Chapter 7 - Determining "Dispatch" and "Receipt"

Eliza Mik, Singapore Management University
CHAPTER 7  DETERMINING “DISPATCH” AND “RECEIPT”

THE FORMATION OF A CONTRACT IS A CONCEPTUAL CONSTRUCT AND NOT A PHYSICAL FACT.¹

INTRODUCTION

[7.1] This chapter discusses the basic concepts used in determining the moment of contract formation: “dispatch” and “receipt.” “Receipt” is the main component of the principle, “dispatch” - of the exception. Either term can be tied to various events in the transmission of an electronic acceptance from the system of the sender to the system of the addressee. Determining the moment of “receipt” or “dispatch” must be distinguished from determining whether electronic acceptances become effective on receipt or on dispatch. Chapter 6 attempted to establish the legally relevant event; this chapter attempts to select specific elements in the communications infrastructure, which can be used to establish when this event is deemed to occur.

Dispatch and receipt are questions of fact. It can be objectively ascertained when a message enters or leaves the transmission channel or network, when it reaches a mail-server or when it becomes available for retrieval. It is by no means clear, however, which of these events bears legal significance.² Consequently, the application of the simple principle that “acceptance must be communicated” encounters unprecedented difficulties.

It may seem unusual to “dissect” the time of contract formation into two separate chapters and deal with effectiveness separately from “dispatch” and “receipt.” Such differentiation is necessary: defining the above terms raises different issues than those involved in making the choice between the principle of receipt and the postal exception. While the latter mainly relates to the speed of transmission, reliability and choice of communication method, the former concern the client-server model and the fact that messages traverse multiple networks. To date, such division was not necessary. Neither “dispatch” nor “receipt” was given much consideration or analysed in terms of accessibility, legibility or ability to

¹ Corbin para 3.26
process. Similarly, there was no need to dissect the individual components of the communication infrastructure. Such analyses are required once contracts are formed on-line.

“Dispatch” and “receipt” raise two sets of problems. First, open electronic networks are characterized by a number of risks, which have no counterparts in traditional communications. Second, due to the increased complexity of communication systems and the multiplicity of terminating devices, it becomes more difficult to select the particular point in time where dispatch or receipt is deemed to occur.

Practically all Internet-based methods of communication can be regarded as instantaneous. Substantial delays may, however, occur between specific stages in the communication process. The length of these delays depends on which element of the infrastructure is regarded as the point of dispatch or receipt. The moment of contract formation and - in some instances - the very existence of the contract depends on which point is selected.

Apart from establishing the precise time of contract formation, “dispatch” and “receipt” allocate communication risks. While the principle of receipt and the postal exception constitute basic tools of risk distribution, the latter requires further refinement in light of the increased risk of on-line communications. Messages are not only transmitted over an unreliable communication channel but also processed. “Processing” encompasses trans-coding, translation and reformatting. Each of these operations aims to adapt the message to the requirements of the next step in the transmission. Each time processing occurs there is a risk that the contents of the message will be interfered with and/or rendered illegible.

Even if an offer provides when acceptance becomes effective, it is doubtful that it specifically defines which events constitute dispatch or receipt. While intention remains decisive, parties rarely allow for the increased complexity of the communication landscape. Applying the offer and acceptance model to on-line transactions requires the development of default rules that reflect the intricacies of communications over open electronic networks, especially with regards to the client-server model. This is one of the instances where the novel transacting environment creates problems with few equivalents in the real world.

**Roadmap**

[7.2] This chapter commences with some general considerations, highlighting the main differences between traditional communications and those occurring on-line. It proceeds with an overview of the principles relating to “dispatch” and “receipt” and emphasizes the relative simplicity of the communication scenarios, which serve as the basis for the existing legal framework.

Next, the chapter describes a number of novel problems inherent in on-line communications. Taking email as an example, it describes the risks inherent in its transfer. The relationship between “receipt” and “notification” is revisited with regards to the difficulties of ensuring the legibility of messages on the side of the addressee. The chapter continues with a discussion of “deemed receipt” in those cases where the communication failure is attributable to the addressee, but the rejection of the message is justified or reasonable.

Subsequently, the chapter critically analyses the provisions relating to “dispatch” and “receipt” contained in the MLEC, the CUECIC, the ETA and the UETA. The focus is on how those regulations approach the distribution of communication risks in client-server architectures and to what extent, if any, they create Internet-specific rules for the time of contract formation.

Email remains the point of reference as it creates the most complex problems. Web-based interactions and instant messengers are mentioned only marginally because they raise a different set of issues. The problems presented in this chapter are common to all electronic messages, not just acceptances.
GENERAL CONSIDERATIONS

[7.3] The following paragraphs present a number of general considerations, which must precede any discussion relating to “dispatch” and “receipt” in open electronic networks.

Simplifications

[7.4] The technical complexity of communications over open electronic networks defies easy description. Numerous simplifications are therefore unavoidable. The discussion cannot include each possible client application, terminating device and network architecture. Even the most basic scenarios, however, illustrate the difficulties in applying the offer and acceptance model in an environment consisting of multiple interconnected networks. Discussing the client–server model alone conveys the complexity of the problems. The aim of this chapter is to be illustrative, not exhaustive. Any attempt to encompass all possible permutations is doomed from the outset and broad generalizations are unavoidable. Such generalizations may lead to unfair results in specific situations. Rather than looking for universal rules, it is better to focus on the additional factors that must be taken into account in determining the precise moment of contract formation. While some ground principles can be established, an in casu examination of the particular situation is always required. This chapter deals only with the basic communication scenarios but points to potential complications that inevitably arise when additional elements are included in the analysis.

Network Environments

[7.5] Being a network of networks, the Internet is a heterogenous communication environment where each network retains some individual characteristics. The Internet is not like the post or like the telephone. Despite its ubiquity, it does not (yet) have the uniformity of one global system where all participants can seamlessly exchange messages. Apart from a set of core protocols, which are a condition of transmitting data over the Internet, the application layer (i.e. the layer closest to the user) is characterized by a multiplicity of competing protocols and standards. Not all of them are interoperable. The basic unit in a networked environment is a LAN, which generally consists of a collection of computers in a single building or area. LANs often employ proprietary protocols that differ from the transport environment of the Internet. Routing from one environment to another may involve a conversion between the “idiosyncrasies of the two original networks” and require significant “repackaging” of messages. Such conversions are not always successful.

An electronic acceptance travels from the network of the sender to the network of the addressee. Senders do not know and generally cannot anticipate the receiving environment, i.e. the addressee’s mail-server, security policies, if any, the client application and the terminating device used to access, retrieve and display messages. The question arises: to what extent, if any, should senders allow for the idiosyncrasies of the addressee’s environment?

Physical and conceptual divisions

[7.6] It is often impossible to draw a physical line as to when risk should pass or to pinpoint the specific network element or device where certain processes occur. Both the Internet and the client-server architecture are networking concepts that may not readily translate into physically separable pieces of hardware. It can always be debated where transmission starts or where the Internet “begins:” at the dial-up modem, telephone socket or the outgoing mail-server? Similarly, the division between the user

---

4 See Chapter 2
5 Brookshear p 136
6 Brookshear p 138
environment and the message-handling environment, although obvious from a technical perspective, does not translate into clear demarcation lines relating to specific machines. Determining the network element a message must pass through or arrive at for dispatch or receipt to occur, is therefore ridden with difficulties. Even the terminology used in this chapter would raise the eyebrows of some computer scientists: is it correct to speak of “devices,” “servers,” “networks” and “information systems”? Technically, servers and clients are processes, not discrete pieces of machinery. The following discussion often treats those processes as if they were spatially separable, whereas in many instances their separation is only logical.

**Terminological Sensitivity**

[7.7] When attempting to define “dispatch” and “receipt,” the implications of the terminology must be fully understood. There may be significant differences in the time of formation depending on whether a message “reaches,” “enters” or “becomes available.” It is not only the network element that must be selected but also the verb, which describes the relationship between the message and the given element. Consequently, the existence of the contract may hinge on the selection and/or construction of a single word. It could be claimed that such situation not uncommon in the real-world. This time, however, this single word must derive from an understanding of the technologies underlying communications over open electronic networks.

**THE EXISTING PRINCIPLES**

[7.8] To date, the terms “dispatch” and “receipt” were subject to little legal analysis. Textbooks on contract do not contain a separate chapter or section discussing either term. Unlike in Chapter 6, where the paragraphs dealing with the “general principles” pertaining to the time of formation occupied multiple pages, the “general principles” pertaining to “dispatch” and “receipt” require far less space. The principle can be simply stated as: to be effective, acceptance must be communicated. As indicated in Chapter 6, the term “communication” carries many possible meanings and can be tied to numerous events in the contract formation process.8

When the PAR applies, acceptance is effective when a properly addressed letter is posted.9 Dispatch is associated with “posting”: placing a letter in a letterbox of the postal service or handing it to a postal employee. If dispatch is proper, it is generally irrelevant whether the letter ever reaches the addressee. Upon posting, the offeree loses control and is not responsible for “accidents happening at the post office.”10 The post does not act as the agent of either the sender or the addressee; it only transmits letters and is regarded as an independent third party.11

Postal communications involve at least two distributing platforms, the post offices of the sender and the addressee respectively, as well as two mailboxes, the sender’s and the addressee’s. The addressee’s mailbox can be located at his or her address or, in the case of PO boxes, at the post office. All these “components” are regarded as forming one system and no distinction is made between the delivery of a letter to the post office or its placement in a mailbox in the street.12 When the PAR applies, addressees bear the risk of all accidents during the time letters remain in the sender’s mailbox, as well as

---

7 For a detailed explanation of Mail User Agents, Mail Transfer Agents and the Mail Handling Environment, see: D Crocker, Internet Mail Architecture (2005) SMTP Internet Draft
8 Chapter 6 [6.5]
9 Carter on Contract [03-350]
10 Household Fire and Carriage Accident Insurance Co Ltd v Grant (1879) LR 4 Ex D 216 at 219
12 Corbin para 3.2
during their subsequent transfer to the sender’s post office. Even if a letter is lost during these initial stages, there is a valid acceptance and a contract is formed. If the PAR does not apply, letters are received when they come into the addressee’s possession, or when they are deposited in a place designated for that type of communications.\(^\text{13}\) Despite an early English case, where a letter sent in a sealed envelope was not considered received until it was opened by the addressee personally,\(^\text{14}\) it is not necessary that the letter be read or even opened.

In the case of telegrams, dispatch occurs at the telegraph office where the machine is located.\(^\text{15}\) It is not clear whether the message must leave the machine or whether typing the message “into” the machine suffices. Unlike telegrams, telexes can be received directly in the office.\(^\text{16}\) In Entores Ltd v Miles Far East Corporation\(^\text{17}\) and Brinkibon v Stahag und Stahlwarenhandelsgesellschaft mbH,\(^\text{18}\) the contracting parties operated their own telex machines.\(^\text{19}\) No additional steps to send or access messages were necessary and there was no dependence on intermediaries. In Leach Nominees Pty Ltd v Walter Wright Pty Ltd,\(^\text{20}\) the telex machine used by the sender was operated by third parties and acceptance was considered dispatched when the offeree committed the message to a public telex operator, not when the message was sent from the telex machine.

Slightly more analysis has been devoted to “receipt,” mainly in relation to the receipt of notices after office hours and the malfunctioning of the terminating device. Generally, receipt is associated with the arrival of the message at the addressee’s machine, for example, when the telex is physically reproduced in the recipient’s office during business hours.\(^\text{21}\) If arrival occurs after business hours, receipt is deemed to take place only once the office is re-opened on the following business day.\(^\text{22}\) The law deems certain occurrences as constituting receipt, presumably because they enable communication in the normal course of events. Thus, there may be a difference between technical receipt and legal receipt. For receipt to occur, the addressee’s terminating device need not be attended and need not be maintained in proper working order. If the terminating device malfunctions due to the addressee’s fault, the latter is deemed to have received the message or estopped from denying receipt.\(^\text{23}\) Although technically the message is never received, acceptance is effective and a contract is formed. If, however, a given communication failure is not the fault of the addressee, there is no receipt and therefore no contract.\(^\text{24}\) The existence of a contract may hinge on a technicality—the reason of the communication failure.

Existing principles relating to dispatch and receipt developed around simple communication scenarios. As a result, apart from logic and a general sense of fairness, there is little guidance how to apply the offer and acceptance model in more complex situations.

---

\(^{13}\) See: CISG Art 24, which states that a message is received when it is delivered to the offeror personally, to the offeror’s place of business or mailing address, or to the offeror’s habitual residence. P Fasciano, above at note 11 at 997

\(^{14}\) Arrowsmith v Ingle [1810] 3 Taunt 234

\(^{15}\) Henkel v Pape (1870) LR 6 Exch 7; Bruner v Moore [1904] 1 Ch 305; Cowan v O’Conner (1888) 20 QBD 640 at 642; Brinkibon v Stahag und Stahlwarenhandelsgesellschaft mbH [1983] 2 AC 34 at 38


\(^{17}\) [1955] 2 QB 327

\(^{18}\) [1983] 2 AC 34

\(^{19}\) In both instances, the interactions were taking place between principals who operated their own telex machines, Brinkibon v Stahag und Stahlwarenhandelsgesellschaft mbH [1983] 2 AC 34 at 42

\(^{20}\) [1986] 85 FLR 427 at 434

\(^{21}\) Tenax Steamship Co Ltd v Owners of the Motor Vessel ‘Brinmes’ (The Brinmes) [1974] 3 All ER 88 at 93

\(^{22}\) Tenax Steamship Co Ltd v Owners of the Motor Vessel ‘Brinmes’ (The Brinmes) [1974] 3 All ER 88; Schelde Delta Shipping BV v Astarte Shipping Ltd (The ‘Pamela’) [1996] 2 Lloyd’s Rep 249

\(^{23}\) Carter on Contract [03-410]

\(^{24}\) Entores Ltd v Miles Far East Corporation [1955] 2 QB 327 at 333
NOVEL PROBLEMS

[7.9] The following paragraphs describe a number of novel factors that must be included in the discussion when messages can be considered “dispatched” or “received.” None of these factors, taken in isolation, introduces the need for detailed legal analysis. It is their combined effect that creates a host of legal problems.

Number of originating and terminating “devices”

[7.10] When communicating over the telephone, fax or telex there is only one machine on each side of the communication channel: the sender’s originating and the addressee’s terminating device. Even if the communication process is mediated by the post or a telecommunication provider, it is generally clear when a message is dispatched or received. Only the originating and the terminating devices are taken into account, not the underlying communications infrastructure, that is - the intermediating devices. From the perspective of the transacting parties, communication is from phone to phone or from fax-machine to fax-machine.

Most communications over open electronic networks are based on the client-server architecture. In the case of email, there are at least two originating devices, the sender’s mail-client and the outgoing mail-server, and two terminating devices, the addressee’s incoming mail-server and the mail-client. Each of these devices could constitute the point at which acceptance become effective. Does dispatch occur when a message leaves the mail-client or the mail-server? Does receipt occur when a message reaches the mail-client or does arrival at the mail-server suffice? The decision has important implications for the time of formation, as there may be substantial delays between the moment a message arrives at the server and the moment it is transferred to the client.

In traditional communications one could examine the underlying telecommunications infrastructure, for example, switches or branch exchanges in the case of telephones. This infrastructure, however, has never been the subject of analysis from a contract law perspective and such need does not arise now. When parties talk over the phone, “dispatch” and “receipt” occur at their respective telephones and not at their public branch exchanges. The number of switches, intermediating carriers and interchange points involved in an international call is inconsequential. In communications over open electronic networks, different devices operate on various layers of the TCP/IP protocol. As this thesis focuses on processes occurring at the application layer,25 the discussion excludes devices or network elements operating at lower layers, such as routers, switches or bridges.26 In both instances, the intermediating devices remain transparent to the communicating parties and irrelevant from a contract-law perspective. As clients and servers operate at the application layer each of them can be regarded as a terminating or originating device.

To add complexity to the discussion, all communications at a distance involve multiple intermediaries.27 Some of them form part of the transmission channel, others can be regarded as belonging to the respective spheres of control of the sender or the addressee. Telecommunication carriers and the post are independent third parties and can be regarded as part of the communications infrastructure. Problems arise in evaluating the legal position of ISPs, which often provide some of the infrastructure used by the communicating parties, usually mail-servers. It is difficult to decide whether a particular device

25 See Chapter 2 [2.3]
26 Some definitions proposed by the model regulations include the network in the discussion. Technically, a network commences at the router or gateway, which operate at different layers of the TCP/IP stack. Depending which layer is analysed, a different device can be regarded as the first or last point in the network. Certain applications, such as firewalls, may operate across multiple layers; e.g., content filtering at the application layer and packet filtering on the network layer.
27 See Chapter 6 [6.15]
should be regarded as an originating/terminating device or as part of the general transmission channel. The time of formation may depend on the answer to this relatively simple technical question.

**Communication Risks**

[7.11] Open electronic networks introduce a number of risks that differ from those involved in traditional communications. These risks are illustrated by an example. RFC 3463 “Enhanced Mail System Status Codes”\(^{28}\) describes the reasons why an email may not be delivered or be delivered in unreadable form. Below is a non-exhaustive list of conditions precluding the receipt or legibility of an email. Problems may concern:

1) the recipient’s address,\(^ {29}\) mailbox,\(^ {30}\) or mail system,\(^ {31}\)
2) the delivery system,\(^ {32}\)
3) the protocol used to send the message,\(^ {33}\)
4) failures in translation, trans-coding or otherwise unsupported message media,\(^ {34}\)
5) security restrictions on the side of the receiving mail server.\(^ {35}\)

In sum, the risks inherent in email communications include:

(a) transmission risk, the risk of travelling over the Internet from the sender’s mail-server to the recipient’s mail-server. The transmission path is “assumed to be under the control of the destination or intermediate system administrator.”\(^ {36}\)

(b) storage risk at the receiving mail-server. The mail system is “assumed to be under the general control of the destination system administrator.”\(^ {37}\)

(c) access/retrieval, risks of the recipient accessing the mail-server and downloading the message.

(d) reproduction risks resulting from the processing of the message by the recipient’s mail-client. “Message content or media issues are under the control of the sender and the receiver, both of which must support a common set of supported content types.”\(^ {38}\)

---

\(^{28}\) RFC 3463 (2003) G Vaudreuil (“RFC 3463”)
\(^{29}\) RFC 3463 p 5; e.g. bad destination mailbox address, system address, mailbox address syntax.
\(^{30}\) RFC 3463 p 6; e.g. mailbox disabled or full, message exceeds administrative limit
\(^{31}\) RFC 3463 p 7; e.g. mail system full, available storage has been exceeded. Recipient may not be able to delete material to make room for additional messages; system not accepting network messages, message too big for system, larger than per-message size limit; system incorrectly configured.
\(^{32}\) RFC 3463 p 8; e.g. no answer from host, connection attempt was not answered, remote system busy or down.
\(^{33}\) RFC 3463 p 9, e.g., result of wrong protocol version.
\(^{34}\) RFC 3463 p 10; e.g. media not supported, conversion required and prohibited — content of the message must be converted before it can be delivered; such prohibitions may be the expression of the sender in the message itself or the policy of the sending host, conversion required but not supported — the message content must be converted in order to be forwarded but such a conversion is not possible or practical by a host in the forwarding path.
\(^{35}\) RFC 3463 p 11, e.g. delivery not authorized.
\(^{36}\) RFC 3463 p 4
\(^{37}\) RFC 3463 p 4
\(^{38}\) RFC 3463 p 4
Most of the above risks have equivalents in traditional communications and are comparable to technical failures or bad maintenance. Some, however, are novel. It is difficult to find real-world analogies for “wrong protocol version” or “failure in transcoding.” Telephones belong to the same universal system of circuit switched communications. It may be impossible to terminate a call or the quality of the call may be too low to discern the words spoken by the other party. The inability to communicate will not, however, be the result of any of the parties using the wrong phone or the incorrect transmission protocol. Similarly, letters are sent by the post, which is part of a universal postal system. The latter regulates the size of envelopes, parcels and mailboxes.

It is possible to allocate each of the above communication risks to one of the parties or to one of the intermediaries. If an electronic acceptance does not arrive at its destination due to the fault of an intermediary, the question arises which of the parties should bear the risk. The intermediary at fault may not be in contractual relationship with either contracting party and cannot be regarded as belonging to either party’s sphere of control. It may also be difficult to regard it as part of the general transmission infrastructure. For example, should the risks inherent in the operations of the “intermediate system administrator” mentioned under point (a) be borne by the sender or by the addressee? Even those risks that cannot be prevented or mitigated by either party must be placed on one of them. Any distribution of communication risks will therefore contain an element of arbitrariness. A communication failure must be attributed to an intermediary; the intermediary must in turn be allocated to the sphere of control of either party.

A number of broad assumptions can be made: there are only two possible risk-bearers, the sender (offeree) and the addressee (offeror). Intuitively, risks relating to dispatch should be borne by the sender, risks relating to receipt - by the addressee. It must further be assumed that (a) risks that can be prevented or mitigated by a party should be borne by that party; (b) intermediaries who remain in a contractual relationship with one of the parties should belong to this party’s sphere of control, i.e. the risks inherent in their operation should be borne by this party; (c) each party should be responsible for the part of the infrastructure it owns or controls.

The general transmission risks are roughly apportioned by the principle of receipt and the postal exception. The risks inherent in the operation of the originating and terminating information systems are allocated by defining “dispatch” and “receipt.” The moment of contract formation must be established with the full realization of its implications for the distribution of communication risks between the contracting parties. In particular, it must be remembered that the earlier the risk is transferred from the sender, the more risk is borne by the addressee.

**Receipt and legibility**

[7.12] Despite the fact that for receipt to occur addressees need not attend or maintain their devices or open each letter that arrives in the mailbox, it can be assumed that they do so at their own risk and that, generally, receipt implies the ability to learn about the contents of the message. While actual knowledge of acceptance is not required for its effectiveness, the ability to gain such knowledge by reading the message is presumed. The offeror should be informed whether the offeree decided to accept or reject the offer.  

In Internet-based communications, “receipt” (in the sense of arrival at the addressee’s mail-client or server) does not imply that the message can be read. The reason for this unusual situation is that the addressee’s mail-client may not be able to process and display a message composed on the sender’s mail-client. Addressees may not be able to read messages in certain formats or from certain sources. Senders,  

---

39 Carter on Contract [03-310]  
40 The problem is practically non-existent in instant messengers, as both parties must use the same system.
in turn, cannot always anticipate the addressees’ client application. Its characteristics may not be
apparent from the email address.

The problem differs from the failure to maintain a terminating device. In the current situation,
both the originating and the terminating device function correctly. The addressee’s mail-client, however,
is unable to trans-code or translate a message, resulting in its illegibility or different arrangement of its
contents.41 Neither party is at fault or unreasonable, both the sender’s and the addressee’s client
applications are widely used. Senders cannot be blamed for composing and dispatching messages from
Microsoft Outlook or Eudora, addressees cannot be blamed for receiving messages on hotmail.com. Yet,
one mail-application may not be able to display a message composed on the other. Similar problems arise
in the case of email attachments. If an attachment is sent in a proprietary format, such as the latest
version of Microsoft Word, the addressee may not be able to view the file unless he or she obtains
converting software or installs the same version.

In paper-based communications the “format” of a letter is not problematic. What is placed in an
envelope is identical to what is delivered to the addressee. Letters can be lost or damaged, but are not
rewritten by postal employees or by the addressee’s mailbox.42 Letters may be written in foreign
languages and necessitate a translation or encrypted and require decryption. In both instances the
addressee obtains “unreadable” content. In both instances, however, it is the sender who intentionally
dispatched the letter in an “unreadable” form, most likely to preserve the confidentiality of its contents.
The contents were not rendered unreadable in transit or altered by the addressee’s system. With
electronic communications, illegibility may be the result of processing by one of the intermediating
systems, most probably the addressee’s client. It cannot be assumed that proper dispatch and successful
transmission result in receipt enabling communication.

The problem of illegible acceptances must be acknowledged but not over-exaggerated. Garbled,
altered or incomplete email messages occur frequently enough to warrant legal attention and are
statistically more likely to occur than in the case of traditional communications. The mere fact that there is
no single case on “garbled acceptances” speaks for itself.43

The addressee’s inability to process messages originating from the sender’s system raises two
issues: is there receipt if a message cannot be read (i.e. does not enable communication) and are senders
obligated to ensure that messages are readable (i.e. do they bear the risk of illegibility)? There are two
possible approaches.

First, it is commonly understood that if receipt fails without the fault of the addressee, there is no
contract. As in the case of traditional communications, senders should not bear the risk of the proper
functioning of the addressee’s terminating devices, in this case - the mail-server and/or mail-client. The
“ability to process” cannot, however, be subsumed under the category of “proper functioning” as there is
nothing improper about the addressee’s system and the inability to read a message is most likely the
result of incompatibilities between mail-client software, not bad maintenance. If both parties use popular
systems, neither party is at fault. As it is impossible to fairly allocate the risk of illegibility, it is safest to
assume that there is no receipt and therefore no contract. Accordingly, as long as there are differences in
email applications, on-line transactions will increase the number of instances where no contract was

41 For a detailed explanation of compatibility problems between email clients see: Avoiding and Surmounting E-Mail
Incompatibility Problems, available at www.gustavus.lib.ak.us/computer/training/readable-email.htm; When
Problems Occur with HTML Email, available at www.enewsbuilder.net/enewsbuilder/e_article000050099.cfm. See
discussion of the limitations of email as a means of giving notice.
42 Chissick & Kelman pp 76, 81
43 In Henkel v Pape [1870] 23 LT 419, the offeror sent the offeree a telegraphic message offering to buy three rifles,
the word “three” was transcribed as “the.” The offeror was held liable to purchase fifty rifles.
formed due to the fact that the addressee was not at fault. At the same time, recipients of illegible messages should be obliged to immediately notify the sender about such occurrence to enable them to resend the message.

Second, it is possible to adopt an “orthodox” approach and regard receipt as more than a mechanical fact, such as the arrival at a specific machine. Consequently, it could be claimed that senders must ensure that messages are readable. While this approach is consistent with the classic theory of the meeting of minds and the requirement of communication, it also implies that the sender’s risk extends to the moment the recipient can read the message. As a result, senders would bear the risks of the message’s retrieval from the addressee’s mail-server, the risk of intermediary storage as well as the risks inherent in the processing and reproduction by the addressee’s mail-client. Senders would bear risks of events over which they do not have any control and which they cannot predict. To mitigate those risks, they would be forced to provide messages in multiple formats or inquire about the characteristics of the addressee’s system prior to the dispatch of the email containing acceptance. This would, however, require a relatively high level of IT literacy on both sides of the transaction and possibly the installation of additional email applications to provide for multiple possibilities.

Alternatively, all emails could be sent in plain text. Although only the latter possibility guarantees universal legibility, it seems unrealistic as most email relies on the enhanced formatting capabilities of HTML. It is just as unrealistic to require that everybody exchanged email in plaintext, as it is to require that everybody used the latest versions of an email application, which supports multiple formats and message content encodings. Requiring that senders ensure legibility would not only extend their risk beyond those encountered in traditional communications but have far-reaching implications for the general usage of email in on-line contracting.

The risk of illegibility becomes easier to apportion when one party uses an outdated, proprietary or uncommon email application. While it remains difficult to speak of fault, at least the problem becomes attributable to one of the parties. In practice, courts will face difficult situations with the answer to the question whether there was receipt hinging on a technicality. Legal analysis will include an examination of email applications used by the parties.

Deemed Receipt

[7.13] The previous sections focused on the increased risk of failed receipt and the risk of illegibility. This section discusses the addressee’s right to reject a message and preclude receipt. A situation rather uncommon in traditional communications.

Generally, if failed receipt is not the addressee’s fault there is no contract. 44 If failed receipt is attributable to the addressee, for example, due to bad business practice or failure to maintain the terminating device, the addressee is estopped from denying receipt. 45 A contract is formed. Open electronic networks create a number of situations where receipt fails due to reasons attributable to the addressee but the latter cannot be estopped from denying receipt. The addressee may reject a message, such rejection may, however, be justified or reasonable. Justified restrictions placed on incoming communications must be distinguished from bad maintenance, such as failure to empty one’s mailbox or update the email application.

While the offeror’s “right to reject” a message containing an acceptance may appear incomprehensible at first, it can be explained on the basis of the growing security concerns created by

44 Entores Ltd v Miles Far East Corporation [1965] 2 QB 327 at 333 by Denning LJ
45 Tenax Steamship Co Ltd v Owners of the Motor Vessel ’Brinmes’ (The Brinmes) [1974] 3 All ER 88 at 113 per Megaw LJ; Car and Universal Finance Co Ltd v Caldwell (1965) 1 QB 525, see also: S Hill, Flogging A Dead Horse – The Postal Acceptance Rule and Email; (2001) JCL, vol 17, p. 157
viruses, trojan horses, worms and unsolicited commercial email, otherwise known as spam. Individually and collectively, these phenomena pose a threat to any resource or application hosted on mail-servers and mail-clients, or to the network as a whole. It must be assumed that any person connected to the Internet has the right - and sometimes a legal obligation - to protect his or her network resources from the above threats by appropriate technical measures.

Protective measures, such as spam filters, firewalls and anti-virus software, operate on various points in the network. For example, anti-virus software and spam filters may be implemented on servers or on client machines. The individual settings of these methods depend on the security policy of the addressee. Depending on the type and configuration of a given measure, messages may be precluded from entering the mail-server, the mail-client or the network. There is always a risk of so-called false positives - the rejection of messages that carry legitimate content. Security measures are justified but create the risk that they will occasionally “file out” an acceptance. Who bears the risk of rejected acceptances?

In deciding whether the rejection of a particular message is permitted, it must be considered whether the security measures are reasonable in light of the resources being protected. As a security policy that appears conservative and restrictive on one day, may turn out to be lenient and permissive three months later, courts will find it difficult to determine the reasonableness of the individual settings of a protective measure. If the rejection of a message is unjustified or unreasonable (i.e. if the security setting were too high), the default situation is reverted to – deemed receipt and the formation of a contract. This places the risk of unjustified or unreasonable security measures on the addressee. The latter must regularly monitor so-called “quarantined” messages, i.e. emails that have not been permitted inside his or her network or mail-server but kept in an external repository for inspection before final deletion.

The addressee’s protective measures must, however, also be taken into account by senders. The latter should make certain basic assumptions regarding the addressee’s ability to receive messages. Care must be taken not only with regards to the correct address, but also regarding the format of messages, the address the message is send from, the size of messages and the text in the subject line. Sending a 300MB file to an email account which is generally known to provide little storage is as unreasonable as putting the words “sex” or “$$” in the subject line or sending corporate communications from a hotmail account. In both instances, the sender faces a high likelihood of failed receipt - even the least conservative security software will reject messages containing the said words, many corporate networks reject messages dispatched from hotmail and similar services.

Where the rejection is justified or reasonable in light of the prevailing security practices, addressees cannot be estopped from denying receipt and no contract is formed. As the evaluation whether rejection was justified or reasonable occurs post factum, in many instances there will be uncertainty as to whether receipt occurred and a contract exists. Legitimate messages carrying acceptances may fall victim to conservative filter settings and firewalls. There will be no receipt unless the rejection of the message was unreasonable, such as in the case of misconfigured filter software. Determining whether the addressee is “at fault” will require a consideration of multiple additional factors. As in the case of problems relating to legibility, a more nuanced approach must be developed.

46 E Zwicky, S Cooper, Building Internet Firewalls, 2nd ed, Sebastopol 2000, par 16.1.2.1, 16.1.2.2
47 C Hunt, TCP/IP Network Administration, 2nd ed, Sebastopol 1997, Chapter 12
48 Ford & Baum p 144
49 Greenstein & Feinman p 276
PROPOSED SOLUTIONS

[7.14] The following sections examine the provisions relating to the time of formation proposed by the MLEC, the CUECIC, the ETA and the UETA. They illustrate the difficulties in providing simple rules that could be universally applied to all on-line communication scenarios. Historically, the MLEC constitutes the first attempt to define “dispatch” and “receipt” and is therefore analysed in greater detail. The CUECIC is discussed in parallel with the MLEC. The ETA is examined to the extent its provisions differ from those of the MLEC. UETA provides an example of a North American solution, which slightly diverges from the MLEC approach. The regulations propose default rules absent agreement.50

Three observations must be made before proceeding. First, to avoid interference with existing legal principles, none of the model regulations contains substantive rules prescribing whether electronic acceptances become effective upon dispatch or upon receipt.51 They try to electronically replicate the tests used for dispatch and receipt in paper-based communications, namely: “the moment when the communication left the sphere of control of the sender and the moment when it entered the sphere of control of the recipient.”52 Second, none of them acknowledges the client-server model, which constitutes the common denominator of most Internet-based communications. Third, the regulations stop short of prescribing that messages must be received in legible form and do not establish a general obligation to adequately maintain or monitor information systems.

For the sake of clarity, the terms “message,” “sender” and “addressee” are used throughout the discussion although the above regulations may use different terminology.53

Defining “Dispatch”

[7.15] The following paragraphs review the definitions of “dispatch.” The main problem relates to determining whether, assuming that the PAR applies, electronic acceptances are effective upon leaving the mail-client or the mail-server. Two common threads in the discussion are the loss of control and the placement of the message in the transmission channel.

Under MLEC Art 15 (1) dispatch of a message occurs “when it enters an information system outside the control of the originator or the person who sent the message on behalf of the originator.” The definition relies on three keywords: “control,” “entry” and “information system.” The latter is defined as “a system for generating, sending, receiving, storing or otherwise processing data messages.”54 It remains unclear whether “information system” refers to clients, servers or the whole network.55

Control

[7.16] The MLEC associates loss of control with the start of transmission.56 Technically, transmission commences when the outgoing mail-server introduces the message into the transport environment.57 Pressing the “send” button only transfers the message from the mail-client to the mail-server.

The mail-client is on the sender’s computer and therefore generally under his or her control.58 Mail-servers are generally operated by ISPs. In many instances there is a discrepancy between the loss of

50 E.g. MLEC Art 15 (1) and Guide to Enactment para 20
51 See: Carter on Contract [03-430] on the lack of substantive rules regarding contract formation in the ETA
52 A/CN.9/528 para 149
53 E.g. MLEC Art 2 uses “data message” and “originator,” UETA Section 2 (7) uses “electronic record”
54 MLEC Art 2 (f)
56 Guide to Enactment para 101
control and the start of transmission. If senders do not operate their own mail-server and choose an ISP to provide this service, they exercise no control over the mail-servers. In such situation, dispatching the message from the mail-client is synonymous with “loss of control.”

Art 15 states that loss of control encompasses situations where senders use the services of “persons who send messages on their behalf.” Consequently, the moment of dispatch depends on whether the ISP is regarded as acting on the sender’s behalf or as an independent third party.

It has been suggested that this moment should depend on the actual control of the mail-server and on the possibility to retract the message. The ability to retract is illusive even if the mail-server is controlled by the sender and need not be discussed any further. The moment of dispatch raises a general question about the role of intermediaries in the communication process. Some intermediaries are chosen by the parties, others are implicit in the functioning of the communications infrastructure and form part of the transmission channel. Are ISPs like the post or telecommunication carriers? In the case of the post, “transmission” commences when letters are placed in the mailbox, not delivered to the post office. The mailbox, however, constitutes part of the postal system. The latter, in turn, is not considered as an agent of either the sender or the addressee but an independent third party. It could be claimed that if both Internet connectivity and mail-servers were provided exclusively by Australia Post or a single government-owned telecommunications provider, such “ISP” would bear more similarity to the post and the mail-server could be regarded as part of the transmission infrastructure. Leaving the mail-client would be synonymous with the loss of control, similar to placing a letter into a mailbox.

Such view must be opposed. Mail-servers are not mailboxes and ISPs are not independent third parties. ISPs are chosen by and remain in contractual relationships with senders. ISPs provide the sender’s part of the communication infrastructure. Even if senders exercise no technical control over mail-servers, they must be taken to assume the risks of their operation (i.e. uptime, configuration, frequency of dispatch). The fact that a person chose to use an ISP instead of running his or her own mail-server should not be determinative for the moment of formation. Furthermore, the latter should not depend on the particular system the message was dispatched from. After all, a sender might dispatch the acceptance from his or her home computer (where the mail-server is provided by the sender’s ISP) or from an Internet café (where the mail-server is provided as part of the general service). If the moment of dispatch depended on the actual control of the mail-server, it would occur when leaving the mail-server in the first scenario and, possibly, when leaving the mail-client in the second. It would be in the sender’s interest (assuming the PAR applied) not to use his or her ISP or in fact, any infrastructure owned or controlled by them.

Most importantly, the earlier the sender’s risk ceases, the sooner it is transferred to the addressee. If “dispatch” depended on the actual control of the mail-server and the ISP was not regarded as acting on the sender’s behalf, the addressee would bear the risks of operation of the sender’s mail-server. It appears more correct to treat the mail-client and the mail-server as one device. Although, technically, they perform two independent operations, their “common goal” is to place the message in the transport environment.

58 For the sake of simplicity we disregard whether the sender uses a shared computer, e.g. in an Internet café. It is also irrelevant whether the mail-client takes the form of a browser, as in the case of web-mail, or a dedicated email application, such as Outlook.
59 P Fasciano, above at note 11 at 996; see also: Chissick & Kelman p 82
60 If a mail-server is configured to pass messages onto the Internet at short time intervals, the only way of retracting a message is to immediately disconnect the mail-server. If the sender uses an ISP, the ability to retract generally does not exist.
The comments to Art 15 complicate matters by stating that systems outside the sender’s control may be systems of an intermediary or the addressee.61 The assertion that the intermediary’s system is outside the control of the sender appears to contradict Art 15 (a) where “control” relates to the sender or to persons acting on his or her behalf. The definition of “intermediary” focuses on the relationship between originators and addressees, not on relationships with intermediaries, who only receive, transmit or store messages.62 It could be assumed that the MLEC draws a distinction between intermediaries acting on the sender’s behalf and intermediaries forming part of the general transmission infrastructure. Art 15 and the definition of “intermediary” suggest otherwise.63 Consequently, the MLEC appears to differentiate the moment of dispatch depending on the actual control of the mail-server. If the PAR applied to email, the time of formation would depend on the sender’s control of the outgoing mail-server.

**Entry**

[7.17] The term “entry” is used to define both “dispatch” and “receipt.” “Entry” denotes the availability for processing within an information system.64 The “availability for processing” does not, however, relate to or imply legibility.65

Dispatch does not occur if the message reaches the addressee’s system but fails to enter it66 either because the system does not function properly, or, “while functioning properly cannot be entered into by the data message.”67 An addressee is not placed under “the burdensome obligation to maintain its information system functioning at all times.”68 It appears questionable why the addressee’s obligations relating to system maintenance are discussed under “dispatch” not “receipt.” Assumedly, the comment relates to ‘bounce back’ notifications: dispatch does not occur if senders are informed of delivery failure. In such scenario, senders are obliged to re-send the message.

“Entry” should be consistent with “loss of control.” As the MLEC does not clarify whether control is lost when messages leave or enter outgoing mail-servers, “entry” can relate to the transport environment or to the mail-server. In the latter situation, dispatch would occur despite the message being queued on the outgoing mail-server. This would mirror the traditional principle that letters are considered sent when placed in a mailbox. Mailboxes, however, form part of the postal system and can be regarded as part of the transmission channel whereas the mail-servers are either operated by the sender, or persons acting on his or her behalf.

[7.18] The CUECIC replaces “entry” with “leave.”69 As the definition of “information system” is identical to the one in the MLEC,70 it remains unclear whether messages must leave the mail-client or the mail-server.71

[7.19] The ETA presents an even more intricate approach. According to Section 13 (1) if a message “enters a single information system outside the control of the originator,” dispatch occurs when it enters

---

61 MLEC Guide to Enactment para 101
62 MLEC Guide to Enactment para 38
63 See MLEC Art 2 (e) and Art 15 as well as paras 38, 39 and 40, where the term “intermediary” points to third parties other than senders and addressees and encompasses persons dealing “on behalf of another person.”
64 MLEC Guide to Enactment para 103
65 MLEC Guide to Enactment para 103
66 MLEC Guide to Enactment para 105
67 MLEC Guide to Enactment para 104
68 MLEC Guide to Enactment para 104
69 CUECIC Art 10.1
70 CUECIC Art 4 (g)
71 A/CN.9/528 para 149: The preparatory works elaborate that information systems must be distinguished from “information service providers or telecommunication carriers that might offer intermediary services or technical support infrastructure for the exchange of data messages.”
that system. According to section 13 (2) if a message “enters successively two or more information systems outside the control of the originator,” dispatch occurs “when it enters the first of those information systems.”

By definition, messages travelling over the Internet pass through multiple information systems. ETA does not define “control” or explain the relationship between the successive systems. The concept of single information system does not facilitate the distinction between mail-clients and mail-servers, or between mail-servers and the transmission environment. It is irrelevant how many systems a message passes through if all those systems are beyond the sender’s control. To complicate matters, mail-servers and mail-clients can often be regarded as part of the same information system.  

The Explanatory Memorandum to the Electronic Transactions Bill 1999 associates dispatch with the beginning of the electronic communication. It also states that dispatch occurs when the message “enters the originator’s Internet service provider’s system.” As a result, the ETA regards the sender’s outgoing mail-server as remaining outside his or her control and associates the commencement of transmission with dispatch from the sender’s mail-client. This solution is not only inconsistent with the technical functioning of email but also, as discussed above, implies an earlier commencement of risk for the addressee. The Explanatory Memorandum does not provide for the possibility that the mail-server might be under the sender’s control.

[7.20] UETA Section 15 (a) establishes that a message is sent when it:

1. is addressed properly or otherwise directed properly to an information processing system that the recipient has designated or uses for the purpose of receiving messages of the type sent and from which the recipient is able to retrieve the message;
2. is in a form capable of being processed by that system; and
3. enters an information system outside the control of the sender or of a person that sent the message on behalf of the sender or enters a region of the information processing system designated or used by the recipient, which is under the control of the recipient.

Apart from the loss of control, UETA emphasises that dispatch must be “proper.” Senders must have “specific information, which will direct the [message] to the intended recipient.” Messages must also be capable of being processed by the addressee’s system. It is in the interest of both parties to refrain from using proprietary or less popular formats. In other words, messages must be sent to the right system in the right format, thereby increasing the likelihood of receipt and legibility. Messages that cannot be processed by the addressee are not dispatched. The level of detail can be explained by the fact that the effectiveness of electronic acceptances on dispatch is more likely in the US.

UETA Section 15 (a) (3) recognizes that messages may technically never leave the information system under the sender’s control. It is unclear whether “information system” refers to a network, computer or service provider. Absent an explanation whether the term relates to a physical or logical division, the control test is difficult to apply. It can be claimed that when parties communicate on the same LAN or intranet they remain within a closed network and are therefore beyond the focus of this analysis.

---

72 see below at [7.25]
73 Electronic Transactions Bill 1999, Explanatory Memorandum p 12
74 Electronic Transactions Bill 1999, Explanatory Memorandum p 12
75 UETA Section 15, comment 2
76 UETA Section 15, comment 2; see also: S Williston above at 11 para 6:35
77 UETA Section 15, comment 2
79 see definition of “information system” in UETA Section 2
Similarly, popular service providers like hotmail.com can be regarded as one logical entity, one information system - despite its distributed architecture.

**Defining “Receipt”**

[7.21] The following sections examine the definitions of “receipt,” which determines the moment of contract formation whenever electronic acceptances are subsumed under the principle. The length of time messages may spend on the addressee’s incoming mail-server can be considerably longer than the length of time messages generally spend on the sender’s outgoing mail-servers. The implications of the definition for the exact moment of formation are therefore wider reaching than in the case of “dispatch.”

According to MLEC Art. 15 (2), “receipt” occurs

- (a) if the addressee has designated an information system for the purpose of receiving messages, receipt occurs:
  - (i) when the message enters the designated information system; or
  - (ii) if the message is sent to an information system of the addressee that is not the designated information system, when the data message is retrieved by the addressee;
- (b) if the addressee has not designated an information system, receipt occurs when the message enters an information system of the addressee.

The provision raises a number of interrelated problems. The terms “entry” and “retrieval” cannot be understood without narrowing down the definition of “information system.” Further complexity is added by the term “designation.”

**Information System**

[7.22] The moment of receipt depends on whether a message is sent to a designated or non-designated information system. The scope of the term is unclear. A broad meaning implies an early cessation of the risks borne by the sender. For example, if “information system” encompasses the whole network, entry occurs when a message enters the router or gateway, or any first point that is considered as belonging to the network.\(^\text{80}\) The sender would not bear the risks of any occurrences within the network, including protective measures placed before the mail-server. A narrower meaning exposes the sender to the risks occurring before the message arrives at a particular point within the network. The existence of a contract or the moment of its formation, may hinge on the definition of “information system.” The MLEC is inconclusive - “information system” can include a communications network, an electronic mailbox or even a tele-copier.\(^\text{81}\)

**Entry and retrieval**

[7.23] In the case of designated information systems receipt occurs upon entry. It is unclear which part of the system must be “entered.” Messages pass through and enter a number of network elements before becoming available to the addressee. There are many possible points of entry that could be regarded as decisive for the time of formation. Depending on the definition of “information system,” it could be mail-servers, mail-clients, firewalls, proxy servers and routers.

Absent designation, receipt occurs on retrieval. What element of the information system does “retrieval” point to? As described earlier,\(^\text{82}\) messages are generally delivered to incoming mail-servers, not mail-clients. Mail-clients retrieve messages via POP3 or access them through IMAP. Assuming that the

---

\(^{80}\) The choice of computer network device would also depend on which layer of the TCP/IP protocol is examined.

\(^{81}\) See definition in MLEC Art 2 (f) and Guide to Enactment para 40

\(^{82}\) See Chapter 2 [2.6], Chapter 6 [6.19]
MLEC does not differentiate between protocols, any method to view the message is included in the term “retrieval.” Technically, however, messages may not be transferred onto the mail-client and remain on the mail-server. Consequently, the relevant point seems to be the mail-server, as this is where messages can be retrieved from.

It can be assumed that “entry” also relates to the mail-server. Such interpretation is dictated by the fact that this is the earliest moment when a message becomes available for retrieval and therefore the earliest point in time when the sender’s risk could cease. Sending messages to non-designated systems extends the sender’s risk: receipt occurs only when the message is actually retrieved. The delay between “entry” and “retrieval” may be substantial. Messages may remain on the mail-server for extended periods of time before being retrieved. The provision is open to manipulations as addressees may know about the message and intentionally fail to retrieve it.

With non-designated systems, senders bear the risks inherent in the delay between entry and retrieval, between the moment a message becomes available (i.e. retrievable) and the moment it is retrieved. During this period, the offer may still be withdrawn even if the acceptance is already on the mail-server, technically available to be retrieved and read. Even if the mail-server crashes due to a fault of the addressee (for example, due to bad maintenance), there is no receipt. This would constitute an alteration of the traditional principles, where the malfunctioning of the terminating device due to the fault of the addressee does not preclude receipt. This argument could be countered with the observation that the mail-server need not be regarded as the terminating device but part of the transmission channel. In sum, the lack of clarity with regards to what constitutes designation is exacerbated by the lack of clarity regarding whether it is the addressee’s client or mail-server that constitutes the terminating device.

[7.24] CUECIC abandons the distinction between “entry” and “retrieval.” According to Art 10.2, receipt occurs when messages become “capable of being retrieved by the addressee at an electronic address designated by the addressee.” Receipt at a non-designated address occurs when messages become “capable of being retrieved by the addressee at that address and the addressee becomes aware that the message has been sent to that address.” The provision raises two sets of problems.

First, in non-designated addresses, the objective component (availability) is supplemented by a subjective element (awareness). It is unclear why awareness relates to the message’s dispatch, not receipt. It can be assumed that once the addressee knows that a message has been sent, he or she must monitor the relevant system for incoming communications – even if such system is not designated.

Second, “awareness” raises problems of proof. “Awareness” was considered more “equitable than holding the addressee bound by a message sent to an information system that the addressee could not reasonably expect would be used in the context of its dealings with the originator or for the purpose for which the data message had been sent.” At the same time it was admitted that “awareness” gives power to the addressee to effect receipt and places a heavy evidential burden on senders. Considering the vagueness of “designation,” in many instances receipt could exclusively depend on “awareness.” This would constitute an alteration of the traditional principles which regard “receipt” as an objective event, unrelated to any subjective occurrences on the addressee’s side.

83 A/60/17 para 78
84 A/60/17 para 82 During the preparatory works it was admitted that the provision created legal uncertainty as “awareness” is a subjective circumstance not easily proven by the sender. It was held, however, that awareness could be proven by other objective evidence”.
85 A/CN.9/528 para 143
86 A/CN.9/528 para 144
Third, messages are presumed to be capable of being retrieved (i.e. available) when they reach
the addressee’s electronic address. Messages need not enter. The CUECIC disregards the fact that,
technically, messages may reach the system, be rejected by a protective measure and not become
retrievable. Receipt would occur despite such rejection, even if the latter was justified.

Designation

[7.25] The implications of “designation” are far-reaching. The delay between entry and retrieval may be
considerable and defer the moment of contract formation - even if the communication method is
instantaneous. Absent a general obligation to monitor information systems, new messages may remain
unretrieved for extended periods. In non-designated system, receipt depends exclusively on the
addressee’s discretion or awareness.

Despite its significance the MLEC does not define “designation.” Designation is not
synonymous with ownership or control; the designated system need not be a system of the addressee.
The term covers a system specifically designated, for example, “where an offer expressly specifies the
address to which acceptance should be sent”. The comments state that the mere indication of an email or
telecopy address on a letterhead does not constitute designation. One must ask: what does? Contract
formation may be precluded or delayed on the basis that an acceptance was sent to a non-designated
system. The problem brings to mind “alternative acceptances” – an “acceptance” communicated via a
method other than that requested may not be regarded as acceptance. In Chapter 5, the issue concerned
the offeree choosing the wrong method of communicating acceptance, in this discussion, the issue
concerns choosing the wrong address or information system.

While the CUECIC uses “designation” in relation to “electronic address,” not “information
system,” the MLEC appears to use these terms interchangeably. The relationship between “information
system” and “electronic address” must be briefly examined. Electronic addresses generally refer to
accounts on mail-servers. One mail-server can host multiple accounts. Multiple mail-servers may be part
of the same information system. This can be explained by looking at the structure of an email address. The
latter consists of a character string identifying the individual account, the symbol @ and the name of the
mail-server that should receive the message. The name of the mail-server is specific to the domain in
which it is located, i.e. the network to which the server belongs. The second part of an email address
could be regarded as pointing to an information system, whereas the first part as indicating an individual
account.

Under the MLEC it is unclear whether “designation” refers to the whole information system (i.e.
all machines in the domain) or to the individual accounts. Due to the breadth of the term “information
system,” designation could imply that all email accounts hosted on a mail-server being part of the domain
are designated. Taken to the extreme, the MLEC solution would permit acceptances to be sent to any
account belonging to the information system or domain. The problem is solved in the CUECIC, which limits
“designation” to individual accounts.

87 CUECIC Art 10, see also CISG Art 18
88 A/CN.9/528 para 80, concerns were expressed over technologies restricting receipt.
89 For general discussion see: Ch H Martin, The UNCITRAL Electronic Contracts Convention: Will it be Used or
90 It was stated difficulties in applying Section 15 cannot be overcome by defining “designated information system.
A/CN.9/528 para 148
91 MLEC Guide to Enactment para 102
92 MLEC Guide to Enactment para 103
93 Chapter 5 [5.20][5.21]
94 See also: Carter on Contract [03-430], where it is assumed that the designation of an information system is
synonymous with the provision of an email address.
95 Brookshear pp 141 -142
These problems do not arise in postal communications: there is usually one address per entity and a direct correlation between “address” and “mailbox.” Unquestionably, in larger companies each department or branch may have its own, physical mailbox. There is no division, however, into designated and non-designated mailboxes. Whatever address is published or made known as the address of a company or person, all letters sent to it are effective unless specifically indicated otherwise in the offer. Distribution to the respective persons and departments is handled internally. “Designation” obligates senders to investigate the correct address without imposing an equivalent obligation on addressees to clearly designate their systems. If a system, address or device is held out to receive communications, its designation should be implied regardless of whether such system, address or device is regularly checked for new messages. This would mirror the traditional rules of receipt. Under the regime created by the MLEC and the CUECIC receipt may not occur even if an information system held out — as long as it is not expressly designated.

While addressees should not be expected to monitor all of their information systems or electronic accounts, they should monitor those systems that are being held out, such as by providing an email address on a website or business card. If addresses of particular information systems or accounts are disseminated or made public, addressees should not be permitted to claim that such systems or accounts are not designated. How does designation occur absent a specific provision in the offer or prior communications, if not by providing an address or number? While messages of a particular business nature should not be addressed to information systems that senders know or ought to have known are not used for messages of such nature, it appears questionable whether the development of special addressing rules facilitates on-line contracting.

[7.26] According to UETA Section 15 (b) a message is received when:

1. it enters the information processing system that the recipient has designated or uses for the purpose of receiving messages of the type sent and from which the recipient is able to retrieve the message; and
2. it is in a form capable of being processed by that system.

Associating “receipt” with “entry” precludes recipients from “leaving messages with a server or other service in order to avoid receipt.” Receipt is synonymous with availability for retrieval and does not depend on the addressee’s awareness. Receipt is precluded, however, if a message is sent to an address that is neither designated nor used for a given purpose. UETA leaves open the question whether receipt occurs upon the addressee’s actual knowledge of the message. It does, however, specify that the message must be “processable” — short of prescribing legibility, it requires that senders take into account the characteristics of the addressee’s mail-client.

Most importantly, UETA introduces de facto designation. In first time transactions between strangers establishing the “designated” or “used” system is difficult. Acceptances occur in response to offers and it could be assumed that the offer or any previous correspondence may provide an indication of which address is to be used. The moment of receipt will largely depend on the source from which a given address was obtained.

96 A/CN.9/528, para 145
97 See: D Giles, You’ve Got Mail….or Have You? (2000) 3 Internet Law Bulletin 12 at 14, who suggests that to avoid the consequences of designation people may use disclosures like “nothing in this email constitutes designation for the purposes of….”
98 A/CN.9/528, para 145
99 UETA Section 15 (b) comment 3
100 UETA Section 15 (e) comment 5
101 UETA Section 15 comment 3
[7.27] The ETA Section 13 (3) states that in the case of designated information systems, receipt occurs upon entry. If no system was designated, receipt occurs when the message comes to the addressee’s attention. The Explanatory Memorandum presumes that designated systems are regularly checked for messages. Absent designation, however, receipt is tied exclusively to a subjective event. It is unclear whether “coming to the attention” requires knowledge of the message’s existence or knowledge of its contents. “Existence” does not imply that the message can be retrieved or read and could be limited to a general awareness that the message is available on the mail-server. “Contents” assumes that the message can be retrieved and displayed.

Web-based interactions and instant messengers

[7.78] Problems of defining the exact moment of contract formation are less prominent in the case of Instant messengers and websites. As described in the previous chapter with regards to the effectiveness of electronic acceptances, both web-based interactions and dealings via instant messengers occur “as if” face-to-face. Consequently, their effectiveness is tied to receipt. It can also be claimed that in face-to-face dealings dispatch is concurrent with receipt therefore the division is not justified. Moreover, both in the case of web-based interactions and instant messengers, it could be claimed that the parties exchange messages within the same system. This approach is reflected in CUECIC Art 10.1. The latter provides that if the message has not left the information system under the control of the originator, dispatch occurs when the message is received. This provision applies to situations “such as the posting of information on a website.” Although in the case of web-based interactions effectiveness would occur upon receipt, the “receipt” provisions of any of the model regulations to not readily fit the mechanics of downloading websites. This process involves the addressee requesting websites from web-server, which are made available by the sender. Under the MLEC, ETA or the UETA a website is received when it enters the addressee information system, under the CUECIC – when it is capable of being retrieved. Despite such differences in wording, the only common-sense interpretation is that websites are “received” when they are displayed to the addressee. Problems of designation or retrieval do not occur as it is always the addressee who requests (i.e. retrieves) websites from web-servers. Most importantly, the definition of “receipt” is simplified as there is only one client (the browser) and one server (the web-server). The addressee retrieves messages directly from the sender – not from its own server.

A similar, common-sense approach must be adopted with regards to instant messengers. As indicated, some instant messengers involve the intermediation of a server throughout the communication process, in others, the server “drops out” after the initial connection is established and parties communicate on a peer-to-peer basis. Receipt occurs when both parties can see the message on the screen. Due to the lack of one standardized instant messaging platform, it is impossible to discuss all possible permutations. In both instant messengers and web-based interactions there is virtually no delay between dispatch and receipt, furthermore, it is generally impossible to “split up” dispatch or receipt into a process involving delays between its respective stages. The user requests a website from a web-server and downloads it onto his or her client, a sender types an instant message which immediately becomes visible to both parties of the communication process.

102 UETA Section 13 (3) ETA
103 Electronic Transactions Bill 1999, Explanatory Memorandum p 12
104 Electronic Transactions Bill 1999, Explanatory Memorandum p 12
105 Wilmot, Christensen & Butler [3.9.4]
106 CUECIC Art 10 par 1
Conclusion

[7.29] The difficulties in determining the time of formation of contracts formed via email relate primarily to the delays that occur in the initial and final stages of the communication process, between the sender’s originating mail-client and the outgoing mail-server and - most importantly - between the incoming mail-server and the addressee’s mail-client. The mail-server model of communications renders it difficult to apply principles, which developed around postal communications.

Attempts to define “dispatch” and “receipt” also shed new light on the concept of instantaneousness. Email can only be described as instantaneous if it is the mail-server that is regarded as the point of dispatch and receipt. Model laws, however, seem to favour a principle based on the actual control of the communication infrastructure. Their verbatim reading implies that it is the mail-client that must be taken into account when determining the moment of dispatch. At the same time, model laws associate “receipt” with “availability,” which in turn points to the addressee’s mail-server. As a result, the mail-server is separated from the mail-client in the case of dispatch but treated as one device for the purposes of receipt: dispatch occurs when a message leaves the mail-client but is received when it reaches, or enters, the mail-server.

The role of ISPs remains unclear. Attempting to map paper-based principles onto the on-line environment, model laws seem to treat ISPs like the post, i.e. like part of the transmission channel. It is forgotten that – unlike the post – the sender has a choice whether to run his or her own mail-server. The sender has also a choice in the selection of ISPs. It remains unclear whether the mail-server should be regarded as part of the transmission channel or as a terminating or originating device. A common-sense and technically correct approach would treat mail-clients and mail-servers are one device, i.e. disregard message transfers between mail-clients and mail-servers. The transmission of the message would commence only after it left the mail-server.

Client-server model aside, additional problems arise from the heterogeneity of the networked environments and possible incompatibilities between the client applications of the transacting parties. Two factors which are often overlooked by legal literature. The definition of “receipt” raises issues pertaining to the legibility of messages and the addressee’s right to reject due to security concerns. Model regulations introduce additional complications by failing to narrow the scope of the term “information system,” associating receipt with “designation” and introducing subjective elements into the discussion, such as “awareness” of receipt.

Despite the existence of detailed provisions in the model laws, determining the time of dispatch and receipt occurs in the absence of clear rules. This adds to the uncertainties related to whether “electronic acceptances” should be effective on “dispatch” or “receipt.”