTA A. PRESKA
Chief United States District Judge

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

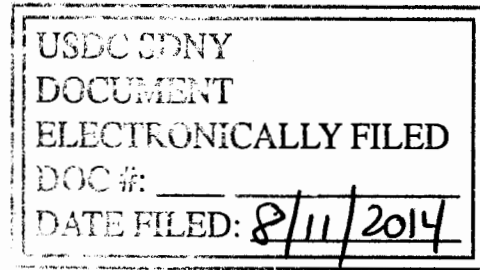
In the Matter of a Warrant to Search a Certain
E-Mail Account Controlled and Maintained By
Microsoft Corporation

Case Nos. 13-MAG-2814; M9-150

NOTICE OF APPEAL

Notice is hereby given that Microsoft Corporation, movant in the above named case, hereby appeals to the United States Court of Appeals for the Second Circuit from the order entered in this action on July 31, 2014, and the corresponding Memorandum to the Docket Clerk entered on August 6, 2014, adopting and affirming the Memorandum and Order of the Magistrate Judge entered on April 25, 2014.

Dated: August 11, 2014



4654010280
505
8-11-14
PP

Respectfully submitted,



E. Joshua Rosenkranz
Robert M. Loeb*
Brian P. Goldman*
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019-6142
Tel: 212.506.5380
jrosenkranz@orrick.com
rloeb@orrick.com
brian.goldman@orrick.com

Nancy Kestenbaum SDNY Bar # NK9768
Claire Catalano SDNY Bar # CC7432
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
Tel: 212-841-1000
nkestenbaum@cov.com
ccatalano@cov.com

Guy Petrillo
Nelson A. Boxer
PETRILLO KLEIN & BOXER LLP
655 Third Avenue
New York, NY 10017
Tel: 212.370.0330
gpetrillo@pkbllp.com
nboxer@pkbllp.com

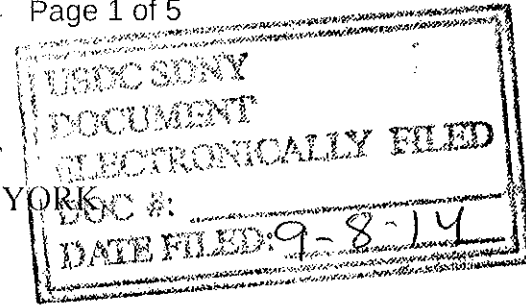
James M. Garland*
Alexander A. Berengaut*
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401
Tel: 202.662.6000
jgarland@cov.com
aberengaut@cov.com

**Admitted pro hac vice*

Bradford L. Smith
David Howard
John Frank
Jonathan Palmer
Nathaniel Jones
MICROSOFT CORPORATION

Counsel for Microsoft Corporation

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK



In the Matter of a Warrant to Search a
Certain E-Mail Account Controlled and
Maintained By Microsoft Corporation

Case Nos. 13-MAG-2814; M9-150

STIPULATION REGARDING CONTEMPT ORDER

In response to the Court's order of August 29, 2014, lifting the stay in execution of the July 31, 2014 order, the parties to this proceeding, Microsoft Corporation and the United States of America, hereby jointly stipulate:

1. Microsoft has not fully complied with the Warrant, and Microsoft does not intend to so comply while it in good faith seeks further review of this Court's July 31 decision rejecting Microsoft's challenge to the Warrant.
2. While Microsoft continues to believe that a contempt order is not required to perfect an appeal, it agrees that the entry of an order of contempt would eliminate any jurisdictional issues on appeal. Thus, while reserving its rights to appeal any contempt order and the underlying July 31 ruling, Microsoft concurs with the Government that entry of such an order will avoid delays and facilitate a prompt appeal in this case.
3. The parties further agree that contempt sanctions need not be imposed at this time. The Government, however, reserves its right to seek sanctions, in

addition to the contempt order, in the case of (a) materially changed circumstances in the underlying criminal investigation, or (b) the Second Circuit's issuance of the mandate in the appeal, if this Court's order is affirmed and Microsoft continues not to comply with it.


Accordingly, to facilitate appellate review of this Court's July 31 ruling, the parties jointly request that the Court enter the attached order.

Dated: September 4, 2014
New York, New York

Respectfully submitted,

PREET BHARARA
United States Attorney

By:


JUSTIN ANDERSON
SERRIN TURNER
Assistant United States Attorneys
(212) 637-1035 / -1946

Counsel for the United States of America

/s/ Guy Petrillo

Guy Petrillo
Nelson A. Boxer
PETRILLO KLEIN & BOXER
LLP
655 Third Avenue
New York, NY 10017
Tel: 212.370.0330
gpetrillo@pkbllp.com
nboxer@pkbllp.com

/s/ James Garland

Nancy Kestenbaum SDNY Bar # NK9768
Claire Catalano SDNY Bar # CC7432
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
Tel: 212-841-1000
Fax: 212-841-1010
nkestenbaum@cov.com
ccatalano@cov.com

/s/ E. Joshua Rosenkranz

E. Joshua Rosenkranz
Robert M. Loeb
Brian P. Goldman*
ORRICK, HERRINGTON
& SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019-6142
Tel: 212.506.5380
jrosenkranz@orrick.com
rloeb@orrick.com
brian.goldman@orrick.com

James M. Garland*
Alexander A. Berengaut*
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401
Tel: 202.662.6000
Fax: 202.662.6291
jgarland@cov.com
aberengaut@cov.com

**Admitted pro hac vice*

Bradford L. Smith
David Howard
John Frank
Jonathan Palmer
Nathaniel Jones
MICROSOFT CORPORATION

Counsel for Microsoft Corporation

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a
Certain E-Mail Account Controlled and
Maintained By Microsoft Corporation

Case Nos. 13-MAG-2814; M9-150

ORDER

In accord with the parties' joint stipulation, and to permit prompt appellate review of this Court's July 31 ruling, this Court holds Microsoft Corporation in contempt for not complying in full with the Warrant, and imposes no other sanctions at this time. The Government may seek sanctions in the case of (a) materially changed circumstances in the underlying criminal investigation, or (b) the Second Circuit's issuance of the mandate in the appeal, if this Court's order is affirmed and Microsoft continues not to comply with it.

SO ORDERED.

Dated: September 8, 2014

New York, New York


LORETTA A. PRESKA
Chief United States District Judge

CERTIFICATE OF SERVICE

Justin Anderson affirms, under penalty of perjury, that he is employed in the Office of the United States Attorney for the Southern District of New York, and that, on today's date, he caused a copy of this submission to be served by this Court's electronic filing system on counsel of record in this matter.

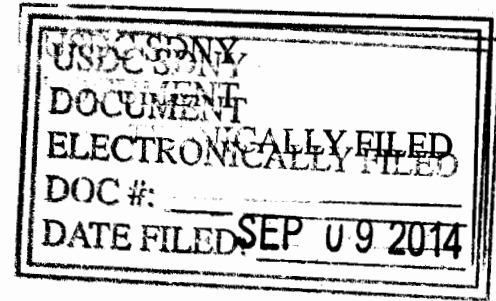
Dated: September 4, 2014
New York, New York


JUSTIN ANDERSON
Assistant United States Attorney
Tel: (212) 637-1035

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain
E-Mail Account Controlled and Maintained By
Microsoft Corporation

Case Nos. 13-MAG-2814; M9-150



AMENDED NOTICE OF APPEAL

Notice is given that Microsoft Corporation (“Microsoft”), movant in the above-named case, hereby amends its Notice of Appeal to the United States Court of Appeals for the Second Circuit from the Memorandum to the Docket Clerk entered in this action on July 31, 2014, and the corresponding Order entered on August 11, 2014 (Dkt. No. 80), adopting and affirming the Memorandum and Order of the Magistrate Judge, entered on April 25, 2014. Microsoft filed its Notice of Appeal on August 11, 2014 (Dkt. No. 81). On September 8, 2014, the Court issued an order holding Microsoft in contempt. (Dkt. No. 92).

Microsoft hereby amends its Notice of Appeal to include an appeal from the Court’s Order of September 8, 2014 (Dkt. No. 92).

Dated: September 8, 2014

Respectfully submitted,



E. Joshua Rosenkranz
Robert M. Loeb*
Brian P. Goldman*
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019-6142
Tel: 212.506.5380
jrosenkranz@orrick.com
rloeb@orrick.com
brian.goldman@orrick.com

Bradford L. Smith
David Howard
John Frank
Jonathan Palmer
Nathaniel Jones
MICROSOFT CORPORATION

Guy Petrillo
Nelson A. Boxer
PETRILLO KLEIN & BOXER LLP
655 Third Avenue
New York, NY 10017
Tel: 212.370.0330
gpetrillo@pkblp.com
nboxer@pkblp.com

Nancy Kestenbaum SDNY Bar # NK9768
Claire Catalano SDNY Bar # CC7432
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
Tel: 212-841-1000
nkestenbaum@cov.com
ccatalano@cov.com

James M. Garland*
Alexander A. Berengaut*
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401
Tel: 202.662.6000
jgarland@cov.com
aberengaut@cov.com

**Admitted pro hac vice*

Counsel for Microsoft Corporation

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain
E-Mail Account Controlled and Maintained By
Microsoft Corporation

Case Nos. 13-MAG-2814; M9-150

CERTIFICATE OF SERVICE

I, E. Joshua Rosenkranz, hereby certify that on September 9, 2014, I caused to be served via FedEx Priority Overnight delivery a true and correct copy of Microsoft Corporation's AMENDED NOTICE OF APPEAL upon the United States Attorney for the Southern District of New York at the following address:

Justin Anderson
Serrin Turner
United States Attorney's Office for the Southern District of New York
One St. Andrew's Plaza
New York, NY 10007

Dated: September 8, 2014


E. Joshua Rosenkranz
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019-6142
Tel: 212.506.5380
jrosenkranz@orrick.com
Counsel for Microsoft Corporation