— Impersonation in Electronic Commerce —
“Legal Rules for Allocating Risks of Impersonation and Repudiation by Sellers in
Commercial Transactions on the Internet”

This thesis is submitted in partial fulfillment of
the requirements for the Honours degree of Bachelor of Laws in Monash University
Research Subject 512
(Course Code: LAW 5207),
Faculty of Law
Monash University
September 1998

By G. Brendan Macmillan
Abstract

"Should you be bound by your word even if you did not say it?"

Yes, according to the recipient-based liability of credit cards, provided that the word appeared to be yours from the recipient’s point of view. This is contradicted by a resounding No from the traditional view that you cannot be liable for impersonations.

The ability to rely on appearances is very attractive for internet commerce. Such commerce is electronic and takes place at a distance, where there is no physical presence and it is often difficult to authenticate the sender’s identity. Enabling recipients to rely on an appearance, without bearing the risk of impersonation, could be the key to the internet marketplace.

Internet commerce is potentially highly lucrative. The internet is faster, cheaper and further reaching than any other medium; it could overthrow the tyranny of distance once and for all, and open the world up for commerce even more than water-carriage ever did. But a lack of certainty and safety for recipients will stifle its growth. This thesis argues that recipient-based liability is possible, but only if each reliance on your word is registered - just as are your credit card transactions.

The internet: electronic, distant, broad

The internet is an electronic medium, far-reaching to many and distant points on the globe. This presents problems: the problem of electronic authentication at a distance is that personal contact and other means of authentication are generally not available. The breadth of the internet is a problem because many people may be deceived by an incorrect authentication: since the potential number of recipients may be in the millions or billions, this factor is not inconsequential.

Electronic Because the internet is electronic in nature, traditional tokens and paper-based methods of authentication are not available. A piece of paper cannot be transmitted digitally - only a representation of it can be. The same is true
of biological identifiers (such as fingerprints and handwritten signatures). In this
digital form, they lose their status as tokens and can only facilitate authentication
if they are kept secret.

However, the inappropriateness of tokens in an electronic medium largely has
been solved with encryption, which involves a secret encryption key. Addresses are
another means of authentication as a message sent to your address may be presumed
to have been received by you.

Chapter 2 discusses these authentication mechanisms of tokens, secrets and ad-
dresses in greater depth.

Distance  One of the great advantages of the internet is that distant locations can
be accessed (almost) as easily as those that are local. A serious problem with this
is that it becomes very difficult to authenticate the origin\(^1\) of messages. There is no
physical presence, and little in the way of surrounding circumstances; impersonation
is easy on the internet. Recipients would be reluctant to rely on such messages, thus
stifling commerce.

To combat this, there have been several proposals for recipients of an “electronic
signature” to rely on it completely, even if it turned out to have been sent by an im-
poser. One such proposal is article 13 of the UNCITRAL Model Law, the subject of
Chapter 4. This would be convenient and safe for recipients, who need only consider
the appearance of the signature, and not seek alternative means of identification.
This shifts the risk of impersonation from the recipient to the purported sender.

Broad  The internet is possibly the broadest means of communication that the
world has ever seen. It is global and instant. This makes it an “open environment”
in the sense that one may communicate with any number of people and contract
with each of them.

Unfortunately, this large number of potential recipients renders the above allo-
cation of risk infeasible.

Allocating Risks

“Should you be bound by your signature if you did not sign it?”

5Sender-based Liability Consider the traditional liability rule for signatures\(^2\) that
you are not liable for forgeries. If you signed then you are bound; but if you did not
sign, then you are not bound - it is based on your point of view. Even if the forgery

\(^1\)Chapter 1 argues that identification is essential for trust, which is essential for commerce,
though often the identification need only be that the party is the same as that to a previous course
of dealing, or that the person selling the gold is the same person who owns it.

\(^2\)We focus on the identification function of signatures; not as indicators of a special kind of as-
sent, nor their ritual, ceremonial or certainty roles. Note that in commerce, actual “identification”
is not always required: you want to be sure that the person selling you the gold is the same person
who owns that gold; but you do not necessarily care if that person is Joe Bloggs or John Smith.
is excellent and indistinguishable from your own, you are not bound, provided you can prove this. Although an excellent forgery might fool a handwriting expert and thus a court in its forensic examination, you can lead evidence beyond the signature itself to show that it must have been forged: you were in Peru on that day with two broken arms. Such evidence is of course not limited to what the recipient could have known at the time of receipt.

For example, a rogue impersonates me and purports to sell my gold to a third party. The third party pays for the gold and the rogue promises delivery under a contract of sale - in my name. However, by the forgery-rule, this contract does not bind me. The rogue is happy; the third party is unhappy; and I am sanguine.

The third party learns their lesson: they rely on a signature at their peril, and so are motivated to seek other indicia of authenticity. They take the decision of whether to rely on the signature or not, and also bear the risk of their being mistaken.

**Recipient-based liability**  Consider an alternative rule by which you are liable for forgeries. Such a rule would be attractive for the electronic transactions at a distance of the internet because it would provide certainty for recipients.

The scenario now plays out quite differently: the rogue again pretends to be me and enters a contract to sell my gold to a third party. This time, the third party knows that if the signature looks authentic at the time of signing, a court will uphold the contract and it will be enforceable against me - whether I was impersonated or not. The rogue again makes off with the money; but when the third party seeks to enforce the contract against me and I complain that I was impersonated, the court replies:

> “We don’t care if you didn’t sign it. We don’t care if you were in Peru with your arms broken. We don’t care if it _was_ a forgery. It appears to be your signature; you are liable”.

The rogue is happy. The third party is happy. I am unhappy.

What can I do about this situation? I could make my signature more difficult to forge, using very complex and intricate sworls, be trained by a hand-writing expert, and use a quill pen so that each change in pressure of my hand is registered on the paper. I could make it very difficult to forge. And let us assume that I could say to the world that my signature is not to be relied upon over the value of $50. Now, a rogue comes along and thinks: “It’ll take me weeks just to learn this guy’s signature. A lot of work! And for a measly $50? It’s just not worth it!” By making the signature more difficult to forge, and by reducing the rewards, it seems we can make forgery a non-issue.

Assuming it is my responsibility to make my signature difficult to forge, I am arguably at fault if a rogue does forge it, because I must not have gone to enough trouble. Recipient-based liability may begin to seem reasonable. However, these rules apply in an _open environment_, where the signature is good to the whole world. A rogue impersonating me could enter a transaction with one person for $50, and
with someone else for another $50, and with every person in the country or in the world. The total liability might be $50 million or $50 billion. It is difficult to determine just what the potential liability would be, but it could be large: the rogue reconsiders, and decides that $50 billion is worth a few week’s work after all.

What could I do in the light of this crushing liability? I could make my signature even harder to forge, so that it is so difficult that it is not worth the trouble for even $50 billion. It is hard to imagine a signature that is that difficult to forge. It comes down to a question of balancing the difficulty of impersonation against the potential reward to a rogue; and that the breadth of the internet multiplies this reward to many time larger than it might at first appear to be. The adequacy of security must be weighed against not just the probability of failure; but also the consequences.

And that is my first point: that recipient-based liability rules cannot work in an open environment – without something more.

**Existing recipient-based liability** An extraordinary but necessary incident of this recipient-based approach is that the recipient could sometimes be able to rely on a message that only *appeared* to originate from the sender, despite a court finding in reality that it did not so originate. That is, the sender could be held to their signature *even though they did not sign it*. But this extraordinary result is not without precedent.

An EFTPOS card is an example of such a recipient-based scheme: withdrawal or payments by a rogue in possession of the card and PIN are deemed to be from the owner\(^3\); in that the owner’s bank account is debited, and the owner has no right as against the bank to reverse the transaction\(^4\). Evidence that the transaction was not entered into by the owner of the card is to no avail.

This thesis argues that the only way for a recipient-based scheme to be workable is for liability to be limited in some way, just as it is with credit cards and EFTPOS cards. Such *loss limitation devices* are discussed in section 3.2. Limitation of actual losses allows a party’s legal liability to be limited - but without it, such reallocation is merely an exercise in rearranging deckchairs.

It is argued that one reason for the forgery rule for signatures is because they also operate in an open environment. Without such a rule, an imposter could bind you to any number of contracts.

**Registration of reliance**

The problem of recipient-based liability is the open environment. It is possible to provide recipients with the convenience and certainty of a pin-point of identification,

\(^3\)Other rules contained in the EFT Code of Conduct soften this basic allocation of risk, having regard to whether the card was reported as stolen and so on; but the basic rule may be construed as stated.

\(^4\)Of course, the owner has a cause of action as against the rogue; but in practice this is not very helpful, as the rogue usually is long gone.
simply by closing the environment. This may be done by reducing the number of potential recipients - as in EDI\(^5\) - or it may be done using registration.

The idea of registration is to prevent multiple (or overlapping) reliances. It is an old idea that is reused again and again in various legal regimes, such as in credit card transactions and the Torrens land system. The paramount purpose of these systems is that registration reflects the true state of affairs, so that the register may be relied upon as accurate by other parties, thus providing a single point of information whose appearance reflects reality. This provides convenience and certainty for recipients. Without a registration system, multiple-selling of land \(^6\) or multiple-spending of money is possible; for identification on the internet, it is the generalised danger of multiple-reliances.

**Conclusion**

Chapter 5 brings together the ideas discussed throughout the thesis to form a principled basis for allocating risks of impersonation in internet commerce.

---

\(^5\)Electronic Data Interchange - where two parties agree to exchange data electronically. Typically, this data comprise orders that are legally enforceable. For example, a large department store may automate its inventory control, so that orders are automatically placed with supplies when stocks levels fall beneath a threshold.

\(^6\)or of overlapping interests, such as multiple mortgages etc
Acknowledgments

I would like to thank Mark Sneddon for asking exactly the right questions (it has taken me over two years, but I think I may have finally answered them), Nicholas Pengelley for his sage advice and rather astonishing ability to conjure up research articles, Shane Brunning, Sky Christensen, Michael Wilkinson for heroic stamina through extended discussions, Michael Attipa for an insight that caused me a lot of thought, Chris Betts and Tony Jansen for their embarrassingly perceptive commentary, advice and proofreading, Ian Macmillan for his challenging questions and warm encouragement and the many, many with whom I have discussed the ideas in this thesis, including (in no particular order) Jamie Scuglia, Lloyd Allison, Bruce Dyer, Chris Wallace, Rob Rendell, Jane Brion, Prof. McCredie, Jeff Goldsworthy, Jeannie Paterson, Elizabeth Lanyon, John Glover and Jaqui Lipton.

I gratefully acknowledge Melissa de Zwart’s supervision of this thesis and I also wish to thank the Faculty of Law and the Department of Computer Science and Software Engineering of Monash University, which have facilitated this thesis in many ways, and whose academics, staff and students have made available their intellectual power to this quest; indeed, several of the above persons are members of these bodies.
Contents

1 Electronic Commerce .................................................. 1
  1.1 The Internet .................................................. 1
  1.2 The Necessity of Trust ......................................... 2
  1.3 The Origin of Trust ........................................... 3
  1.4 Identification ................................................. 4
  1.5 Authentication Risks ........................................... 5

2 Authentication Technology ........................................ 7
  2.1 Tokens .......................................................... 8
    2.1.1 Imprints .................................................. 8
    2.1.2 Biometrics ................................................. 9
    2.1.3 Tokens cf Information ................................... 10
  2.2 Secrets ........................................................ 11
    2.2.1 Choice .................................................... 12
    2.2.2 Transmission ............................................. 12
    2.2.3 Encryption ............................................... 13
    2.2.4 Control cf Intrinsic risk ................................ 15
  2.3 Addresses ...................................................... 17
    2.3.1 Callback .................................................. 17
    2.3.2 Internet Addressing ..................................... 18
    2.3.3 Forging Return Addresses ................................ 19
  2.4 Conclusion ..................................................... 20

3 Administration Risks ............................................... 23
  3.1 Application .................................................... 23
  3.2 Limitation ..................................................... 24
    3.2.1 Breadth ................................................... 25
    3.2.2 Independence ............................................. 26
    3.2.3 Registering Reliance ................................... 27
  3.3 Revocation ..................................................... 28
  3.4 Conclusion ..................................................... 28
4 Article 13 31
  4.1 The Operation of Article 13 ........................................ 31
  4.1.1 Appearances ..................................................... 32
  4.1.2 Control .......................................................... 33
  4.1.3 The Notice exception ......................................... 35
  4.1.4 The Knowledge exception ..................................... 35
  4.1.5 Consequences of Attribution ................................. 37
  4.2 The ECEG position on Article 13 ............................... 37
  4.3 Conclusion ....................................................... 39

5 Conclusion 41
Chapter 1

Electronic Commerce

1.1 The Internet

“As by means of water-carriage a more extensive market is opened to every sort of industry than what land-carriage alone can afford it, so it is upon the sea-coast, and along the banks of navigable rivers, that industry of every kind naturally begins to subdivide and improve itself.”
- Adam Smith

The information-carriage of the internet may open a yet more extensive market than water-carriage ever did, for the internet is cheaper, faster and connects more broadly.

But just how does the internet differ from existing forms of electronic communication, such as the telephone? “Electronic” commerce is not new; after all, the telegraph is now obsolete technology. The phone, telex and fax also have been with us for some time. All are cheap, fast, convenient and connect broadly over the world. As in the industrial revolution, it is automation that makes the difference.

Ironically, the flow of commerce on the internet is damned by the very things that bless it: while automation opens a wider market; fraud may also be automated and over an equally broad extent of market.

“The net offers Australian business - dogged by the tyranny of distance for two centuries - the chance to turn small domestic markets into large global ones, using the wonders of digital technology to approach customers previously beyond reach [to sell various physical goods].” - Australian Financial Review, Editorial

Unfortunately, the tyranny of distance still dogs the delivery of goods: delivery

---

1 An Inquiry into the Nature and Causes of the Wealth of Nations (1776) Book 1, Chapter 3.
2 EDI (Electronic Data Interchange) has even automated contract formation since the 70’s.
times for CDs on the internet vary from days to weeks\textsuperscript{4}. However, delivery of \textit{information goods and services} is possible over the internet itself. CDs are a case in point, for depending on the speed of connection, the information contained in the CD can be delivered in a matter of minutes, not days or weeks, and without the expense, risk and uncertainty of international shipping\textsuperscript{5}. The on-line execution of contracts - delivery and payment\textsuperscript{6} - truly would overthrow the tyranny of distance.

By lowering entry and transaction costs, the extent of market of both buyers and sellers may be increased - and hence the wealth of the nation.

\section{The Necessity of Trust}

Commerce on the internet, as elsewhere, requires trust. Unfortunately, trust on the internet is a real problem that must be solved before we can reap the benefits of information-carriage. This section shows why trust is essential to commerce.

Commerce is the exchange of one thing for another. This corresponds with the commonsense notion of a bargain: for example, you might purchase a peppercorn for a dollar in a sale of goods. A promise of future performance may also form part of an exchange. Trust is a confident expectation or reliance\textsuperscript{7}. To trust someone is to expect them to perform their side of the bargain; and to perform it properly. You might trust someone to keep their promise to deliver the peppercorn; and that the peppercorn is up to standard.

In an atmosphere of mutual trust and respect, the issue of trust is not apparent. You chat with merchant, recounting your adventures on the high seas amongst the aromatic sacks of spices, and the exchange of peppercorn and coin might as well be simultaneous. There is no sense of vulnerability as you relinquish your coin. But when you trade at a distant port, where that respect is stripped away and replaced with mutual suspicion, the role of trust becomes conspicuous by its absence. You are fearful of letting the merchant have your coin until he gives you the peppercorn - he might take the coin, and then claim that you never gave it to him! But the merchant does not trust you either; he thinks that if he gives you the peppercorn, you will run off without paying. Deadlock.

It is tempting to suggest that a \textit{simultaneous exchange} could resolve this childish dilemma, so that neither party need go first. But is this really possible? Or does

\textsuperscript{4}This irony is well-illustrated by the story of an internet transaction to a room full of impressionable journalists: after completing the “instant” transaction, the demonstrator quickly turned off the application. But not quickly enough to hide the message displayed: “Please allow up to 6 weeks for delivery”.

\textsuperscript{5}Another advantage of information goods is that a claim of non-receipt can be rectified by simply resending the goods, with insignificant cost to the seller.

\textsuperscript{6}The problem of payment on the internet is beyond the scope of this dissertation; but has received much attention, with proposals for electronic money and safe credit card payment (using the proposed Secure Electronic Transactions standard, or SET). Of course, Electronic Fund Transfers (EFT) have been used by banks for many years now.

\textsuperscript{7}combining the first and second definition given in the Shorter Oxford Dictionary
one party necessarily lose control of their consideration before the other? A series of thought experiments will confirm that trust is always required at some level\(^8\). In addition, the physical presence of simultaneous exchange is not available on the internet.

If trust is essential for commerce, then the ceaseless exchange of coin and promise and thing that permeates our lives and creates our wealth also implies tremendous trust. How is this trust established? Why do we trust some people and not others? The keys are reputation, rapport and recourse.

### 1.3 The Origin of Trust

Trust usually requires identification: Little Red Ridinghood trusted her grandmother, but this trust was to no avail when her grandmother was impersonated by a wolf. Sometimes it is not enough to trust someone; but you must also confirm that it is they who you are dealing with. Trust and identification are distinct issues, but trust rests on identification.

When poised at the threshold of a transaction, we can look in three directions for a reason to trust the other: backward to the past, to the present, and forward to the future.

**Past** Trust based on the past is quite reliable\(^9\) and may be built up over a course of dealing, the trust reposed increasing with each successive transaction. Unfortunately, past acts can only suggest the nature of the party concerned, without guaranteeing that they will carry on in the same manner. Their inner nature may change; or we may have been taken in by a clever act. This might be known as the “extended courtship” theory of trust.

You prefer to deal with a merchant you know has been trustworthy in the past, rather than an unknown stranger or someone with a positive reputation for untrustworthiness. This type of trust hinges on accurate identification, for your trust is misplaced if you are fooled by an imposter, as was Little Red Ridinghood.

Other forms of reputation can also establish trust, such as by word of mouth, recommendation by independent body (eg RACV, Choice Magazine) and the partisan recommendations of advertising, packaging and salesmanship, but again some

---

\(^8\)Escrow makes the trust explicit. If you and the merchant both trust me, then I can facilitate trade between you by acting as an *escrow agent*. For example, you give your coin to me and the merchant gives me the peppercorn, and you both trust me to complete the transaction. If the merchant reneges, and refuses to give me the peppercorn, I simply return your coin with no harm done. Escrow agents are employed in international shipping (usually banks), with payment and delivery evidence by irrevocable letters of credit and bills of lading, respectively.

form of identification is required to assure us that the party we are dealing with is the same one advertised.

**Present**  However, when the recommendation occurs in the present, no identification is required; for example, when the other says “trust me” - and we do. This might be called the “love at first sight” theory of trust. Although instant rapport is possible, it generally takes some time. That is, it is based on the past.

The distinction between the present and past forms of trust is between walking into the merchant’s storehouse for the first time and judging it at face value, and choosing a merchant you have dealt with before who has a good reputation.

**Future**  The availability of recourse in the future is the third basis for trust. Recourse can take many forms; we here focus on legal recourse and recourse against the other’s reputation. The hard work of establishing a good reputation leads to a desire to protect this investment, and to provide a means of identification which facilitates consumers relying on this reputation from the past. Thus, the threat of damage to reputation in the future provides a basis for trust today. For recourse to be effective, the other must have something to lose - such as funds or reputation; and some way to lose it - such as through a court or word of mouth; as well as being identifiable. This might be described as the “retribution” theory of trust.

Only trust based entirely on the present needs no identification - but “love at first sight” is the least reliable basis of trust. Trust based on the past and trust based on the future both require some form of identification.

### 1.4 Identification

Identification itself may be weak or strong. Weak identification is where you deal with same person each time, but you do not know who they actually are. For example, a fellow commuter lets you into traffic. After you have switched lanes, you wave a thank-you. You are certain that it is the same person who lets you in and who you wave at - but you do not know who they are. Strong identification is when you also know who that person is: you stop beside them at traffic lights, look across and recognise an old friend: “It’s you!”

Some of the dangers of weak identification are that multiple personas may be used, and that legal recourse to the actual person is not available.

**Legal recourse**

Legal recourse would seem to demand strong identification of the actual party, and presence in the jurisdiction.
1.5. AUTHENTICATION RISKS

However, judgement in a civil case is usually in the form of damages, suggesting that a fund\textsuperscript{10} associated with the identity might be sufficient to satisfy judgement. This is similar to the present situation with companies, where only the company itself is liable for judgements against it, as an artificial person, rather than the management or shareholders. A problem occurs where the liability exceeds the fund, or where the gravity of a crime committed by the company requires that the persons behind it be punished. A fund limited to the purchase price of a transaction would assure customers that at least they could get their money back; but would not necessarily meet these requirements of justice or regulation.

On the other hand, an inability to meet liabilities is a familiar scenario\textsuperscript{11} - and the “limited liability” company explicitly shields shareholders from such liability. The inadequacy of the proposed fund at times would simply be more of the same. The deficiency of weak identification is more a problem of regulation and justice than of commerce.

In conclusion, it seems that reputation and legal recourse against a fund of money could engender the trust necessary for commerce; but the restraining hand of justice would be frustrated in some cases. Note that recourse against this fund would require access to a legal entity that is strongly identified. However, regulation and the protection of the public good require strong identification. At any rate, it is suggested that legal recourse acts mainly as a safety net; reputation is the mainspring of trust.

It is not suggested that parties need not be identified; but that inaccurate identification is not fatal to commerce.

1.5 Authentication Risks

Identification is essential for reputation and recourse - for without knowing to whom it relates, reputation is meaningless; and without a target, recourse (legal or otherwise) is absurd. Identification is essential for internet commerce, as identification brings into play both reputation and recourse.

Two dangers flow from unreliable identification: you may enter a transaction with someone who you believe to be $X$ - but who is actually a rogue who makes off with your money. This is the danger of impersonation. Secondarily, you may enter a transaction, and then you yourself claim (falsely) to be impersonated, and repudiate the contract. Where identification is unreliable, repudiation can be difficult to prove.

An inked signature stamp illustrates the ways in which such an identification may be unreliable: a rogue may steal the stamp; the stamp itself may be counterfeited by inference from examples of its use; and thirdly, the signature stamp may not belong to who it was thought to in the first place. These risks are named the control,

\textsuperscript{10}This fund could be provided by an insurer.

\textsuperscript{11}This scenario is so common that specific bankruptcy and insolvency laws have been developed to handle it.
intrinsic and application risks.

**Control risk** The control risk is that control may be lost of the identifying mechanism: note that the person holding the device is most able to prevent this.

**Intrinsic risk** The intrinsic risk is a risk that neither the holder nor the recipient can prevent it - it is an inherent weakness in the identification mechanism itself. However, note that the party choosing the particular device does have some influence, for some devices are more easily counterfeited than others. Even within the one family of devices, there is variation; for example, an intricate and fine signature stamp is more difficult to counterfeit than one that is simple in design and rough in manufacture.

**Application risk** The application risk is named after the risk in credit cards that the applicant used another’s name when filling out the application form. Clearly, this is not a risk of the identification mechanism itself, but of its administration. Equally clearly, the purported sender can be in no way held responsible.

The control and intrinsic risks are discussed in the next chapter on Authentication Technology; while the application risk is covered briefly in the chapter on Administration Risks.