INTERNET LAW FOR THE BUSINESS LAWYER

Second Edition

Juliet M. Moringiello
Editor

ABA
American Bar Association

Contents

CHAPTER 15

Commercial (B2B) Electronic Commerce Law

Phillip Schmandt

I. Introduction

This chapter addresses the negotiation of contracts governing the exchange of electronic commercial information between companies over the internet and the laws that should be taken into consideration when negotiating contracts governing those exchanges of information. Often this realm is referred to as "B2B" (business to business), to distinguish it from "B2C" (business to consumer) and "B2G" (business to government). This chapter also addresses some policy implications that should be considered as more and more commercial data is held in a digital form that allows for more dynamic and powerful manipulation, aggregation, or analysis of the data, and how anticipating possible regulation of such data may influence contract terms.[1]

Commercial information is most commonly transmitted over the internet when businesses exchange information electronically that previously was exchanged through mail, fax, phone, or value added networks (VANs) using dedicated phone lines. The electronic business documents addressed in this chapter span most of the purchase-to-pay cycle, including the following common examples:

- Documents relating to the selection of a vendor, such as electronic requests for proposals, or documents relating to prequalification or bid eligibility, such as electronically submitted safety, environmental compliance, or financial records;
- Documents relating to the decision to purchase individual products or services, including electronic catalogs or price sheets, sometimes with "punch through" capability that allow the purchaser to proceed immediately from the catalog to check out and purchase;

- Documents relating to ordering, purchasing, and invoicing, such as purchase order, order acknowledgements, invoice, and invoice acknowledgements, as well as intermediate documents such as change orders, shipping notices, and their respective acknowledgements.

This chapter does not address the electronic formation or transmission of the actual contract between trading partners. Nor does it address electronic payments or the exchange of commercial paper (checks, etc).

A. *Understanding the Business Drivers that Shape How B2B Electronic Document Systems Are Deployed*

Typically, a purchaser of goods and services will implement a system for the exchange of commercial electronic data and electronic business documents that the purchaser is prepared to send or receive electronically. The purchaser then asks its suppliers to utilize this system when communicating with the purchaser in connection with their sales to the purchaser.

While the most prominent aspect of these systems is their technological face (such as a specific platform, portal, or software program operated by the purchaser or its service provider), it is important to remember that each such technology carries with it unique business processes for both the sender and the receiver that transform how their respective business is conducted when compared to using paper or other means of exchanging data. Those business processes can relate to how the data is input, how internal approvals of the data are handled, how the data can be changed, how follow-up communications are made (do you log on to that platform to find messages or are they sent via e-mail), and how the data is used by or displayed to the recipient.[2] Transforming existing business processes to the demands of the new technology being used is often more challenging than installing the technology itself. When referring to such a system, this chapter refers to both the technology and the associated business processes.

There are several business reasons to implement such an electronic system. For example, the chief financial officer (CFO) may want to increase transparency within the company and centralize control of purchases by having all purchases of supplies flow through a single electronic system. By centralizing all purchases, the company can maximize its purchasing leverage and costs can be better tracked. There can be significant challenges to implementing a centralized business process and system when a global corporation has different computer systems and business processes all over the world. Nestle's motivation to increase centralized control over purchasing and the obstacles it faced in doing so were described by *The Economist* as follows:

> Nestle, for example, sells more than 100,000 products in 200 countries, using 550,000 suppliers, but it was not using its huge buying power effectively because its databases were a mess. On examination, it found that of its 9m records of vendors, customers and materials around half were obsolete or duplicated, and of the remainder about one-third were

> inaccurate or incomplete. The name of a vendor might be abbreviated in one record but spelled out in another, leading to double-counting.[3]

Alternatively, the motivation to exchange business documents electronically may be to reduce staff through automation and eliminate manual entry of data and the errors associated with manual processes. One source estimates that European firms implementing an electronic invoice processing system were reducing the cost of handling each invoice from 8.6 euros to 1.8 euros.[4]

Suppliers, meanwhile, may see an automated electronic invoicing system as a means to reduce the amount of time between product or service delivery and payment. Purchasers may also qualify more easily for early payment discounts by installing automated systems.

It is important for both the client and the lawyer to understand the motivation that is driving the business unit's desire to implement an electronic business document system, as it is that motivation that often informs the type of system selected. If transparency and central control are the motivators, then the CFO will be most interested in enlisting the participation of the largest suppliers, as that is where most of the money flows. On the other hand, if eliminating costs is the motivator, then the primary target may be on-boarding the smaller suppliers, whose handling cost per amount invoiced will invariably far exceed the largest suppliers.[5]

Typically, a purchaser selects the system it wants to adopt based on its own business needs. Those business needs and motivations often differ from the business needs or motivations of the supplier, which can often trigger the need for more formal negotiations to ensure both parties' needs are met. Often the purchaser makes the use of its selected electronic system mandatory for suppliers wishing to be eligible for future contracts or bids with the purchaser, which not only requires licensing and use of the specific technology, but also imposes new business processes tied to that new technology. That business reality can significantly impact the leverage of the parties in those negotiations.

B. The Role of Service Providers: A New Business and Legal Relationship

The electronic document system may be operated by the purchaser and installed within the purchaser's own computer systems behind its firewall, in which case the issues to be considered relate solely to changes brought to the relationship between the purchaser and the supplier through the new system and processes[6]. Alternatively, and more commonly, the new electronic system is controlled and operated by a third party, often referred to as a "hub," "electronic market place," "e-purchasing service provider," or a "network." This chapter uses the network or service provider nomenclature. When a network is involved and receives, transmits, uses, manipulates, stores, or holds the electronic data, then both the purchaser and the suppliers must consider a brand new relationship with this intermediary and the implications of a third party handling the electronic business documents and the electronic commercial information contained therein.

There are several hundred companies that offer a variety of services relating to handling and transmitting electronic commercial data. Most of them focus on one industry sector, such as shipping, aerospace, mining, or chemicals. Some of the larger companies offering these types of services span multiple industry sectors. Some examples of both sorts of companies include Ariba,[7] Quadrem (recently acquired by Ariba), Basware,[8] ADP (which acquired the company formerly known as Digital Oilfield),[9] and Xign (acquired by JP Morgan Chase).[10] The service provider marketplace is in flux and is likely to undergo considerable consolidation in coming years.[11]

This chapter is intended for a lawyer representing a company that wishes to implement such an electronic business data exchange process and to introduce it to that company's suppliers. It is also intended as a guide for the lawyer whose client has just received a letter from its most valuable customer informing the client it must implement this new process within 60 days or lose the customer. What legal issues should those lawyers alert their clients to?

Many of the principles discussed in this chapter will apply equally to "cloud computing" or software as a service (SaaS) offerings, where a company offers to receive, transmit, store, and make available via the internet information that traditionally has been stored behind a company's firewall.

II. Background: No Regulatory Framework Exists to Protect Commercial Data Akin to Personal Data, so Caveat Emptor Rules the Day

Most laws governing the protection of use of data on the internet relate to personally identifiable data of human beings. Very few laws govern commercial data transmitted over the internet or other electronic means. For example, of the data security and breach laws passed by all of the United States (Alabama, Kentucky, New Mexico, and South Dakota have no data security breach laws), Puerto Rico, and the Virgin Islands as of the date of this chapter, none of them govern commercial data.[12]

Similarly, the European Union's (EU's) 1995 data protection directive and the transposed member legislations are focused on data of personal individuals but not commercial data.[13] In 2012 the EU announced a plan to update the data protection directive, which is also focused on personal data of individuals.[14] Of course it is possible that electronic commercial business documents, particularly safety records and similar documents, may contain personally identifiable data of employees, in which case compliance with those laws is required. However, the bulk of electronic commercial documents do not and, except as noted, this chapter assumes that the electronic business documents are devoid of personally identifiable data.

Because the current legal framework governing electronic commercial data is so sparse, the guiding principle in this sphere remains caveat emptor. The

terms and conditions agreed to by the parties will govern most, if not all, the parameters for the use of that data and the delivery of the services. Those terms and conditions are typically in the form of a "click license" that an employee of the corporation must accept before being given access to the services. While the terms of these electronic contracts are examined in this chapter, the issues surrounding the formation of these contracts, including whether employees have authority to bind their employers to those contracts, is generally outside the scope of this chapter.[15]

The practitioner should expect that electronic ordering and invoicing systems will become increasingly common in the future. While it is difficult to determine accurately, it is commonly estimated in North America and Europe that roughly 20 percent of all companies use some form of electronic invoicing, but only 5 percent of invoices are sent using electronically structured data that can be automatically read (or "consumed") by a computer.[16]

A. *Understanding Unstructured versus Structured Data and the Business/Legal Implications*

When evaluating any estimates on percentage of invoices sent electronically, it is important to clarify what is understood as "electronic." Most agree that an invoiced e-mail in PDF or Word format is no more electronic than a faxed invoice, as those formats typically use unstructured data. Unstructured data is defined as: "an electronic format that cannot without prior interpretation (e.g., reading by a human being, scanning and/or optical character recognition) be automatically consumed by an external information system."[17] Examples of unstructured data include Adobe PDF, TIFF, JPEG images, or e-mails themselves. Unstructured data depends on a human eye to be read and must be reentered manually into the recipient's own accounting systems, therefore introducing additional labor and costs associated with the unstructured electronic document.

Electronic invoices using structured data, meanwhile, can be read by another computer system and can automatically be reflected in the recipient's own computer systems, without human intervention. The structured data is commonly formatted in Extensible Markup Language (XML). XML is a computer language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.[18]

Structured data depends on using a preagreed structure, format, and content standards for the exchange of data and therefore anticipates a greater degree of planning and cooperation between the trading partners. This means that the parties should anticipate allocating more resources to establishing the relationship between the trading partners than is the case with unstructured data and may require a separate agreement to address electronic messaging. However, in a 2010 study, Deutsche Bank concluded that it is the use of structured data that represents the tipping point for enterprises in achieving levels of automation that significantly impact the business and reduce costs.[19]

Not only can structured data be automatically consumed by and entered into the recipient's computer system, it can also be easily queried, organized, and

manipulated. It would take a clerk untold person-hours to sort through years of e-mailed invoices to determine the relationship between the deviations in widget prices over time and the total availability of a key widget component in a given region, but this information could be garnered nearly instantaneously from structured data. That is why unstructured data opens the possibility of much more extensive data mining—extracting valuable commercial information that reveals trends and correlations from massive amounts of collected data, while not revealing any piece of information that an individual trading partner could pinpoint as its own confidential information.

One analyst has described the promise of structured data as follows:

> The new data paradigm exemplifies information liquidity, where data as a service delivers market information from a platform and where the data is morphed between collaborating partners.[20]

While structured data brings the benefit of being consumed automatically by the recipient's computer systems, it also introduces the complexity of requiring one trading partner's computer system to talk to the other's. For example, a human reading an invoice can discern that "Five pounds of roofing nails" means the same thing as "nails, roofing, five lbs.," but alas a computer cannot. In order for the recipient's computer system to understand an invoice generated by the sender, their respective computer systems must either be identical (never or rarely) or some system must be introduced to transform the original electronic data into a new data set that can be read by the recipient's computer system. When both computer systems can read and consume the exchanged electronic documents using structured XML data, the trading parties are said to have an integrated connection.

That integrated connection forms not only a new business relationship, but a new legal relationship, as well.

III. The Legal Framework

Some of the key laws that should be considered when sending or storing commercial documents electronically and a brief summary of their implications are provided below:

Stored Wire and Electronic Communications and Transactional Records Act, aka the Electronic Communications Privacy Act (ECPA); 18 U.S.C. Section 2701 et. seq.—The ECPA prohibits the international interception of any wire, oral, or electronic communications and the international divulging of the content of any communications, except under limited circumstances (including at the request of law enforcement). The ECPA, which amended the Federal Wiretap Act, applies both to communications in transit and those held in electronic storage. Service providers will want to avoid allowing unauthorized access to information they hold to avoid potential violations of this law.

Economic Espionage Act of 1996 (EEA); 18 U.S.C. Section 1831 et. seq.—The EEA criminalizes the theft or misappropriation of a trade secret if made with the knowledge or intent that the theft will benefit a foreign power or injure the owner of the trade secret.

Gramm-Leach-Bliley Act (GLBA); 15 U.S.C. Sections 6801 - 6809—Among other changes, the GLBA created the "Financial Privacy Rule" and "Safeguards Rule" to protect consumers' nonpublic personal information. The Financial Privacy Rule requires financial institutions (which is broadly defined in the GLBA) to provide consumers with privacy policy notices on an annual basis and upon changes to the privacy policy. The Safeguards Rule requires financial institutions to maintain information security plans that will protect customer nonpublic personal information.

Health Insurance Portability and Accountability Act (HIPAA)—HIPAA created a "Privacy Rule" and a "Security Rule" to establish regulations for the use, disclosure, and protection of Protected Health Information (PHI). These rules apply to healthcare-related "covered entities" as described in HIPAA. HIPAA requires administrative, physical, and technical safeguards for protection of electronic PHI.

Sarbanes Oxley Act of 2002[21]—For public companies that are required to file assessments regarding the effectiveness of their internal control structure under Section 404 of the Sarbanes Oxley Act, they should understand and assess how the role of their service provider in handling transactions could impact the company's own internal controls. At least three items should be considered:

First, are there procedures in place to ensure all e-commerce transactions are initiated, recorded, processed, and stored in a manner consistent with Section 404.

Second, the filing company's Enterprise Security Program, covering physical, administrative, and security controls should include protections for its electronic data while it is held by the company and the service provider. That electronic data is a company asset and, therefore, the company needs to demonstrate how it protects that asset;

Third, if the network handles a "significant class" of transactions, then it should, at a minimum, provide clear and enforceable service-level agreements and the trading partner should have a designated individual for monitoring compliance with that service-level agreement. In addition, the public company customer of a network is likely to require the network to provide the form of audit mandated by the Public Company Accounting Oversight Board (PCAOB). That form of audit, formerly known as a "Type II SAS 70 Audit," has, since June 15, 2011, been governed by the "Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization."[22]

The cost for such an audit, and the control objectives for the audit, should be agreed on between the customer and the service provider in advance. The audit should cover a time period and be of such scope and result as to provide sufficient evidence to support a favorable assessment by the customer of its internal controls over financial reporting and its auditors' attestation and report for each fiscal year. In addition, the parties should agree on whether the

customer may view the entire audit or merely the certification regarding the audit, as many service providers view the results of the audit itself as confidential. Finally, the parties should address remediation in the event an audit reveals a material inadequacy or insufficiency and the timetable to implement a corrective action plan.

Antitrust Considerations—Any network handling data from competitors, and any customer sending data to that network, has to consider possible antitrust limitations on what can be done with that data and with whom it can be shared. In its 1996 *Statement of Antitrust Enforcement Policy in Health Care,* the Federal Trade Commission (FTC) allowed electronic marketplaces in the healthcare industry a "safe harbor" to distribute aggregated pricing data if the aggregated data met certain criteria, such as being more than three months old, aggregated by a neutral third party and aggregated with data from at least five sources with no individual source providing more than 20 percent of the collective market share.[23]

That analysis, however, was specified to the healthcare industry. Therefore, careful consideration should be given to determine what are likely safe-harbor parameters of other industries. Any such safe harbor, of course, relates only to past commercial date, as sharing planned future prices or similar date would not be permissible. In the FTC B2B Report issued in 2000, the FTC identified five considerations:[24]

1. Market structure
2. Who is sharing the information?
3. What type of information is being shared?
4. How old is the information?
5. How accessible is the information through other means?

The overall question to be answered is whether there a reasonable balancing of competitive concerns with potential consumer benefits regarding: the specificity of shared data, suppliers' access to the competitively sensitive data, freshness of the data, and data anonymity.[25]

These types of questions, unfortunately, do not lend themselves to clear, bright-line answers, which underlines the need for caution and care.

Electronic Signatures in Value-Added Tax (VAT) or Non-VAT Jurisdictions. Jurisdictions that impose a VAT invariably have unique and complicated regulations governing electronic invoices. This is to ensure that the taxpayer claiming a deduction based on the invoice can demonstrate that the invoice represents a legitimate expense. Most jurisdictions rely on a technological solution, such as an advanced electronic signature, to prove the authenticity of the origin (the sender is really who the invoice claims it is) and the integrity of the content (the content has not been altered) of the electronic invoice. In June 2011, the European Union amended its VAT Directive to allow member states to rely on "business controls" rather than any one technological solution.[26] The European member states have until January 1, 2013, to transpose the amended VAT Directive, at which time the full implications of the new requirements can be assessed.

Note that proving the integrity of the content of an electronic invoice is inevitably challenging if the electronic invoice must be converted from one format to another in order for it to be automatically consumed in both the sender's and the recipient's computer systems. When converting the format of an electronic invoice, by definition one must alter its content. Section IV Code of Practice for Electronic Invoicing in the European Union, adopted in February 2012 (discussed below) to implement the amended VAT Directive. calls on European member states to allow such a conversion and to permit the storage of only the converted invoice so long as there is a process to demonstrate the reliability of the conversion process.[27]

Jurisdictions without VAT tend to place significantly less emphasis on the need to electronically sign documents such as invoices, which are often not signed even in the paper world.

In the United States, to the extent one needs to demonstrate such documents have been signed, the practitioner should look to the federal E-Sign legislation or the applicable state's Uniform Electronic Transactions Act.[28]

IV. Negotiating Contracts with Trading Partners and Service Providers

In 1994, both the European Union and the American Bar Association approved a model form of agreement for trading partners who wish to exchange electronic documents using a format known the UN/CEFACT form of Electronic Data Interchange (EDI).[29] That form of agreement is a helpful starting point for any negotiations regarding the exchange of electronic documents. However, that agreement was crafted before the wide adoption of XML, which is a much more dynamic and rich form of electronic messaging than traditional EDI and therefore introduces more variability in the relationship and creates a greater need for data protection. One commentator has described data aggregation as something that will "radically alter the landscape."[30]

The emergence of XML and internet transmission has fundamentally changed the role of networks. In the past, third-party VANS that transmitted EDI data offered primarily "pipeline services," i.e., a conduit for transmitting data without opening or storing it. Today, networks offer a suite of additional services that may range from opening the "electronic envelope" and manipulating data in order to transmit it to the recipient to operating a portal where data is manually input by users so it may be displayed and analyzed by the network for the benefit of its customers. Networks may transform data from one XML protocol to the other or analyze the data to provide spend analysis or price validation.

With the network's greater control and access to data comes a greater need to reach an agreement on how the data may be used, who owns the data, and the confidentiality of data. In addition, the emergence of XML and internet transmissions has multiplied the number of networks, making it more difficult

to establish effective privity of contract between the networks and each party transmitting or receiving data. Whereas it was previously common to EDI for a buyer and supplier to each hire a single VAN to transmit and receive all their data, now buyers and suppliers may each engage several networks to perform different tasks in relation to data.

This Model Trading Partner agreement is between the two trading parties, but does not purport to govern the relationship between the trading partners and any network that may hold or manipulate the electronic messages.

In February 2012, the European Committee of Standardization (known by its French acronym CEN) approved a model form of interoperability agreement between two electronic invoicing service providers, each serving a different customer.[31] The Model Interoperability Agreement adopted by CEN addresses only the relationship between the two service providers and does not address either the relationship between the two trading partners or between the trading partners and their service providers.

At the same time as it approved the Model Interoperability Agreement, CEN also adopted a Code of Practice for Electronic Invoicing in the European Union.[32] The goal of the Code of Practice is to identify best practices that should be implemented by trading parties, service providers (networks), and public administrations that will promote the uptake of electronic invoicing.

These two model agreements and the Code of Practice provide a helpful framework for answering many of the questions that arise in the context of negotiating agreements relating to electronic documents. Other sample clauses are also provided below when none of the model documents address the issue.[33]

1. **Who owns the data?**[34] The agreement should clearly identify who owns the data covered by the agreement. As between the parties, the issue of who owns the data can be extremely delicate. The price at which a supplier sells and the price at which a buyer buys is likely to be seen by both the supplier and the buyer as a trade secret and neither will want to relinquish control of this information to the other.

The Model Trading Partner agreement does not address ownership of the data.

One possible resolution is co-ownership pursuant to a clause like the following:

> The Sender and Receiver who are parties to the Transaction are co-owners of, and jointly retain in common, all right, title and ownership in the Transaction and the Data, provided that each may use the Transaction and Data in accordance with this Agreement without accounting to the other.[35]

The Model Interoperability Agreement addresses ownership as follows:

> The Sender and Receiver, jointly or individually, as applicable, retain all rights, title and ownership in the Data and any works derived from the Data. All intellectual property rights associated with the Data, including trade secrets, are retained

> by the Sender and Receiver, except the limited license to use the Data in performing the Services.

It is not expected that networks would want to assume ownership of the data they transmit—and indeed they should be aligned with the trading partners in disclaiming such ownership, as otherwise defenses available to them under the Digital Millennium Copyright Act might not be available. It is helpful, therefore, to structure the relationship between the trading partner and the network as a license to use the electronic data, with the terms of the license clearly specifying when and how the data may be used.

2. **How can the network or service provider use the data?** If a third party, such as a service provider, has consent from either the sender or the recipient, the regulatory framework described above places no limits on its use of the transmitted data. Therefore, the terms of the contract with third-party service providers, not the law, will govern permitted uses of data transmitted over the internet.

The Model Interoperability Agreement strikes the following balance on the issue of how a network may use the data it transmits:

> Each Party[36] agrees not to sell or make commercial use of Data it handles, transmits or stores under this Agreement, except in furtherance of the Services as permitted by this Agreement.

The EU's Code of Practice instructs service providers that they must gain the consent of both trading parties if data is to be used for any purpose other than that contemplated in the agreements between the service provider and the trading partners:

> Service Providers must respect the confidentiality of the data they transmit or handle and must not use data except in furtherance of the services authorized by Customers. Any deviations from this must be agreed in advance with each of the Trading Parties.

Obviously, this means both the service provider and the customer should weigh carefully what uses are authorized in their agreement.

3. **What about confidentiality agreements?** The drafters of the Model Trading Partner agreement viewed EDI as another method of communication, and left confidentiality issues to be addressed by the trading parties under their general commercial agreement.

The Model Interoperability Agreement, which considers a third-party provider holding commercial information of the trading parties, does imposes a confidentiality obligation:

> The Parties undertake to keep confidential the content of the Agreement, the E-Invoices, Electronic Business Documents

> and Data, together with all technical, commercial or financial information relating to the other Party, its operations or its Customer that comes to their knowledge. The Parties may, however, disclose to their Customers in general terms that the Agreement exists and include the other Party in a list of entities with whom the Party has interoperability agreements. The Parties may disclose E-Invoices, Electronic Business Documents and their associated Data to such Party's Customer who is the sender or recipient of the E-Invoice or Electronic Business Document. The Parties undertake not to disclose the confidential information referred to above to a third party without a prior written consent from the other Party. If it is necessary for a Party to give its employees or advisers information that is subject to confidentiality, the information may not be disclosed to other persons than those for whom it is necessary to receive such information and who are bound by a confidentiality undertaking either by agreement or by law.

In the age of XML data and aggregated data, a traditional confidentiality agreement, whether in an ancillary commercial agreement or in an electronic data agreement, may no longer be sufficient. If the trading partners do not want their data included in analyses of price trends or similar information on an aggregated basis, they should explicitly address this as otherwise they may be subject to an interpretation that the confidentiality obligation has been observed as long as no information identifying the party or a single transaction of the party was disclosed. This is addressed in the Model Interoperability Agreement with the following explicit statement:

> The obligations of confidentiality and restrictions on use of Data in this Agreement apply to Data even if it is in anonymous or aggregated form and any works derived from the Data. Notwithstanding the foregoing, each Party may disclose aggregated Data based on all or substantially all of the transmissions it handles during a time period for the purpose of advertising the total volume of transactions or spending handled by its systems during that time period, so long as pricing or other competitively sensitive information of the Customers is not disclosed.

This language permits the network to advertise its total transaction volumes and spend during a specified time period, which is how networks often seek to differentiate themselves. However, it protects the trading partners as the network can only use the data for the purpose of performing the services it has been hired to perform for the trading partners.

One recent survey of sample provisions in the current marketplace governing how service providers may use the commercial data they handle found

that most service providers' terms and conditions allow almost unfettered use. Some examples include:

> *Service Provider may use the bidding information submitted by Suppliers in the course of Service Provider Sourcing Services projects to determine general price trends in various supply industries, to create predictive analyses useful for estimating likely market prices, and to evaluate suppliers appropriate for inclusion in future spend management projects in similar markets. Service Provider may also use such bidding information in the publication of "high level" sourcing project results, provided that such publication (i) does not directly or indirectly identify Supplier or Buyer by name or provide a third party with sufficient information to allow a third party to identify Supplier or Buyer, (ii) is aggregated with data from at least four (4) comparable suppliers from a single project, (iii) does not specifically identify Supplier's products or services, or the prices of those products or services, and (iv) does not identify Supplier as a participant of any specific project.*
>
> *Service Provider also retains the right to analyze, aggregate and report statistically sound summaries of the transactions flowing through the Marketplace.*
>
> *Service Provider will use anonymized information gleaned from registrations and from auctions conducted on our web site to provide better service to our customers. Service Provider may also analyze the information including performing a trend analysis to better serve its customers.*
>
> *In addition, Service Provider maintains the right to disseminate Data you send to Service Provider, so long as such Data is in an anonymous, aggregated form so as not to identify you.*[37]

Clauses such as these avoid the statutory framework for protection of commercial data described above as those statutes only come into play when there is unauthorized access to the commercial data. These clauses, of course, authorize such access.

4. **Who pays for the cost of integration?** The cost to establish an integrated connection can be a few thousand dollars or in the hundreds of thousands of dollars. Does the customer pay because it requested the connection or is this a new cost of doing business for the supplier? Even if the initial costs are agreed on, the parties need to address costs caused by future changes in computer systems or document requirements.

To gain an appreciation of some of the technical issues involved in creating an integrated connection, it may be helpful to review the 12-page technical appendix to the Model Interoperability Agreement, which lists some of the questions the two service providers both have to answer in order to create that connection.

The Model Trading Partner agreement addresses service provider fees with the general principle that each trading partner is responsible for any fees or costs assessed by its chosen service provider. This suggests that when the buyer selects the service provider and its suppliers are requested to use that same service provider, the suppliers should not be obligated to pay that service provider's fees.

The drafters of the Model Interoperability Agreement concluded that interoperability among networks will be enhanced if neither network charges another for the initial setup or integration, as the amount of those costs is highly dependent on how prepared each service provider is to establish a new interconnection and how that service provider has previously configured its own systems—something that each service provider is in a better position to control. The Model Interoperability Agreement provides as follows:

> Parties carry all their own costs including development and implementation of the interoperability Services as well as all on-going maintenance and other costs required during the use of the Interoperability Services.

5. **Transaction fees?** As of the date of this publication, the electronic commerce marketplace has not sufficiently matured to determine if it will adopt the internet service provider business model, where each customer pays only her selected network provider, or whether the networks will charge a connection fee to each other or the other's customer. Some networks operate on the basis of only the buyer pays, which makes it easier to attract suppliers. Other networks require both buyers and suppliers to pay, which spreads the costs and allows lower fees, but generates friction when a supplier is asked to pay for the network it did not select.

The issue of liability and limits of liability are naturally closely associated to the issue of fees. If a network operates on the model that only buyers pay, then those networks are likely to be unwilling to accept any liability vis a vis a nonpaying supplier. Nor will those networks offer guarantees of service availability or service-level agreements. If the supplier is itself a publicly traded company that must demonstrate compliance with Sarbanes Oxley, the prospect of sending financial transactions to an entity that will accept no liability for its mistakes in handling the data can be even more chilling than the prospect of paying fees to an entity it did not select. From the service provider's perspective, it would make no commercial sense to make a service available for low or no cost and then assume the risk of significant liability.

The Model Interoperability Agreement provides an option for service providers to charge each other a per-transaction fee. This compromise is expected

to work well when service providers using the same business model seek to interoperate. Service providers that charge only their buyer customers will likely choose not to charge each other an interoperability fee as they have no one to pass that charge through to. Meanwhile, service providers that charge both buyers and suppliers will likely assess a fee that each calculates it can pass through. The real difficulty will arise when service providers with differing business models seek to enter into an interoperability agreement. Time will tell how this plays out.

6. **What standards will you use?** The Code of Practice calls on service providers to "use and support royalty free standards for invoice content published by international standards organizations."[38] The Model Interoperability Agreement addresses the use of standards in three ways: First, the technical "Description of Services" Appendix allows the service providers to agree in advance on the standards to be used (this is similar to the Model Trading Partner Agreement). Second, the Model Trading Partner Agreement contains optional advisory language by which the service providers agree to "cooperate to maximize the use of open and freely available" standards for format and transmission protocols. Third, the Model Interoperability Agreement contains the following prohibition, which has the practical effect of requiring an integrated connection, which will likely use an open standard: "No Party shall require the other Party to manually enter Data or upload or download documents from its website or other location."[39] This emphasis on open standards seeks to avoid the scenario where individual trading parties are required to create or accept electronic business documents based on incompatible standards for multiple customers or suppliers—an outcome that would lead electronic invoicing to increase, not decrease, costs.

7. **What constitutes receipt?** Should you insist on acknowledgements? The parties should agree on what constitutes receipt of an electronic document and who, if anyone, will send an acknowledgement of that receipt. In this context it is helpful to differentiate among a "technical acknowledgement," which means that the document has been received by the party and meets the transmission protocol based on the agreed configuration; a "business response acknowledgement" which can provide a continuum of meanings, ranging from confirming the data has been properly formatted and meets the agreed syntactic requirements (i.e., fields requiring numeric values have numbers and not text); and a "substantive acknowledgement," which means the document has been reviewed and approved (we have received your invoice and it has been approved for payment). While a service provider may agree to send a technical acknowledgement, only the recipient trading partner should send a substantive acknowledgement.

This raises the question of how to apply the "mailbox" rule and when any contract periods that begin on receipt of a document should be commenced. If payment is due within 30 days of receipt of an invoice, when does that 30-day period begin? Does receipt by the electronic marketplace constitute receipt of the document? Does that change if the electronic marketplace serves as the outsourced accounts payable (or receivable) department of one party? The parties should also address if acknowledgements of receipt will be delivered, the impact of a failure to send acknowledgment, and who will pay for that transmission.

The Model Interoperability Agreement provides the following sample clause for receipt of electronic documents:

> The E-Invoices and Electronic Business Documents that are identified in the Description of Services are deemed to have been transferred to the Receiving Party when the Message containing an E-Invoice or Electronic Business Document is made available to the Receiving Party's system in accordance with the Description of Services and the Sending Party has received a Technical Acknowledgment of receipt. Prior to such receipt, responsibility for the E-Invoice or Electronic Business Document remains with the Sending Party.

8. **What security and transmission protocols will be used?** The parties should agree on a level of security for the transmissions and data storage. The FTC has recently issued security rules for financial data, which can serve as a guidepost even if your company is not subject to those requirements. They are posted at http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.

A fundamental question to be answered is whether the data should be encrypted either during transmission or while stored.

9. **What happens to electronic documents after termination of the agreement?** Both the service provider and the trading partners want clarity on what information is to be returned or deleted following termination of the contract and what information may be retained. For information that may be retained, there should be clear rules governing how and when that information may be used.

V. Conclusion and Some Policy Questions

Should similar protections afforded to personal data be afforded to commercial data? Because so little data being transmitted today is structured data, which can be easily manipulated and organized, there is little attention placed on this question. The era of electronic commercialized data remains in its infancy. But if 95 percent of an industrial sector's commercial transactions, such as automotive, healthcare, or mining, were accessible in structured electronic format, would society encourage or discourage allowing third parties unfettered access to such

data? The difference introduced by exchanging business documents containing structured data via a network is that when the network holds structured data of many competitors, it can assemble information previously kept secret and reveal dramatically different types of market trends, correlations, and information while never revealing any information identifiable to a single market participant.

If networks were to sell such data on an aggregated basis to reveal price trends or average prices, this could fundamentally change how business is conducted and what business information is available to direct the marketplace. On the one hand, this access could provide competitive benefits for consumers, as markets in virtually all products would become more transparent and more similar to markets for commodities, where average "live" prices could be accessed within moments. On the other hand, for markets for products that are not commodities, price signals could be highly misleading, as quality terms (warranty, terms and conditions, customer service, etc) may override price concerns. And more fundamentally, the trading partners that generate this data and consider it to be confidential trade secrets may object to that use, especially if their data is included in reports or analyses that benefit their competitors.

This line of inquiry leads to questions that are broader than the individual relationship between a trading partner and a network and could profoundly impact how some commercial markets operate: should networks that hold ever increasing volumes of commercial data be permitted to sell the data on an aggregated basis to interested parties, even if the trading parties involved consent? If four competing automakers use the same network to purchase key supplies from their suppliers, may the four competitors purchase data that allows them to track the average or median price being charged by their competitors? Is this not extremely likely to lead to monopsony power for buyers? May a fifth automaker who does not use that network purchase the same data as it related to the prices being charged to its four competitors? What of a hedge fund investigating the supply chain costs of all four of the automakers and wishing to compare them to the fifth automaker?

At some point, society will need to come to grips with the question of whether commercial information that is today discrete, private, and confidential may be made public and, if so, how the information may be used. Are the answers to these questions purely an issue of contract law or should the state impose minimum levels of protection to commercial data, as well as personal data?

Venture firms invested a total of $2.4 billion in 2011 in companies providing services related to "big data"—a buzz word that refers to the newfound ability to collect and analyze massive amounts of information. That compares to $1.5 billion in 2010 and $1.1 billion in 2009.[40]

As more companies move to the exchange of electronic data in structured format that can be more dynamically manipulated, and increasing amounts of commercially sensitive data is held "in the cloud," it is possible that government regulation will address how this data may be used. It is possible that just as we today have a body of consumer law to address transactions between parties with relatively unequal bargaining power and the general body of commercial law to address similar types of transactions involving actors with equal bargaining

power, there will emerge distinct laws protecting personally identifiable information (akin to consumer law) as well as separate laws protecting and governing commercial information (akin to general commercial law).

While general commercial law developed first and consumer law later emerged as its subset, in the context of electronic information, the law has developed first with respect to personally identifiable information and has yet to evolve with respect to electronic commercial law. In order to minimize the impact of possible regulation of electronic commercial law, today's contract negotiators would be wise to anticipate how self-regulation could protect them and seek to address as much as possible by contract so as to minimize the potential impact of future regulations.

Endnotes

1. Blogs or websites following this commercial area include http://purchasinginsight.com/, the e-invoice gateway, http://www.e-invoice-gateway.net/, Jason Busch's Spend Matters, http://www.spendmatters.com, and on LinkedIn, the e-invoicing platform, http://www.linkedin.com/groups/Einvoicing-Platform-online-electronic-invoicing-715727
2. The phenomenon of how each technology carries with it its own unique processes for businesses can be analogized to the unique processes associated with how individuals share their data in two common social media platforms, Facebook and Twitter. The methods for inputting a post on Facebook vary from the methods for "tweeting" on Twitter. There are different character limits, ways of adding attachments (photos), ways to receive responses, and ways of organizing the information to be captured later. All of these are controlled by the technology platform and the individual user has to adapt to those system requirements to participate. While those processes are more complex in the business world (for example, they involve financial or other competitively sensitive information that has already been organized in one manner by the business's own systems and they relate to departments of people working together perhaps globally versus a single individual), this analogy provides a glimpse into how reorganizing the business processes around the needs of a particular technology platform can be more challenging than installing the technology itself.
3. "The Data Deluge," The Economist, February 27, 2010.
4. http://www.ebrc.fi/kuvat/215-229.pdf
5. A very helpful overview of the practical considerations when implementing an electronic invoicing solution is provided in "E-Invoicing

Comes of Age—Discovering What's Possible From the Latest Electronic Invoicing/Invoicing Automation Capabilities," Spend Matters, 2011 Volume 2: P2P and Working Capital—Bridging Technology & Collaboration to Drive Savings and Cash.

6. It is important (but often difficult) to determine if an electronic data exchange system operated behind a purchaser's firewall is actually operated by the purchaser or if, in fact, it is operated by a third-party service provider that has access to that data and the purchaser's systems. If it is the latter, then the sender of the data should consider seeking protections regarding how that service provider can use, disclose, or combine such data as outlined in this chapter.
7. www.ariba.com
8. www.basware.com
9. *See e.g.*, http://www.openinvoice.com/
10. http://www.jpmorgan.com/tss/General/Order-to-Pay/1159317518404
11. A European association of companies providing electronic invoicing services, as of the date of this chapter, counts 39 members and continues to grow. http://www.eespa.eu/ See also "The Role of Interoperability in Creating an Efficient Global B2B Transaction Platform," David Evans, SSRN Working Paper November 2010, listing "an early critical mass" of 22 service providers in North America and Europe.
12. See: http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx
13. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT
14. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
15. See Christina Kunz, Click-through Agreements: Strategies for Avoiding Disputes on the Validity of Assent, 57 Bus. Law. 401 (Nov. 2001) and Browse-wrap Agreements: Validity of Implied Assent in Electronic Form Agreements, 59 Bus. Law. 279 (Nov. 2003).
16. See Deutsche Bank Research, May 3, 2010 "E-invoicing—Final step of an efficient invoicing process," The Institute of Financial Operations/IAPP issued a 2011 e-Invoicing survey report, which found: "in a 'typical month,' 59% percent of respondents suggested that 'fewer than 20%' of their invoices were 'fully electronic.'" 11.9 percent and 8.8 percent of respondents respectively reported 21 to 40 percent and 41 to 60 percent of their invoices were fully electronic. Only 2.7 percent of respondents reported that over 81 percent of their invoices were fully

electronic. http://www.dbresearch.de/PROD/DBR_INTERNET_DE-PROD/PROD0000000000257196.PDF

17. See Code of Practice for Electronic Invoicing for European Union and Glossary attached thereto, available at: ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA16463.pdf.

18. A portion of an XML invoice using the language format of the Petroleum Institute for Data Exchange (PIDX) may, for example, look something like this: -<pidx:Pricing> -<pidx:UnitPrice> <pidx:MonetaryAmount>9.35</pidx:MonetaryAmount> <pidx:UnitOfMeasureCode>EA</pidx:UnitOfMeasureCode> <pidx:CurrencyCode>USD</pidx:CurrencyCode> </pidx:UnitPrice> </pidx:Pricing> -<pidx:Tax> <pidx:TaxTypeCode>StateSalesTax</pidx:TaxTypeCode> <pidx:TaxExemptCode>NonExempt</pidx:TaxExemptCode> <pidx:TaxRate>6.25</pidx:TaxRate> -<pidx:TaxAmount> <pidx:MonetaryAmount>4.97</pidx:MonetaryAmount> <pidx:CurrencyCode>USD</pidx:CurrencyCode> </pidx:TaxAmount> </pidx:Tax> -<pidx:Tax> <pidx:TaxTypeCode>CountyParishSalesTax</pidx:TaxTypeCode> <pidx:TaxExemptCode>NonExempt</pidx:TaxExemptCode> <pidx:TaxRate>.5</pidx:TaxRate> -<pidx:TaxAmount> <pidx:MonetaryAmount>.4</pidx:MonetaryAmount> <pidx:CurrencyCode>USD</pidx:CurrencyCode> </pidx:TaxAmount> </pidx:Tax>

19. See Deutsche Bank Research, May 3, 2010 "E-invoicing—Final step of an efficient invoicing process." The benefits of electronic invoicing seem to be clear. But the lion's share of savings is not made by cutting printing or postage costs but by implementing efficient processes for receiving and dispatching invoices and integrating them with other business operations. Electronic invoices can be processed directly by the companies' other IT systems, thereby averting the costs and potential errors of transferring data across different media. http://www.dbresearch.de/PROD/DBR_INTERNET_DE-PROD/PROD0000000000257196.PDF

20. "How the Cloud Makes Financial Data More Liquid," Chris Lamb, www.readwritecloud.com (Oct. 23, 2011).

21. PUBLIC LAW 107 - 204 - SARBANES-OXLEY ACT OF 2002, http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html

22. *See* http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx

23. *See* Department of Justice and Federal Trade Commission "*Statements of Antitrust Enforcement Policy in Health Care,*" 2003, Statement 6, www.ftc.gov/reports/hlth3s.htm

24. See *Entering the 21st Century: Competition Policy in the World of B2B Electronic Marketplaces,* Federal Trade Commission, October 2000.

See also, *Antitrust Guidelines for Collaborating Among Competitors*, Department of Justice and Federal Trade Commission, April 2000. For antitrust considerations in the European Union, see "Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee, Enhancing Trust and Confidence in Business-to-Business Electronic Markets," COM 2004, 479. 20 July 2004 ("Another major concern is that participants or owners of B2B e-markets may distort competition, e.g., through bundling purchasing or selling power or by sharing sensitive business information. . . . The exchange of information on prices, participants, etc. in an oligopolistic market with only few players is more likely to raise competition concerns than in an e-market with many buyers and sellers." At 6.

25. *The Economics of Information Sharing and Competition,* Gregory S. Vistnes, ABA Section of Business Law, Presentation, April 17, 2009.

26. Directive 10858/10/EC amending Directive 2006/112/EC, adopted 23 June 2010 http://register.consilium.europa.eu/pdf/en/10/st10/st10858.en10.pdf

27. g) Section IV.g of the Code of Practice provides: "Public Administrations should allow conversion of electronic invoices to other formats, providing this has been done in a controlled process ensuring that the integrity of the content is not affected (i.e., the information required for VAT compliance purposes remain correct)".

28. The Electronic Signatures in Global and National Commerce Act, 15, U.S.C. ch. 96. For state adoption of the Uniform Electronic Transactions Act, see the helpful compilation by the National Conference of State Legislatures at http://www.ncsl.org/issues-research/telecom/uniform-electronic-transactions-acts.aspx

29. "The Commercial Use of Electronic Data Interchange: A Report and Model Trading Agreement," The Business Lawyer, Volume 45, Number S and European Commission Recommendation 1994/820/EC

30. "[A]ggregation tools will also play a role in this new world. The ability to aggregate date from radically different domains (not just different trading venues), the ability to combine structured and unstructured data, [and] the new dynamic portioning models will radically alter the landscape." "How the Cloud Makes Financial Data More Liquid," Chris Lamb, www.readwritecloud.com, October 23, 2011.

31. Pending official publication by CEN, available here: http://einvoicegw.evolaris.net/knowledgebase/ModelInteroperabilityAgreeme/

32. Pending official publication by CEN, available here: http://www.cen.eu/CEN/sectors/sectors/isss/activity/Pages/einvoicing_2.aspx

33. Organizations representing specific industry sectors have also developed model or suggested terms, which favor their individual members. *See e.g., Industry Standards for E-Marketplace Participation Agreements*

published by the National Association of Wholesale Distributors in August 2001 and *Good Trading Practices in Electronic Bidding Processes: Reverse Auctions* published by the Aluminum Foil Container Manufacturers Association.

34. This chapter does not address the question of whether or how data can be owned, but assumes it can be owned on one of the following bases: (1) as personal property ownership of the physical "bits" of electronic data,(2) as trade secrets to the extent the information qualifies under state law and the parties take measures to protect them as trade secrets, and (3) copyright to the extent copyrightable, or (4) database or similar compilation of information. For an interesting discussion of this topic relating to personal data and asking whether a writ of *replevin is available* to seek a return of electronic data, s*ee*, *Who Owns You Online,* PCMag.com, March 19, 2012, http://www.pcmag.com/article2/0,2817,2401771,00.asp

35. Because in common law, tenants in common have an obligation to account to each other for their use of the common property, it is important to disclaim this obligation in this context.

36. The "Parties" are the two networks or service providers signing the Interoperability Agreement.

37. *See* Comments to the FTC Privacy Roundtable, "The Need to Protect Commercial Data in B2B Exchanges," Schmandt, Garon, Lifshitz, Santos, and Stephan, February 22, 2010. http://www.ftc.gov/os/comments/privacyroundtable/544506-00093.pdf

38. Code of Practice, Section 111 (Trading Partners), Paragraph 3.

39. Model Interoperability Agreement, Section 5.6.

40. *Venture Capital Sees Big Return in Big Data*, Sarah McBride, Business and Financial News, ThomasReuters, February 17, 2012.