DATA SECURITY MANAGEMENT

JURISDICTIONAL ISSUES IN GLOBAL TRANSMISSIONS

Ralph Spencer Poore

INSIDE
Legal Issues; Specific and General Jurisdictions; Technical Issues; Protective Technologies; The Long View

INTRODUCTION
In the information age where teleconferences replace in-person meetings, where telecommuting replaces going to the office, and where international networks facilitate global transmissions with the apparent ease of calling one’s next-door neighbor, valuable assets change ownership at the speed of light. Louis Jionet, Secretary-General of the French Commission on Data Processing and Liberties stated: “Information is power and economic information is economic power.” Customs officials and border patrols cannot control the movement of these assets. But does this mean companies can transmit the data that either represents or is the valuable asset without regard to the legal jurisdictions through which they pass? To adequately address this question, both the legal issues and the practical issues involved in transnational border data flows are discussed in this article.

LEGAL ISSUES
All legally incorporated enterprises have Official Books of Record. Whether these be in manual or automated form, these are the records that governmental authorities turn to when determining the status of an enterprise. The ability to enforce a subpoena or court order for these records reflects the effective sovereignty of the nation in which the enterprise operates. Most countries require enterprises incorporated, created, or registered in their jurisdiction to physically maintain Official Books of Record within their border.

PAYOFF IDEA
Today, the operations of international organizations require the ability to electronically transmit all kinds of information to all corners of the world. However, many legal issues stand in the way of enabling the free flow of this information. This article focuses on these problem areas so that potential challenges and solutions can be understood prior to them presenting “show-stopper” hurdles.
ders. For example, a company relying on a service bureau in another country for data processing services may cause the official records to exist only in that other country. This could occur if the printouts reflected only a historic position of the company, perhaps month-end conditions, where the current position of the company — the position on which management relies — exists only through online access to the company’s executive information system. From a nation’s perspective, two issues of sovereignty arise:

- The other country might exercise its rights and take custody of the company’s records — possibly forcing it out of business — for actions alleged against the company that the company’s “home” nation considers legal.
- The company’s “home” nation may be unable to enforce its access rights.

Another, usually overriding factor, is a nation’s ability to enforce its tax laws. Many nations have value-added taxes (VATs) or taxes on publications, computer software, and services. An organization’s data may qualify as a publication, as computer software, or even as services in some jurisdictions. Thus, many nations have an interest in the data that flows across their borders because it may qualify for taxation. In some cases, the tax is a tariff intended to discourage the importation of computer software or publications in order to protect the nation’s own emerging businesses. More so than when the tax is solely for revenue generation, protective tariffs may carry heavy fines and be more difficult to negotiate around. With the advent of Internet businesses, determining a business’ nexus for tax purposes has become even more complex. Such business may have income, franchise, and inventory or property tax issues in addition to sales tax, excise tax, and import or export duties. Business taxes, registration or license fees, and even reporting requirements depend on the applicability of a given jurisdiction.

National security interests can include controlling the import and export of information. State secrecy laws exist for almost all nations. The United States, for example, restricts government classified data (e.g., Confidential, Secret, Top Secret), but also restricts some information even if it is not classified (e.g., technical data about nuclear munitions, some biological research, some advanced computer technology, and — to varying degrees — cryptography).

Among those nations concerned with an individual’s privacy rights, the laws vary greatly. Laws like the United State’s Privacy Act of 1974 (5 USC 552a) have limited applicability (generally applying only to government agencies and their contractors). The United Kingdom’s Data Protection Act of 1984 (1984 c 35 [Halsbury’s Statutes, 4th Edition, Butterworths, London, 1992, Vol. 6, pp 899-949]), however, applies to the commercial sec-
tor; as does the 1981 Council of Europe’s Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (an excellent discussion of this can be found in Anne W. Brandscomb’s Toward a Law of Global Communications Networks, The Science and Technology section of the American Bar Association, Longman, New York, 1986). Privacy laws generally have at least the following three characteristics:

- They provide notice to the subject of the existence of a database containing the subject’s personal data (usually by requiring registration of the database).
- They provide a process for the subject to inspect and to correct the personal data.
- They provide a requirement for maintaining an audit trail of accessors to the private data.

The granularity of privacy law requirements also varies greatly. Some laws (e.g., the U.S. Fair Credit Reporting Act of 1970 [see 15 USC 1681 et seq.], require only the name of the company that requested the information. Other laws require accountability to a specific office or individual. Because the granularity of accountability can differ from jurisdiction to jurisdiction, organizations may need to develop their applications to meet the most stringent requirements (i.e., individual accountability). In this author’s experience, few electronic data interchange (EDI) systems support this level of accountability (UNCID Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission, ICC Publishing Corporation, New York, 1988. All protective measures and audit measures are described as options, with granularity left to the discretion of the parties).

To further complicate data transfer issues, patent, copyright, and trade secret laws are not uniform. Although international conventions exist (e.g., General Agreement on Tariffs and Trade [GATT]), not all nations subscribe to these conventions, and the conventions often allow for substantial differences among signatories. Rights one might have and can enforce in one jurisdiction might not exist (or might not be enforceable) in another. In some cases, the rights one has in one jurisdiction constitute an infringement in another jurisdiction. For example, one may hold a United States registered trademark on a product. A trademark is a design (often a stylized name or monogram) showing the origin or ownership of merchandise and reserved to the owner’s exclusive use. The Trademark Act of 1946 (see 15 USC 1124) provides that no article shall be imported that copies or simulates a trademark registered under United States laws. A similar law protecting, for example, trademarks registered in India might prevent one from using the trademark in India if a similar or identical trademark is already registered there.

Disclosure of information not in accordance with the laws of the jurisdictions involved may subject the parties to criminal penalties. For exam-
ple, the United Kingdom’s Official Secrets Act of 1989 clearly defines areas wherein disclosure of government secrets is a criminal offense. Most nations have similar laws (of varying specificity), making the disclosure of state secrets a crime. However, technical information considered public in one jurisdiction might be considered a state secret in another. Similarly, biographical information on a national leader may be mere background information for a news story in one country, but be viewed as espionage by another country. These areas are particularly difficult since most governments will not advise one in advance as to what constitutes a state secret (as this might compromise the secret). Unless an organization has a presence in each jurisdiction sensitive to these political and legal issues to whom one can turn for guidance, competent legal advice should be sought before transmitting text or textual database materials containing information about individuals or organizations.

From a business perspective, civil law rather than criminal law may take center stage. Although the United States probably has the dubious distinction as the nation in which it is easiest to initiate litigation, lawsuits are possible in most jurisdictions worldwide. No company wants to become entangled in litigation, especially in foreign jurisdictions. However, when information is transmitted from one nation to another, the rules can change significantly. For example, what are the implied warranties in the receiving jurisdiction? What constitutes profanity, defamation, libel, or similar actionable content? What contract terms are unenforceable (e.g., can one enforce a nondisclosure agreement of ten years’ duration)?

In some jurisdictions, ecclesiastical courts may have jurisdiction for offenses against a state-supported religion. Circumstances viewed in one jurisdiction as standard business practice (e.g., gifts) may be viewed in another jurisdiction as unethical or illegal. Even whether an organization has standing (i.e., may be represented in court) varies among nations. An organization’s rights to defend itself, for example, vary from excellent to nil in jurisdictions ranging from Canada to Iran, respectively.

Fortunately, companies can generally choose the jurisdictions in which they will hold assets. Most countries enforce their laws (and the actions of their courts) against corporations by threat of asset seizure. A company with no seizable assets (and no desire to conduct future business) in a country is effectively judgment-proof. The reverse can also be true; that is, a company may be unable to enforce a contract (or legal judgment) because the other party has no assets within a jurisdiction willing to enforce the contract or judgment. When contracting with a company to develop software, for example, and that company exists solely in a foreign country, one’s organization should research the enforceability of any contract and, if there is any doubt, require a bond be posted in one’s jurisdiction to ensure at least bond forfeiture as recourse.
Specific and General Jurisdiction

In September 1997, in Bensusan Restaurant Corp. v. King (1997 U.S. App. Lexis 23742 (2d Cir. Sept. 10, 1997)), the 2d U.S. Circuit Court of Appeals held that a Missouri resident's Web site, accessed in New York, did not give rise to jurisdiction under New York’s long arm statute. The court ruled there was no jurisdiction because the defendant was not physically in New York when he created the offending Web page. However, a similar case in California with a similar ruling was reversed on appeal (Hall v. LaRonde, 1997 Cal. App. Lexis 633 (Aug. 7, 1997)). Citing the changing “role that electronic communications plays in business transactions,” the court decided that jurisdiction should not be determined by whether the defendant's communications were made physically within the state, instead concluding that “[t]here is no reason why the requisite minimum contacts cannot be electronic.”

To comply with due process, the exercise of specific jurisdiction generally requires that the defendant intentionally took advantage of the benefits of the jurisdiction, and thus could have expected to be hauled into court in that jurisdiction. The nature of electronic communications and their growing role in commerce have contributed to findings that defendants’ Internet communications constitute “purposeful availment” (legalese for intentionally taking advantage of the benefits) and establish jurisdiction. For example, in California Software Inc. v. Reliability Research Inc. (631 F. Supp. 1356 (C.D. Cal. 1986)), the court held that a nonresident’s defamatory e-mail to a resident was sufficient to establish specific jurisdiction. The court noted that, as modern technology makes nationwide commercial transactions more feasible, it broadens the scope of jurisdiction.

Courts have also pointed out the distinguishing features of the Internet when holding that a Web site gives rise to specific jurisdiction for infringement claims arising out of the site’s content. In Martz Inc. v. Cybergold Inc. (947 F. Supp. 1328, 1332, 1334 (E.D. Mo. 1996)), the court suggested that Web site advertising more likely amounts to purposeful availment than advertising by direct mail or an “800” telephone number, noting the “different nature” of electronic communications.

Conceivably, a Web site could reflect contacts with a state’s residents that were sufficiently continuous and systematic to establish general jurisdiction over the site owner. Courts have held, however, that the mere creation of a Web site does not create general jurisdiction. See, for example, McDonough v. Fallon McElligott, Inc. (1996 U.S. Dist. Lexis 15139 (S.D. Cal. Aug. 6, 1996)). Further, courts have held in more traditional contexts that merely placing advertisements in nationally distributed periodicals, or communicating through a national computer-based information system, does not subject a nonresident to jurisdiction. See, for
example, Federal Rural Elec. Ins. Corp. v. Kootenai Elec. Corp. (17 F.3d 1302, 1305 (10th Cir. 1994)).

This area of law is evolving rapidly, with many jurisdictions asserting what amounts to extraterritorial jurisdiction on the basis of electronic transactions into, through, or out of their territory. The Council of Europe’s Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data is but one of many examples. The entire area of cryptography, for example, is another. In January 1999, France dramatically eased its long-standing restriction on the use of cryptography within its jurisdiction. This announcement came only six weeks after France joined with 32 other countries signing an update of a document known as the Wassenaar Agreement. Signatories to this agreement promised to tighten restrictions on the import or export of cryptography. The so-called “long arm” provisions of many laws and the lack of consensus among nations on important issues — including privacy, intellectual property rights, communications security, and taxes — will challenge (or plague) us for the foreseeable future.

TECHNICAL ISSUES

Any nation wishing to enforce its laws with regard to data transmitted within or across its borders must have the ability (1) to monitor/intercept the data, and (2) to interpret/understand the data. Almost all nations can intercept wire (i.e., telephone/telegraph) communications. Most can intercept radio, microwave, and satellite transmissions. Unless an organization uses exotic technologies (e.g., point-to-point laser, extremely low frequency (ELF), super high frequency, spread spectrum), interception remains likely.

The second requirement, however, is another matter. Even simple messages encoded in accordance with international standards may have meaning only in a specific context or template not inherent in the message itself. For example, “142667456043052” could be a phone number (e.g., 1-426-674-5604 x3052), or a social security number and birthday (e.g., 142-66-7456 04/30/52), or dollar amounts ($14,266.74 $560,430.52), or inventory counts by part number (PN) (e.g., PN 142667 Quantity 45, PN 604305 Quantity 2), or zip codes (e.g., 41266, 74560, 43052). Almost limitless possibilities exist even without using codes or ciphers. And this example used human-readable digits. Many transmissions may be graphic images, object code, or compressed text files completely unintelligible to a human “reading” the data on a datascope.

From the preceding, one might conclude that interception and interpretation by even a technologically advanced nation is too great a challenge. This is, however, far from true. Every “kind” of data has a signature or set of attributes that, when known, permits its detection and identification. This includes encrypted data, where the fact of encryption
is determinable. Where transmitting or receiving encrypted messages is a crime, a company using encryption risks detection. Once the “kind” of data is determined, applying the correct application is often a trivial exercise. Some examples of such strong typing of data include:

- rich-text format (RTF) documents and most word processing documents
- SQL transactions
- spreadsheets (e.g., Lotus 1-2-3, Microsoft Excel)
- DOS, Windows, UNIX, and other operating system executables
- standardized EDI messages
- ASCII vs. EBCDIC

If this were not the case, sending data from one computer to another would require extensive advanced planning at the receiving computer — severely impacting data portability and interoperability, two attributes widely sought in business transactions.

Countries with sufficient technology to intercept and interpret an organization’s data can pose an additional problem beyond their law enforcement: that of government-sponsored industrial espionage. Many countries have engaged in espionage with the specific objective of obtaining technical or financial information of benefit to that country’s businesses. A search of news accounts of industrial espionage resulted in a list that included the following countries: Argentina, Cuba, France, Germany, Greece, India, Iran, Iraq, Israel, Japan, North Korea, Peoples Republic of China, Russia, South Korea, and Turkey. Most of these countries have public policies against such espionage, and countries like the United States find it awkward to accuse allies of such activities (both because the technical means of catching them at it may be a state secret; and because what one nation views as counter-espionage, another nation might view as espionage).

Protective Technologies

For most businesses, the integrity of transmitted data is more important than its privacy. Cryptographic techniques a business might otherwise be unable to use because of import or export restrictions associated with the cryptographic process or the use of a privacy-protected message, can be used in some applications for data integrity. For example, the Data Encryption Standard (DES), when used for message authentication in accordance with the American National Standard X9.9 for the protection of electronic funds transfers between financial institutions, may be approved by the U.S. Department of the Treasury without having to meet the requirements of the International Trade in Arms Regulations (ITAR). (Note that technological advances can also impact this; for example, the
key space exhaustion attack in January 1999 of a DES Challenge was successful in 22.25 hours. Both the U.S. and French governments made policy changes that permit stronger cryptography for export and import that had previously been permitted.

Integrity measures generally address one or both of the following problems:

- unauthorized (including accidental) modification or substitution of the message
- falsification of identity or repudiation of message

The techniques used to address the first problem are generally called message authentication techniques. Those addressing the second class of problems are generally called digital signature techniques.

Message authentication works by applying a cryptographic algorithm to a message in such a way as to produce a resulting message authentication code (MAC) that has a very high probability of being affected by a change to any bit or bits in the message. The receiving party recalculates the MAC and compares it to the transmitted MAC. If they match, the message is considered authentic (i.e., received as sent); otherwise, the message is rejected.

Because international standards include standards for message authentication (e.g., ISO 9797), an enterprise wanting to protect the integrity of its messages can find suitable algorithms that should be (and historically have been) acceptable to most jurisdictions worldwide. With some exceptions, even the Data Encryption Algorithm (DEA), also known as the Data Encryption Standard (DES), can be used in hardware implementations of message authentication. For digital signature, this may also be true, although several excellent implementations (both public key and secret key) rely on algorithms with import/export restrictions.

The data protected by digital signature or message authentication, however, is not the problem, as both message authentication and digital signature leave the message in plaintext. Objections to their use center primarily on access to the cryptographic security hardware or software needed to support these services. If the cryptographic hardware or software can be obtained legally within a given jurisdiction without violating export restrictions, then using these services rarely poses any problems.

Digital signature techniques exist for both public key and secret key algorithm systems (also known respectively as asymmetric and symmetric key systems). The purpose of the digital signature is to authenticate the sender's identity and to prevent repudiation (where an alleged sender claims not to have sent the message). The digital signature implementation may or may not also authenticate the contents of the signed message.

Privacy measures address the concern for unauthorized disclosure of a message in transit. Cipher systems (e.g., DEA) transform data into what
appear to be random streams of bits. Some ciphers (e.g., a Vernam cipher with a key stream equal to or longer than the message stream) provide almost unbreakable privacy. As such, the better cipher systems almost always run afoul of export or import restrictions. The United States is currently working on the Advanced Encryption Standard (AES) to replace DES. One of the policy issues with the AES will be its exportability, as it will allow 128, 192, and 256 bit encryption keys. (The National Institute of Standards and Technology expects AES to be available by 2003.)

In some cases, the use of codes is practical and less likely to run into restrictions. As long as the “codebook” containing the interpretations of the codes is kept secret, an organization could send very sensitive messages without risk of disclosure if intercepted en route. For example, an oil company preparing its bid for an offshore property might arrange a set of codes as shown in Exhibit 1. The message “RED SUN NOVEMBER MAY MAY” would make little sense to an eavesdropper, but would tell the company representative that the maximum authorized bid is 900 (the units would be prearranged, so this could mean $900,000).

Other privacy techniques that do not rely on secret codes or ciphers include:

- Continuous stream messages (the good message is hidden in a continuous stream of otherwise meaningless text). For example,

  `THVSTOPREAXZTRECEEBNKLIWSYAINNTHELAUNCHGBMEAZY`

contains the message “STOP THE LAUNCH.” When short messages are sent as part of a continuous binary stream, this technique (one of a class known as steganography) can be effective. This technique is often combined with cipher techniques when very high levels of message security are needed.
• Split knowledge routing (a bit pattern is sent along a route independent of another route on which a second bit pattern is sent; the two bit streams are exclusive-OR'ed together by the receiving party to form the original message). For example, if the bit pattern of the message one wishes to send is 0011 1001 1101 0110, a random pattern of equal length would be exclusive-OR'ed with the message 1001 1110 0101 0010, to make a new message 1010 0111 1000 0100. The random pattern would be sent along one telecommunication path and the new message would be sent along another, independent telecommunication path. The recipient would exclusively OR the two messages back together, resulting in the original message. Since no cryptographic key management is required and because the exclusive-OR operation is very fast, this is an attractive technique where the requirement of independent routing can be met.

• The use of templates (which must remain secret) that permit the receiver to retrieve the important values and ignore others in the same message. For example, in the string used above,

```
THVSTOPREAXZTRECEEBNKLIWSYAINNTHELAUNCHGBMEAZY
```

used with the following template

```
XXXXXXXXNNXXXXNXXXXXXXXXXXNXXXXXXNXXXXXXXXXXXXXXXXXXXX
```

where only the letters at the places marked with “N” are used, reveals a different message, RETREAT.

The first technique can also be effective against traffic analysis. The second technique requires the ability to ensure independent telecommunication routes (often infeasible). The third technique has roughly the same distribution problems that codebook systems have; that is, the templates must be delivered to the receiver in advance of the transmission and in a secure manner. These techniques do, however, avoid the import and export problems associated with cryptographic systems.

In addition to cryptographic systems, most industrialized nations restrict the export of specific technologies, including those with a direct military use (or police use) and those advanced technologies easily misused by other nations to suppress human rights, improve intelligence gathering, or counter security measures. Thus, an efficient relational database product might be restricted from export because oppressive third-world nations might use it to maintain data on their citizens (e.g., “subversive activities lists”). Restrictions on software export can sometimes be averted by finding a nation in which the desired product is sold legally without the export restriction. (Note: check with legal counsel in your enterprise’s official jurisdiction as this work-around may be illegal —
some countries claim extraterritorial jurisdiction or claim that their laws take precedence for legal entities residing within their borders.) For example, the Foreign Corrupt Practices Act (see 15 USC 78) of the United States prohibits giving gifts (i.e., paying graft or bribes) by U.S. corporations even if such practice is legal and traditional in a country within which that U.S. corporation is doing business. Similarly, if the People's Republic of China produces clones of hardware and software that violate intellectual property laws of other countries but that are not viewed by China as a punishable offense, using such a product to permit processing between the United States and China would doubtlessly be viewed by U.S. authorities as unacceptable.

THE LONG VIEW
New technologies (e.g., Software Defined Digital Network [SDDN] and Frame Relay) will make networks increasingly intelligent, capable of enforcing complex compliance rules and allowing each enterprise to carefully craft the jurisdictions from which, through which, and into which its data will flow. North America, the European community, Japan, and similar “information-age” countries will see these technologies before the turn of the century. But many nations will not have these capabilities for decades.

Most jurisdictions will acquire the ability to detect cryptographic messages and process cleartext messages even before they acquire the networking technologies that would honor an enterprise’s routing requests. The result may be a long period of risk for those organizations determined to send and receive whatever data they deem necessary through whatever jurisdictions happen to provide the most expeditious routing.

The use of public key infrastructures (PKIs) and the reliance on certificate authorities (CAs) for electronic commerce will force many changes in international law. The jurisdictional location of a registration authority (RA), for example, may dictate whose personal data can be captured for registration. In a ruling by the EC Privacy Council early in 1999 with regard to IP addresses, it was determined that a static IP address constituted privacy-protected data, just as a name and mailing address would. The existence of a CA in a jurisdiction might constitute a nexus for an assertion of general jurisdiction or for taxation if the certificates signed by this CA are used for commercial purposes. Although this technology promises solutions to many problems — including restricting access to data on a selective basis that could bind jurisdictions — it also introduces rapid change and complexity with which societies (and legal systems) are already struggling.

SUMMARY
Data flows daily from jurisdiction to jurisdiction, with most organizations unaware of the obligations they may incur. As nations become more so-
phisticated in detecting data traffic transiting their borders, organizations will face more effective enforcement of laws, treaties, and regulations — ranging from privacy to state secrets, and from tax law to intellectual property rights. The risk of state-sponsored industrial espionage will also increase. Because organizations value the information transferred electronically, more and more organizations will turn to cryptography to protect their information. Cryptography, however, has import and export implications in many jurisdictions worldwide. The technology required to intelligently control the routing of communications is increasingly available, but will not solve the problems in the short term. Rather, the advancing technology will complicate matters further in two ways:

- where the controls become available, it will make indefensible their non-use
- where the controls are used, it will make the jurisdictions intentional, thereby strengthening the state’s case that it has jurisdiction

With more legal entities asserting jurisdiction, conflict of laws cases will increase. Implicit contracts will become extremely hazardous (e.g., an e-mail message might be sufficient to constitute a contract, but what are its default terms?). Ultimately, the need for effective commerce will prevail and jurisdictional issues will be resolved. But for the near term, jurisdictional issues in global transmissions remains a growth industry for legal professionals, politicians, lobbyists, tax accountants, and electronic commerce consultants.

Companies will need to exercise care when they place their data on open networks, the routings of which they cannot control. They will need to understand the jurisdictions in which and through which their global information infrastructure operates. The information security professional will want to have competent legal assistance on his or her team and to stay well-informed. The effectiveness of the enterprise’s information security program is now irreversibly intertwined with the jurisdictional issues of global electronic commerce.

Ralph Spencer Poore is an Area Practice Leader, Electronic Commerce, for Ernst & Young LLP.