PAYMENTS PROVIDERS AND INTERMEDIARIES AS DEFINED IN THE LAW OF THE INTERNET.

.

Author: Craig S Wright

University registration number: 05028244

Index

Objectives.....3

Introduction.....4

Internet Intermediaries.....5

The postal acceptance rule.....6

Proposal summary.....10

Bibliography.....11

Cases.....12

Statues and Regulations.....13

Objectives

To consider look at the effects of legal liability as it pertains to Internet Intermediaries. Such examples would include defamation and copyright violations on ISP's where a subscriber has breached their legal obligations as well as the hosting of illicit materials (such as child porn).

In carrying out my project my aim is to:

1. Analyse English law as it relates to Internet Intermediary liability
2. Review the current cases
3. Consider the opinions of practitioners, academics, the Law Commission and the press/public
4. Analyse reforms/proposals for reform in other jurisdictions and the changes to the EU and the consequential effects that this will have on Internet Intermediaries.
5. Suggest how, if reform is needed, this should be effected
6. Detail the Impact of Internet Intermediary Liability across different groups and the economy

Introduction

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[1].

Having studied the following topics/subjects as a part of my Masters training, and coupled with my past work experience, I believe that the study of intermediary and payment provider liability is a topic that I could address well:

- Law of International Trade
- Commercial Law
- Competition Law
- E-Commerce Law
- International Trade Finance Law

The foremost dilemma with the study of electronic law is the complexity and difficulty in confining its study within simple parameters. Internet and e-commerce do not define a distinct area of law as with contract[2] and tort law. Electronic law crosses many legal disciplines, each of which can be studied individually. The range of areas of law that electronic, e-commerce, and Internet law touch upon is vast leading to uncertainty within Internet law and the extent to which this covers intermediaries.

The difficulties in transferring cash payments over large distances and between people who may have never met and may never meet has created a need for payment intermediaries in Internet transactions. Payment intermediaries provide both

[1] 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 . 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.

[2] 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. The **Electronic Communications Act 2000** [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

trust and some realistic means for a purchaser to transfer consideration to the seller reliably. For instance, if a buyer on an online auction site comes up with the highest bid incurring a debt, a payment intermediary would be involved in order to arrange a transfer of funds either from the purchases banking account or via some payment card system for finalising the transaction.

All of this adds to the risk of fraud requiring the intermediary to hold large quantities of personal information allowing them to identify and track the purchaser. Sellers are thus unable to engage in small transactions or micropayments due to the cost associated with managing losses from malfeasance and the system is required to protect personally identifiable information.

Internet Intermediaries

It was originally argued that widespread disintermediation[3] would occur over the Internet. It was originally believed that the Internet would provide a means to allow transacting parties to deal directly with each other. The opposite has occurred with additional layers being formed rather than removed. There are two primary reasons for this growth of intermediaries, the first is related to the need to connect to the Internet and the second derives from both trust and the availability of payment. In either case any transaction conducted over the Internet will not be in person. The consequence being that cash exchanges cannot occur, and the third-party will need to provide the trusted source of funds. The simple need to connect also derives from the distance that may be involved. When communicating across vast distances in small amounts of time and intermediary is always needed. In the past telecommunications carriers provided fax and phone services to satisfy this transaction. In effect what the Internet has done is to supplant fax, telephony, telex and electronic data interchange (EDI) with new and more universally accepted protocols. It would be rare to find any two parties with enough resources to construct and connect a global internetwork themselves.

The issue of trust surrounds payments creating opportunities for both payment and auction intermediaries. In a contemporary transaction for the sale of a product any

3.See, Shapiro, Andrew L., Digital Middlemen and the Architecture of Electronic Commerce, 24 OHIO N.U. L. REV. 795 (1998).

one individual would not be able to assemble the essential resources necessary to reach a global market. The growth of auction intermediaries such as eBay[4] has created the ability to offer products and services internationally creating global markets. The consequence is that intermediaries have created market segments that were not thought possible and did not previously exist curtailing the expected disintermediation of the Internet.

All of this has come with a cost. Many of the expected benefits of frictionless sales and the ability to relay information quickly and been lost as small payments are not available. Intermediaries have needed to implement systems to control security risks, account for fraud and credit card reversals and to maintain excessive levels of private information. This model only achieves privacy through the ability to restrict access to information between the parties involved and the payment intermediary.

In this privacy model, payment providers and intermediaries hold full information on the identity of individuals and other parties making transactions. Although the public is firewalls from viewing information associated with any transactions, both the intermediary and other counterparty such as the intermediaries providing risk services must all hold detailed information about the client or customer.

The postal acceptance rule and payments on the Internet

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).

[4] Ebay.com states its purpose to be "the world's online marketplace; a place for buyers and sellers to come together and trade almost anything!" (for a detailed description, see http://pages.ebay.com/help/newtoebay/questions/about-ebay.html).

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.

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.

In a similar manner to the web, a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a payment intermediary. This form of contractual negotiations is distinct 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. Thus far, payment intermediaries have been required a system such as DigiCash and EGold use intermediaries as a solution to the double spending problem.

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;

(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, 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 a limited value system such as

micropayments, digital signatures would be able to provide much of the solution but the cost of ensuring that intermediaries are covered against fraud and loss makes the use of micropayments infeasible in today's Internet.

The result of this is that commerce on the Internet has come to rely nearly exclusively on payment intermediaries with the associated costs and processing electronic payments. For the majority of day-to-day transactions, the system works well enough. The inherent weaknesses of the trust-based model come through the need to mitigate fraud and the associated economic costs that this creates. Micropayments would require the introduction of micropayments that are economically infeasible to mediate. To be of use, such a system would rely on either the buyer or the seller being willing to place trust in the other party to a level where they would prefer to walk away from a transaction than to dispute it. Mediation, arbitration and disputes that lead to court processes increase the friction of trade and increment transactional costs.

Micropayments and even small casual transactions are thus precluded from being used and as with cases theory of the firm, intermediaries grow into the size that is economically viable. Many economic solutions fail to be implemented or developed due to the transactional frictions that exist. At present, no mechanism exists to make payments over communication channel without a trusted payment intermediary.

Electronic payment systems including digital currency systems of the past have always required third-party interactions. Systems including Digicash and EGold have looked to incorporate system such as traitor tracing and methodologies to expose parties who engage in fraudulent transactions or double spending. Some early electronic systems would use a timestamp server created by announcing the hash of a contract or transaction using a USENET system or even publication in newspapers. This would prove the existence of data at a point in time but due to a lack of automation did little to limit the costs associated with micropayments.

Both Digicash and EGold required a central party that can check for the existence of double-spends. This trusted central authority. or mint, would validate transactions ensuring that double spends did not occur or, if they were to occur would engage in activities such as *traitor tracing* for the publishing of the malfeasance private key. Mint based models such as Digicash relied on banking systems that acted

as payment intermediaries. These intermediaries would act to decide on the ordering of payments and implement fraud measures similar to that involved in credit card companies. This need for a trusted intermediary removes the capability of these systems to engage in very small transactions.

It was originally believed[5] that digital cash or electronic money would be created or minted allowing for some type of universal credit and would facilitate Internet transactions. Although a few systems did emerge, the vast majority of transactions that occur across the Internet are made by means of traditional means such as credit cards.[6] Rather than digital cash being minted, a new type of payment intermediary developed. Peer to peer (P2P) payment systems,[7] such as PayPal, emerged allowing individuals to receive transactions directly[8], bypassing merchants and act as a means of consolidating payment methods by providing a mechanism to interact with various banks and payment card institutions directly.

Peer-to-peer processing networks have aided the growth of auction intermediaries such as eBay.[9] Payment card providers, P2P systems, and other entities that act as a mechanism to facilitate commercial transactions[10] also have the capability to stop illicit transactions and act as revelatory enforcement points. A commercial site distributing child pornography from Nigeria cannot be run profitably without an economical method of receiving consideration. If the site operators cannot reliably receive payment, they will quickly shut down. As the financial gatekeepers, payment intermediaries can be used to prevent illicit activity over the Internet. Either through proactive actions or upon the receipt of court orders and Internet payment intermediary could be used as an aid to curtail undesirable activities occurring across

---

5 Anderson et al. in their Dec 1997 presentation "*Exploring Digital Cash*" argued that digital cash would "*likely continue to evolve remarkably quickly*".

6 In 2002, roughly ninety percent of internet transactions used credit cards. Ronald J. Mann, *Regulating Internet Payment Intermediaries*, 82 TEXAS L. REV. 681, 681 (2004).

7 In this context, P2P stands for "person-to-person." The term is to be distinguished from the more common use of the same acronym to describe the peer-to-peer file sharing discussed in the context of piracy.

8 *See* Mann, at 683.

9 Id.

10 Because of the fluidity of payment mechanisms on the internet, there are a wide variety of service providers of various kinds (such as organisations like Checkfree, Cybernet & Authorize.net) that might or might not be regarded as intermediaries, depending on the circumstances. For purposes of this Essay, however, we focus on the dominant intermediaries like Visa, MasterCard, and PayPal.

the Internet. Unfortunately, we demonstrate that these new P2P systems suffer from the same costs and limitations of their predecessors and that these limitations add a minimum cost of any Internet transaction and stop the ability for payment processes to engage in small or micro transactions effectively.

Proposal summary

In this dissertation we will investigate the existing laws that apply to Internet intermediaries and the systems used by the financial gatekeepers to control malfeasance over the Internet. In this dissertation I shall seek to define the various intermediaries that define the foundations of the Internet. I will look at the existing remedies both in tort, contract and criminal laws and contrast this across the present liability schemes and sanctions that apply both in traditional and electronic arenas.

Although the Internet has changed the backdrop of the economy and society, it has not radically changed the nature of either civil or criminal transgressions. Rather it has added a layer of complexity through the speed and volumes of transactions that it has enabled. The issue for the law and society is not an introduction of new crimes or new transgressions, but an enhanced capability both to engage in these activities and also the increased capacity to find them. Here again another issue develops with the juxtaposition of security and privacy. The increased ability of the intermediaries to monitor and control our actions is directed by the need to protect personal liberty. The incorrect balance of these forces leading to either too little security and a possible finding of negligence (or worse) or the breach of controls designed to protect society and the possible criminal effects of these actions.

Further, the added layer of complexity has limited the possibilities for new forms of commerce that were promised at the birth of the Internet. The inability to offer micropayments has stifled the growth and development of new and novel technologies leading to the sale of privacy and personal information. Anonymity and leaky international boundaries impede the prosecution of the primary malfeasors. The malfeasors require payment intermediaries to process their transactions, and the requirements that are imposed on intermediaries to track and trace this form of risk has led to the collapse of the eCash payment system and the inability of pre-existing systems to provide micropayments services.

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) "C*ontract 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. 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)
9. 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.
10. Furmston, M.P. "*Cheshire, Fifoot & Furmston's Law of Contract*". London: Butterworths, UK
11. 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]
12. 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"
13. Hallberg, Bruce A. (2005) "*Networking: a Beginner's Guide*, 4/e" McGraw-Hill Professional USA (p. 84)
14. Lim, Yee Fen (2002) "*Cyberspace Law, Commentaries and Materials*", Oxford University Press UK
15. 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

16. Lord Justice Auld (Sept 2001); "*A Review of the Criminal Courts of England and Wales*" http://www.criminal-courts-review.org.uk
17. Leroux, Olivier (2004) "*Legal admissibility of electronic evidence 1*", International Review of Law, Computers & Technology; Volume 18, Number 2 / July 2004; Pp 193-220
18. Macdonald, E & Poyton, D (2000), *"A Particular Problem for E-Commerce: Section 3 of the Unfair Contract Terms Act 1977*", WebJCL
19. McKendrick, Ewan (2005) "*Contract Law*" 6th Edition, Palgrave MacMillan Law Masters, UK [1]
20. McKendrick, Ewan (2005) "*Contract: Text and Materials*" 2nd Edition, Oxford: Oxford University Press, UK [2]
21. Poole, J. (2005) "*Casebook on Contract Law*" 7th edition, Oxford: Oxford University Press, UK
22. Reed, Chris (2000), "*What is a Signature?*" Journal of Information, Law and Technology, Volume 2000, Number 1, 2000
23. Reed, Chris (2004) "*Internet Law Text and Materials*", 2nd Edition, Cambridge University Press, UK
24. Roe, Michael (1997) "*Cryptography and Evidence*", A dissertation submitted for the degree of Doctor of Philosophy in the University of Cambridge
25. Schu, Reinhard (1997) "C*onsumer Protection and Private International Law in Internet Contracts*" International Journal of Law and Information Technology (1997) 5 Int J L & IT 192.
26. Smith, J.C. (2000) "*Smith & Thomas: A Casebook on Contract*". 11th Edition, London: Sweet & Maxwell, UK
27. Stone, R. (2005) "*The Modern Law of Contract*" 6th Edition. London: Cavendish
28. Treitel, G.H. (2003) "*The Law of Contract*". 11th Edition, London: Sweet & Maxwell
29. 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.
30. Vaughan, Jane; Sewards, Tanya & Kelso, Ross (1997) "*The Law of Internet Commercial Transactions*", Centre for International Research on Communication and Information Technologies, Australia.

Cases

1. ***Adams v. Lindsell***, 1 Barnewall and Alderson 681, In the King's Bench (1818)
2. ***Brinkibon Ltd v Stahag Stahl*** (1983) 2 AC 34 (House of Lords, UK)
3. ***Eliason v Henshaw***, 17 US 225, 4 Wheat. 225 (1819)

4. ***Entores Ltd v Miles Far East Corporation*** [1955] 2 QB 327 (Court of Appeal, United Kingdom)
5. ***Goodman v J Eban Ltd*** [1954] 1 QB 550
6. ***Hayes v. Brown*** [1920] 1 KB 250
7. ***Hill v. R.*** [1945] KB 329
8. ***Household Fire Insurance Co v Grant*** [1879] 4 Ex D 216
9. ***Hyde v Wrench*** (1840) 3 Beav 334
10. ***J. H. Tucker & Co.Ltd. v. Board Of Trade*** [1955] 2 All ER 522
11. ***L'Estrange v. Graucob*** [1934] 2 KB 394, 403 per Scrutton LJ
12. ***Lyell v. Kennedy*** (No 3) (1884) 27 Ch D 1
13. ***Manchester Diocesan Council for Education v Commercial & General Investments*** [1970] 1 WLR 241
14. ***MARK WILLIAMS and another(1) vs. AMERICA ONLINE***, INC. 2001 WL 135825 (Mass. Super., February 8, 2001)
15. ***Saunders v. Anglia Building Society*** [1971] AC 1004.
16. ***Stevenson v McLean*** (1880) 5 QBD 346

Statues and Regulations

1. **Directive 1999/93/EC** of the European Parliament and of the Council of 13 December 1999 on a **Community framework for electronic signatures**
2. **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
3. Law of Property (Miscellaneous Provisions) Act 1989 (c. 34)
4. 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.
5. **Sale of Goods** (United Nations Convention) Act 1994
6. Statutory Instrument 2000 No. 1798 (C. 46) ELECTRONIC COMMUNICATIONS **Electronic Communications Act 2000** (Commencement No. 1) Order 2000; Electronic Communications Act 2000
7. Statutory Instrument 2002 No. 318; **The Electronic Signatures Regulations 2002**
8. Statutory Instrument 2003 No. 2431, **The Land Registration Act 2002** (Transitional Provisions) (No 2) Order 2003
9. **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)]

10. **Uniform Electronic Transactions Act**, 1999; USA
11. **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))
12. **US: Restatement 2d of Contracts**, S 56 & The United States Framework for Global Electronic Commerce