January 2007

Chapter 4 - Identification and Attribution

CHAPTER 4 IDENTIFICATION AND ATTRIBUTION

"… COMMERCE, ON A LARGE SCALE, CAN PROSPER ONLY WHEN PEOPLE CAN DEAL CONFIDENTLY WITH PEOPLE THEY HAVE NEVER MET AND HAVE NO REASON TO TRUST."[1]

INTRODUCTION

[4.1] The previous chapter dealt with intention and automation. It established that computers cannot be parties to a contract and that computer-generated output is always attributable to a person.[2] It stated that the automation of the contract formation process does not prevent the existence of intention. This chapter deals with intention and identification. It examines to what extent, if any, contractual intention is affected by the difficulties of ascertaining the identity of the other party.[3]

Persons have the right to choose with whom to contract. Such choice is often based on the creditworthiness or special skill(s) of the other party. Consequently, intention may be directed at a particular person. Such intention can be evaluated as part of the offer and acceptance model or from the perspective of the doctrine of mistake, assuming such exists.[4] Questions of intention relate to contract formation whereas mistake is generally considered a vitiating factor affecting the validity or enforceability of a contract.[5] In certain circumstances, however, a mistake as to the identity of the other party prevents formation. Irrespective of the approach, the intention to contract with a specific person is evaluated objectively and presumes the possibility of identifying this other person. This is where the idiosyncrasies of the novel transacting environment come into play.

---

[1] W Diffie, S Landau, Privacy on the Line: the Politics of Wiretapping and Encryption, Cambridge 1998, p 48

[2] This chapter replaces "user" with "person," "computer-generated output" with "message."

[3] A distinction between "person" and "party" may be warranted: a message is always sent by a "person." In that sense there is also a party. It is questionable whether such person is a party in the contractual sense if he or she never intended to bear the legal consequences of a message.

[4] For a detailed discussion see: S Smith, P Atiyah, An Introduction to the Law of Contract, 6th ed, Oxford pp 76, 77, who speak of mistakes in formation; see also: Law of Contract para 4.73

[5] Carter on Contract [02-030]

Problems of identification are not new but become exacerbated by the online environment. Strangers transact with strangers, they deal at a distance, the information about the other party is scarce and unreliable.[6] Moreover, persons often assume different identities for their on-line activities.

Problems of identification are usually discussed in relation to attribution. Absent statutory provisions or agreement, open electronic networks do not change the basic principle of attribution: a person is responsible for the legal effects of an act, if he or she performed or authorized such act. Problems of attribution are therefore not Internet-specific. Attribution, however, remains a favourite topic of legal literature. It is often discussed in the context of re-creating trust in on-line commerce: knowing who one is dealing with and knowing that the contract will be performed.[7] Attribution focuses on accountability for an act, intention relates to the existence and contents of a contract. Both attribution and the intention to contract with a specific person are premised on the possibility to identify this person. Problems of attribution can generally be reduced to problems of identification.

Just as no thesis on on-line contract formation can be complete without a discussion of electronic agents, it must include a discussion of digital signatures. The latter constitute the most heralded method of identification and unquestionably the most popular topic of early "Internet-Law" literature. This chapter approaches the topic of digital signatures with some scepticism. They can be regarded as an example of misplaced focus and hype, a dubious solution to a problem that may not exist – as in the case of automation and electronic agents. Despite the temptation to exclude them from the thesis altogether they must be mentioned to set the stage for some later discussions and to clarify their limited role for contract law.

Roadmap

[4.2] The introductory part continues with a number of caveats and clarifications which delineate the scope of discussion. Attribution and identification are distinguished from the search for functional equivalents of signatures and the fulfilment of formal requirements. The basic concepts used in the discussion are presented. The relationships between "person," "name" and "identity" are examined.

Subsequently, the chapter analyses digital signatures. If digital signatures cannot reliably identify the sender of a message, then a fortiori, identification based on less advanced technologies is questionable. The model law approaches to digital signatures and attribution are discussed. The emphasis is placed on the unauthorised use of signature creation data.

Finally, so-called mistaken identity cases are revisited. The possibility of holding a contract void due to a mistaken belief as to the other party's identity is analysed in light of the difficulty of ascertaining such identity and the diminished value of identities as means of identifying persons. The focus is taken off the person misrepresenting his or her identity and placed on the mistaken party. The chapter also examines some distinctions traditionally made in mistaken identity cases. The most recent in the line of cases, Shogun Finance Ltd v Hudson,[8] is examined. How would this case be resolved if the party purporting to be somebody else used the digital signature issued in the name of the party he or she purports to be?

[6] L Lessig, Code and other Laws of Cyberspace, New York 1999, pp 28, 30, 31; J K Winn, Open Systems, Free Markets, and Regulation of Internet Commerce (1998) 72 Tul L Rev 1177 at 1213

[7] A H Boss, Searching for Security in the Law of Electronic Commerce (1999) 23 Nova L Rev 585 at 592; see also: Report paras 3.1.1, 3.1.2

[8] Shogun Finance Ltd v Hudson [2004] 1 AC 919

Caveats and Clarifications

[4.3] Before abandoning the topic of attribution and commencing a discussion of digital signatures a number of clarifications must be made.

Attribution and proof

[4.4] There is no attribution chapter in any textbook on contract. The principle that one is responsible for one's actions requires no elaborations. The output of electronic acts, such as emails or clicks, should only be attributed to the person who undertook or authorised those acts. Consequently, one of the challenges of on-line contracting consists in determining this person or actual identity of the other party. Usually, "identifying the person with whom you are dealing also identifies who is liable (responsible) in law. But it is not always so."[9] The practical question is whether the risk that the purported sender is not who he claims to be is sufficiently high to merit further inquiry.[10] It is the recipient who must prove that the sender dispatched the email.[11] Attribution is therefore a question of proof, [12] not contract formation. Attribution can be discussed in the context of the difficulties of determining the actual sender, or – in broader terms - the originating computer.[13] As information pointing to specific computers or users is easily spoofed, hidden or manipulated[14] the recipient of message or the user of a website has little guarantee that the other party is who he or she claims to be or – more importantly – that such party can be held accountable. Internet-specific problems related to attribution are, however, related to questions of proof and evidence – not contractual intention.

Attribution and Signatures

[4.5] Attribution is often discussed alongside digital signatures, which in turn are analysed in the context of formal requirements. The arguments usually commence with a description of the functions performed by traditional signatures and demonstrate that digital signatures can perform these functions.[15] This chapter does not follow this sequence. Analysing digital signatures for identification purposes differs from analysing their use for the fulfilment of formal requirements. Determining whether a "signed" electronic document meets formal requirements is distinct from determining who signed the document. Assuring enforceability is pointless if there is no-one to enforce the contract against.

The functions of signatures need not be recited.[16] Neither is there a need is to compare traditional signatures to digital ones or determine whether the latter can satisfactorily perform the functions of the former. Such descriptions have been made elsewhere.[17] The significance of traditional

---

[9] Nimmer & Towle para 6.02

[10] Nimmer & Towle para 6.02

[11] Nimmer & Towle para 6.02

[12] Nimmer & Towle para 6.01

[13] D E Sorkin, Technical and Legal Approaches to Unsolicited Electronic Mail (2001) 35 USFL Rev 325; D Dickinson, An Architecture for Spam Regulation (2004) 57 Fed Comm L J 129; A Y Strauss, A Constitutional Crisis in the Digital Age: Why the FBI's "Carnivore" does not Defy the Fourth Amendment (2002) 20 Cardozo Arts & Ent L J 231; L Noah, Establishing Legal Accountability for Anonymous Communication in Cyberspace (1996) 96 Colum L Rev 1526

[14] Compuserve Inc v Cyber Promotions Inc 962 F Supp 1015, 1020 (1997)

[15] S Christensen, The Statute of Frauds in the Digital Age – Maintaining the Integrity of Signatures (2003) 10 MurUELJ 4; Ch Reed, What is a Signature? (2000) JILT (3); A McCullagh, P Little, W Caelli, Electronic Signatures: Understand the Past to Develop the Future (1998) UNSWLJ 56

[16] See MLEC Art 7 and Guide to Enactment paras 38, 39; MLES Guide to Enactment para 19; ABA Digital Signature Guidelines pp 5-7

[17] J K Winn, The Emperor's New Clothes: the Shocking Truth about Digital Signatures and Internet Commerce (2001) 37 Idaho L Rev 353 at 359: "[t]rying to use asymmetric cryptography as a signature on a contract is like trying to fit a square peg into a round hole."

signatures for attribution purposes is limited. Signatures do not automatically attribute a document to the person bearing the name contained in the signature. They do not carry a presumption of authenticity and do not reverse the burden of proof.[18] If traditional signatures do not automatically burden the purported signer with whatever he or she purportedly signed, neither can their functional equivalents. At least not in Australia.

Attribution in the real world is, however, often performed on the basis of handwritten signatures. This is so despite the fact that the latter need not be legible and identify the signatory.[19] Handwritten signatures are, however, specific to the signatory. There is a unique, biometric association between a person and her signature. A discrepancy between the name in the signature and its biometric characteristics prevents the attribution of the signed document to the person bearing that name. Due to the liberal approach as to what can constitute a signature, neither a biometric link nor a name are required.[20] Open electronic networks break all biometric links between a person and the output of his or her acts and alter the quality and quantity of information available to the recipient.

Terminology

[4.6] Analysing problems of identification requires a precise and consistent terminology. It also requires a clear sequence of analysis. In particular, the relationship between identification, attribution and authentication must be explained. As in the case of electronic agents, many "legal" problems are created by wrong or confusing terminology.

Authentication

[4.7] To "authenticate" means, amongst others, "to establish as genuine."[21] The term can be used in multiple senses: to authenticate a document means to "associate oneself" with its contents, as in "to sign."[22] "Authentication" may also involve the validation of documents. For attribution purposes, "authentication" refers to the verification of a person's identity.[23] Authenticating documents must therefore be distinguished from authenticating persons. The meaning depends on which side of the transaction is examined: senders authenticate messages, recipients authenticate the senders of messages.

"Authentication" must be set apart from "identification." To "identify" means to recognise as a particular person.[24] Identification is the process of presenting an identifier to a system so that the system can recognize an entity and distinguish it from others.[25] Identification answers the question: who are you? Authentication consists in proving who you are.[26]

Authentication comprises two steps: identification and verification. The second step involves the presentation of authentication information that corroborates the association between the person and the identifier. Authentication information consists in something a person knows (password, PIN), possesses

---

[18] See: Report para 4.5.77

[19] Toh See Kiat p 79; H K Towle, E-Signatures – Basics of the US Structure (2001) 38 Hous L Rev 921 at 986

[20] MLEC Guide to Enactment para 54

[21] Macquarie Dictionary; for a discussion of various meanings of "authentication" see: H K Towle, above at note 19 at 926, 927,928; B Schneier, Secrets and Lies: Digital Security in a Networked World, New York 2000, p 73

[22] See: GUIDEC II Glossary p 31

[23] ABA Guideline 1.4; RFC 2828, Internet Security Glossary, R Shirey (2000) ("RFC 2828") p 13

[24] Macquarie Dictionary

[25] RFC 2828, p 75

[26] B Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World, New York, 2003; p 182

(token, smartcard) or is (biometric data).[27] Access to authentication information often enables the assumption of the identity verified by this information.

In real life, identification and authentication occur concurrently, traditionally taking the form of recognizing a person's facial features and/or voice.[28] On the Internet, authentication is performed remotely. Authentication technologies produce evidence of different probative value in establishing that messages came from the purported source.[29] The quality of an authentication procedure depends, amongst others, on the security of authentication information.

Non-repudiation

[4.8] Legal literature often uses the term "non-repudiation."[30] Repudiation is the false denial of responsibility for an act.[31] Non-repudiation provides evidence of the signer's identity thereby preventing him from successfully disavowing the message.[32] It consists in the ability to prove that a message originated with a certain person.[33] Non-repudiation can be regarded as either a prerequisite or a consequence of attribution. Both deal with the question: can a message be indisputably linked to a sender? Both are technology-dependent and come in varying degrees. Non-repudiation concerns proof, attribution – accountability.

Person, Identity and Name

[4.9] Attribution goes beyond determining whether a person is who he or she claims to be. It encompasses the question: who is the other person? This is not a matter of semantics only. A name-holder cannot be attributed with the message only because his or her name was used. Only persons, not names or identities, are parties to a contract. Persons are identified by names.[34] Ideally, names should be uniquely attached to persons, pointing to the accountable person.[35] Names, however, are not unique.[36] Once taken on an open global network, they start losing their association with persons.[37]

"Persons" must be distinguished from "identities." It is always a person who assumes an identity - that of an existing person or a fictitious one. It is always a person who enters a shop, writes a letter or sends an email. Persons assume different identities for different roles. Transacting under a different identity is not prohibited and need not constitute a misrepresentation or impersonation of a third party.

---

[27] RFC 2828, p 15

[28] Schneier, above at note 26 p 184

[29] H K Towle, above at note 19 p 947

[30] "non-repudiation" must be distinguished from "repudiation" in the sense of anticipatory breach of contract, see: Carter & Harland [1928]

[31] Ford & Baum p 333

[32] ABA Guideline 1.20 and comments 1.20.1 and 1.20.2

[33] Ford & Baum p 336

[34] N Ferguson, B Schneier, Practical Cryptography, Indianapolis 2003 ("Ferguson & Schneier") p 323

[35] See also: RFC 2693, SPKI Certificate Theory, C Ellison et al; (1999) p 8

[36] B Schneier, above at note 25 p184

[37] Ferguson & Schneier p 324. To illustrate the point: The uniqueness of identifiers is easier to achieve in closed systems. Information systems require uniqueness. Email addresses can be designed to be unique. Email addresses, however, do not point to persons. There is only one email account issued to "liz.mik" at hotmail.com. There is also one "liz.mik" at yahoo.com. "Liz.mik" is locally unique within the hotmail and yahoo namespaces respectively but due to its association with different web-mail providers, (i.e. address information appended to the name) it attains global uniqueness – there is only one liz.mik@hotmail.com and only one liz.mik@yahoo.com. The problem remains: anyone can assume the screen name "liz.mik" and register the relevant email account. There is no authentication process upon sign-up at hotmail or yahoo. Unless identity escrow is used, the real identity of the person registering the account remains unknown. See: A M Froomkin, Flood Control on The Information Ocean: Living with Anonymity, Digital Cash and Distributed Databases (1996) 15 J L & Com 395 at 422

"Identities" must be distinguished from "names." Both names and identities point to persons. As persons cannot be distinguished by names alone, they are co-defined by their attributes. Space does not permit a more detailed elaboration of the relationship between "name" and "identity." "Identity" can be regarded as a construct of a name and one or more attributes.[38] This interpretation underlies the common understanding of "identity theft", i.e. the theft of identifying information in order to engage in transactions as the person whose identifying information was stolen.[39] In many instances "identity" can be used interchangeably with "name." In others, legal analysis requires the separation of these concepts.

While identification always precedes attribution, the core concept is authentication – the verification of an identity. When analysing attribution or identification, one always encounters problems of authentication.

Identification and Privacy

[4.10] Problems of authentication intersect with privacy concerns posed by the Internet.[40] E-commerce requires methods of establishing accountability, which in turn requires the identification of the other party. Privacy protection, on the other hand, aims at hiding the real identities of persons and preventing any association between them and their electronic activities.[41] The more personal information is revealed and the easier the access to such information, the greater the risk of unauthorized use.[42] "Personal information" can often serve as "authentication information"[43] and be used to assume the identity of its subject.[44] Attempts to authenticate the other party may also violate privacy laws.[45] Accordingly, it may not be possible to request any additional authentication information to ascertain the identity of the other party.

REMOTE AUTHENTICATION – DIGITAL SIGNATURES

[4.11] The following sections describe the practical problems of remote authentication using digital signatures as an example. The analysis delves into some technical detail to establish the extent, if any, digital signatures can serve as a method of on-line authentication. The reason for including a discussion on digital signatures in a thesis on contract formation is that they occur in practically all analyses of on-line contracting, creating the impression that on-line contracts are premised on their use.[46] Furthermore, their deployment may, in certain circumstances, alter attribution principles creating a parallel regime for on-line contracting. To narrow the scope of discussion, three preliminary points are necessary.

---

[38] See: MLES Guide to Enactment para 117, discussing "identity" and "identification"

[39] H K Towle, Identity Theft: Myths, Methods, and New Law (2004) 30 Rutger's Computer & Tech L J 237 at 238, 241; see also: J Lynch, Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks (2005) 20 Berkeley Tech L J 259 at 260; C Pastrikos, Comment: Identity Theft Statutes: Which Will Protect Americans the Most? (2004) 67 Alb L Rev 1137

[40] W Diffie, S Landau above at note 1 p 125; for practical illustrations see: G M Schober, Colloqium on Privacy and Security (2002) 50 Buss L Rev 703

[41] for a discussion of anonymity on the Internet see: A M Froomkin, above at note 37

[42] H K Towle, above at note 39 at 262, 263 on the "Collision between Identity Theft and Privacy;" See generally: A Taipale, Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd (2004-2005) 7 Yale J L & Tech 123

[43] See also definition of "personal information" in the Privacy Act (Cth) 1988 Section 8

[44] J Grijpink, Biometrics and Identity Fraud Protection (2005) 21 CLSR Com 254

[45] Nimmer & Towle para 6.03[3]

[46] see e.g. A McCullagh, Legal Aspects of Electronic Contracts and Digital Signatures, in A Fitzgerald ed, Going Digital 2000, Legal Issues for E-commerce, Software and the Internet, 2nd ed, Sydney 2000

First, digital signatures rely on asymmetric cryptography. Cryptography is used for the preservation of confidentiality, key exchange and for authentication purposes, amongst others.[47] This paragraph deals solely with the use of digital signatures for authentication.

Second, digital signatures are the subject of numerous model regulations[48] and statutes.[49] Focusing primarily on formal requirements, the regulations distinguish between electronic and digital signatures. The former relate to any electronic representation of a name, such as letters or digitised handwritten signatures, the latter rely on one technology, asymmetric cryptography. The regulations can be divided into three categories: minimalist, prescriptive and hybrid. [50] The first facilitate the use of electronic signatures without imposing a specific technology and define the requirements electronic signatures must meet to fulfil the functions of traditional signatures. The minimalist approach focuses on the intention of the signer and the signature's ability to identify him.[51] The second approach establishes a legal framework based on a public key infrastructure and adopts asymmetric cryptography as the means of creating digital signatures. The third combines the minimalist and the prescriptive approach and endows digital signatures with specific legal effects while also recognising less sophisticated technologies.[52] All three acknowledge the general permissibility of electronic or digital signatures and prohibit any discrimination on the ground that a document was signed electronically. They differ to the extent that some equate digital or electronic signatures with handwritten signatures, without reversing the burden of proof, while others create technology-dependent presumptions.[53] It is beyond the scope of this thesis to analyse these approaches in detail.[54] The regulations are mentioned to the extent they introduce different attribution rules.

Third, digital signatures are one of many authentication technologies. Another method relies on biometrics, the individual traits of a human body. Only biometric-based methods of authentication can establish the actual person who performed an act. Such technologies are, however, still in their infancy. Apart from high costs of implementation, they encounter numerous problems related to the process of enrolment and subsequent matching. Biometric-based technologies also introduce a trade-off between reliability and convenience on one end and intrusiveness and privacy concerns on the other.[55] Their use in open systems being practically non-existent, they are not included in the discussion.

---

[47] See generally: W Stallings, Cryptography and Network Security, Principles and Practice, New Jersey, 2003

[48] UNCITRAL Model Law on Electronic Signatures ("MLES") American Bar Association Digital Signature Guidelines; International Chamber of Commerce, General Usage for International Digitally Ensured Commerce II ("GUIDEC II")

[49] Utah Code Ann par 46-3-101 et seq,; German Digital Signature Law 1997; Electronic Signatures in Global and National Commerce Act" (Public Law 106-229); see also: Nimmer & Towle para 6.10

[50] see GUIDEC II, p 55

[51] see. e.g. Electronic Signatures in Global and National Commerce Act (Public Law 106-229)

[52] see e.g. Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signature prohibits any discrimination on the grounds that the signature is in electronic form while at the same time requiring member states to give legal effect to "advanced electronic signatures" which are created by "secure signature creation devices."

[53] For a detailed discussion of the distinction between "pure" facilitation and the provision of specific legal effects, see: A H Boss, above at note 7 at 600-609

[54] see: B P Aalberts & S van der Hof, Digital Signature Blindness, Analysis of Legislative Approaches toward Electronic Authentication, November 1999, available at http://cwis.kub.nl/-frw/people/hof/ds-fr.htm

[55] M Crompton, Biometrics and Privacy (2002) PLPR 32

A Cryptographic Solution

[4.12] Cryptography is the science of keeping information secret.[56] The need to encrypt arises whenever information must be shared at a distance and there is risk of third party interception. Encryption requires an algorithm and a key. Encryption algorithms, or "ciphers," are mathematical procedures; keys are alphanumeric characters that initiate the encryption or decryption process. Only the key must be kept secret, the cipher is widely available.[57] The longer the key, the more difficult it is to guess. Length of key aside, once it must be transmitted over an insecure network there is a risk of compromise.[58]

The main challenge in cryptography is key exchange.[59] This problem is prominent in symmetric key cryptography, where the same key is used to encrypt and de-crypt. Asymmetric key cryptosystems, on the other hand, use a public and a private key.[60] A message encrypted with the public key can only be decrypted with the private one – and the other way round. Because asymmetric algorithms are significantly slower than symmetric ones, data is usually encrypted with a symmetric algorithm. Subsequently the symmetric key is encrypted with the recipient's public key. The recipient uses his private key to decrypt the symmetric key. In other words, the private and public keys are only used to exchange the symmetric key.[61]

Digital Signatures

[4.13] Digital signatures are an application of asymmetric cryptography[62] and rely on the indisputable mathematical correspondence between the private and the public key.[63] They are a derivative of the private key and a so-called "hash function."[64] The latter reduces a message of any length to fixed length output, termed message digest. Identical texts run through the hash function produce the same message digest.[65] The message digest is encrypted with the private key; the output of this operation is the digital signature. The hash ties the private key to the message, ensures message integrity and renders it impossible to re-use the digital signature. [66] Digital signatures guarantee that a specific message was transformed with a specific private key.

Assumptions of the model

[4.14] The digital signature model requires that the public key be accessible to everyone and the private key exclusively to its authorized user. It also requires that a trusted third party guarantees the association between the public key and such user. The correspondence between the key-pair is worthless unless there is a method to verify that it belongs to a given person. There is, however, no natural association between a person and a key-pair.[67] As "anyone with a set of keys could potentially assume another party's identity,"[68] it must be attested that a given public key belongs to a specific person. Consequently, digital

---

[56] Ford & Baum p101
[57] Ferguson & Schneier p 23
[58] Greenstein & Feinman p 233
[59] M E Hellman, An Overview of Public Key Cryptography, IEEE Communications Magazine, 50th Anniversary Commemorative Issue, 2002, originally published in (1978) 16 IEEE Communications Magazine 6
[60] For a detailed description see: Ferguson & Schneier p 26; B Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, 2nd ed, New York 1996, pp 33-40
[61] This is a "hybrid cryptosystem," see: Ferguson & Schneier p 28,
[62] Ford & Baum p 109
[63] W Stallings, above at note 47 pp 262, 380
[64] H Dobbertin, Secure Hashing in Practice (1999) 4 ISTR 53; see also ABA Digital Signature Guideline 1.12
[65] Ford & Baum p 113; J K Winn, above at note 17 at 386
[66] for a step-by-step description of the process, see: MLES Guide to Enactment para 62 or H M Deitel, e-Business & e-Commerce, How to Program, New Jersey 2001, p 206; ABA Digital Signature Guidelines, p 13
[67] Ch Sundt, PKI – Panacea or Silver Bullet? (2000) 5 ISTR at 54
[68] H M Deitel, above at note 66 p 206

signatures cannot function as a stand-alone application but must be supported by a public key infrastructure ("PKI") or a web of trust (as in the encryption program Pretty Good Privacy, "PGP").[69]

PKI & PGP

[4.15] The cornerstone of PKI is a Certification Authority ("CA"), which generates and manages Digital Certificates ("DCs").[70] CAs can be part of an institutionalised structure[71] or private companies. A DC is a digital document containing information about the person it was issued to ("subscriber")[72] and the public key. Usually the key-pair is generated during the procedure of issuing the DC, in other models keys are generated by the subscriber and subsequently submitted for certification.[73] The DC binds the identity of a subscriber to a key-pair. CAs confirm the identity of applicant before issuance. The authentication process ranges from simple verifications that an email belongs to a particular person,[74] to elaborate procedures entailing notarised documents. [75] The less comprehensive the authentication process, the weaker the assurance that the subscriber is who he or she claims to be.[76] PKI encounters multiple problems in its implementation: a complex infrastructure, the lack of interoperable standards and an inherent suitability for closed environments, amongst others.[77] A comprehensive critique of the PKI model is presented elsewhere.[78]

PGP replaces the centralized CA[79] with a so-called "web of trust" - a group of users that cross-certify each other's certificates by vouching for the validity of the association between a public key and a person.[80] The DC is published on a public server and everyone who is convinced of its authenticity can give it a stamp of approval in the form of his/her digital signature. The more signatures on a DC, the more trustworthy the public key of its owner.

The Quality of Associations

[4.16] To identify a sender (and to attribute the message to the sender) a number of associations must be established. The first is between a name and a person. This association is verified during the issuance of the DC and forms the basis for the second, the one between the DC and the subscriber. The quality of the authentication procedure performed by the CA determines the quality of the association between the subscriber and the key-pair. The DC only links a key-pair to an identity – not to a physical person. The associations between the private key and the digital signature as well as between the private key and public key are based on a mathematical relationship. They are therefore unquestionable.

It is the association between the subscriber and the digital signature that is problematic. A private key is not like a pen, a tool producing different yield depending on who used it. Anyone who gains

---

[69] Ford & Baum pp 251, 275

[70] see: Ferguson & Schneier p 29, Ford & Baum p 182

[71] see: www.agimo.gov.au/infrastructure/gatekeeper, the Australian Government's PKI strategy

[72] the public-key certificate format is defined in the ITU X.509 standard, see: Ford & Baum p 198

[73] for key generation see: K G Patterson, G Price, A Comparison Between traditional Public Key Infrastructures and Identity-based Cryptography (2003) 8 ISTR 57 at 57,58

[74] P Landrock, Challenging the Conventional View of PKI – Will it Really Work? (1999) 4 ISTR 36

[75] S Marsh, Identity and Authentication in the E-conomy (2002) 7 ISTR 16

[76] for an explanation of identity verification upon certificate issuance see: D S Anderson, What Trust is in These Times? Examining the Foundation of On-line Trust (2005) 54 Emory L J 1441

[77] S Garfinkel, E Spafford, Web Security and Commerce, Cambridge 1997, p 90; T Palmer, PKI needs good Standards (2003) 8 ISTR 6 at 7

[78] For a comparison of PKI theory and practice, see: Ferguson & Schneier p 326

[79] Ford & Baum p 275

[80] See: An Introduction to Cryptography, PGP Corporation White Paper (2005) p 25

access to the private key can produce a valid digital signature.[81] There is no natural link between the digital signature and the subscriber, comparable to the biometric link between a person and her handwritten signature or the mathematical correlation between the public and private keys. Legal discussions often mistake the strength of the cipher, the length of the key or the trustworthiness of the CA for the quality of the association between the digital signature and the subscriber.

It is misleading to focus on the reliability of the technology, when the weakest element of the model is outside the CA's control.[82] While the public key is stored in a publicly accessible repository managed by the CA, the private key is "at the mercy" of the subscriber,[83] usually stored on a networked computer, sometimes on the very system which hosts the digital signature application. Networked computers can be accessed remotely by both authorized and unauthorized persons.[84] The question is not one of forging (i.e. cracking) the private key but accessing it. Access control, (i.e. the prevention of unauthorized use of a resource)[85] involves the presentation of authentication information.[86] The security of a resource depends on the access control measures protecting it. The computationally intensive discovery of the private key is usually unnecessary if the key is protected by a password or PIN, which can be hacked with little effort.[87] If the private key can be accessed by anyone who knows a 4 digit PIN, the security of the key depends on the ability to guess or intercept the PIN.[88] The key is the protected resource, the PIN is the authentication information required to access the resource. In sum, digital signatures are not forged but private keys are used without authorization.

The identification of the sender of a digitally signed message, requires that the CA correctly authenticated the applicant during the certification procedure, the CA is trustworthy, the information contained in the DC is correct[89] and the private key remains under the exclusive control of the subscriber.

The last factor depends on the access control measures to the computer where the private key is stored. The security of the key is a function of the security of the authentication information. A message signed with a digital signature can be repudiated by the subscriber on ground that:

a) "This is not my key-pair" - incorrect authentication upon issuance, and/or
b) "I did not use my digital signature" – the private key or the authentication information necessary to access the private key were use by an unauthorised person.[90]

---

[81] J K Winn, above at note 16 at 385; for interesting access scenarios see: Cem Kaner, The Insecurity of the Digital Signature (1997) at www.badsoftware.com/digsig.htm; S Matthews, Authorization Models – PKI versus the Real World (2000) 5 ISTR 66 at 66; A Srivastava, Is Internet Security a major issue with respect to the slow acceptance rate of digital signatures? (2005) 21 CLSR 392 at 397; S Mason, Validating Identity for the Electronic Environment (2004) 20 CLSR 3; see also ABA Guidelines 1.24.1, 4.3; for a step-by-step description of the process, see: MLES Guide to Enactment para 62 and H M Deitel, above at note 66 p 206

[82] Feinman & Greenstein p 151

[83] S Garfinkel, E Spafford, above at note 77 p 90; Ford & Baum p 188

[84] B Schneier, above at note 20 p 176

[85] RFC 2828, p 7

[86] Greenstein & Feinman p 231

[87] B Schneier, above at note 26 pp 104, 105

[88] See e.g. ABA Guideline 4.3: "To safeguard the private key, access to it should require entry of a personal identification code, or the presentation of some other fact uniquely within the knowledge or control of the subscriber rightfully holding the private key."

[89] i.e. represents the association of key-pair and subscriber, the validity of the DC relates to suspension and revocation

[90] Ferguson & Schneier p 337; Nimmer & Towle para 6.03[3]

Model Approaches to Attribution and Digital Signatures

[4.17] Model laws confirm that the legal effects of a message are borne by the sender if it was sent by him or her or with his or her authority.[91] Some regulations, however, modify this principle: messages can be attributed to persons even if these persons did not send them. Recipients, in turn, may be entitled to rely that a message is sent by the purported sender, [92] if it is reasonable of them to do so. In the real world, attribution does not occur solely because somebody forged a person's signature or used a person's name. Once digital signatures (or other authentication technologies) are deployed, some provisions protect the recipient's reasonable reliance and "punish" the person whose "signature" was used. Attribution can be based on the loss or unauthorized use of the private key. The following sections briefly review the attribution rules proposed by some model laws.

MLEC & MLES

[4.18] The MLEC and the MLES introduce modified attribution rules. MLEC Art 13 ("Attribution") establishes a presumption that under certain circumstances a message is considered as that of the purported sender.[93] The recipient is entitled to regard the message as coming form the sender, if the message resulted from the "actions of a person whose relationship with the [sender] enabled that person to gain access to a method used by [the sender] to identify messages as its own."[94] It is unclear, whether the "relationship" covers unauthorized access and use of the method. As unauthorized use is generally synonymous with the lack of any relationship between the owner of a resource and its actual user, the provision may not cover situations where the private key is obtained by "hacking" into the sender's computer.[95] The presumption is qualified, however, if the recipient knew or should have known, "had it exercised reasonable care,"[96] that the message was not that of the sender.[97] Separate provisions regulate situations where the sender agreed to be bound by messages "signed" with the use of the authentication procedure. This could be an agreement between the contracting parties or system rules, such as between a subscriber and a certification provider.

The MLEC separates attribution from "signature." Taking into account, however, that unlike in the case of traditional signatures, Art 7 ("Signature") requires not only an intention to sign, but also the identification of the signatory, electronic signatures under the MLEC can serve attribution purposes. Accordingly, the MLES does not elaborate on Art 13, but continues the topic of attribution with regards to Art 7, focusing on the reliability of the authentication method. [98]

Despite claims that the MLES is neutral with regards to the authentication technology used,[99] it is drafted "with PKI in mind."[100] The signatory is expressly obliged to protect the private key and notify the

---

[91] MLEC Art 13 ("Attribution of Data Messages"), UETA Section 9 ("Attribution and Effect of Electronic Record and Electronic Signature"), ETA Section 15 ("Attribution of Electronic Communications")

[92] MLEC Guide to Enactment para 85

[93] S Mason, Electronic Signatures – Evidence (2000) 18 CLSR 242 at 243

[94] MLEC Art 13 (3) (b)

[95] MLEC Guide to Enactment para 87 states, however, that either the sender or the addressee can be responsible for "any unauthorized data message that can be shown to have been sent as the result of negligence of that party."

[96] MLEC Art 13 (4) (b)

[97] See: MLEC Art 13 (3) (b), (4) (b), Guide to Enactment para 83; similarly (5) precludes the sender from disavowing the message, unless the addressee knew or should have know that the message was not that of the sender.

[98] For an explanation of the relationship between Art 6 MLEC and the MLES, see MLES Guide to Enactment paras 68 & 71

[99] MLES Guide to Enactment para 5

[100] MLES Guide to Enactment para 28; see also Art 2, which define "certificates" and "certification service providers."

relying party and the CA, if any, of its compromise.[101] The signatory's obligations are mirrored by those imposed on the relying party. The latter must take reasonable steps to verify the reliability of an electronic signature, and, where such signature is supported by a certificate, verify the validity of such certificate.[102] It is ignored that even a thorough examination of the certificate does not reveal whether the private key was used by the subscriber and that the reliability of the technology does not give a guarantee that it was used by an authorized person.

Despite the above, the MLES directs member states to establish a presumption or substantive rule based on the technical characteristics of the signature.[103] Going beyond the simple recognition of electronic signatures, it attaches consequences to the signatory's failure to fulfil the obligations under Art 8. These may range from the signatory being liable for damages or estopped from denying the binding effect of the signature.[104]

The MLEC and MLES impose a high IT literacy on both transacting parties. Subscribers must be aware of the security risk of storing private keys. Recipients must examine the contents of digital certificates and evaluate the reliability of the respective technologies. The reasonableness of the recipient's reliance must be balanced against the subscriber's ability to safeguard the private key. From the subscriber side, the main difficulty is protecting of the private key from unauthorized use, from the relying party's side – establishing whether the private key was used by the subscriber.

ETA, UETA and CUECIC

[4.19] Unlike the UNCITRAL regulations, ETA and UETA do not introduce any special attribution rules associated with the use of authentication technologies. The ETA provides that a person is attributed with a message if it sent the message.[105] UETA provides that electronic signatures have an identical legal effect as traditional signatures.[106] UETA introduces the concept of "security procedure," which serves the purpose of verifying that an electronic signature is that of a specific person.[107] The use of such procedure, however, is not accorded any special legal effect. Security procedures can facilitate the burden of proof, but do not reverse it and do not impose any special obligations on the transacting parties. The CUECIC does not contain any provisions on attribution.[108]

Modified attribution rules for on-line transactions expose the sender's of digitally signed messages to more risks than senders of messages, which have not been signed digitally thereby indirectly discouraging the use of this particular authentication technology. They also necessitate the establishment of a complex technical and legal infrastructure.

---

[101] MLES Art 8 ("Conduct of the Signatory")
[102] MLES Art 11 ("Conduct of relying party") para 73
[103] MLES Guide to Enactment para 119
[104] MLES Guide to Enactment para 141
[105] ETA Section 15
[106] UETA Section 9, comments 2 and 4.
[107] UETA Section 2 (11)

[108] The ABA Guidelines contain a clear presumption of attribution when a digital signature was used. Apart from stating that a digitally signed message is "written" and satisfies signature requirements, they impose the obligation to safeguard the private key and list the factors to be taken into account when establishing reasonable reliance; see: paras 5.1, 5.2, 5.4, 5.6.

MISTAKEN IDENTITY

[4.20] The difficulties of identification in the on-line environment shed new light on cases of so-called mistaken identity. The latter are a type of unilateral mistake, where only one party is mistaken. The other knows of the mistake or caused it. Contracts are rarely void for mistake.[109] A buyer's mistake as to the quality and value of the acquired goods is inconsequential, so is the seller's mistake regarding the creditworthiness of the buyer.[110] The impact of mistake on the contract formation process can only be debated if the mistake is "operative."[111] A detailed discussion of "mistake" would by far exceed the scope of this thesis, particularly in light of the fact that each textbook on contract law approaches the problem differently. This chapter "carves out" one problem and maps it onto the on-line environment. In certain circumstances, if a party is mistaken as to the identity of the other party – there may be no contract (i.e. it may be void ab initio). As mistake concerns the subjective intention of a contracting party, there is an inherent tension between "mistake" and "objectivity."

Problems of mistaken identity have recently been revisited in Shogun Finance Ltd v Hudson.[112] A discussion of Shogun would require nothing short of a separate thesis. The following paragraphs focus on its implications for contract formation, or in broader terms – on the existence of contractual intention. The discussion does not aim at providing a new taxonomy of "mistake" or criticizing the existing doctrine on the subject.[113] It focuses on its practical aspects in light of the difficulties of on-line identification.

Shogun deals with the scenario where "crook (C) fraudulently represents to the owner of goods (O) that he is another identifiable person (X) and on that basis O parts with goods to C by way of sale."[114] Is there a contract between O and C? If a contract exists but is voidable, C passes good title to an innocent purchaser. If the contract is void, such purchaser cannot obtain valid title. The protection of innocent third parties plays a prominent role in all mistaken identity cases. The issue is less relevant between O and C, as the mistaken party can rescind for misrepresentation.[115] Little attention is usually devoted to the carelessness of O, not to mention X, the person C purports to be. The majority in Shogun held that no contract was formed between the finance company Shogun (O in the model example) and C. The decision was predominantly based on the construction of the written contract between Shogun and the person named in the contract.

Basic principles

[4.21] Before Shogun, the leading authority on mistaken identity was Lewis v Averay, [116] where Lord Denning MR held that a mistake as to identity renders a contract voidable, not void. The inconsistent case law distinguishes between dealings face-to-face[117] and instances where the parties are contracting via correspondence.[118] In the first scenario, the owner is presumed to intend to deal with the person in front of him, in the latter, the parties are described in the document. The principles are not applied consistently, the "blurring" factors being the protection of innocent purchasers, the exact moment the representation is made, and the actual intention of the mistaken party. In practical terms, the division is between making a contract with the person one intends to deal with or with the person one actually deals with. Problems

[109] Carter & Harland [1248]; Carter on Contract [22-130]
[110] Carter & Harland [1213]
[111] Carter & Harland [1201]
[112] Shogun Finance Ltd v Hudson [2004] 1 AC 919
[113] see: D W McLauchlan, Mistake of Identity and Contract Formation (2005) 21 JCL 1
[114] Shogun Finance Ltd v Hudson [2004] 1 AC 919 at 930 per Lord Nicholls
[115] Treitel p 342
[116] [1972] 1 QB 198
[117] Lake v Simmons [1927] ACN 487; Ingram v Little [1961] 1 QB 31; Phillips v Brooks Ltd [1919] 2 KB 243; Lewis v Averay [1972] 1 QB 198
[118] Cundy v Lindsay (1878) 2 App Cas 459; King's Norton Metal Co Ltd v Edridge Merrett & Co Ltd (1897) 14 TLR 98

arise when intention is directed towards a person one has never met before. While in Cundy v Lindsay[119] the contract was held void because O only intended to contract with the person named in the correspondence, in King's Norton Metal,[120] O was held to intend to contract with the writer of the letter. In the latter case, there existed no other entity of the assumed name, in the former, O knew of a company dealing under the name assumed by C.

The above distinctions, although upheld by Shogun, seem difficult to maintain in transactions conducted on-line.

Identity and attributes

[4.22] A distinction is drawn between mistake as to identity and mistake as to attribute(s). The prevalent view is that the former renders a contract void, the latter - voidable.[121] A further refinement is that certain attributes are so important that they form part of a person's identity and a mistake as to them can render the contract void.[122] Creditworthiness, however, is not one of them.[123] Accordingly, O who parted with goods on the basis of a fraudulent misrepresentation is interested in proving the fundamental importance of the buyer's identity. If the contract is void, O retains title to the goods.

A general point first. Contracts are formed with persons - not with identities or attributes. An identity need not be unique to a person: a person can have multiple identities, the same identity can be lawfully used by multiple persons. What can be unique, though, are attributes, or rather combinations thereof. Even when identity is claimed to be of fundamental importance, such as in contracts for specialized services, it is important only because it points to a person with specific attributes. After all, "identity is but an amalgam of various attributes."[124]

In on-line transactions, the "fundamental importance" of identity may be difficult to establish. This relates to the fact that the assumption of a different identity for on-line transactions is more widespread than in the real-world. People assume various electronic identities, be it due to privacy concern or as an expression of personal freedom. The web abounds with "George Bushes." Nobody can believe that he or she is contracting with the president of the United States and later claim that the identity of the other party was fundamental because he or she wanted to purchase the president's coffee mug.

It may also not be clear whether a misrepresentation of identity occurred. The existence of a real person using a given identity may be accidental and unknown to both O and C. C might be assuming what he or she thinks is a fictitious identity. If C does not pretend to be X, C is X.[125] There is no prohibition to adopt a different identity, as long as its use is not designed to escape liability or impersonate another entity. "Fundamental importance" of identity aside - there is no possibility of holding a contract void ab initio.

To illustrate: when someone transacts under the name Pussycat, the other party cannot claim that: a) "I intended to contract with another Pussycat," or, b) there is no Pussycat and therefore there should be no contract. There is a Pussycat. It is the person who sent the message signed "Pussycat." Similarly, if one assumes the name John Smith, one is John Smith. Pussycat and John Smith are equally valid electronic identities, although there is probably no credit card issued in the former name. The

[119] Cundy v Lindsay (1878) 2 App Cas 459
[120] King's Norton Metal Co Ltd v Edridge Merrett & Co Ltd (1897) 14 TLR 98
[121] Cheshire, Fifoot & Furmston p 279
[122] Treitel p 277, 267
[123] Treitel p 278; The Law of Contract para 4.106
[124] Cheshire, Fifoot & Furmston p 280
[125] Treitel p 274

association between person and name occurs only in O's mind. O's accidental knowledge of a person bearing a particular name demonstrates that the importance of identity is purely subjective.

When differentiating between identity and attributes, the difference between "name" and "identity" comes into play. There are a numerous motivations to contract with one particular person. It is illogical, however, to assume that one intends to contract with a person because of her name. Names constitute a pure reference, without regard to any attributes. Only some names (such as Bill Gates) imply the existence of certain attributes. If it was the actual person that was of fundamental importance - one should speak of mistake as to name or person, not identity.[126]

The importance of "identity" is limited to cases where the performance of the contract is specific to a given person.[127] This would be the case of professionals with particular skills or situations described in Boulton v Jones,[128] Said v Butt[129] or Sowler v Potter.[130] The identity-attribute distinction must be approached with caution whenever the transaction is of mass-market character, the seller is willing to contract with anybody and the contract can be performed by anybody.[131]

Method of communication: face-to-face and "in writing"

[4.23] On-line transacting renders it difficult to maintain the division between contracts formed face-to-face and those formed in writing. The legal explanation is that the mistake is identical in both situations:[132] O deals with one person but intends to deal with another. O deals with the writer of the letter or email, the person in front of him or on the other end of the telephone line. The technical explanation is that transactions are often a mixture of face-to-face dealings and correspondence. As not all on-line communications meet the requirements of "writing"[133] or enable a real-time communication approximating the qualities of "face-to-face" interactions,[134] they may be difficult to categorize as one or the other. The effect of the mistake - and ultimately the existence of a contract - cannot depend on the communication method or the distance between the parties.[135] In particular, it cannot depend on the fact whether a particular statement appeared on screen or on a paper document.

The communication method does, however, determine the quality and quantity of authentication information.[136] In Phillips v Brooks, the face-to-face scenario is described as enabling the identification of the other party by sight and hearing.[137] When dealing at a distance, via email or instant messengers, O is limited to validating the digital certificate of the purported sender, if any, or verifying the address information. "Authentication across a network … is more difficult than authenticating someone standing in front of you, simply because the authentication mechanisms are easier to fake and harder to verify."[138] Accordingly, the method of communication bears on the difficulty of authenticating C.

---

[126] the difficulty of defining "identity" is stressed by S Smith above at note 4 p 77; it must be noted that S Smith speaks of mistake as to person and mistake as to identity, p 76. It is unclear whether this division was introduced intentionally.
[127] The Law of Contract para 4.109
[128] (1857) 2 H & N 564, 157 ER 232
[129] [1920] 3 KB 497
[130] [1940] 1 KB 271
[131] Chitty on Contracts, 26th ed, vol 1, London 1989 para 356
[132] D W McLauchlan, Parol Evidence and Contract Formation (2005) 121 LQR 9 at 9
[133] see Chapter 8
[134] see Chapter 6
[135] S Smith, P A Atiyah, above at note 4 p 84
[136] Chissick & Kellman p 73
[137] Philips v Brooks [1919] 2 KB 243 at 247
[138] B Schneier, above at note 26 p 191, see also: H K Towle, above at note 39 at 238

Carelessness of mistaken party

[4.24] C is not the only person responsible for the mistake. C misrepresented who he or she is, but it is O who relied on this misrepresentation. As the intention to contract with a specific party is evaluated objectively, the party pleading mistake as to identity should have taken reasonable steps to authenticate the other party.[139] Most cases are characterized by some carelessness on the side of O. Being concerned with risk allocation, today's courts may proceed as if they had to decide whether a person has been negligent.[140] Holding the contract void rewards the careless O and punishes an innocent purchaser.

O's intention is evaluated on the basis of his or her behaviour: were O's efforts to authenticate C reasonable in light of the available information? According to Treitel: "[i]f a party takes the risk that the facts are not as he supposed them to be, or if he is simply indifferent as to the matter to which the mistake relates, the validity of the contract cannot be affected."[141] If O would not have contracted with C, had O not believed C to be X, why didn't O verify who he was dealing with, i.e. establish that X is X? In Cundy v Lindsay,[142] O verified neither the signature nor the actual address of the person ordering the goods. Taking into account that C did not forge O's signature and gave his own address, a simple inquiry could have revealed the fraudulent misrepresentation. In Ingram v Little,[143] O verified that X lived at the stated address but did not verify whether C was X, i.e. failed to authenticate C. Such authentication was performed in Lewis v Averay,[144] where C produced an "impressive looking pass" describing him as X. Unfortunately, O failed to validate the pass.

In Shogun, C produced the driving license of a Mr. Patel. Assuming that the driving licence contained a photo of the real Mr. Patel, C must have resembled him or replaced the picture with his own. C also forged the signature on the licence. The complicating factor was that C did not deal with O directly but via a car dealer. While the interactions with the latter can be described as face-to-face, the relationship with the former was embodied in a written contract. On the basis of a fax copy of the drivers licence, O confirmed the creditworthiness of Mr. Patel. O never verified whether the person presenting the licence was Mr. Patel.[145] In other words, no authentication of C and no validation of the document took place. The claim that the identity of the purchaser was of primary importance should only be upheld if any steps were taken to verify this identity,[146] alternatively, if the reliance on C's representations was reasonable and required no further proof. By verifying the attribute of creditworthiness of X, without confirming that C is X, Shogun's actions indicated that identity was irrelevant. Shogun was willing to contract with anyone creditworthy. Identity was only a means of verifying creditworthiness.

Contract formation perspective

[4.25] Mistaken identity can also be approached from a contract formation perspective. Allegedly, O's intention to contract with X prevents the meeting of minds if the other person is not X. O's mistake negatives the correspondence between offer and acceptance.[147] By the same token, as C knows of O's actual intention (to contract with X), no contract can be formed.[148] Many arguments speak against such

---

[139] Cheshire, Fifoot & Furmston p 274, 280

[140] The Law of Contract para 4.108, see also: H M Howard, The Negligent Enablement of Imposter Fraud: A Common-Sense Common Law Claim (2005) 54 Duke L J 1263 at 1271-1276

[141] Treitel p 279

[142] Cundy v Lindsay (1878) 2 App Cas 459

[143] Ingram v Little [1961] 1 QB 31

[144] Lewis v Averay [1972] 1 QB 198

[145] C Elliot, No Justice for Innocent Purchasers of Dishonestly Obtained Goods: Shogun Finance v Hudson (2004) 5 JBL 381 at 386

[146] The Law of Contract para 4.107

[147] The Law of Contract para 4.73; Carter on Contract [22-070]

[148] Cheshire, Fifoot & Furmston p 274, see also Lake v Simmons [1927] AC 487

approach. As indicated, O's intention to contract with X only, injects a subjective element into the discussion.[149] Furthermore, O's intention can be negatived only if it is clear that O intended to contract exclusively with X.[150] Consequently, there should be external indicia of such intention, e.g. efforts to authenticate X.

The principle that an offer directed to X can only be accepted by X remains debatable[151] and can be regarded as an example of one of the rare cases where identity becomes a contractual term. It must also be appreciated that O intends to deal with C and with X.[152] Such a distinction, however, does not enter his mind. O believes that C is X and intends to contract with C in this belief. The question remains: is O's belief reasonable?[153] Applying the reasoning in Lord Birkenhead's dissenting judgment in Shogun, fraud does not negative intention or vitiate consent.[154] Intention induced by fraud "is regarded by law as sufficient to found a contract."[155]

The test as to how the promisee understood the words spoken to him[156] cannot be applied as it was the promisee who induced the mistaken belief as to his or her identity. Without claiming that the test of "detached objectivity"[157] is more amenable to evaluating O's intention, O's subjective state of mind cannot negative agreement and render the contract void.[158] Furthermore, C's knowledge of O's intention cannot destroy the correspondence between offer and acceptance as C's identity is not a term of the contract and remains external to its content.[159] Identity becomes a term when it implies certain unique attributes. Otherwise, the contract has the same terms and subject matter,[160] irrespective of the other party's identity. It is intentionally made and does not cease to be an agreement "because it has been actuated by a mistaken motive."[161]

Accountability of X

[4.26] An issue that never arose in the mistaken identity cases was the potential accountability of X: the person whose identity was used. X was never held liable on the ground that somebody used his or her identity or on the ground that O's reliance on the information about X (as presented by C) was reasonable. The situation could change if the transaction included the use of digital signatures - if X was the subscriber named in a DC. If the Shogun scenario was mapped onto an electronic setting and decided in line with the rules established in the MLEC, MLES or the ABA Guidelines, O behaviour would be evaluated in light of the reasonableness of his or her reliance on the authentication information provided by C. Similarly, the position of X would differ, as the latter would not only have the duty to safeguard the information that permits the replication of his identity but would also be obliged to inform a third party of any compromise of such information. In the Shogun scenario, the mistake as to C's identity could have been avoided if there existed a duty to inform the motor vehicle register of the loss of a driver's license and if there was a possibility for O to validate the status of the license against a centralized database. In

[149] Carter on Contract [22-330]
[150] Taylor v Johnson [1932] AC 161 at 217; see also: Cheshire, Fifoot & Furmston p 274
[151] Boulton v Jones (1857) 2 H& N 564, see also Carter on Contract [22-310]
[152] Carter & Harland [1248]
[153] Associated Japanese Bank (International) Ltd v Credit du Nord SA [1988] 3 All ER 902, 913 per Steyn J; McRae v Commonwealth Disposals Commission (1950) 84 CLR 377 at 408 per Dixon J and Fullgar J
[154] Shogun Finance Ltd v Hudson [2004] 1 AC 919 at 932; see also: Whittaker v Campbell [1984] QB 318
[155] Shogun Finance Ltd v Hudson [2004] 1 AC 919 at 932
[156] Ashington Piggeries Ltd v Christopher Hill Ltd [1972] ACN 441 at 502
[157] Solle v Butcher [1950] 1 KB 671, 693 CA as per Lord Denning; Leaf v International Galleries Ltd [1950] 2 KB 86 at 89; Carter on Contract [22-180]; see also: E Stern, Objectivity, Legal Doctrine and Law of Mistaken Identity (1995) 8 JCL 15 at 19
[158] Carter & Harland [1248]; Carter on Contract [22-180]
[159] Carter on Contract [22-340]
[160] Bell v Lever Brothers Ltd [1932] AC 116 at 227
[161] Cheshire, Fifoot & Furmston p 271

sum, modified attribution rules would bring X into the discussion and burden him or her with the risk of unauthorized use of his or her identity.

Conclusions

[4.27] Problems of authenticating the other party to the contract concern mainly issues of proof and evidence. As in the case of problems of attribution, they need not be included in discussions of on-line contract formation. At the same time, the difficulties of remote authentication shed new light on the distinctions drawn in mistaken identity cases. These distinctions have accumulated critique even before the emergence of on-line transactions. It is questionable whether contracts should be treated as void for mistaken identity if the value of "identity" as a means of distinguishing between persons can be doubted. The fundamental importance of "identity" can only be sustained on the assumption that the party claiming mistake as to identity has undertaken reasonable efforts to authenticate the other party. As Internet-based methods of communication change the quality and quantity of authentication information, it becomes more difficult to evaluate the reasonableness of such efforts. On a practical level, on-line authentication efforts are doomed from the outset as there is no method of reliably establishing the identity of the person at the other end of the communication channel - notwithstanding the deployment of remote authentication technologies based on digital signatures.

Digital signatures do not identify the sender. The existence of a trusted third party does not change anything in this regard. Digital signatures can function as a reliable authentication mechanism only if the end user computer was secure. The reliability of any remote authentication technology depends on the security of the network or the security of the authentication information required to deploy such technology. The security of the network and the computer of the end-user are almost impossible to achieve in open environments, such as the Internet. Just like a person cannot be made accountable for all calls made from his or her equipment,[162] a subscriber named in a digital certificate cannot be held accountable for the unauthorized use of his or her private key.

Endless recounts of Alice and Bob exchanging secret keys with the help of certification authority Carol should be abandoned and replaced with the simple observation that identification on open electronic networks is difficult - if not next to impossible. Digital signatures, apart from being a misnomer, can only function in secure environments or closed networks. They can serve as tools of identification (and attribution) on the basis of an agreement, where subscribers agree to bear the legal effects of messages "signed" with the private key. In sum, unless the subscriber agrees to be bound in the event of an unauthorized use of a private key, the risk is borne by the recipient of the digitally signed message. A digital certificate, a certification authority or a complex encryption algorithm do not provide any assurance that the private key was used by the subscriber.

As in the case of electronic agents, digital signatures are a misnomer and unnecessarily blur legal analysis. Digital "signatures" are not signatures but a remote authentication technology built on a hybrid cryptosystem. Last but not least, even if some model laws provide that digital signatures can fulfil the same functions as traditional signatures, their importance from a contract law perspective is limited, as the existence, validity or enforceability of a contract rarely requires a signature.

[162] Federal Trade Commission v Verity International Ltd 124 F Supp 2d 193 (SDNY 2000)