

**THE USA PATRIOT ACT:
WHEN JURISDICTIONAL GOALS AND PRIORITIES
CLASH ACROSS BORDERS**

KENNETH K. DORT

**PARTNER
MCGUIREWOODS LLP**

**INTERNATIONAL TECHNOLOGY LAW ASSOCIATION
ANNUAL MEETING AND WORLD CONFERENCE**

CHICAGO, ILLINOIS

APRIL 26-27, 2007

**THE USA PATRIOT ACT:
WHEN JURISDICTIONAL GOALS AND PRIORITIES
CLASH ACROSS BORDERS**

TABLE OF CONTENTS

I.	INTRODUCTION	3
II.	PATRIOT ACT.....	5
	A. Background	5
	B. Patriot Act Jurisdiction	6
	C. Amendments to FISA – Section 215 Orders.....	7
	D. National Security Letters	8
	E. <i>Doe v. Ashcroft</i>	10
	F. Legislative Effects of <i>Doe v. Ashcroft</i>	11
III.	GLBA, HIPAA AND THEIR PROTECTIONS	13
IV.	IMMUNITY UNDER THE PATRIOT ACT	14
V.	EXCEPTIONS UNDER GLBA AND HIPAA.....	16
VI.	CROSS-BORDER CONSIDERATIONS.....	17
VII.	PRACTICE CONSIDERATIONS.....	20
	A. Privacy Protection Considerations	21
	B. Response Considerations – NSLs/Section 215 Orders.....	22
VIII.	CONCLUSIONS.....	23

**THE USA PATRIOT ACT:
WHEN JURISDICTIONAL GOALS AND PRIORITIES
CLASH ACROSS BORDERS**

BY

KENNETH K. DORT¹

I. INTRODUCTION

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, otherwise known as the “Patriot Act,” passed in 2001 and reauthorized in 2006, greatly expanded the American federal government’s surveillance and information gathering powers.² One such power that has received particular scrutiny is that granted by Section 215 of the Patriot Act, which authorizes the FBI to require the production of any record, paperwork, or other “tangible thing” from any entity “subject to United States jurisdiction.”³ This is the power that has caused the most controversy and generated the most media attention – recall that this is the provision that purports to allow the FBI to, among other things, obtain the lists of books that people have checked out from public libraries. A parallel

¹ Mr. Dort is a partner with McGuireWoods LLP in Chicago, Illinois, specializing in information technology and intellectual property law issues, including software development and licensing, systems development and integration, data encryption and security, trade secret protection, and patent/copyright/trademark licensing and protection. He is an experienced litigator who has handled cases at the trial and appellate levels throughout the United States in the above areas and others, such as patent, copyright and trademark infringement, breaches of data security systems, information systems development and implementation failures, open source licensing, trade secret misappropriation, and related areas of complex commercial litigation. He also advises clients on general corporate issues, business strategies and related areas of information technology and intellectual property law at the national and international levels. He is a member of the ITechLaw Board of Directors and is Chairman of its Membership Committee, and can be reached at kdort@mcguirewoods.com. Mr. Dort also recognizes the assistance of Adam Grove, an associate at McGuireWoods LLP, whose contribution to this paper is gratefully acknowledged.

² Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

³ *Id.*

line of authority is the expansion of the power to issue so-called “national security letters” (“NSLs”) pursuant to Section 505 of the Patriot Act. Each of these investigative tools and their collective effect on cross-border information technology transactions is examined in turn below.

While the outcry over the perusal of book lists by the FBI for suspicious behavior is understandable, a potentially more far-reaching consideration exists. Libraries are not generally under a specific duty to keep their records private. In contrast, there are many businesses and individuals which *are* required by statute to keep confidential the information they possess and/or control about third parties. This consideration raises a clear conflict. What happens when the FBI submits a Section 215 request for information which another statute mandates to be confidential? Could a receiving party find itself in a situation where it would have to choose between (i) violating an arguably valid subpoena/order served upon them by the FBI, or (ii) violating a federal statute that demands that the receiving party withhold the very information contained in documents demanded by the FBI (and to which it is arguably entitled under the Patriot Act)?

This paper will examine the potential conflict between (i) the federal government’s authority to compel disclosure of tangible things under the Patriot Act, and (ii) the potentially conflicting privacy obligations under two specific statutes – namely, the Graham-Leach-Bliley Act (“GLBA”)⁴ and the Health Insurance Portability and Accountability Act (“HIPAA”).⁵ Two specific questions that this paper will explore are (i) whether recipients faced with the conflicting legal obligations of disclosure and non-disclosure as described above are: (1) required to disclose the protected information in

⁴ Pub. L. No. 106-102, 113 Stat. 1338 (1999).

⁵ Pub. L. No. 104-191, 110 Stat. 1936 (1996).

question, and (2) if they are required to disclose, could they be held civilly or otherwise liable for disclosing that protected information.

We will see that the broad language of the Patriot Act and its lack of a superiority or subordination clause have indeed set the stage for potential conflicts with other federal statutes – and also the laws of other nations. As we will demonstrate, however, GLBA and HIPAA purport to resolve this conflict by providing for exceptions authorizing the disclosure of information to law enforcement in certain situations. Unfortunately, no such solution exists as to conflicts created by the application in the United States of foreign laws governing the disclosure of foreign-sourced data.

In analyzing this scenario, this paper will close with a series of practice considerations aimed at resolving the issues raised when a client is faced with the prospect of an NSL or Section 215 Order.

II. PATRIOT ACT

A. BACKGROUND

Originally enacted in October 2001, the Patriot Act was formulated in response to the September 11, 2001 terrorist attacks against the United States. The Patriot Act dramatically expanded the authority of American law enforcement authorities with the stated goal of fighting terrorism in the United States and abroad. As part of its original sunset provisions, the Patriot Act was renewed (with amendments and/or revisions) on March 9, 2006 pursuant to the USA PATRIOT Improvement and Reauthorization Act of 2005.⁶

⁶ Pub. L. No. 109-177, 120 Stat. 192 (2006).

The Patriot Act was intended to amend the already-existing infrastructure for federal intelligence gathering created by the Foreign Intelligence Surveillance Act of 1978 (“FISA”), which is codified at 50 U.S.C. §§1801-1811, 1821-29, 1841-46, and 1861-62. In particular, FISA created the Foreign Intelligence Surveillance Court (“FISC”) and authorized it to evaluate requests for surveillance warrants submitted by federal law enforcement agencies (essentially the FBI). The court is staffed by eleven judges appointed by the Chief Justice of the United States, serving seven-year terms.

Proceedings before the FISC Court are *ex parte* and non-adversarial. The court hears evidence presented by the FBI through the United States Department of Justice. The proceedings are confidential. There is no statutory provision for seeking a release of any information regarding such hearings, or for the record of information actually collected. Any denials of warrants by the FISC may be appealed the Foreign Intelligence Surveillance Court of Review. The Court of Review is comprised of a three-judge panel. Its sessions are rare -- since its creation, the court has only convened once (in 2002).

B. PATRIOT ACT JURISDICTION

Those entities subject to the reach of the Patriot Act are those entities “subject to United States jurisdiction.”⁷ In particular, this provision applies to individuals physically located within the borders of the United States, and business entities and their assets physically located within the borders of the United States. In essence, if a person or entity possesses anything located within the borders of the United States, that “thing” is subject to production under the Patriot Act.

The question becomes more difficult for items/data located outside of the United States, yet possessed or controlled by United States citizens or corporations (*i.e.*, those

⁷ Section 106 of the Patriot Act; *see also* 50 U.S.C. §§1701-02.

organized under United States federal or state law) or entities controlled by United States citizens or corporations. Section 106 of the Patriot Act, through the application of various Executive Orders,⁸ might be available to provide the basis for production under such circumstances, yet to date this has not been attempted or considered by a court of law.

What is clear, however, is that anything within the physical borders of the United States is subject to production under the Patriot Act.

C. AMENDMENTS TO FISA – SECTION 215 ORDERS

The basic tool under the Patriot Act for the production of information is authorized by Section 215 of the Patriot Act, which amended Title V of FISA. This amendment is codified at 50 USC §1861 (“Section 1861”). Section 1861 began its life as relatively minor amendment to FISA in 1998 to allow the federal government to obtain records from certain entities for foreign intelligence and international terrorism investigations⁹. Specifically, the federal government was permitted to require a “common carrier, public accommodation facility, physical storage facility, or rental vehicle facility to release records in its possession.” The power granted by this language contains two limitations. First, the federal government was only able to obtain “records.” Second, the federal government could only obtain such records from companies in the transportation and storage/hotel industry.

The Patriot Act substantially expanded the limited scope of Section 1861. Instead of just “records,” the FBI could now demand any “tangible things (including books,

⁸ Executive Order 13224 (dated September 23, 2001) defines “United States person” to mean any “United States citizen, permanent resident alien, *entity organized under the laws of the United States (including foreign branches)*, or any person in the United States.” (emphasis added.) See also Executive Order 12333 (dated December 4, 1981).

⁹ Pub. L. No. 105-272.

records, papers, documents, and other items).” Also, the restriction to the transportation and storage/hotel industries was eliminated. Essentially, the FBI gained the authority to demand any tangible thing from any person or entity, with only two real restrictions. First, the request must be made pursuant to an international surveillance or terrorist investigation, and second, the basis for seeking the “tangible things” cannot be solely an activity protected by the First Amendment. As noted above, it is also important to note that the FBI’s requests for production are reviewed by a FISA judge, so there is judicial oversight in the process. *See* Section I.E., *infra*.

The Reauthorization Act reset the sunset provisions applicable to Section 215 to December 31, 2009.¹⁰

D. NATIONAL SECURITY LETTERS

In addition to Section 215 Orders, so-called “national security letters” are authorized under four different statutes (in addition to the Patriot Act itself).¹¹ The “national security letter” originated in 1978 for use in terrorism and espionage investigations. They were limited to use against “foreign powers” or persons whom the FBI had reasonable cause to believe were agents of a “foreign power.” Compliance was voluntary, and states’ consumer privacy laws often allowed institutions to decline these requests.

In 1986, Congress passed the Electronic Communications Privacy Act (“ECPA”), which included tools similar to NSLs. Still, the ECPA likewise failed to identify any penalties for non-compliance. In 1993, Congress amended the ECPA to (i) expand the

¹⁰ Section 102(b) of the Reauthorization Act, Pub. L. No. 109-177, 120 Stat. 195 (2006).

¹¹ Right to Financial Privacy Act, 12 U.S.C. §3414 (2000 & Supp. IV 2005); Electronic Communications Privacy Act, 18 U.S.C. §2709 (2000 & Supp. IV 2005); Fair Credit Reporting Act, 15 U.S.C. §1681u (2000 & Supp. IV 2005); National Security Act, 50 U.S.C. §436 (2000).

restrictions regarding "foreign powers," and (ii) permit the use of NSLs to obtain information on persons not under direct investigation.

However, NSLs did not fully mature until the advent of the Patriot Act. Once passed in 2001, Section 505 of the Patriot Act greatly expanded the use of NSLs, allowing their use in connection with the investigation of United States residents or visitors who are not suspects in any criminal investigation. It also granted this authority to federal agencies other than the FBI, presumably to grant to the Department of Homeland Security the same authority to use NSLs. In 2006, the Reauthorization Act added specific penalties for non-compliance and disclosure.¹²

Two key aspects of NSLs as initially promulgated were (i) their non-disclosure provisions, and (ii) the absence of judicial supervision regarding their issuance. Since created in 1978, the typical NSL contained a proviso forbidding the recipient from revealing any aspect of its existence: its issuance, contents or receipt.¹³

Unlike other subpoenas and warrants, however, no judicial approval is required for an NSL's issuance. An NSL may be issued by "the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director" with no checks and balances in place until after the NSL has been delivered.¹⁴

¹² See Section I.E., *infra*.

¹³ Right to Financial Privacy Act, 12 U.S.C. § 3414(a)(3)(A) (2000 & Supp. IV 2005); Electronic Communications Privacy Act, 18 U.S.C. § 2709(c) (2000 & Supp. IV 2005); Fair Credit Reporting Act, 15 U.S.C. § 1681u(d) (2000 & Supp. IV 2005);); National Security Act, 50 U.S.C. § 436(b) (2000).

¹⁴ 18 U.S.C. §2709.

E. *DOE V. ASHCROFT*

This absence of judicial oversight was the basis for *Doe v. Ashcroft*,¹⁵ which attacked the constitutionality of NSLs, specifically as authorized in 18 U.S.C. §2709 (requiring communications companies such as internet service providers or telephone companies to produce service records). Commenced by an ISP in conjunction with the American Civil Liberties Union, the plaintiffs challenged the constitutionality of Section 2709, specifically its provision pertaining to issuance and non-disclosure. In 2004, the court held that Section 2709 violates the First and Fourth Amendments, holding in particular that the provisions for issuance of an NSL without opportunity for judicial review violated the Fourth Amendment and that the provisions for perpetual non-disclosure violated the First Amendment. 334 F.Supp.2d at 494, 522.

Compelled by these judicial determinations, the Reauthorization Act allowed for greater judicial supervision over the NSL issuance process and scaled back the original limitations on non-disclosure. *See* Section II.F., *infra*. To date, however, there remains no requirement to seek judicial review or approval *prior to* the issuance of an NSL.

Another effect of *Doe v. Ashcroft* has been greater congressional oversight of the NSL issuing process. The Reauthorization Act also included requirements for semi-annual reporting to Congress.¹⁶ Although the details remain classified, a non-classified audit of those NSLs issued is required. In the most recent report, issued on April 28, 2006, the Department of Justice reported to Congress that in 2005:

"[T]he Government made requests for certain information concerning 3,501 United States persons pursuant to National Security Letters (NSLs). During this time frame,

¹⁵ 334 F.Supp.2d 471 (S.D.N.Y. 2004) (Marrero, J.).

¹⁶ 50 U.S.C. §1862(b).

the total number of NSL requests . . . for information concerning U.S. persons totaled 9,254."¹⁷

Similarly, a March 2007 Department of Justice audit of the FBI's use of NSLs determined that the FBI had issued 39,346 requests on 10,232 non-U.S. persons plus 6,519 U.S. persons in 2003, 56,507 requests for 2004 (8,494 non-U.S., 8,943 U.S. persons), and 47,221 requests in 2005 (8,536 non-U.S., 9,475 U.S. persons).¹⁸

F. LEGISLATIVE EFFECTS OF *DOE V. ASHCROFT*

In addition to the foregoing reporting requirements, the Reauthorization Act also effected the following amendments to NSL issuance procedures and non-disclosure limitations:

- Authorizing judicial review of the NSL process:¹⁹
 - Permitting the challenge to the validity of an NSL request;
 - Permitting the challenge to the scope of an NSL non-disclosure provision;
 - Permitting judicial modifications to an NSL if found to be “unreasonable, oppressive or otherwise unlawful;”
- Clarifying Enforcement Procedures:²⁰
 - Permitting Attorney General to seek order to compel compliance in federal court;
 - Codifying disobedience with NSL as punishable as contempt of court;
- Authorizing closed court proceedings:²¹
 - Allowing open proceedings for contempt hearings
 - Mandating that all records and evidence be kept under seal;
 - Allowing government to request that evidence be considered *ex parte* and *in camera* on proper showing;

¹⁷ Report Submitted Pursuant to the Foreign Intelligence Surveillance Act of 1978, William E. Moschella, United States Assistant Attorney General, April 28, 2006.

¹⁸ A Review of the Federal Bureau of Investigation's Use of National Security Letters, U.S. Department of Justice, Office of the Inspector General, March 2007.

¹⁹ Section 115 of the Reauthorization Act, Pub. L. No. 109-177, 120 Stat. 211 (2006), enacting new 18 U.S.C. §3511.

²⁰ *Id.*

²¹ *Id.*

- Mandating a limited approach to non-disclosure with exceptions:²²
 - Permitting the government to seek a non-disclosure order upon showing that disclosure would endanger any individual or the national security of the United States, or interfere with any diplomatic relations of the United States;
 - Contact with counsel is now permitted for purposes of formulating a response, but recipient must identify those persons who will be working on aggregating the data for any production;
- Imposing punishments for violations of NSL non-disclosure provisions:²³
 - Knowing and willful violation of non-disclosure provisions – up to one year in prison;
 - Violation with intent to obstruct an investigation or judicial proceeding – up to five years in prison; and
- Libraries are excluded from reach of NSLs (with exceptions):²⁴
 - Traditional role as lender of books and other materials provides exemption from reach of NSLs;
 - Libraries still subjects to NSLs with respect to any provision of electronic communications services to patrons.

The Reauthorization Act also amended Section 1861 to refine the scope and limitations on the issuance and use of Section 215 Orders as follows:

- Provides for greater Congressional oversight of the process;²⁵
- Provides for enhanced procedural protections such as:
 - Promulgation of “minimization standards;”
 - No loss of privileged status for produced material;²⁶
- Requires all Section 215 applications to include “statements of fact” demonstrating “reasonable grounds to believe that the tangible things sought are relevant” to an otherwise authorized investigation;²⁷
- Provides for judicial review of NSLs and Section 215 Orders:
 - Procedure created for challenges to FISA Court decisions;
 - Authorizes FISA Court judge to modify proposed Section 215 Orders;

²² Section 116 of the Reauthorization Act, Pub. L. 109-177, 120 Stat. 213-217 (2006), amending 18 U.S.C. §2709(c)(1); 15 U.S.C. §1681u(d)(1); 15 U.S.C. §1681v(c)(1); 12 U.S.C. §3414(a)(3)(A); 12 U.S.C. §3414(a)(5)(D)(I); and 50 U.S.C. §436 (b)(1).

²³ Section 117 of the Reauthorization Act, Pub. L. No. 109-177, 120 Stat. 217 (2006), enacting new 18 U.S.C. §1510(e).

²⁴ 18 U.S.C. §2709.

²⁵ 50 U.S.C. §1862(b).

²⁶ 50 U.S.C. §1861(g).

²⁷ 50 U.S.C. §1861(b).

- Provides FISA Court of Review and United States Supreme Court with jurisdiction to consider appeals of FISA judges' decisions;²⁸
- Provides for non-disclosure limitations by:
 - Expressly permitting recipients to consult with attorneys on responding and/or challenging orders;
 - Precluding disclosure of attorney identifications; and
 - Providing a one-year moratorium on challenges to non-disclosure provisions, subsequent to which challenges shall be heard by FISA Court judges.²⁹

As a result of the passage of the Reauthorization Act, the appellate activities following the entry of the court's decision in *Doe v. Ashcroft* were either dismissed as moot or remanded for further consideration.³⁰

III. GLBA, HIPAA AND THEIR PROTECTIONS

While the Patriot Act grants the FBI broad powers to compel almost any party to produce almost any piece of tangible evidence, there are also federal statutes that impose a contradictory mandate – that is, which require a party *not* to disclose information. As noted above, a party could find itself in the untenable situation of receiving a subpoena or order to disclose information pursuant to the Patriot Act that they are mandated not to disclose under another statute. GLBA and HIPAA are two such privacy-mandating statutes, and we shall examine them below.

GLBA, enacted in 1999, provided for multiple reforms in the financial services sector. Included in these reforms were provisions directing financial institutions to take steps to safeguard their customers' non-public information (codified at 5 U.S.C. §§6801-6809). Specifically, Section 6802 limits a financial institution's ability to distribute a

²⁸ 50 U.S.C. §1861(f).

²⁹ 50 U.S.C. §186(d).

³⁰ *See Doe I v. Gonzales*, 449 F.3d 415, 418-19 (2d Cir. 2006) (declaring as moot Doe I's Fourth Amendment claim given passage of 18 U.S.C. §3511 allowing challenges to the legality of NSLs, but remanding to the trial court for additional consideration of Doe I's First Amendment arguments as applied to revised version of 18 U.S.C. §2709(c)).

customer's "non-public" information to non-affiliated third parties, which could conceivably create a conflict with the information disclosing requirements of the Patriot Act. "Non-public" personal information is defined as personally identifiable information that is provided by the customer, results from a transaction the customer performs or is performed for the customer, or information the financial institution otherwise obtains.³¹ Such information could certainly be of interest to federal investigators attempting to track down the identities of those financing terrorist operations.

Likewise, HIPAA mandates reforms for the health care sector on a scale similar to what GLBA did for the financial services sector. Like GLBA for financial information, HIPAA provides for reforms intended to protect personal health/medical information. Those reforms were implemented pursuant to the myriad regulations governing the disclosure of medical information as promulgated by the Secretary of Health and Human Services.³² In particular, HIPAA provides that protected health information may not be used or disclosed, except as specifically permitted under 45 CFR 164.³³

IV. IMMUNITY UNDER THE PATRIOT ACT

We have seen that the Patriot Act allows the FBI to compel information disclosure, and that GLBA and HIPAA contain broad requirements to keep that same information confidential. The next question is whether this conflict is resolved within any of the statutes themselves, and for this we begin with the Patriot Act. Recall that we asked two specific questions with regard to this conflict - first, whether an entity is required to disclose information if the Patriot Act conflicts with another statute, and

³¹ 15 U.S.C. §6809.

³² See 45 CFR 160-64.

³³ See 45 CFR 164.502(a)

second, whether the entity could be held liable for disclosing that information. The answer to the first question is that disclosure is required, and the answer to the second question is that under certain circumstances the party is protected from liability.

The Patriot Act allows the FBI to compel disclosure of tangible things. Therefore, under the Patriot Act an individual served with a subpoena under Section 1861 will be required to disclose the information unless the Patriot Act itself contains a clause stating that it is in some way subordinate to other laws requiring that the information in question be kept private. There is no such subordination clause in the Patriot Act, and so individuals subpoenaed for information under the Patriot Act must disclose the information or will be in violation thereof, subject of course, to the recently enacted provisions permitting challenges to the terms of Section 215 Orders. *See* Section II.F., *supra*.

While the Patriot Act does mandate disclosure, it does provide relief to both the disclosing party and the party whose information is being disclosed. For the disclosing party, Section 1861(e) explicitly states that anyone complying in good faith with an information request under the Patriot Act “shall not be liable to any other person” for producing the information.³⁴ Accordingly, this provision will provide protection to a party receiving an FBI-initiated subpoena under Section 1861 from liability for disclosing the otherwise protected information. Likewise, for the party whose information is being disclosed, Section 1861(e) states that the production of tangible things under Section 1861 shall not be deemed to constitute a waiver of any privilege in any other proceeding or context. In essence, this provision becomes an automatic protective order for privileged information.

³⁴ *See* 50 USC §1861(e).

An additional issue arises from the Patriot Act's lack of any form of supremacy clause. While the Patriot Act states that a party will not be liable for disclosing information, what if another federal law provides just as clearly that the disclosing party will be liable? There is no clear proviso in the Patriot Act that it supersedes other federal statutes. This means that unless the statutes requiring that information not be disclosed have some exception, then a disclosing party would find itself at the mercy of a court to determine the intent of Congress and what the party was supposed to do – either disobey a subpoena, or divulge confidential or privileged information. Fortunately, both GLBA and HIPAA contain clauses that allow for the disclosure of information to law enforcement agencies in certain circumstances.

V. EXCEPTIONS UNDER GLBA AND HIPAA

We have seen thus far that GLBA and HIPAA contain broad requirements to keep certain information confidential, and that the Patriot Act contains an equally broad requirement that parties disclose that same information if the FBI demands it. Furthermore, the Patriot Act does not explicitly resolve this apparent conflict. The final question that remains is whether the conflict is resolved somewhere in GLBA and HIPAA themselves, and the answer for both of these statutes is yes.

GLBA contains an exception in text of the statute itself. Section 1602(e)(8) states that a financial institution may disclose a customer's information to comply with a properly authorized federal subpoena.³⁵ HIPAA contains an exception similar to that in GLBA. It is contained in the regulations codified in the federal register, in the same place as the broad language prohibiting disclosure of medical information, at 45 CFR

³⁵ As the demands for information by the FBI under Section 1861 are reviewed and signed by a judge, they are deemed the equivalent of subpoenas.

164.502. The most pertinent exception for the purposes of the Patriot Act is found at 45 CFR 164.512(f)(1)(ii). This regulation provides that information may be disclosed for the purposes of law enforcement in compliance with a court order.

VI. CROSS-BORDER CONSIDERATIONS

In view of the foregoing environment in the United States, a non-American enterprise desiring to engage an American firm for purposes of outsourcing its data management and storage functions to the latter firm has a serious set of circumstances before it. Assuming that the non-American's jurisdiction is more protective of personal information than is the United States, the former faces a very difficult decision if in fact the proposed outsourcing contemplates the actual transfer of data into the United States.

In particular, assuming that the non-American company must exercise more care than its American counterpart in the protection of private data in its possession, the existence of the Patriot Act and its operation over the American outsourcing firm puts the non-American in the position of jeopardizing the very data over which it has primary responsibility in its home jurisdiction. Indeed, the very act of transferring private data into the United States – with the possibility of disclosure by the American firm in response to a Patriot Act order – might place the non-American company in legal jeopardy back home.

On the other hand, the American firm faces reciprocal difficulties of its own. For example, although the Patriot Act's immunity provisions would most likely protect it from liability within the jurisdiction of the United States, those same provisions may be unavailing overseas. Indeed, those very provisions which would protect it within the United States might well be deemed unenforceable and without merit outside of the

United States – particularly in those jurisdictions deemed more “pro-privacy” than the United States.

The most efficacious resolution of this situation would be the implementation of a statutory provision providing some form of “safety valve” relieving the parties of the conflict in question – essentially mandating the more restrictive approach in the event of conflict. Alternatively, the nations in question could resolve the conflict via treaty or similar agreement that would have the force of law domestically.³⁶

There is recent precedent for such an approach. For example, in October 2006, the United States and the European Union put in place (and set to expire on July 31, 2007 absent implementation of a superseding agreement) an understanding of how the United States Department of Homeland Security may access the passenger lists of European airlines while simultaneously protecting the privacy of the passengers in question.³⁷

Likewise, the United States and the European Union have agreed on the implementation of “Safe Harbor” provisions for the protection of private information.³⁸ By that approach, United States companies can certify that they will comply with the provisions of the European Union Directive on Data Protection (the “Privacy Directive”). By this approach, a number of important benefits accrue to United States and European Union firms. For example, benefits for United States organizations participating in the safe harbor will include:

- All 25 Member States of the European Union will be bound by the European Commission’s finding of “adequacy;”

³⁶ Such as in the United States, where Article VI of the Constitution provides that such treaties as properly ratified “shall be the supreme Law of the Land.” U.S. CONST., ART. VI.

³⁷ See “Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security” dated October 6, 2006. See www.eurunion.org/newsweb/HotTopics/PNRAgreementOct06.pdf.

³⁸ See, e.g., the United States Department of Commerce’s website on the implementation and enforcement of the Safe Harbor at www.export.gov/safeharbor/index.html.

- Companies participating in the safe harbor will be deemed “adequate” and data flows to those companies will continue;
- Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted; and
- Claims brought by European citizens against U.S. companies will be heard in the United States subject to limited exceptions.³⁹

The safe harbor framework offers a simpler and cheaper means of complying with the adequacy requirements of the Privacy Directive, which particularly benefits small and medium enterprises.

Similarly, a European Union organization can be assured that it is sending information to a United States organization participating in the safe harbor by viewing the public list of safe harbor organizations posted on the Department of Commerce’s website (<http://export.gov/safeharbor>). This list became operational at the beginning of November 2000, and contains the names of all United States companies that have self-certified to the safe harbor framework. This list is regularly updated, so that it is clear who is assured of safe harbor benefits.⁴⁰ In particular, it is potentially arguable that compliance with the Directive’s “safe harbor” principles might provide protection to a United States firm complying with Patriot Act production orders. Of the seven “safe harbor” principles that United States firms must honor, the principle on “security” is relevant here:

Security: Organizations must take reasonable precautions to protect personal information from loss, misuse and *unauthorized access, disclosure*, alteration and destruction.⁴¹

³⁹ See www.export.gov/safeharbor/sh_overview.html.

⁴⁰ *Id.*

⁴¹ *Id.*

(emphasis added). Certifying to the safe harbor will assure that European Union organizations know that the United States company provides "adequate" privacy protection, as defined by the Privacy Directive. While not defined, "unauthorized access [and] disclosure" in the "security" principle could be argued to protect an American firm producing information under the Patriot Act as authorized access and disclosure, thus avoiding violation with the principle in question. Significantly, this argument has not been addressed by any judicial or regulatory body – either in the United States or Europe.

Accordingly, while parties can agree at the private level to take appropriate protective measures to safeguard data delivered to it, the existence of the Patriot Act and the power it grants the federal government over data held in the United States perpetuates uncertainty in the foregoing safe harbor efforts. While the current approach applicable to the airline industry provides a positive model for action in other economic sectors, such action needs to be undertaken promptly.

As of this writing, no such actions have been implemented, thus forcing businesses to implement contractually those protections deemed most beneficial to minimize the risks now resulting from the Patriot Act.

VII. PRACTICE CONSIDERATIONS

The Patriot Act has substantially expanded the power of the American federal government to obtain the records of almost any entity in the United States. A direct result of this development has been the increased precariousness of the confidential status of data held by American companies but aggregated and transferred from outside the United States' borders – particularly from those nations which maintain stricter privacy protection standards than presently found in the United States. Putting aside the political

debate over the efficacy and/or legality of the United States' approach, the current statutory/regulatory environment must be addressed and dealt with directly and immediately.

A. Privacy Protection Considerations

In view of the absence of controlling authority over the conflict between national statutes and regulations, parties at the international level must undertake a very precisely drawn calculus of risk and reward. Accordingly, parties contemplating cross-border transactions by which data will be transported into the United States from overseas should consider the following points:

➤ **NON-AMERICAN OWNERS OF DATA**

- Anticipate the possible production of information without its knowledge;
- Determine how such production would affect its obligations at home to its client;
- Require American firms to contest the production to the fullest extent of applicable law;
- Ascertain whether the transaction can be conducted without loss of data control and/or without transfer to United States;
- Ascertain exposure to criminal authorities at home given current state of United States law; and
- Modify data collection notification disclaimers to reflect that data will be transferred to the United States with resultant possibility of disclosure.

➤ **AMERICAN FIRMS MANAGING FOREIGN-SOURCED DATA**

- Consider exposure to overseas outsourcing firm;
- Consider exposure to overseas originator of data;
- Consider implementation of provisions absolving all parties from liability for compliance with all applicable statutes (mirroring Patriot Act immunities);

- Consider exculpatory clauses excusing lack of notice in event of Section 215 Order as mandated by Section 1861;
- Consider exculpatory clauses permitting compliance with domestic laws without breach of underlying contract; and
- Consider indemnification from foreign outsourcing firm for any third-party actions.

B. Response Considerations – NSLs/Section 215 Orders

In addition to the foregoing considerations, all companies operating in the United States should also have in place policies and procedures aimed at responding to requests for production pursuant to either an NSL or a Section 215 Order. Such policies and procedures should provide at a minimum as follows:

- The creation of a privacy/compliance officer responsible for:
 - Implementation of all procedures and policies;
 - Serving as liaison between counsel (in-house and outside), management, outsourcing client and data source;
 - Serve as formal recipient of all information requests;
 - Responding to all requests for information;
 - Overseeing the production of all requested data;
- Confirm that a formal request for information is being made;
- All requests (formal or otherwise) must be referred to the privacy officer;
- For all formal requests:
 - Ascertain validity thereof and need to prepare challenges thereto;
 - Determine time constraints/deadlines;
 - Determine the scope of the request;
 - Determine the level of secrecy required and implement all necessary protective measures;

- For all informal requests:
 - Determine time constraints/deadlines;
 - Determine the scope of the request;
 - Determine the level of secrecy required;
 - Submit a demand for a formal request in order to bring matter within scope of statutory review procedures.

VIII. CONCLUSIONS

At present, a significant chasm exists between the protection of private information in the United States and other nations of the world. Until the leading economic centers of the United States, Canada, the European Union and such Asian leaders as India, Japan and China are able to negotiate a means to handle these differences, resolution will remain uncertain at best. This uncertainty will continue to play a significant role in the conduct of business transactions that deal with the handling of private information. Meanwhile, until appropriate national measures are enacted, those enterprises operating at the international level will have to continue to structure their own contractual provisions to handle the risks arising from the current policy imbalance between the United States and its overseas trading partners.