ELSEVIER

Computer Law & Security Review

Mistaken identity, identity theft and problems of remote authentication in e-commerce

Eliza Mik

Singapore Management University, Singapore

ABSTRACT

Keywords:
Identity theft
e-commerce
Authentication
Digital signatures

The problem of mistaken identity in e-commerce transactions brings together seemingly unrelated issues: privacy, network security, digital signatures – and classic contract law. Combining an academic exercise with the practical implications of the insecurity of the Internet, this paper draws some unexpected conclusions regarding cases of mistaken identity and exposes flaws in popular legal arguments on the subject. Problems of mistaken identity must be analysed afresh with a number of factors in mind: the more widespread use of fictitious identities in on-line transactions, the higher incidence of identity theft and the greater difficulty of authenticating the other transacting party. The trend to preserve the privacy of Internet users indirectly clashes with efforts to ensure transactional security in e-commerce. An indispensable prerequisite of the latter is the ability to identify the other party to the contract. The problem of mistaken identity is not new – but it assumes a different scale in e-commerce transactions.

© 2012 Eliza Mik. Published by Elsevier Ltd. All rights reserved.

> *… 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]

1. Introduction

The choice to contract with a specific individual is often based on her special skill(s) or characteristics. Contractual intention may therefore be directed at a *particular* person. The resulting legal problems can be evaluated as part of the offer and acceptance model or from the perspective of the doctrine of mistake.[2] Offer and acceptance relate to contract formation; mistake is generally considered a factor affecting the validity of a contract. This paper focuses on mistake, in particular, on the technological aspects of mistakes pertaining to the identity of the other contracting party. In e-commerce, identities are embodied in information, not flesh.[3] Transactions occur over an open and inherently insecure network. It is therefore necessary to re-evaluate existing approaches to cases of mistaken identity. It becomes unavoidable to account for the fact that identifying the actual, physical person behind a click or an email may be next to impossible. Problems of identification are traditionally discussed alongside attribution, not intention. Attribution focuses on accountability for an act, intention relates to the existence of a contract. Both attribution and the intention to contract with a specific person require the ability to identify this person. As it is the recipient

---

[1] W Diffie, S Landau, Privacy on the Line: the Politics of Wiretapping and Encryption, 48 (1998).
[2] S Smith, Atiyah's An Introduction to the Law of Contract 76–77 (2006).
[3] Lucy Cradduck, Adrian McCullagh, *Identifying the Identity Thief: is it time for a (smart) Australia Card?* I.J.L. & I.T. (16) 2, 125, at 127 (2008).

who must prove that the (alleged) sender dispatched the message, attribution is predominantly a question of proof.[4] Before asking who is accountable for the transaction, it must be established whether a contract exists. The presence and effect of a vitiating factor must be taken into account prior to – or at least in parallel with – any discussions of contractual liability.

A mistake as to identity is a unilateral mistake: one party is mistaken, the other knows of the mistake or caused it. Generally, a mistake as to the identity of the other party renders a contract voidable.[5] In some circumstances, however, such mistake may render the contract void *ab initio*. It is these circumstances that require revision in light of the characteristics of e-commerce transactions.

1.1. The problem

In the classic scenario crook (C) fraudulently represents to the owner of goods (O) that he is another person (X) and on that basis O parts with goods to C by way of sale. 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 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. Little attention is usually devoted to the carelessness of O or to X, the person C purports to be. This problem has recently been revisited in *Shogun Finance Ltd v Hudson*.[6] The majority in *Shogun* held that no contract was formed between O and C. The decision was predominantly based on the construction of the written contract between O and X, the person named in the contract.

While difficulties of identification arise in all first time transactions between strangers, e-commerce transactions seem to exacerbate these difficulties and shed new light on the aforementioned legal problem. The possibility of holding a contract void (i.e. non-existent) due to a mistaken belief as to the other party's identity must be re-analysed with two factors in mind: *first*, a more widespread use of fictitious identities in on-line transactions than in the real world and a higher incidence of identity theft; *second*, the practical problems of remote authentication over insecure networks such as the Internet.

1.2. Terminology

Some terminological clarifications are necessary. "Identification" is the process of distinguishing one entity from another. "Authentication" has multiple meanings: to "establish as genuine" or to "associate oneself" with a document, as in "to sign."[7] For present purposes, "authentication" refers to the verification of an identity.[8] Authenticating documents differs from authenticating persons: senders authenticate *messages*; recipients authenticate the *senders* of messages. Authentication involves the presentation of authentication information that confirms the association between a person and an identifier. Authentication information consists in something a person *knows* (password, PIN), *possesses* (token, smartcard, passport) or *is* (biometric data). Access to authentication information enables the assumption of the identity verified by this information. In this sense, the term "identity *theft*" denotes the unauthorized use of authentication information relating to an existing person. Knowledge or possession of authentication information does not automatically imply that the person with such knowledge or possession *is* the person to whom the information rightfully belongs.[9] Lastly, as all e-commerce transactions are conducted at a distance, it seems more correct to speak of "remote authentication."

1.3. Broader context

Legal problems never exist in a vacuum. Mistaken identity and difficulties of authentication intersect with general privacy and security concerns posed by the Internet. The process of authentication requires the disclosure of authentication information. Privacy protection, on the other hand, aims at hiding the real identities of persons and preventing any association between them and their on-line activities.[10] Privacy protection requires the limitation of both the collection and the disclosure of authentication information. The more such information is revealed and the easier the access to such information, the greater the risk of its unauthorized use.[11] After all, "personal information" may serve as "authentication information."[12] Authentication information can be used to create *and* to verify an identity. In practice, using the authentication information of another person amounts to assuming the identity of such person. Accordingly, there is an inherent tension between privacy and the need to authenticate the other party in an e-commerce transaction. Privacy requires anonymity; e-commerce requires the disclosure of real identities. While being a tool to achieve privacy, anonymity is also a means of avoiding accountability. Privacy preservation measures may prevent effective authentication, whereas authentication attempts may violate privacy laws.

Additional complications arise from the fact that the Internet is an inherently insecure network. Practically every computer, or device, connected to the Internet can be

---

[4] W Ford, M S Baum, Secure Electronic Commerce, Building the Infrastructure for Digital Signatures and Encryption 336 (2001) ("*Ford & Baum*") p 336; another term used in legal literature is "non-repudiation."

[5] *Lewis v Averay* [1972] 1 QB 198.

[6] [2004] 1 AC 919 ("*Shogun*").

[7] Oxford English Dictionary; S Mason, *Validating Identity for the Electronic Environment*, 20 CLSR 3 at 166 (2004).

[8] R Shirey, RFC 2828, *Internet Security Glossary*, 13 (2000).

[9] Nicholas Bohm & Stephen Mason, *Identity and its Verification*, [2010] 26 CLSR 43–51, at 44.

[10] For a discussion of anonymity on the Internet see: A M Froomkin, *Flood Control on The Information Ocean: Living with Anonymity, Digital Cash and Distributed Databases*, 15 J L & Com 395 at 422 (1996).

[11] Holly K Towle, *Identity Theft: Myths, Methods, and New Law*, 30 Rutger's Comp & Tech L J 237 at 262 (2004) on the "Collision between Identity Theft and Privacy;" A Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 Yale J L & Tech 123 (2004–2005).

[12] J Grijpink, *Biometrics and Identity Fraud Protection*, [2005] 21 CLSR 254.