Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Electronic Contracting In An Insecure World

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

ELECTRONIC CONTRACTING IN AN INSECURE WORLD

GIAC Legal Issues (GLEG)

SANS Legal Issues in Information Technology

and Information Security, LEG-523

Author: Craig S Wright

Craig.Wright@bdo.com.au

Adviser: Carlos Frederico Cid

Accepted : 14th Jan 2008

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Index

Abstract 3

An introduction to contractual formation 4

Issues with electronic contracting 6

What is an "Electronic Contract" 7

E-mail 9

The postal acceptance rule 11

World Wide Web 13

Invitation to treat, offers and acceptance 15

Electronic agency issues 18

Acceptance in unilateral contracts 19

Other issues in Contractual formation that impact offer and acceptance 19

Jurisdiction and communication of acceptance 20

What is an "Electronic Signature" 21

Issues with electronic contracting 25

Electronic Conveyancing 25

Risk 27

Other issues 29

Conclusion 30

Bibliography 32

Cases 35

Statues and Regulations 36

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Abstract

The rise of the Internet as a commercial tool has created a level of uncertainty surrounding the law of offer and acceptance.

The United Kingdom's "***Electronic Communications Act 2000***" endows electronic signatures with the force of law. This has been stated to represent the final piece of the puzzle (*McCarthy, 2002*) in creating an enforceable electronic contract in the UK.

However, the legislation alone may not ensure that there are no areas of uncertainty in electronic contract formation.

The paper covers the legal aspects of electronic contracts and the technologies that aid in the creation and preservation of these instruments and *the implications associated with online contractual dealings and the issues that have created these uncertainties. It closes by addressing the issues with digital signatures and repudiation concerning online transactions.*

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

An introduction to contractual formation

Technological developments and the advent of the Internet have led to new paradigms in international as well as local commercial activity. These changes have reduced the certainty of contractual negotiations leaving a commonly held belief that the law of offer and acceptance does not readily apply to such transactions when conducted online (*Rasch, 2006*).

Dealings and transactions that formulate or initiate contractual negotiations are not restricted to the written word. The law of offer and acceptance applies to new technology in the same way that applied to technological advances of the past. This paper explores the issues that have created uncertainty around contractual dealings. To do this, it is necessary both to look into the origins of contractual law and to investigate cases that will apply too and formulate the conditions necessary to create contractual certainty in commerce.

The increased use of international commercial transactions using the Internet is another concern. In the past, international commercial transactions were generally restricted to negotiations between commercial entities. The Internet has increased the scope of business to consumer dealings, and even consumer-to-consumer transactions across jurisdictional borders (*Department of Communications, Republic of South Africa, 1999*). For this reason, the formation of contract using the Internet creates segregation into two initial categories. These categories include both those negotiations that occur strictly within a single jurisdiction, and next, those negotiations that involve multiple legal jurisdictions.

Another concern focuses on the relationship of parties. Many Web based transaction engines act as third parties during the process of offer and acceptance. This interaction can complicate the formation of contract. Because of this, it is necessary to determine the legal standing of the third party (***Debenhams Retail***

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Plc v Customs and Excise Commissioners **[2004]**). The third party could be a party to the contract, an agent or one of the two contracting parties, or may just be an ancillary facilitator or medium, across which, and through whom the contractual bargaining occurs (*McKendrick [1], 2005, Pp163-164*).

Lord Steyn (In the *Forward* of Treitel, 1999) reminds us "*. . . it is wise for practitioners to bear in mind that the higher you go in the legal system the more important it is to concentrate on the footholds of the secure theoretical foundations.*"

Without legislation detailing the legal position of electronic contracts, the process of offer, acceptance and the terms of a contract created using the Internet will establish itself by means of the general law of contract. This will happen for the most part in the same manner as for the negotiation of terms of a contract in the physical world (*Lee, 2002, Pp 62-100*). Thus, establishing offer, acceptance and the terms of a contract remains the same whether the form is in writing, orally, or implied though the conduct of the parties in the same manner as existed prior to the rise of ecommerce over the Internet.

Next, in assessing whether the **Electronic Communications Act 2000** [ECA] (*Statutory Instrument 2000 No. 1798*) has alleviated uncertainty in the formation of an electronic contract, it is necessary to investigate both the definition of an electronic contract and to consider other supporting legislation. In itself, the ECA cannot ensure that there are no areas of uncertainty in the formation of an electronic contract. This paper will explore the effects of the ECA on contract formation within the UK looking in particular at its effect on contract formation and certainty.

In stating that the ECA has not removed all uncertainty from electronic contract formation, we need to explore two arguments. Firstly, subsequent legislation such as the **Electronic Signatures Regulations 2002** [ESR] (*Statutory Instrument 2002 No. 318*) has been introduced to assuage uncertainty surrounding technologies

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

such as digital signatures. By this argument, it logically must follow that if additional legislation was needed to improve on the ECA, that the law could buy itself not remove all uncertainty in electronic contract formation nor was it the "final piece of the jigsaw in creating an enforceable electronic contract".

Next, there is the alternative argument that contractual formation is inherently uncertain in and of itself (*Gamage & Kedem, 2006*). Being that electronic contracts form a logical subset of the contractual superset and that there is uncertainty within contract formation in general; it must naturally follow that there are areas of uncertainty, which will remain in the formation of electronic contracts, subsequent to the introduction of the ECA. The ECA, though having alleviated many difficulties facing the formation of electronic contracts, cannot in itself remove contractual uncertainty.

Issues with electronic contracting

The Internet is fundamentally a means of communication. Issues with law that have arisen because of the Internet are thus a result of the differences between communication in the physical world and communication using the Internet. Contractual negotiations are the result of a series of communications that create a legally binding agreement. For this reason, there is little difference between contracts made online than those formed through face-to-face communication. The facts surrounding the form of the communication are the primary difficulty.

At the most fundamental level, the existence of an offer and an acceptance is one of the primary requirements for the creation of a contract. The set of laws used to determine whether there has been a valid offer and an acceptance created across the Internet or a mere invitation to treat have their lineage in the case law concerning postal and telex communications.

It is important to remember is that the Internet is not a single communications channel. The Internet is a collection of

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

separate protocols used to communicate over the same physical connection. The result of this collection of protocols is that different legal issues will apply to the individual communication protocols. Protocols such as e-mail correspond to the process of sending a letter by post. A result of this is that we can match the physical world laws to the corresponding situations created by each of the individual Internet protocols. In this manner, we may see that the World Wide Web could be analogous to a mail order catalogue based purchasing system. The same principles govern the process of contractual creation whether or not the process is faster.

As an offeror may stipulate the method of acceptance (***Eliason v Henshaw [1819] & Manchester Diocesan Council for Education v Commercial and General Investments*** [1970]), it would be wise for parties to agree to the form of acceptance prior to the conclusion of the contractual negotiations.

A further important issue that surrounds Internet contracting is the general rule of law that, for an acceptance of an offer, it must be "communicated" to the offeror (*McKendrick [1], 2005; Pp43 – 44*). Under normal circumstances, the offeror must actually receive the acceptance before a contract will come into existence.

What is an "Electronic Contract"

When contrasting contractual principles, it is clear that where a contract is not required to be in writing (*Columbia Law Review, Apr., 1929 Pp. 497-504; Columbia Law Review, Jun., 1907, pp. 446-449; McKendrick, E, 2005, p 184*), that little additional uncertainty could be created where the contract is completed electronically. In fact, it is clear that electronic evidence must hold greater weight than verbal evidence (*Lord Justice Auld, Sept 2001, Cpt 11*). What is not clear is the extent of the weight attached to the various forms of electronic evidence. The strength of a digital signature algorithm and the security surrounding the mechanisms used to sign an electronic document

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

will respectively influence the weight associated with any piece of electronic evidence.

It has been argued that the digital contract may appear on the computer screen to consist of words in a written form but merely consist of a virtual representation (*Allison et al, 2003*). The ECA has removed the uncertainty and doubt surrounding the question as to the nature of electronic form used in the construction of a contract. In this, the ECA specifies that the electronic form of a contract is to be accepted as equivalent to a contract in writing.

An electronic contract has a twofold structure. Thought of electronically, the contract is a sequence of numbers and code saved to some electronic or magnetic medium. Alternatively, the contract becomes perceptible through a transformation of the numeric code when broadcast to a computer output device such as a printer or screen(*Bainbridge, 2000; Reed, 2004; Brownsword, 2000*). Prior to the passing of the ECA, this dichotomy exasperated the uncertainty contiguous with whether an electronic contract can be regarded as being a contract in writing.

The English legal doctrines of offer, acceptance and consideration when coupled with an intention to create legally binding relations define the necessary conditions for the creation of a contract. There is no necessity for the most part [*Excluding contracts such as for the transfer of real property, which are covered by a variety of specific acts*] that any contract be concluded in writing.

The question as to whether contracts performed electronically are legalistically equivalent to writing comes more to a question of evidential weight and the application of the parole evidence rule (*Durtschi, 2002; Lim, 2002*). By stating that electronic contracts are equivalent to writing, the ECA has in effect, forbid the introduction of extrinsic evidence which could change the terms of the electronic contract.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The question would remain as to a determination of whether the electronic communications contain the final agreement between the parties. Where some, though not all, of the terms are agreed in the electronic communication, a partial integration will result in the allowing of extrinsic evidence (*Treitel, 2003*).

The ECA did little to suppress the disputes surrounding the evidential weight attached to an electronic signature due to the receipt of a number of objections [Eg., *London Borough of Newham for the National Smart Card Project (2003)*] prior to the passing off the bill. Accordingly, when the Act was passed on 25 May 2000 its provisions as to the weight of electronic signatures did not meet the objectives of the ***EC Directive on Electronic Signatures*** and where less detailed. Section 7(1) provides:

> *'In any legal proceedings-*
>
> *(a) an electronic signature [176] incorporated into or logically associated with a particular electronic communication or particular electronic data, and*
>
> *(b) the certification [177] by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data.'*

E-mail

There are a number of contractual issues associated with e-mail. There are for example, numerous debates over the applicability of the postal rule. When sending an e-mail, there are several potential moments of acceptance. These are:

1. The first moment occurs when the e-mail departs the sender’s outbox controlled by the sender. In Internet-based e-mail transactions, the e-mail cannot be recall once it has left the sender's outbox. This is a situation analogous to the postal rule.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

2. The next is the instant of recept of the e-mail into the recipient's inbox. At this point, the e-mail is accessible to the recipient.
3. The next possible instant that could potentially be the moment of acceptance is when the recipient collects the e-mail from the mail server into the mail client's inbox. At this point, the recipient has received the e-mail.
4. Finally, there is an argument for defining the moment of acceptance as the point when the recipient has opened or read the e-mail.

The additional inclusion of features such as e-mail recall (in products such as Microsoft Outlook), read receipts and send receipts (in most e-mail servers and client) further obfuscate the moment that could be considered the time when acceptance was made.

E-mail is the digital equivalent of a letter sent through the post. All normal functions of postal mail transpire through e-mail. This includes not only the ability to send advertisements or invitations to treat (***Partridge v Crittenden*** [1968]), but also equally offers and acceptances.

It must be remembered that the "*question of whether the mailbox rule applies to e-mail is one that the courts have not yet answered. Its applicability seems to depend on whether e-mail is deemed to be more like instantaneous communication than like traditional mail services. Unlike real time chat e-mail, however, it is probably not instantaneous in the sense of this rule*." (*Cavazos & Morin, 1994*).

E-mail, maybe fast, but it is not instantaneous. Failed delivery, rerouting, damage in delivery or simply delayed all arise with E-mail. For this reason, e-mail, may be argued to most closely mirror a postal letter delivery.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The postal acceptance rule

The postal acceptance rule states that where an acceptance is to be sent by post, the contract associated with that acceptance is considered as concluded at the moment of posting the letter, not when the letter is received (or in fact if the letter is received). If the offeror does not wish to conclude, the contract through acceptance via the post, s/he may stipulate the form of acceptance. (The "*postal acceptance rule*" was introduced to present assurance to the "new" British penny post. It dates back to ***Adams v. Lindsell,*** 1 Barnewall and Alderson 681, In the King's Bench (1818); See also ***Household Fire Insurance Co v Grant*** [1879] 4 Ex D 216).

Lim (2004) points out that there have been at least "twelve theories or explanations offered for the postal acceptance rule". He further notes that two of these theories apply particularly well to Internet-based contractual transactions. The first theory hypothesises that the postal acceptance rule is applicable to Internet transactions as the communication proceeds through a third party. Next, an argument exists for the theory that the postal acceptance rule applies to e-mail, as it is a non-instantaneous means of communicating.

Contractual acceptance through e-mail remains unsettled by judicial review or decision. As such, there is still a high degree of uncertainty surrounding the issues of offer and acceptance related to the formation of contracts through e-mail based communication. In the US, this issue has been determined through statutory intervention (*Uniform Electronic Transactions Act, 1999; USA*). In the UK, the issue remains unclear even following the ECA.

In cases concerning international transactions, the *Sale of Goods (United Nations Convention) Act 1994* may be applied. This act overrides the concept of "postal acceptance" is and as an alternative presents the approach that acceptance "*will become effective at the moment the indication of consent reaches the*

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

offeror". In practice, the acceptance transpires at the instant that the communication arrives at the offeror's computer. While no decided cases on this point are available as guidance, the courts have traditionally been disinclined to extend the application of the postal acceptance rule.

Although telex, faxes and e-mail are separate technologies, they share many features. In both **Entores v. Miles Far East Corp (**[*1955] 2 QB 327*) and **Brinkibon Ltd v Stahag Stahl** (1983), the courts declined to extend the application of the postal acceptance rules.

Lord Wilberforce (***Brinkibon Ltd v Stahag Stahl*** *[1983]*) stated at 42, "*where the condition of simultaneity is met, and where it appears to be within the mutual intention of the parties that contractual exchanges should take place in this way, I think it a sound rule, but not necessarily a universal rule*". The issue of "read receipts" for e-mail could be an important factor in a future decision. Lord Fraser of Tullybelton (*at 43*) differs somewhat in his judgement from Lord Wilberforce, stating that:

> *"A party (the acceptor) who tries to send a message by telex can generally tell if his message has not been received on the other party's (the offeror's) machine, whereas the offeror, of course, will not know if an unsuccessful attempt has been made to send an acceptance to him. It is therefore convenient that the acceptor, being in the better position, should have the responsibility of ensuring that his message is received."*

From the above cases, we can see that technological differences such as the inclusion of read and sent receipts. Further, the arguable position of e-mail as to whether it is or is not "instantaneous" has created a level of uncertainty in contracting as "*the question of the applicability of the postal acceptance rule to e-mail acceptances has not been judicially settled.*" (*Lim, 2002, p66*).

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The postal acceptance rule as a generally consideration does not to apply to Web-based communications. This is because most Web-based systems employee mechanisms such as check-sums to maintain constant communication between the client and server systems. The constant verification this communication channel provides for the implication that communications take place though an immediate send process. Thus, both parties receive communications instantaneously.

The UK Government has not adopted the Model Law (*As contained in the Electronic Commerce (EC Directive) Regulations 2002, SI 2002/2013*), which would have put to rest the postal rule argument concerning email. The regulations do however unmistakably declare the point at which an order is legally supposed to be communicated. Regulation 11(2)(a) states that where businesses contract, *"the order and the acknowledgement of receipt will be deemed to be received when the parties to whom they are addressed are able to access them"*. Where contracts complete by email are concerned, the instant of completion would be the time when the email is presented to the person to whom it is addressed and not when the message is actually received by their email server.

World Wide Web

"*Click-wrap*" or "*click-through*" contracts are the most commonly formed Web-based contract (*Dunn, 2001; Durtschi et al., 2002*). These contracts may start with a Web-based advertisement (in invitation to treat) or some other collateral offer for consideration. These Web-based orders are generally included when the customer "clicks" and acceptance button (such as one labelled; "accept", "submit", "proceed to check out" or some other similar phrase).

This form of contractual negotiations is different from e-mail and deserves separate consideration. *"Click-wrap"* Internet contracts (*Reed, 2004*) have their own issues, but they still mirror many of the technologies that have preceded them.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

As the response to the offer or acceptance immediately displays on the customers Web browser, web based communications fulfil the requirements of an instantaneous transaction. There are some possible avenues of dispute with this analogy. For instance, what happens when a customer accept to finalise the transaction, but their Internet link drops before they receive the reply? To answer this question we need to look to the case of **Entores Ltd v Miles Far East Corporation [1955]**.

Lord Denning at 333[1] states the position of the law with regards to contracts conducted via telex: *"It is not until his message is received that the contract is complete…"*

From Lord Denning's analogy, we may see that a *"contract is only complete when the acceptance is received by the offeror: and the contract is made at the place where the acceptance is received."* (***Entores Ltd v Miles Far East Corporation*** *[1955]*). Thus, the contracting party's are under an equitable obligation to notify each other of any failure. In cases where communications have failed and one of the parties is left believing that the contract was successfully negotiated, the other party would be

[1] **Entores Ltd v Miles Far East Corporation**; Lord Denning at 333 *"Suppose a clerk in a London office taps out on the teleprinter an offer which is immediately recorded on a teleprinter in a Manchester office, and a clerk at that end taps out an acceptance. If the line goes dead in the middle of a sentence acceptance, the teleprinter motor will stop. There is obviously no contract. The clerk at Manchester must get through again and send his complete sentence. But it may happen that the wine is not go dead, yet the message does not get through to London. Thus, the clerk at Manchester may tap out his message of acceptance and it will not be recorded in London because the ink at the London end fails, or something of that kind. In that case, the Manchester clerk will not know of the failure but the London clerk will know of it and will immediately send back a message 'not receiving'. Then, when the fault is rectified, the Manchester clerk will repeat his message. Only then is there a contract. If he does not repeat it, there is no contract. It is not until his message is received that the contract is complete…"*

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

estopped from denying the contract if they had not taken reasonable steps to notify the other party of the failure.

In cases of where both of the contracting parties normally reside and contract within the European Union, additional statutory requirements apply. The electronic commerce regulations (*Statutory Instrument 2002 No. 2013*) as introduced by Parliament in the UK in 2002 override the postal rule in some instances and may require a separate acknowledgement through means such as e-mail for Web-based transactions. *Paragraph 11*, for instance states: *"the order and the acknowledgement of receipt will be deemed to be received when the parties to whom they are addressed are able to access them"*.

Although this directive does not change in the position of contracts negotiated solely by e-mail (Ibid, Para 9 (4) *"The requirements of paragraphs (1) and (2) above shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications."*), it does set the boundaries required for Web-based transactions.

Invitation to treat, offers and acceptance

A display of goods is as a rule an invitation to treat (***Pharmaceutical Society of Great Britain v. Boots Cash Chemists [1953]***). Further, there is a supporting rationale behind treating the display as an invitation to treat rather than as an offer (***Fisher v Bell*** [1961]). However, where a machine makes the display, the display is likely to construe an offer (***Thornton v Shoe Lane Parking*** [1971]).

This poses the difficult question of how to treat a Website. An advertisement is an invitation to treat and many web sites do little more than act as electronic billboards. At the other extreme there are organisations who deal online completely for all phases of the commercial process. These organisations may have no facilities to accept orders other than through the web site and use electronic agents to conduct negotiations.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

It is thus important to note that the facts of the individual case will have a large part to play in solving contractual issues involving the web. Partridge v Crittenden (**Partridge v Crittenden** [1968]) and Fisher v Bell (**Fisher v Bell** [1961]) demonstrate that not all advertisements satisfy the requirements to be an offer, but rather may just be an invitation to treat.

Carlill v Carbolic Smoke Ball Company [1893] conversely supported the decision that an advertisement was a unilateral offer where certain provisions applied. It is easy to see that the form of the contract will give rise to different results. It is not always clear if the "purchaser" is also the party making the offer, or the acceptance (***Daulia v Four Millbank Nominees Ltd*** [1978]).

From the above cases, we can see where much of the perceived inconsistency lies. The difficulty in determining the legal status of a web site is thus not the issue with the law, but with determining where the facts best match prior case law. It is not possible to group all web sites in the same proverbial basket. What needs to be decided initially is the actual status of the web site in legal terms. This, and thus the difficulty, is a matter of fact not law.

In an attempt to deal with the complexities that have appeared from the development of online consumer transactions, the ECC e-commerce law requires the supplier to issue a receipt for the order (*See Article 52 of the e-commerce law - the Electronic Commerce (EC Directive) Regulations 2002; commonly called the Electronic Commerce Regulations*). This receipt is generally issued by e-mail.

In a recent case, Argos (***Neumann, 2002;*** [*Argos Ltd, an online retailer based in the UK, received GBP 1 million worth of orders when it mis-priced Sony Nicam televisions in its online catalogue appearing to offer them for GBP 3 instead of the normal retail price of GBP 299*]) defended claims of a breach of contract based

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

on the terms and conditions set on their web site. Argos states that the e-mail is not an order confirmation or order acceptance. In this way, the company has to acknowledge the offer. Argos asserts that they only issue an invitation to treat. Thus, the customer makes the offer to the site.

Amazon.com[2] provides an example of this practice. Amazon has a page defining the terms and conditions associated with the site. Terms designed to protect the seller from entering into a unilateral offer consisting of an agreement that it did not intend to make link to the site for general download. This feature helps ensure that both parties understand the point at which the close of negotiations occurs and forms a binding contract.

A number of offer and acceptance issues that had not been completely resolved remain. In particular, the issue of online software downloads creates its own problems. For instance, does downloading the software constitute acceptance, installing the software, etc? Many software vendor licenses for instance state that the "*loading of the software onto a computer indicates your acceptance of the following terms...*" (E.g. Microsoft Office XP Installation license term[3]) The terms of the agreement are likely to be enforceable if the software company is able to demonstrate that the user had an opportunity to view the terms prior to installing the software.

The US case of ***Williams v America Online Inc*** demonstrates the difficulties that that may occur. In this case, Mr Williams started proceedings in Massachusetts stemming from a class action over the installation of AOL software. AOL asserted that the proceedings must commence in Virginia as the terms state Virginia was the exclusive jurisdiction or any claim. Mr Williams however argued that alterations to his computer came about before he

---

[2] http://www.amazon.co.uk/exec/obidos/tg/browse/-/1040616/026-9370677-1792435)

[3] http://www.microsoft.com/terms

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

agreed to the conditions. Mr Williams described the complicated process by which he had to "agree" to the conditions after the configuration of his computer had already occurred.

Further, Mr Williams demonstrated he was able to click, "I agree" without seeing the terms of service. This meant that the actual language of AOL's terms of service failed to display on the computer screen unless the customer specifically requested it, overriding the default settings.

The court rejected AOL's assertions and stated that:

> *"the fact the plaintiff may have agreed to an earlier terms of service for the fact that every AOL member enters into a form of terms of service agreement does not persuade me that plaintiff's ... have notice of the forum selection cause in the new terms of service before reconfiguration of their computers."*

Any terms of the contract not brought to the attention of the contracting parties (**Roscorla v Thomas** 1842) prior to the acceptance of the contract will be unenforceable. Thus, assurances or terms displayed after the completion of the contract (i.e. after clicking the “accept” button) will not be enforceable. These terms to be enforceable they would either need to be agreed prior to acceptance or the submitting party to the contract would need to give fresh consideration.

Electronic agency issues

The inclusion of electronic agents makes the traditional requirement for a "meeting of minds" more difficult to prove. With many smaller vendors, hosting and creating their own e-commerce enabled web site requires the interaction of a third party. Often, this involves the use of an external service provider, which offloads the Internet shopping trolley function. In this way, smaller vendors can create an e-commerce enabled site quickly and simply.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The issue, which arises in this instance, is in determining the contracting parties. Many small vendors provide little more than billboards style advertising through their web site. The complex task of maintaining the databases, transaction processing, and the shopping cart function becomes simplified when outsourced to another provider. In some instances, a redirection takes the customer to a completely new site or domain.

In such cases, it may be necessary to investigate whether a contractual arrangement has resulted between the client browsing a web site and the transaction agent or if indeed the transaction facilitator is a contractual agent for the Web store vendor (Lim, 2002). Agency has become a specialised area of contract law in itself. As such it will not be covered in any depth in this paper, though it is an area that does require due consideration and may influence the process of offer and acceptance.

Acceptance in unilateral contracts

A unilateral contract (similar to the one implied by the justices in ***Carlill v Carbolic Smoke Ball Company***) will likely result from extravagant boasts and claims made on an organisation’s website that involve some form of consideration. Where a company's web site makes claims about a product and the consumer acts upon those claims, the company may be bound to fulfil their promise.

Other issues in Contractual formation that impact offer and acceptance

The impersonal nature of the Web creates a few issues that may affect the process of offer and acceptance and invalidate a contract rendering it a void. One such issue would involve the age of the contractor. As the Internet is effectively unbounded, the age of the person entering into an electronic contract may be an issue. All incidents, if the person is under 18, any contract is

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

potentially unenforceable against that person. Further, jurisdictional requirements of age may vary.

The subject matter of a contract may render the acceptance invalid if the goods ordered breach regulations in a particular jurisdiction. Examples of this circumstance include both the nature of the goods or the age of the contracting parties.

Jurisdiction and communication of acceptance

The appropriate law of a contract is the system of domestic law that defines the obligations assumed by the parties to the contract. International law does not thoroughly define the requirement needed in a contract. The status is clearest where the parties have explicitly chosen the law that will apply in the contract. The parties may expressly choose the body of law, which will apply to all or part of their contract including offer and acceptance.

The UK requires that the parties must expressly choose to include the Hague Uniform law (*Art.3, s.1 (3) Uniform Laws on International Sales Act 1967*) [ULIS] in the contract terms before it applies to the sale of goods. This can if included have an impact on the process of offer and acceptance. Where there is knowledge of the residence or place of business of the contracting parties who each exist in a different state, several results arise in the case of a web site operation (for instance). Either "*the contract concerns the sale of goods which are to be carried from one state to another or the acts constituting offer and acceptance have been effected in different states or the goods are to be delivered to a state other than that where the acts constituting offer and acceptance have been effected*" (*Schu, 1997*).

Complications may occur if parties reside in a different state from where they hold their e-mail (***Hyde v Wrench*** *1840*) or other accounts (*Treitel, 2003*). Treitel (2003) further states that the communication of acceptance determines the time and place at which the contract is created. The general rule is that a contract

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

is formed at the time and place that the acceptance is received, unless accepted by post, in which case the contract is formed at the time and place of postal of the acceptance. In cases such as this, the location the e-mail is accessed becomes an issue and the time at which the acceptance is made are both critical points. The place where the user accesses their e-mail may affect the acceptance. In many jurisdictions, the time and place of receipt of a message derives from when it is available to the recipient (*Art.1335 Italian Civil Code; US: Restatement 2d of Contracts, S 56; Germany: case RGZ 144, 292*). In the case of e-mail, the time it is available to the recipient is when it arrives on the client's mail server. In this way, the timing and even validity of an offer and acceptance to a contract may come into dispute and may even come into effect in two or more places (***Apple Corps Limited v Apple Computer, Inc***. [2004]).

What is an "Electronic Signature"

Compliance with the EU Directive on Electronic Signatures (*Directive 1999/93/EC*) was accomplished by the UK parliament though the passing on the 8th March 2002 of the Electronic Signatures Regulations 2002. These regulations removed much of the uncertainty surrounding the existing provisions in UK law concerning electronic signatures including the ECA by putting into practice the concept of "*advanced electronic signatures*" (*S 2; Statutory Instrument 2002 No. 318*).

The designation of advanced electronic signatures was directly extracted from the EU Directive on Electronic Signatures (*Appendices I and II of the Directive are directly adopted in the Regulations*). In addition, Article 3 of the Regulations 'Supervision of Certificate Service Providers' implements the requirements of Article 3 of the Directive regarding the registering, recording, publishing, and supervision of CSP by the Secretary of State. Article 4 of the Regulations implements the Directive's Article 6 liability provisions on qualified CSPs. In

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

addition, strict data protection principles included in the Directive regarding CSPs are implemented in Regulations Article 5.

The basic provisions of the ECA regarding electronic signatures are thus expanded in the ESR, which has successfully implemented the EC's framework for digital signatures, and a developed PKI (Public Key Infrastructure) into UK law. The ***Electronic Signatures Regulations 2002*** defined a basic and an advanced electronic signature as follows:

Basic Electronic Signatures are defined broadly to include all types of electronic signature. They are defined in paragraph 2 of the Regulation as "*data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication*."

Advanced Electronic Signatures are defined as an advanced form of electronic signature, which are defined to meet the ensuing requirements as defined in the act:

1. *it is "uniquely linked to the signatory;*
2. *capable of identifying the signatory;*
3. *created using means that the signatory can maintain under his sole control; and*
4. *linked to the data to which it relates in such a manner that any subsequent change of that data is detectable. "*

It is envisioned that an advanced electronic signature will rely on the application of a personal digital certificate provided by a certification service provider ("CSP"). It is believed that this digital signature, supported by an eligible certificate issued by an accredited certification authority (CA) will provide for certainty and non-repudiation to a recipient allowing for the trust in the data integrity and authenticity of the sender's signature and message content.

A digitised electronic signature (which could be related to a electronically scanned image of a paper based signature) is not the same as a digital signature. A digital signature is associated with a unique numerical code and value. This code, when

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

associated with the correct cryptographic algorithm, allows one to verify the authenticity of the author of a digitally signed document with an extremely low probability of error (Lim, 2002); Reed, 2004); van de Graaf, 1987); Vaughan, 1997).

An electronic signature can include a printed name, an e-mail address, and a scanned signature. On the other hand, a digital signature itself is a unique numerical value based on the entire written document that is being signed. The ECA did not define electronic signatures in a manner consistent with ***Directive 1999/93/EC*** (*Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [OJ No. L13, 19.1.00, p. 12]*), which allowed an aspect of uncertainty.

In defining "*Electronic signatures and related certificates*" in s. 7 of the ECA, little clarity was expressed on the difference of a digitised electronic signature and how it is not the same as a digital certificate.

The ESR was passed to clear up the uncertainty surrounding this point and become compliant with the 1999 directive. This act has brought the UK legislation in line with the EC directive while helping to fix the eventual value of a digital certificate. This legislation has the effect of enabling the courts to treat the electronic signature as being equivalent to a manuscript signature. This directly mirrors the provisions of Art. 5(1) **Directive 1999/93/EC**, which grants that such signatures:

> *(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data; and*
>
> *(b) are admissible as evidence in legal proceedings.*

The distinction of "paper document" in (a) is significant. The legal notion of a manuscript or document is particularly extensive. It has been extended to books of accounts (Hill v. R.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

[1945] KB 329), photographs of headstones and houses (Lyell v. Kennedy (No 3) (1884) 27 Ch D 1), and diagrams and plans (Hayes v. Brown [1920] 1 KB 250; J. H. Tucker & Co.Ltd. v. Board Of Trade [1955] 2 All ER 522).

The definition of electronic signatures by the ESR in purely functional terms still will not allow the substitution of an electronically signed document for a manuscript involving a physical signing of the said document. The ***Electronic Communications Act 2000*** has the effect of ensuring that the UK courts treat electronic signatures as producing the same evidential effects as physical signatures (*Leroux, 2004*). This does not adapt the electronic manuscript into a signed physical writing (*Reed, 2000*).

Formal requirements, such as are required for the dispossession of real property, prevent certain transactions from being carried out through electronic communications. The uncertainty as to the formal requirements associated with digital contracting was corrected by the addition of further legislation in the introduction of the ***Land Registration Act 2002***.

It remains uncertain as to whether the courts will amend their characterization of individual signatures from that delineated by Denning LJ in *Goodman v. J Eban Ltd*. (***Goodman v J Eban Ltd*** *[1954] 1 QB 550;* Lord Evershed MR at 55 also supports this assessment. Denning LJ at 56 "*In modern English usage when a document is required to be "signed by" someone that means that he must write his name with his own hand upon it*.")

A certificated advanced electronic signature as defined by the ESR will likely show evidence of all features requisite in that case, excluding the prerequisite for handwriting. It will make obvious that the document has received the individual endorsement of the signing party. There remains the difficulty of deciding whether a personal signature is by nature of form or of function.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Issues with electronic contracting

Electronic networks such as the Internet are primarily communications channels. Although there is much uncertainty surrounding this form of communication, it should be remembered that there are fundamentally few real differences between new communication formats such as the Internet and older electronic measures such as phone lines. Just as in the past where a variety of different communication protocols could use a single carrier line such as a voice phone line (POTS or "*plain old telephone system*" was used for the carriage of telex, facsimile, data transfer and EDI based communications. See also, *Hallberg* (2005) P. 84), electronic mediums such as the Internet are a collection of protocols each with its own and oft separate issues.

The major uncertainty with electronic contracts stems from the facts of the individual dispute. Fundamentally; offer, acceptance and consideration to fill the requirements of creation of the contract. Being that the offeror may stipulate the method of acceptance (***Eliason v Henshaw*** (1819) & ***Manchester Diocesan Council for Education v Commercial and General Investments,*** 1970). it would be prudent for the contracting parties to agree to the form of acceptance prior to the conclusion of the contractual negotiations.

A further important issue that surrounds Internet contracting is the general rule of law that, for an acceptance of an offer, it must be "communicated" to the offeror (*McKendrick [1], 2005; Pp 43 – 44*). Under normal circumstances, the offeror must actually receive the acceptance before a contract will come into existence. Dispute as to form, which may be alleviated to some extent by the ECA, do little to define the instance of communication.

Electronic Conveyancing

The **Law of Property (Miscellaneous Provisions) Act** 1989 requires that contracts concerning real property to be in writing and signed by the parties or their authorised agents. The **Land**

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Registration Act 2002 [LRA] (*Statutory Instrument 2003 No. 2431, The Land Registration Act 2002 (Transitional Provisions) (No 2) Order 2003; which replaced the Land Registration Act 1925*) has introduced changes allowing the introduction of Electronic conveyancing. The act has made the introduction of electronic conveyancing system possible. It has created a framework designed to allow the creation of interest in registered land electronically. Chapter 8 of the act expressly deals with electronic conveyancing.

Section 91(1) provides that Chapter 8 would apply to a document in electronic form only if:

> *(a)the document effects a disposition falling within s 91(2); and*
>
> *(b) the conditions in s 91(3) are met.*

A disposition will fall within s 91(2) if it is:

> *(a) a disposition of a registered estate or charge, or*
>
> *(b) a disposition of an interest which is the subject of a notice in the register, or*
>
> *(c) a disposition which triggers the requirement of registration.*

The conditions in s 91(3) are as follows:

> *(a) the document makes provision for the time and date when it takes effect,*
>
> *(b) the document has the electronic signature of each person by whom it purports to be authenticated,*
>
> *(c) each electronic signature is certified, and*
>
> *(d) such other conditions as rules may provide are met.*

In addition, in s 91(10), The LRA is expressly linked to the ECA:

> *In this section, references to an electronic signature and to the certification of such a signature are to be read*

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

in accordance with section 7(2) and (3) of the Electronic Communications Act 2000 (c. 7).

It was clear that the ECA by itself did not adequately cover the provisions needed to ensure that contracts for the purchase and conveyancing of land could be completed electronically. As a result, s 91(4) of the Land Registration Act required the addition of provisions stating that a document satisfying the above requirements would be regarded as "*in writing and signed by each individual, and sealed by each corporation, whose electronic signature it has*" and that the document is also satisfy the role of performance creating a deed.

The parties to the deed need ensure that the electronic form states the time and date of effect as well as being signed using the electronic signature of both parties. Further, each electronic signature must be certified according to the land registration act. In this instance, the LRA effectively renders the electronic document to be in writing. The explanatory memorandum of the land registration act states, "*the section does not disapply the formal statutory or common law requirements relating to deeds and documents but deems compliance with them. When the section applies, the electronic document is therefore to be treated as being in writing, having been executed by each individual or corporation who has attached an electronic signature to it, and, where appropriate, as a deed*" [*LRA 91*].

Logically, it follows from the requirements to implement the LRA that the ECA alone was not able to mitigate uncertainty in the provisioning of electronic conveyancing in a satisfactorily manner. Again, this shows that although the ECA is a necessary step forward, it in itself was not capable of removing all uncertainty in electronic contracting.

Risk

To be held valid, a signature must:

- provide the identity of the party who signed the document;

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- demonstrate the intention to sign; and
- demonstrate a willingness to adopt the contents of the document as being the signatories own.

Signatures on paper fulfil these requirements through a variety of means. Identity can be ascertained using a forensic comparison of the signature on the manuscript with other signatures, which can be proved to have been created by the signatory. An intention to place ones mark is normally presumed as the performance of adding ones signature to a document is unanimously recognised as signing (***L'Estrange v. Graucob*** [1934] 2 KB 394, 403 per Scrutton LJ).

It is generally only possible to dispute intent to sign where this has been secured by means of a fraud. However, the party disputing the signature bears the burden of disproving the presupposition of an intended to sign. An intention to accept the terms of the agreement are likewise evident as it is common knowledge that the process of signing a document has that consequence. The burden of displacing this presumption is on the party disputing the signature (S***aunders v. Anglia Building Society*** *[1971] AC 1004*) in either case.

An electronic signature, in the form of a digital signature, may satisfy the functional requirements of the law of contracts. It must be noted that the signature itself does not afford sufficient proof of the signatory's identity. Further evidence is required which links the public key (or other method) used to the party. This could be proven though adducing additional extrinsic evidence such as is commonly employed when seeking to determine the identity associated with a signature on a manuscript (*van de Graaf, 1987*).

Extrinsic evidence necessary in the case of electronic signatures, the would need to include:

(a) That the signature key or its equivalent was in the possession of the alleged signatory or his authorised agent;

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(b) That the use of that signature key produces the electronic signature affixed to the document in question; and

(c) That the mathematical probability that some alternative key in the possession of a third party could have created the same signature is sufficiently low to convince the court that the signature was in fact affixed by the signatory. (van de Graaf, 1987).

In the case of the public key encryption systems discussed in part above, proof that the signature verifies successfully with the signatory's public key should be sufficient if that public key can reliably be attributed to the signatory.

In terms of electronic communication, it is not entirely clear how the unique materiality of a written signature can be addressed, nor is how the associating of a electronic communication with a originating author can be achieved given that there not an end of a material document to sign at. The functional counterpart of a "*paper signature*" may be achieved using an approved digital signature. It has been necessary to introduce additional legislation to the ECA in order to achieve these goals.

An electronic signature provides for the requirements of authenticity, intentionality, non-repudiation, and connecting the electronic communication with the signatory to that communication. Thus, the risk associated with a digital signature is similar to that of a paper signature. In each case, it is possible to adduce additional evidence to dispute the signature. Where an "*advanced electronic signature*" has been used, this would reduce the risk significantly.

Other issues

Hyde v Wrench (1840, 3 Beav 334) demonstrates that a counter-offer amounts to a rejection of the original offer. In contracts formed by email, it is essential to ensure that the contract has been concluded and not that a counter offer remains. ***Stevenson v***

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

McLean *(1880, 5 QBD 346)* shows us that a counter-offer should be distinguished from a mere request for information as occurs commonly in email requests.

Conclusion

To establish the formation of an electronic contract using the Internet, the general common law of contract and the doctrine of international law are legitimate. There is little fundamental difference in the process of offer and acceptance in the "real world" to the Internet. Whether conducted by writing, orally, or implied from the conduct of parties contractual negotiations are formed in a similar manner whether completed by telephone, face to face or over the Internet (using methods such as e-mail or the Web).

As with the introduction of all fundamentally new technologies, the Internet has created some level of uncertainty in contracting. However, an offer remains an expression of readiness to enter into a legally binding promise under agreed terms. An acceptance remains to be the willing act of accepting the offer with no further negotiations or dialogue.

True, the Internet has changed commerce, but the foundations of offer and acceptance in contract law remain firm, it is only the evidential requirements of fact that have changed.

The formation of electronic contracts subsists as a subset of all contractual formation. By their very nature and as it is expressed in a large number of contractual disputes which occur every year without dispute as to the content of the contract, contracts are uncertain. Thus it must logically follow that there will always remain a level of uncertainty in electronic contract formation. At best, if all uncertainty associated with the electronic nature of a contract was removed leaving no dispute between the natures of formation whether written, verbal or electronic; there remains room for uncertainty.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

To satisfy the incorporation of electronically signed documents into all the functional and formal requirements for signed writings in English law, additional steps to those in the ECA are necessary. To some extent, this has been achieved through the subsequent introduction of the LRA and ESR. To satisfy the implicit terms contained within the EU directive on electronic commerce (in reference to electronic contracts), further reform may be necessary. E***U Directive 2000/31/EC on Electronic Commerce*** (OJ L 178 p. 1, 17 July 2000, Art. 9(1) states:

> *"Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means."*

The bulk of the English law requirements for signed writings is associated with communications with public bodies (Reed, 2004). The result being that further reform of private legal dealings may naturally follow.

Although it is true to say that the ECA has reduced uncertainty in the formation of electronic contracts, it could not be said that no uncertainty remains.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Bibliography

1. Allison, Arthur; Currall, James; Moss, Michael & Stuart, Susan (2003) "*Digital Identity Matters*" University of Glasgow, UK (August 2003)
2. Bainbridge, D (2000) "Introduction to Computer Law" Longman/Pearson Education: Harlow
3. Beatson, J. (2002) "Anson's Law of Contract". 28th Edition, Oxford: Oxford University Press, UK
4. Beale, H.G., Bishop, W.D. & Furmston, M.P. (2001) "Contract, Cases and Materials". 4th Edition, London: Butterworths, UK
5. Brown, I. and A. (2005) "Chandler Blackstone's Q&A Law of Contract". 5th Edition, Oxford: Oxford University Press, UK
6. Brownsword, Roger, (2000) "Contract law : themes for the twenty-first century:, Butterworths
7. Cavazos, Edward A. & Morin, Gavino (1994) "When Acceptance Becomes Effective: The Mailbox Rule, The Mailbox Rule Revisited, The E-mailbox Rule?" in "Cyberspace and the Law", Chapter 3, MIT Press, USA
8. Department of Communications, Republic of South Africa (1999) "Discussion Paper on Electronic Commerce Policy" http://www.polity.org.za/html/govdocs/discuss/ecomm.html?rebookmark=1 (Viewed 14 July 2006)
9. Dunn, Gary (2001) "On-Line Contract Formation - Contracting Issues for Businesses on the Net", http://www.dunn.com/papers/paper_14.shtml (Viewed 15 July 2006)
10. Durtschi, Cindy; Hillison, William; Pacini, Carl (2002) "Web-Based Contracts: You Could Be Burned!" Journal of Corporate Accounting & Finance, Volume 13, Issue 5 , Pp 11 – 18.
11. Fischer, S & Hurley, A. (1995) "Trade and Commerce - International Trade", in Halsbury's Laws of Australia, Vol 27 Title 420.
12. Furmston, M.P. "Cheshire, Fifoot & Furmston's Law of Contract". London: Butterworths, UK
13. Gamage, David & Kedem, Allon (Nov, 2006), "*Commodification and Contract Formation: Placing the Consideration Doctrine on Stronger Foundations*", The University of Chicago Law Review [73:1299]
14. Gkoutzinis, Apostolos (2003) "Online Financial Services in the European Internal Market and the Implementation of the E-Commerce Directive in the UK" Queen Mary, University of London, 18th BILETA Conference: "Controlling Information in the Online Environment"

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

15. Hallberg, Bruce A. (2005) *"Networking: a Beginner's Guide*, 4/e" McGraw-Hill Professional USA (p. 84)

16. Lim, Yee Fen (2002) "Cyberspace Law, Commentaries and Materials", Oxford University Press UK

17. London Borough of Newham for the National Smart Card Project (2003); *"SMART; Security Isasues, National Smart Card Project"*; Report WP8 – 03 Version 3.0 December 2003

18. Lord Justice Auld (Sept 2001); *"A Review of the Criminal Courts of England and Wales"* http://www.criminal-courts-review.org.uk

19. Leroux, Olivier (2004) *"Legal admissibility of electronic evidence 1"*, International Review of Law, Computers & Technology; Volume 18, Number 2 / July 2004; Pp 193-220

20. Macdonald, E & Poyton, D (2000), *"A Particular Problem for E-Commerce: Section 3 of the Unfair Contract Terms Act 1977"*, WebJCL

21. McCarthy, Justin (2002) *"Consumer Protection in Contemporary Electronic Payment Systems:- A Familiar Wolf in Digital Clothing*?" Cork Law Review, [2002] C.O.L.R. II

22. McKendrick, Ewan (2005) "Contract Law" 6th Edition, Palgrave MacMillan Law Masters, UK [1]

23. McKendrick, Ewan (2005) "Contract: Text and Materials" 2nd Edition, Oxford: Oxford University Press, UK [2]

24. Neumann, Peter G. (2005) "Illustrative Risks to the Public in the Use of Computer Systems and Related Technology", SRI International EL243, Menlo Park CA

25. Poole, J. (2005) "Casebook on Contract Law" 7th edition, Oxford: Oxford University Press, UK

26. Rasch, Mark (2006) "E-mail privacy in the workplace"; Security Focus; http://www.securityfocus.com/comments/columns/412/33856/threaded#33856, (Viewed 02 August 2006)

27. Reed, Chris (2000), "*What is a Signature?*" Journal of Information, Law and Technology, Volume 2000, Number 1, 2000

28. Reed, Chris (2004) "Internet Law Text and Materials", 2nd Edition, Cambridge University Press, UK

29. Roe, Michael (1997) *"Cryptography and Evidence"*, A dissertation submitted for the degree of Doctor of Philosophy in the University of Cambridge

30. Schu, Reinhard (1997) "Consumer Protection and Private International Law in Internet Contracts" International Journal of Law and Information Technology (1997) 5 Int J L & IT 192.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

31. Smith, J.C. (2000) “Smith & Thomas: A Casebook on Contract”. 11th Edition, London: Sweet & Maxwell, UK

32. Stone, R. (2005) “The Modern Law of Contract” 6th Edition. London: Cavendish

33. Treitel, G.H. (1999) “The Law of Contract”. 10th Edition, London: Butterworths

34. Treitel, G.H. (2003) “The Law of Contract”. 11th Edition, London: Sweet & Maxwell

35. van de Graaf, J. & Peralta, R. (1987) “*A simple and secure way to show the validity of your public key*”. In Carl Pomerance, editor, Advances in Cryptology | CRYPTO '87, number 293 in Lecture Notes in Computer Science, pages 128 { 134. Springer-Verlag, 1987.

36. Vaughan, Jane; Sewards, Tanya & Kelso, Ross (1997) “The Law of Internet Commercial Transactions”, Centre for International Research on Communication and Information Technologies, Australia.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Cases

1. ***Adams v. Lindsell,*** 1 Barnewall and Alderson 681, In the King's Bench (1818)
2. ***Apple Corps Limited v Apple Computer, Inc***. [2004] EWHC 768
3. ***Brinkibon Ltd v Stahag Stahl*** (1983) 2 AC 34 (House of Lords, UK)
4. ***Carlill v Carbolic Smoke Ball Company*** [1893] 1 QB 256
5. ***Debenhams Retail Plc v Customs and Excise Commissioners*** [2004] EWHC 1540
6. ***Daulia v Four Millbank Nominees Ltd*** [1978] 2 All E R 557
7. ***Eliason v Henshaw,*** 17 US 225, 4 Wheat. 225 (1819)
8. ***Entores Ltd v Miles Far East Corporation*** [1955] 2 QB 327 (Court of Appeal, United Kingdom)
9. ***Fisher v Bell*** [1961] 1 QB 394
10. ***Goodman v J Eban Ltd*** [1954] 1 QB 550
11. ***Hayes v. Brown*** [1920] 1 KB 250
12. ***Hill v. R.*** [1945] KB 329
13. ***Household Fire Insurance Co v Grant*** [1879] 4 Ex D 216
14. ***Hyde v Wrench*** (1840) 3 Beav 334
15. ***J. H. Tucker & Co.Ltd. v. Board Of Trade*** [1955] 2 All ER 522
16. ***L'Estrange v. Graucob*** [1934] 2 KB 394, 403 per Scrutton LJ
17. ***Lyell v. Kennedy*** (No 3) (1884) 27 Ch D 1
18. ***Manchester Diocesan Council for Education v Commercial & General Investments*** [1970] 1 WLR 241
19. ***MARK WILLIAMS and another(1) vs. AMERICA ONLINE, INC***. 2001 WL 135825 (Mass. Super., February 8, 2001)
20. ***Partridge v Crittenden*** [1968] 2 All ER 421
21. ***Pharmaceutical Society of Great Britain v. Boots Cash Chemists*** (Southern) Ltd. [1953] 2 QB 795
22. **Roscorla v Thomas** (1842) 3 QB 234
23. ***Saunders v. Anglia Building Society*** [1971] AC 1004.
24. ***Stevenson v McLean*** (1880) 5 QBD 346
25. ***Thornton v Shoe Lane Parking*** [1971] 1 All ER 686

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Statues and Regulations

1. Art.1335 Italian Civil Code.
2. Germany: case RGZ 144, 292
3. **Directive 1999/93/EC** of the European Parliament and of the Council of 13 December 1999 on a **Community framework for electronic signatures**
4. **Directive 2000/31/EC** on Electronic Commerce OJ 2000 L 178/1 and Council Directive 94/44/EC on Ce**rtain Aspects of the Sale of Consumer Goods and Associated Guarantees** OJ I 171 7.7.99
5. Law of Property (Miscellaneous Provisions) Act 1989 (c. 34)
6. Resolution adopted by the General Assembly [on the report of the Sixth Committee (A/51/628)] 51/162 Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.
7. **Sale of Goods** (United Nations Convention) Act 1994
8. Statutory Instrument 2000 No. 1798 (C. 46) ELECTRONIC COMMUNICATIONS **Electronic Communications Act 2000** (Commencement No. 1) Order 2000; Electronic Communications Act 2000
9. Statutory Instrument 2002 No. 318; **The Electronic Signatures Regulations 2002**
10. Statutory Instrument 2003 No. 2431, **The Land Registration Act 2002** (Transitional Provisions) (No 2) Order 2003
11. **The Electronic Commerce Directive** (00/31/EC) and the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002 No. 2013). [Includes The Electronic Commerce Directive (00/31/EC) and the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002 No. 2013); On the 21 August 2002 the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002 No. 2013) transposed into UK law the majority of the provisions of the Electronic Commerce Directive (2000/31/EC)]
12. **Uniform Electronic Transactions Act**, 1999; USA
13. **UNCITRAL Model Law on Electronic Commerce** with Guide to Enactment (1996), with additional article 5 bis as adopted (United Nations Model Law on Electronic Commerce (1996))
14. **US: Restatement 2d of Contracts**, S 56 & The United States Framework for Global Electronic Commerce

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced