DELIVERING STRATEGIC SOLUTIONS ACCA'S 2000 ANNUAL MEETING

Session 511: Safe Sales in Cyberspace
Session Paper

Anita Smith, Shaw Pittman

This paper complements the Session Paper produced by my co-presenter Helena Haapio, "How to Avoid Becoming Entangled in the Web", and the article "Safe Sales in Cyberspace" authored by Helena Haapio and Anita Smith, which is included with this session pack and originally appeared in the July/August 2000 issue of the ACCA Docket.

Introduction

"Electronic business is about taking the Internet and adding two ingredients that are natural to capitalism: fear and greed." (David Smith, Internet Strategies Researcher at Gartner Group, November 1999)

The prospect of greater returns from a vastly increased customer base is a tremendous incentive to invest in an electronic trading system and commence or extend your company's cyberspace sales platform. The options for how you might proceed with this enterprise seem to be expanding on a daily basis. Evolving from the old catalogue style websites to more interactive, customer-driven sites and now to fully integrated electronic trading communities (ETCs) and electronic communications networks (ECNs), including industry-wide exchanges known as "Vertical Portals" or "Vortals". Software developers like Oracle, ARIBA and Commerce One have been at the forefront of developing "Engines of Commerce", which provide the platforms and applications - in essence, the tools - to create robust, functionally sophisticated B2B exchanges.

However the prospect of increased business opportunities must be tempered with the risks involved - the fear element, as it were. Ironically, there are risks associated with both doing business electronically and not doing business electronically. Selling in cyberspace involves facing a myriad of known and unknown commercial and legal risks, but not selling in cyberspace means you risk getting left behind.

The concept of Safe Sales has already been introduced in the accompanying article and was expanded on by my co-presenter, Ms. Haapio, in the first half of this session. To sum it up, Safe Sales in Cyberspace are all about sales with built-in quality assurance, risk management and preventive legal strategies. Whereas Ms. Haapio has concentrated on many of the essential elements of closing sales via the internet, I will be focusing on the legal risks associated with the overall operation of your website. In particular, I will be covering the following issues:

- Privacy and Data Protection
- Security
- Tax
- IP

Privacy and Data Protection

In July 1999 Sun Microsystems chief executive Scott McNealy made the shocking claim that "You have zero privacy now. Get over it."

His statement is true in the sense that advancements in technologies have enabled companies and governments to gather and analyze an ever increasing amount of personal data. However, the statement is incorrect in that there has been a notable increase in the regulation of privacy on a global basis, attempting to give back to citizens what technology has taken away.

Privacy is a concern to many customers as well as potential customers. By effectively addressing privacy concerns, you will not only be conforming to the law but also providing the necessary psychological comfort to those who consider privacy a critical issue. Unless your company conducts its transactions anonymously, which is quite difficult for anything other than digitally delivered services (because of the requirement of, among other things, a delivery address), you will need to collect information. Privacy laws and recommendations generally attach to personal data only, so corporate data that your company collects will not necessarily require the same level of privacy protection.

The concepts of privacy and data protection go hand in hand. If you accept that individuals have a right to privacy in relation to their personal data, as most countries now do, then there will need to be some kind of mechanism (both legal and technical) to protect that personal data.

The EU Data Protection Directive which came into force in October 1998 sets out eight 'Privacy Principles', which all EU Member States and countries transferring data through EU Member States must comply with.

The principles state that in relation to personal data:

1. processing must be fair and lawful;

2. collection must only be for one or more specified and lawful purposes;

3. the personal data must be adequate, relevant and not excessive with reference to the stated purpose;

4. data must be accurate and where necessary kept up to date;

5. retention must be finite;

6. processing must be in accordance with data subject rights as set out in the Directive;

7. technical and corporate measures must be implemented to ensure there is no unlawful or unauthorised processing and loss or destruction;

8. transfer outside the European Economic Area is not permitted to countries that do not ensure adequate level of protection for the rights and freedoms of data subjects.

In an effort to make the US a country considered 'adequate' for the purpose of principle number 8, the US and EU have put in place safe harbor provisions meaning that if US companies comply with certain requirements (correlating with the Privacy Principles) they will be considered 'safe' for the purpose of EU personal data transfers.

In the US, the Federal Trade Commission (FTC) has issued recommendations suggesting four principles that should, at a minimum, be included in privacy policies although there are no direct legal ramifications if these are not followed. The only direct remedy an individual would have against a US corporation is to sue them for breach of their own privacy policy.

The FTC principles cover: notice, choice, access and security in relation to personal data. If your company only does business within the US, fulfilling these principles would be sufficient, however we suggest implementing the EU level standards if any of your trading partners are ever likely to be located in the EU.

In general terms this means clearly stating and implementing your company's privacy policy, including obtaining each individual's specific, informed and unambiguous consent. Once your policy has been posted, it is imperative that it be followed. In the EU, each Member State has its own privacy commissioner that can bring actions against non-compliant companies, and in the United States the FTC can bring an action against any company acting contrary to their posted privacy policy. This has already happened to Geocities (www.geocities.com), which collected and distributed data contrary to its stated policy.

Questions to Ask

- How important is privacy to your customers/clients?
- Does your company transfer personal data between the EU and US?
- Does your company have a published privacy policy?
- Does your company's technical architecture support your privacy obligations?

Security

Security is a relative term. There are no forms of security that cannot be compromised, which means that developing effective security procedures involve managing rather than eliminating risk. Depending on the nature and type of business, different security measures may be considered necessary. Interestingly, the capacity to provide greater technological security has led security expectations to rise as well. Security measures that were considered normal in paper-based systems, are now no longer considered acceptable. At a minimum, your company should have enough security measures in place to comply with the requirements of the EU Data Protection Directive, particularly principle number 7 (that is, technical and corporate measures must be implemented to ensure there is no unlawful or unauthorised processing and loss or destruction). The question for your company is what level of security do you actually need and what are you willing to pay for.

There are various kinds of security that matter in the online context:

- physical security, for example security of the buildings where the servers are stored;

- network security, for example where passwords restrict users' access to certain data;

- Internet security, for example the use of firewalls to protect your LANs from infiltration via your company's Internet connection.

Each industry's security requirements differ. For example, a trading platform for a wholesaler of retail goods would likely be less security conscious than a financial institution or government departments - such as Defence or Social Security. However even companies in relatively low-risk industries should consider security implications, especially if they have developed any innovative e-commerce methodologies that could potentially give them a competitive advantage over other organisations in their sector. At a minimum, most companies will want to protect their proprietary and confidential information, including customer and product lists and methodologies for doing business.

Some of the solutions your company may wish to consider are encryption and digital signatures. Encryption is a process of transforming information into a form that is unintelligible by anyone who is not the intended recipient of the data. Encrypted data must be decrypted in order to be intelligible by the recipient. Some forms of encryption include the PGP (Pretty Good Privacy) standard and DES (Data Encryption Standard) for general data, or SET (Secure Electronic Transactions) for financial transfers. Note that there are laws governing the use of encryption technology, and these are frequently being updated as technology changes.

The most noteworthy change in encryption laws in recent times has been the liberalisation of US export restrictions to enable a broader range of encryption products to be exported from the US. If your company requires particularly strong encryption technology, it would be advisable to check on a state by state basis whether such use is lawful.

Whereas encryption technology addresses the problem of eavesdropping or interception by unauthorised parties, it does not address the issues of tampering and impersonation. Digital signatures should be used where it is necessary to guarantee the origin and integrity of a unit of data, and to protect against non-repudiation. Note that in most cases there are no legal requirements requiring the use of digital signatures, but there are laws in the US recognizing the validity of digital signatures as legal signatures for certain purposes, and the EU E-Commerce Directive also contains similar provisions.

Questions to ask

- What level of security does your company need?
- What kind of security can your company afford?
- Does your company use digital signatures?
- What type of encryption does your company need and is it subject to any export restrictions?

Tax

My colleague, Ms. Haapio, has already emphasized the importance of pricing in electronic payments. In particular, she has noted the importance of obtaining and providing accurate information. One aspect of accurate pricing information is the taxes involved. In traditional domestic sales, the buyer and the seller use the same currency, are familiar with the taxes and costs involved, as well as with how to proceed in case of non-payment. This may no longer be the case with your newly established world-wide Cyberspace sales.

Taxation issues can be particularly difficult in relation to online transactions, because the law is still developing. There are several international initiatives in progress relating to taxation issues, including an ambitious initiative by the OECD to standardise the global taxation system for e-commerce.

The ongoing debate as to which electronically delivered products should be considered goods, and which should be considered services, continues. This is an important question for determining which products are governed by the CISG, and also for determining which tax regime applies. The latest EU proposal to the WTO (World Trade Organization) proposes that goods delivered electronically should be considered services and thus fall under the auspices of the GATS (General Agreement on Trade in Services). Goods that are merely ordered electronically, but delivered physically will still be governed by the GATT (General Agreement on Tariffs and Trade). The impact of this taxonomy is important because goods are generally taxed at the purchaser's location and services at the location of the supplier of those services. Whereas it may be easy for posted items to escape the sales tax loop, it will be more difficult for electronically ordered heavy equipment to fall outside the tax regime of the buyer given that customs officers can simply refuse to release items from the docks if sales tax is not paid.

There has been general agreement world wide that e-commerce should be 'tax neutral', although even this basic principle has been challenged by some governments in recent months. The advocates of "tax neutrality" propound that there should be no additional taxes imposed on electronically ordered goods that do not already exist for the more traditional forms of trade. The tax position may change from time to time, and you should seek further advice from a tax expert if this is likely to make a significant impact on the way your company plans to deliver its products.

Questions to ask

- Is your company providing goods or services?
- Is your customer/client base narrow and identifiable or broad and diffuse?
- Which tax laws apply?
- Is your website robustly prepared for a tax audit?

Intellectual Property

1. Copyright

In theory, the content of your website is protected by copyright. In practice, this right is very difficult to enforce in the internet environment where an large number of copies can be made instantaneously, at virtually no cost. There are many people, such as the Electronic Frontier Foundation co-founder John Perry Barlow, who argue that traditional notions of copyright are outmoded in the age of digital copying. Some people actually contend that internet users have an implied license to copy information that companies and individuals have uploaded onto websites because those entities have made the information available in a manner and form that makes copying so easy.

How your company deals with its copyright considerations is a very particular matter. For example, it may be part of your strategy to give copyrighted information away for free as a way of promoting interest in other services that you provide. In any event it is good practice to at least consider including a copyright notice on the site so that users will know that you are asserting copyright in the content.

If your company is concerned about revenue dilution as a result of copyright "leakage" your company should consider alternative methods of protecting the content. For example, the site could be password protected for members or subscribers only. Gaining access to the site would therefore be contingent on those gaining access providing some kind of consideration in return. This could range from signing a formal agreement, to paying a membership or subscription fee, or simply providing certain information that your company would consider valuable (for example, contact details and product preferences.) There are also a range of copyright protection technologies such as watermarking, that can be used to technologically protect valuable content.

2. Trade Marks

Trade marks and service marks are valuable contributors to your company's brands and image. These are assets that you should protect, both on and off the internet. Their relationship with domain names has been described by Ms. Haapio in her Session Paper and presentation. In essence, it is not the case that just because you own the right to a Trade Mark in a particular country and sector, that you automatically have the right to the equivalent top level domain name (i.e. .com) or even the country-specific domain name (e.g. .au or .uk).

Another factor to consider is, if your website operates as a vertical market aggregating products from different suppliers to a particular industry, does your company have a license to use the Trade Marks and Service Marks of the companies whose products and services you sell? This is particularly important if your company is a start-up without a strong brand identity and you want to maximize the good-will associated with those brands that you are distributing.

3. Patents

Your company may wish to consider whether the computer programs you have developed and the business processes associated with your e-commerce initiatives might have the benefit of protection under patent laws. For many years there was considerable doubt over the whether computer programs and business processes could be patented, however a series of recent cases including State Street in the US seem to have opened the floodgates once and for all by upholding patents granted ostensibly to protect business processes and computer programs.

The position in Europe is not as clear as in the US, however it seems that both business processes and computer programs are increasingly being considered legitimate subjects of the patent process. The European Patent Office has issued specific advice on computer programs, but is yet to do so for business processes, in relation to which the position is slightly less clear.

You should note that if your company intends to patent any computer programs in both the EU and US, you should proceed first in Europe where there is no grace period during which an idea can be in the public domain. This means that if a patent is applied for in the US, and therefore enters the public domain, it is likely that the same patent would be rejected in Europe on the basis of not being novel. But conversely, if you obtain a patent in the EU, you have up to one year to obtain the same type of patent in the US.

In any event, any company seriously considering applying for patents in association with its e-commerce ventures should engage the services of a specialist patent agent who will be able to provide the kind of advice necessary to implement a successful patenting strategy on a global basis.

Questions to ask

- Does your website need a copyright notice?
- Does your content require any special copyright protection technologies?
- Does our company possess the necessary rights and licenses to include the information, including trademarks, displayed on it?
- Are any of your company's business processes or computer programs capable of being patented?
- Is the value of the business processes or computer programs sufficient to warrant the time and expense of patenting them?

Conclusion

"The wireless telegraph is not difficult to understand. The ordinary telegraph is like a very long cat. You pull the tail in New York, and it meows in Los Angeles. The wireless is the same, only without the cat." (Albert Einstein)

To paraphrase Albert Einstein, "cyberspace sales are not difficult to understand". If we step back and consider the salient legal issues that arise, they are usually not dissimilar to situations that arise in the normal course of business that is conducted internationally. Already we utilize emails, faxes, telephones and even EDI on a daily basis. Whether your company's cyberspace sales use a catalogue, auction, exchange or barter style of sales; whether your company operates alone or as part of a horizontally or vertically trading community; and whether your target market is concentrated in one or many jurisdictions, applying Safe Sales principles will help to build-in quality assurance and risk management into your processes.

This paper has outlined some of the strategic issues that your company should consider in addition to issues directly associated with closing sales in cyberspace. In each of the above sections, I have set out some of the key questions that you should be asking both internally and of your consultants that have been brought in to assist in developing your internet solution. But in addition to those questions, and core to your business strategy in general should be: What are my target jurisdictions? And which laws apply?

It is not an overstatement to say that an effective e-commerce strategy in your company may involve complete business process re-engineering, including re-evaluating the ways in which sales take place. There may even come a time when goods and services will merge into an ever more seamless continuum and business models will change radically to encompass entirely new paradigms. In the new era of e-commerce

there may not even be "sales" as we now know them, but ongoing relationships between companies where products and knowledge is exchanged and developed. In the meantime, following the steps outlined here and by Ms. Haapio should assist your company in making your transition to global B2B e-sales a safe and successful one.