

Chapter 2

CONTRACTS

Can agents do your grocery shopping...?

La gran corriente de voluntarismo jurídico que lleva a considerar que el origen de las obligaciones se encontraba en la expresión de la voluntad de las partes.

Luis Díaz Picazo, Fundamentos de derecho civil patrimonial, 1ª ed., 1970.¹

Computers are no longer seen as simple communication tools for message transmission in ecommerce but, as we have discussed in the introduction, they are (becoming) capable of initiating transactions and entering into agreements with third parties. The Research Scenario envisages agents that are sufficiently independent to generate such agreements, and the principle issue we need to consider is whether communications by or with agents, i.e. agent based transactions, can form a valid and legally binding contract, and what conditions are required for more secure contracting.

We first set out in section 1 the basic general principles of contract law in Europe. In section 2, we consider certain agents that raise issues relating to contract law, and in section 3 discuss the most important of those issues. In section 4, we comment on certain legislated solutions and other measures that are being suggested for dealing with agent-based contracting, while finally looking in section 5 at recent developments in this area.

¹ *The significant current of legal voluntarism leads us to consider that the origin of obligations was found in the expression of the will of the parties.* Luis Díaz Picazo. Fundamentals of civil property law, 1970, (Authors' unofficial translation).

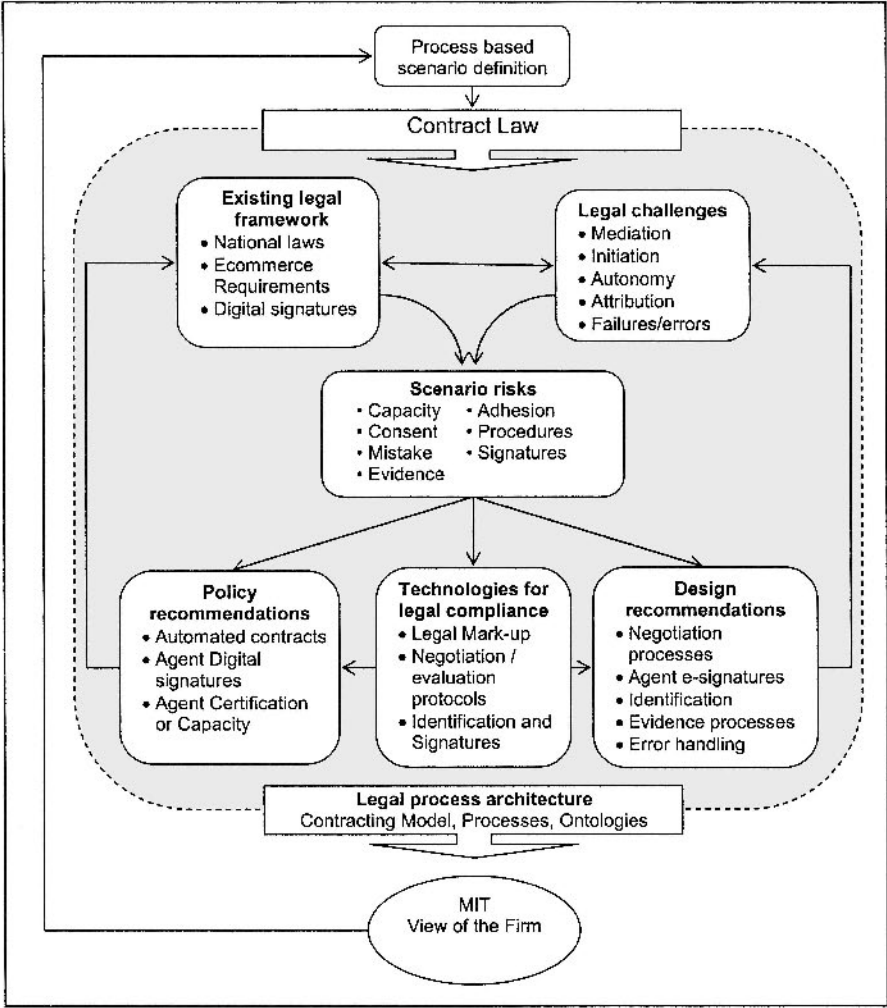


Figure 2-1. Contract Law Analysis

1. OUTLINE OF GENERAL PRINCIPLES OF CONTRACT LAW

1.1 Civil Law and Common Law systems

Contract law is a matter for national jurisdictions and has not (yet²) been harmonised at European level. Although the differences between Civil and Common Law systems are not substantial, some of them are relevant for our purposes in relation to agents (see specific sections below). The following is a brief outline of core contract principles applicable throughout Europe that are relevant for our study (mainly offer, acceptance and, consent (1.2), validity (1.3) and the incorporation of terms (1.4)). Our aim is not to discuss contract law, but to provide a general background showing the areas and concepts that will raise difficulties for the use of agents.

1.2 Formation

Consent: offer and acceptance – a meeting of minds. A contract is generally considered to be formed when all parties to the contract have consented to be bound by the contract: that is to say that there has been a suitably definite offer (not revoked) that has been validly accepted by the other parties. Offers may be made orally, in writing or even by conduct and accepted in any manner reasonable in the circumstances. Consent must be freely given, and may be affected by mistake (including lack of intent), misrepresentation or bad faith (see below). There is some divergence, however, as to what constitutes an offer, as some “offering declarations” may be considered an invitation to treat.

Intention. In Common Law systems, the parties must intend to be legally bound (i.e. not create a “gentlemen’s” agreement”). This issue is incorporated in civil law systems into the validity of the consent. This is the presumption in normal commercial transactions.

Evidence in writing. Some European jurisdictions require contracts to be in writing and signed. In others, except for certain specific contracts specified in legislation (e.g. sale of land, securities, some consumer contracts³), there are no formal requirements for contracts to be in writing and signed by the parties: a verbal agreement is sufficient. The issue is one of evidence (acceptable in court or other dispute resolution procedure) to prove the existence and terms of the contract, for which written documentation signed by the parties is the strongest proof. For this reason,

² See CEC Communication on European Contract Law, 11 July 2001, COM(2001) 398 final http://europe.eu.int/comm/consumers/policy/developments/contract_law/index_en.html and Report of the Study Group on a European Civil Code at <http://www.sgecc.net>

³ Also, in the USA, contracts above a certain sum - \$500 – or for a certain period

contracts may be made over the telephone, by exchange of faxes, emails, website forms, and EDI (electronic document interchange) procedures, i.e. in electronic form.

Signatures. Again, apart from certain specific contracts such as the purchase and sale of land, there is no obligation for any written evidence to be signed by the parties. Signatures authenticate a document, as proof of consent and to prevent repudiation by a party who wishes to avoid being bound.

1.3 Validity and Enforceability

Capacity. To be valid and legally enforceable, all parties who enter into the contract must have legal capacity. This capacity is either an a priori condition for validity (Civil Law systems) or an a posteriori reason for invalidation (Common Law). Generally speaking, only natural or legal persons (organisations with legal identity: corporations, associations) have capacity to contract.

Object and cause. Some civil jurisdictions (e.g. France, Spain) require that a contract should have a definite object and a lawful cause. This is covered in Common Law systems by the concept of determination (the terms of the offer and resulting agreement must be sufficiently clear and determined) and frustration (illegality renders a contract non enforceable).

Consideration. Under Common Law, a party needs to provide “consideration” (a type of compensation to the other party, e.g. payment or a promise to pay) for it to be able to enforce the contract terms against the other party/ies.

Mistake. An error in the minds of the parties, i.e. a mistake as to the desires and intent of the parties (e.g. as to certain terms or the object of the contract in question), will render a contract wholly or partially invalid or voidable, as it vitiates the consent of the parties.

Misrepresentation and good faith. While in Civil Law systems there is often a duty of good faith imposed by law on the negotiators of an agreement, under English Law the principle of *caveat emptor* rules (“buyer beware!”): there is no such duty on the parties, for example to correct an erroneous belief of the other. On the other hand, if a party is intentionally misleading, the other may rescind the contract if it so wishes or maintain the contract and claim damages.

1.4 Incorporation of Terms

It is important for all terms to be known to the parties at the time of consenting (otherwise consent may be vitiated), and “incorporated” into the

contract. A party may not, after agreement, add extra conditions that were not known or incorporated at the time consent was given⁴.

1.5 Other contract issues

Invitations to treat. Common Law systems divide the contracting formation process into two stages: (1) pre-contractual negotiations and advertising, and (2) formal offer/acceptance. It is a question of fact as to what actually constitutes an offer (rather than an invitation to treat, such as an advertisement) - for example a website under English law would be considered an invitation, with the consumer making the offer that is accepted by the ISP. Other jurisdictions could consider the website the offer of the ISP (if the terms were sufficiently definite), with the consumer making the acceptance.

Time and place. For certain purposes, it is important to establish the time and place of formation. The place of formation may determine the competent courts or the law applicable to the contract, while the timing of the messages (offer, acceptance, or revocation or either) may determine whether there is a binding contract and the moment of passing of risk or title.

Absent parties. In distance contracts where the parties are not physically present, several provisions regarding consumer protection apply, legislated on the basis of European directives (see section on Consumer Protection). These provisions cover obligations on the part of suppliers that render a contract voidable if they are not fulfilled.

1.6 Harmonisation efforts

Ole Lando Commission and UNIDROIT Principles of European Contract Law. For the last 20 years or so, various academic projects have aimed to produce a set of contract principles or laws that are common to all European Jurisdictions. This may be the basis for future EC harmonisation, but for the moment these principles must be explicitly incorporated as the legal basis for contracting to have any effect.

UNCITRAL Model Laws. The Model Law on Ecommerce⁵ was adopted in June 1996 – it was drafted by a special commission of the United Nations, to provide a common framework for nations to adopt and adapt their laws for ecommerce. The Model Law is not binding, but provides a model of internationally acceptable rules in order to remove legal obstacles to ecommerce. More specifically, it aims at the legal acceptance of

⁴ Thus, for example in ecommerce, the importance in web pages of including any contracting conditions, either directly on the “Accept” page, or by a visible and easily accessible link.

⁵ UN General Assembly Resolution 51/162 of 16 December 1996, online at <http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>

electronic messages and records. More recently, UNCITRAL adopted a Model Law on Digital Signatures⁶, which establishes a common framework for implementing laws about these signatures in national law. Various countries have used these Model Laws for their ecommerce laws, including Brazil, Thailand, and UEA.

1.7 The legislative framework for electronic contracting

The following table presents a brief list of the major legislated sources of law governing electronic contracts.

Table 2-1. Laws on electronic contracting

Law	Brief summary
EC Directive on Electronic Commerce (Directive 2000/31/EC)	This Directive requires Member States to ensure that their legal systems allow contracts to be concluded by electronic means (Article 9).
EC Directive on a Framework for Digital Signatures (Directive 1999/93/EC)	This Directive establishes a liability, evidentiary and procedural framework for obtaining and using a digital signature.
EC Directive on Distance Contracts (Directive 97/7/EC)	This Directive establishes consumer protections for contracts where parties are not present.
National legislation	European member states are (slowly) incorporating the provisions of the EC Ecommerce Directive into national law.
Other jurisdictions	Many nations have established “Ecommerce laws” for the recognition of electronic contracting, including most specifically USA (UCITA, UETA and ESIGN) and Canada (UECA).

We will now proceed in section 2 to outline the legal issues raised by software agents within the Research Scenario regarding contract law, and then in section 3 discuss these issues in more detail.

⁶ UN General Assembly Resolution 56/80 of 12 December 2001, online at <http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf>

2. CONTRACT ISSUES ARISING IN AGENT TECHNOLOGY WITHIN THE RESEARCH SCENARIO

In the first section, we have seen the main principles of contract law in Europe. In this next section, we will briefly establish the main issues that are raised by agent contracting, either between agent and humans, or between agents. We will consider these issues in relation to the degree of human involvement. At the one end of the spectrum, there are processes where there is human confirmation of a deal (this would include standard online contracting, where the person clicks “I accept”). At the other end, fully automated agent processes require no human involvement at all. If the agent is not a legal person, “on whom is such a contract binding, against whom is it enforceable, who is responsible for any mistakes or non-performance?” are questions that come to mind. These provoking issues are discussed more methodically below.

2.1 Contracting agents

Considering the Research Scenario, it is useful to set out the general processes of shopping agents that include contracting capabilities. We consider three different agents that intervene at different stages of the Consumer Model set out in Chapter 1: advertising, offering, and negotiation/contracting. These software agents are schematically described in the tables below, using the BDI model of agents⁷ and a process description of tasks.

Agent A is a store-based advertising agent, offering products to consumers in accordance with their shopping profile or other input: e.g. the store's current list of offers, an electronically identified product picked up by the consumer, or external data such as time, weather or season. Processing and communications are internal to the store (i.e. closed agent network - e.g. provided by other store network agents) using a Wireless LAN to the customers mobile device⁸. Product identification is provided by RFID tags attached to the products or their packaging.

⁷ The BDI model, represents an agent by three structures: beliefs, desires and intentions. The beliefs of an agent are its model of the domain (information about the environment and cause/effect relationships), its desires provide a list of goals, and its intentions are the things it has decided to do (chosen goals). Wooldridge and Jennings, *Agent Theory and Practice* (1995).

⁸ The agent could also communicate by SMS through an external gateway to a telecom service provider. This raises additional issues of security and confidentiality (e.g. additional layers in the agent communication architecture), especially in relation to any transmitted personal data, although WLAN / Wi-Fi also has its own security problems. See Blanchard C W: *Wireless security*, (2001).

Table 2-2. Summary Description of Agent A

Agent A	Description
Beliefs	Knowledge or beliefs regarding the consumer (customer profile and preferences, current shopping list, past shopping behaviour, extrapolation / inferred rules from such behaviour and preferences), and of the environment: date, time, place, store-related data (stocks, prices, current offers).
Desire	To inform customers of current products, and (better) persuade them to purchase.
Intention	Associating a determined offer to a specific client.
Autonomy / Intelligence	Offers are made without the store's knowledge or review and the agent learns from experience how to best match offers and clients.
Steps	Process
1	Agent A becomes aware of customer within target area for its particular advert (outside store front, within the store, within an area of the store), through external sensors (e.g. a location service agent ⁹ or RFID activation).
2	Agent A considers rules for sending adverts and consults relevant data sources.
3	Agent A sends an advertisement to the customer device (WLAN or SMS), without review by store staff.
4	Agent A monitors and updates customer reaction to message and stores this for further processing in relation to this and other clients, and this and other products

Agent B is a similar store-based selling agent, this time with added functionality for offering features such as contract conclusion and associated services: interconnection with payment systems and fidelity programmes, and home delivery. A more evolved version may have an advertisement linked to a direct “on-click” purchasing process. This may seem not much more than existing online B2C ecommerce sites¹⁰, however agent-based computing is considered for efficient interaction with external data and communication systems and added intelligence for determining the appropriateness of sending the offer, and learning from the acceptance and rejection of the goods or services.

Table 2-3. Summary Description of Agent B

Agent B	Description
Beliefs	The same information processes as Agent A as well as additional data relating to the customer, e.g. home address (probably in the customer profile anyway) and electronic payment details.
Desire	To inform customers of current products and sell them.

⁹ Location issues are considered, but are not specifically relevant to agent transactions, more general issue of location based services and obligations to maintain confidentiality under the new Privacy and Electronic Communications Directive 2002/58/EC (when implemented).

¹⁰ Ecommerce websites are already autonomous if one looks at them from the merchant side: often online sales occur without any review by the seller, and even performance is autonomous (but not necessarily intelligent) in the case of online delivery of digital content.

Agent B	Description
Intention	To sell a specific product to a determined customer, on the occurrence of a certain event.
Autonomy / Intelligence	Determining the appropriateness of sending the offer; making an offer without store review; learning from the acceptance and rejection of the goods or services.
Steps	Process
1-3	As for A
4	Agent B provides a means for accepting the offered product (accept button, voice acceptance, etc).
5A	Agent B records and processes sale: sends a delivery order to a delivery service agent and a payment process order to a payment agent.
5B	The payment agent contacts credit card or electronic payment service provider and processes payment according to relevant system (e.g. adds item to credit card account). This may require confirmation from user of PIN or other identification means. This agent reports successful payment back to Agent B.
6	As for Agent A, step 4: B monitors and updates customer reaction to message and stores this for further processing in relation to this and other clients and products

Agent C is a customer-oriented automatic shopping/buying agent. This agent is resident in a consumer controlled environment / host, searches for products (e.g. based on a current shopping list or an identified product picked up by the client) and even suggests new products to the user and/or purchases them without review. It communicates both with the closed store systems (product and price databases, etc.) and with the open network (alternative shopping sites). It has communication, information retrieval and assessment and negotiation functionalities added to those held by Agent B and (more or less) complete autonomy from the user as orders and purchases may be made without review.

Table 2-4. Summary Description of Agent C

Agent C	Description
Beliefs	The same information processes as Agents A and B as well as additional data relating to the customer: home contents (in a pervasive computing scenario, where the home inputs data to the agent through sensor devices, at the agent's request or on its own initiative); shopping list; user profile and preferences; rule inference from previous behaviour / standard shopping behaviour; other data (e.g. hot weather therefore search for sale and delivery of extra cold drinks) ¹¹ .
Desire	Maximising the customers purchasing potential and life-style.
Intention	Self-determined in relation to the general desire. Specifically, to purchase an item it considers the consumer wants or needs.
Autonomy / Intelligence	Determining the appropriateness of searching for and choosing an item; making a purchase without customer review; learning from the acceptance

¹¹ Each such input is envisaged eventually as the result of individual agent processes: the shopping list agent, the user self-profiling agent, the diary / agenda agent, etc.

Agent C	Description
	and rejection of the goods or services; anticipating future needs.
Steps	Process
1	Agent C determines a need to purchase a specific item through assessment of data inputs and beliefs (e.g. shopping list update, product RFID activation).
2	Agent C searches the network for various stores selling relevant products. This includes certain evaluation criteria (reputation evaluation, closeness to home, brand availability, etc.) and comparison functions, with e.g. the local store product catalogue.
3	Agent C negotiates with store(s) for the quantity, price and other terms of sale. This may involve negotiation with more than one store at the same time, or participating in an auction, in one of various agent systems ¹² .
4	Agent C concludes purchase agreement.
5	Agent C provides delivery and payment details (see Agent B above - the order of steps 4 and 5 may depend on online site / selling agent process).
6	Agent C records transaction and reports purchase (in due course) to customer. The item is removed from the customer's shopping list.

2.2 Contracting issues

It is important to note that we do not intent to deal with general issues of online or electronic contracting in B2B or B2C ecommerce. Most nations have now attempted – or are attempting – to regulate and promote ecommerce by adopting a clear legal framework to allow for online contracting¹³. The more general contract issues raised by online transactions are well researched and published¹⁴, while our topic here is agent-based contracting. Accordingly, we will exclude the following topics:

- The formation and validity of online / electronic contracts - where physical users (persons) explicitly accept a transaction (click “I accept”) and have direct access to contract terms. This topic has been widely discussed and debated.
- The recognition and use of digital signatures for identification, authentication and non-repudiation (generally speaking – we will consider the possibility of digital signatures being provided by agents): again, this has been the subject of wide discussion and research.

¹² Some of the implications of multi-agent systems are discussed in Chapter 6.

¹³ Notably the UNCITRAL Model Law efforts, but also the US laws mentioned above (UCITA, UETA, E-SIGN), and the EC Ecommerce Directive 2000/31/EC.

¹⁴ See for example, IST Projects IMPRIMATUR at www.imprimatur.net, ECLIP at www.eclip.org, and more general books on ecommerce law: *Electronic Commerce: Law and Practice* (M. Chissik and A. Kelman), *Going Digital: Legal Issues for Electronic Commerce, Multimedia and the Internet*, A. Fitzgerald, B. Fitzgerald, P. Cook & C. Cifuentes (eds); *Butterworths e-Commerce and Information Technology Law Handbook* - Jeremy Phillips (Ed); *E-Commerce: A Guide to the Law of Electronic Business* Second edition -Hammond Suddards Edge; *Manual de Derecho Informático*. 3ª edición, Aranzadi, etc. Also, R Juliá-Barceló, *Electronic contracts*, 15 CLSR 3 (1999).

Concentrating on agent issues, and looking at the general outline of contract law above, the following is a list of the most important topics which we will consider in this research. These will be considered in turn below.

- a) Certain conceptual problems, most notably agent-based contract formation and validity:
 - Capacity: do agents have sufficient capacity to enter into a contract? (section 3.1)
 - Consent: can agents provide consent, either of themselves or of the agent user? (section 3.2)
 - Agent failures, errors and the legal apportionment of risk. For example, what happens when an agent purchases the wrong product, or the system crashes? (section 3.2.3)
- b) More practical issues
 - Procedures: can agents distinguish invitations, offers and acceptances? (section 3.3.1)
 - Evidence: can / do the requirements for “in writing” be met? How does one obtain and maintain evidence of an agent-formed contract? (section 3.3.2)
 - Terms: can we ensure that all terms are properly incorporated into a contract? Can the user have or be deemed to have knowledge of the terms? Where is the line between advertising and contract terms? (section 3.3.3)
 - Signatures: can an agent provide a digital signature with binding effect? (section 3.3.4)
 - Consumer rights: how to comply with information, transparency and consent requirements when using agents? (section 3.3.5)

2.3 Secure contracting frameworks

The problem of establishing valid and secure automated electronic contracts is not new: the research on Electronic Data Interchange (EDI) looked into the legal issues raised by agent contracting within a closed messaging framework. This closed network, however, provided a framework contractual solution to most problems, because identified business parties could choose, through a “macro” EDI contract, to accept the validity of agent-based contracts. This made it difficult for transaction participants to repudiate any electronic contract. Open network contracting, where at least consumer parties are not necessarily identified, is another matter. Except perhaps in the context of a supplier-merchant relationship, there are no previous dealings or framework contract to provide easy such contract based solutions.

It is important to keep in mind why we need to consider the contracting capabilities of agents: to provide certainty and confidence for users (both merchants and consumers) so that agent based commerce - specifically transactions within the Research Scenario - may develop. Without any faith in the validity of agent contracts, and the application of legal protections granted to both merchants (e.g. non repudiation) and consumers (e.g. proper performance, consumer protections set out in national and EC legislation), the advanced agent based consumer model may not grow to maturity and achieve the promised ultimate efficiency.

From a practical point of view, the programming of each of the processes of the agent should be considered from a legal point of view. This should result in legal specifications that will cover the design of shopping agents (from basic to advanced), while in addition the specification will evolve as the project evolves: new agents, evolving electronic devices and capacities (currently for example, only UMTS allows sufficient speed and storage for secure mobile communication based agent contracting). Such a study should include an analysis of the stages of the contract formation process to determine:

- What is included / excluded from the terms
- Are there previous representations / “declarations” that are binding? And
- How do you provide evidence of the formation - do you need to email confirmation?

In the next section, we will review the issues outlined above in detail, and try to answer the questions asked. While sections 3.1 and 3.2 cover conceptual issues in relation to contracting regarding capacity and consent, section 3.3 deals with more practical problems such as evidence, procedural regularity and digital signatures.

3. CURRENT LEGAL POSITION ON THESE ISSUES

3.1 Capacity: do agents have sufficient capacity to enter into a contract?

On the basis that only natural or legal persons have capacity to enter into a contract – i.e. not electronic agents – there are three ways to give an intelligent agent the appropriate capacity:

- Establish an independent legal personality for the agent.
- Establish that the electronic agent is an agent (in the legal meaning) of a person, i.e. is acting on behalf of the user.

- Determine that the agent is a communication tool for transmitting the user's consent.

These possibilities should all be considered in the light of the attributes of capacity: benefiting of rights, incurring obligations, having patrimony (assets and liabilities), identification and decision-making capacity – including making mistakes.

3.1.1 Legal personality

Capacity is not the same as legal personality: a minor or mentally “incapacitated” person both have legal personality but are not legally capable of entering into contracts. Traditionally, legal personality is conferred through moral entitlement (e.g. women in the 19th Century), social capacity (clubs, associations, etc.) and legal and business convenience - this last is already done in other fields than technology, such as for corporations or other business organisations. The first two justifications are not applicable as it would be difficult to argue for personality on moral grounds or on social grounds, at least until agents evolve to acquire social capacities (independent interaction with persons) – a scenario not to be discarded, though currently still part of science fiction.

The justification of legal expedience is very attractive: with such personality come assets and liabilities (patrimony) and forms of decision-taking as well as ownership and management and identity. These are concepts that are easily achieved in the world of business, with the different forms of incorporation and business organisation (limited liability companies, partnerships, “sociétés” or “sociedades” of different combinations of persons). As regards agents, it seems that:

- Concepts of ownership and management may also be applied. These issues could be determined in traditional ways such as public registers, recording of decision-taking and parameterisation¹⁵.
- The possibilities of assets and liabilities are more difficult to conceive in relation to software agents. Unless or until agents evolve to the extent of being sentient of these elements, and able to defend (rights) or satisfy them (obligations) and even have a physical place to keep them, some mechanism of transparency (such as the legal construct of agency) would have to attribute any such rights and obligations to the user or definitive beneficiary of the agent actions. One could even go to the extent of conceiving default repositories similar to, in the UK today, the Crown in relation to certain incapable or dead persons (e.g. minors).
- Identification is another thorny problem as agents are not necessarily independent parts of code but may be part of or distributed over an environment / platform or several platforms, that could also include other

¹⁵ C Karnow, *Liability for Distributed Artificial Intelligences* (1996).

elements both hardware and software. It would be hard to identify the extent of the entity. Again, registration of ownership (or user) could solve this problem, though raising questions of cost and ease of implementation.

Despite interesting arguments presented by E. Pelino¹⁶ in favour of agent personality, there is also a problem of the question of "sliding scale" and mutual recognition. At what point or degree of autonomy and decision-making capacity would an agent acquire a separate legal identity? If one agrees that a registration and encryption procedure may be established, what criteria would be used by whom to analyse an agent to determine if it has sufficient attributes, autonomy or capacity for legal personality? How would users and/or registrars deal with the "identity key" which protects the agent from tampering and duplication? And would the personified agents of one jurisdiction be recognised in another, as companies generally are? While we believe that these are issues that are not impossible to solve with an appropriate registration system, this concept does not assist us currently in validating agent-based contracting.

All in all, it does not seem appropriate at the moment to go the extent of establishing legal personality to provide contracting capacity to electronic agents. As we will see below, and until agent technology progresses to such extent that agents acquire higher levels of autonomy and sentience when forms of registration may become desirable, there may be other ways of getting around the issue of contracting capacity of software.

3.1.2 Legal concept of agency

For the sake of clarity, in this section computer agents will be denominated with capital letters (Intelligent Agents) while legal agents will remain in lower case.

Under the law of agency in European countries (and in the US) an agent is a person who acts on behalf of another (called a "principal" or "*mandante*", etc.) and the agent's acts within the scope of its mandate binds that person. Any act outside that mandate is deemed an excess of authority and does not bind the principal unless he/she ratifies it¹⁷.

It seems reasonable to think that a Software Agent could be considered the equivalent of a legal agent. A program given the capacity to sense its environment, deliver instructions to other parties (persons or computers), execute and perform agreements like downloading software or sending data without further input from the agent user, is acting in way very similar to

¹⁶ E Pelino, *Autonomous Software Agents as Legal Persons*, Alfabiite (2002).

¹⁷ See Van Haetjens, *Shopping Agents and Their legal Implications Regarding Austrian Law* (2002) and F. De Miglio et al. *Electronic Agents and the Law of Agency* (2002) for comments on representation rather than full agency

any human being doing the same things as a legal agent for another. Why should the law treat it any differently?

The advantages of this “legal agent” paradigm are several: under the principles of agency, the Software Agent’s decisions and actions bind the principal, who engages his/her responsibility and would respond to any third party who had any claim. The obligations and rights under any contract formed by a Software Agent would be passed on to the principal. The agent itself does need not to have legal capacity to act (for example, a minor may act as agent for an adult) and the human or corporate principal can also ratify the (disclosed) agent’s actions if necessary.

However there are currently several legal difficulties to this construct¹⁸:

- a) Under the law of agency, principal and agent are separate persons¹⁹. A software program is not a person (yet – see section above on legal personality).
- b) The agent has to consent to act as agent for the principal. For Software Agents, this becomes a circular argument: we are trying to solve the problem of agent consent by pretending it is acting on behalf of the principal. So in the end, it is the principal who is consenting to the agency relationship with itself. Neither does the idea of presumed consent from the Software Agent convince.
- c) An agent may be liable for its actions when it acts outside the scope of its mandate – a possibility all the more likely as an agent such as Agent A gains independence, or when its principal is not disclosed to third parties. The principal may or may not ratify such act. We have seen that a Software Agent today has no legal capacity nor any assets or patrimony to respond to any liability.
- d) The acts of an agent acting without disclosing its mandate may not be ratified by the principal.
- e) How does one deal with any action undertaken by the Software Agent by mistake either through an error in programming, initial user parameterisation or subsequent malignant intervention or distortion?
- f) Who is responsible in the case of viruses or errors in the operating system or agent host?

These objections could be solved if legal personality was conferred by law on Software Agents (a new legal fiction such as incorporated persons). It does not seem that legislation is pointing this way yet, as we will see below under the section on consent.

Interesting solutions have been offered to deal with the capacity of Software Agents in relation to agency law. We feel the most convincing has

¹⁸ See also Allen and Widdison, *Can computers make contracts?* (1996).

¹⁹ In most jurisdictions, and even under EC law for example Directive on Commercial Agents, 86/653/EC.

been offered by Kerr²⁰, who suggests that one should only consider the external aspects of legal agency, applied to the legal relationship between the principal and the third party (obligation, liability, ratification, etc) as any disputes would only arise between these persons. One would not apply the internal aspects (the relationship between the principal and the agent), as the conferring of authority on the agent could be deemed by the act of programming or parameterisation of the agent and initiating its activities. This has the advantage of:

- Using the concept of apparent authority²¹. This would apply when a person makes it clear that the Software Agent is acting on his/her behalf: the person is bound towards third parties by the agent's acts. In the context of the Research Scenario, we can consider if the Agent user, consumer or merchant, would make any Agent such as A, B or C appear expressly to act on their behalf. It will in fact be fairly obvious that A and B are performing on behalf of the Store. It may not be so clear who the user behind Agent C is. This apparent authority could be in the programming of the "identity" of the Software Agent, which could include identification or at least a declaration of the existence of the user/principal, as part of the user parameterisation. However, how this concept would apply in a relation between two Agents is unclear.
- Applying the concept of ratification. The user/principal could ratify any act outside the scope of the original mandate (especially with evolving agents that learn and adapt). This is only possible if the Agent discloses that it is acting on behalf of the principal, again something that could be included in the internal programming of the agent for greater certainty and contracting security.

This would deal with objections (a), (b) and part of (c) above, but does not help with problems of undisclosed excess authority, mistake and errors or bugs (objections (d), (e) or (f))²². In relation to autonomous and mobile Agents such as Agent C, the risks of excess authority and mistake grow with the advance of technology, as Software Agents become more functional and independent, carry out more complex transactions – including delegating to or collaborating with other Agents – with more parameters and "experience/learning" features, and as they acquire the capacity to migrate to less controlled environments. These issues are not resolved by the legal

²⁰ I Kerr: *Providing for Autonomous Electronic Devices* (2000), also discussed by E. Weitzenboeck, *Electronic Agents and the Formation of Contracts* (2001).

²¹ This apparent authority is conceptually similar to the theory of "appearance" or "reliance" in some civil law countries – France, Spain, Germany, Netherlands -, where a third party is protected by their legitimate belief in an apparent situation – a sort of "constructive agency" or estoppel. There seem to be limits, to this, however, and the construct would not apply to more advanced software agents.

²² These issues may have legislated solutions: see section 3.2.3 below under "mistake" and errors.

agency scenario and in the lack of any specific legislation²³ need to be dealt with in some other way.

This solution would also require legislation or judicial approval (and indeed, it seems that certain aspects of this theory are incorporated into the Canadian UECA). In Europe, however, the EC Ecommerce Directive has left it up to member states to “ensure their legal system allows contracts to be concluded by electronic means” and it remains to be seen what action will be taken in respect of Electronic Agents (see section 4.4 below – recent legislation).

3.1.3 Communication tools

The use and legal validity of technology to transmit the consent of a natural or legal person is already well established, since the days of the telephone, fax and even, more recently, Electronic Document Interchange (EDI). In these “low-tech” situations, technology does not have to have legal capacity as the person entering into any agreement is the user of the technology, usually a human being or corporation with full legal capacity. The technology is a communication tool.

In relation to software agents, this construct seems the most likely to achieve legal validity at present, even though it may be the most limiting paradigm from an artificial intelligence / independent agent point of view: it denies the autonomy of the technology. Insofar as agents are simple mediators of ecommerce, retrieving or supplying information, putting persons into contact with one another, transmitting the real consent (“I accept” click or statement) of the user, this construct will be the most appropriate. This is certainly the case for Agents A and B. As the word “mediator” implies, the software is only an assistant or tool of the user. This construct deals with all issues of rights, liabilities and obligations as these are attributed or accredited to the user.

The pros and cons of this are discussed below, under the section on attribution of consent. In addition, this view may encounter difficulties as agent technology evolves and it becomes no longer possible to consider the software as simple mediators but as initiators (Agent C), as we discussed in the introduction (Chapter 1).

Arguments have been made against this view on the basis that it may be unfair to automatically attribute to the user all acts of the agents, including mistakes, distortions and unexpected acts (all the more so as agents acquire autonomy) that may have serious legal and practical consequences (imagine Agent C hiring 10 motorcars instead of 1!). In some jurisdictions, as we noted above, there may be a duty of good faith on the counter-party to

²³ UCITA and UECA try to deal with mistake, etc. Failing legislation, it will be up to the courts to decide...

correct or at least question an unexpected request or act in the course of negotiations, a duty which puts them in a difficult situation regarding deciding what to do. It would also not be commercially reasonable to hold a person liable for such unexpected acts which would normally be corrected in non electronic/automated transactions.

Avenues should be explored to see how the excessive liability for unexpected acts could be restricted or minimised, for example:

- Technically: providing for some form of feedback or non-automated communication for counter-parties in doubt. Alternatively, programming for a time period for confirmation and/or rejection (similar to consumer protection laws in distance contracts – though this would cause problems in a supermarket scenario). Certain items that may cause mistake or distortion (identity, addresses, payments, etc.) could be dealt with by communications with trusted third parties. Regarding identity, for example, it has been suggested to create a registry of agents that could confirm original agent objectives for protection against intervening distortion of agent behaviour... This may have difficulties with evolving and learning agents, though limits could be described like in a companies “object” clause.
- Legally: providing some balanced system of liability limitation – similar to the application of the principles of mistake – so that on the one hand users can repudiate a contract that is not in accordance with its instructions, while on the other counterparties are protected from illegitimate repudiations. This could either be in the general law for agent contracting (see attribution of consent – liability limitation, below) or by establishing a framework for an organisation for the registration of agents similar to the one for digital signatures (see paragraph above, though there are doubts about the economic viability of this solution) which would show the contracting capabilities of the agents that have been registered.

3.2 Consent: can agents provide consent, either of themselves or of the agent user?

3.2.1 Subjective and objective consent

As we saw in the outline, a contract is formed when two or more parties agree upon a certain transaction, that is to say they consent to be bound by the terms. There is a slight difference in the content of such consent between Civil and Common Law: Civil Law will look for offer and acceptance while Common Law will also look for an intent to create a legal relationship (as opposed to a simply informal one). However, the greater issue among

European jurisdictions is the conceptual difference between the two legal systems as to intent:

- Civil law will base a contract on a subjective view of intent, the inner will: did the parties really intend to contract²⁴?
- Common law looks only to the expression of such intent – an act –, in what is otherwise known as the objective view of consent: did the parties clearly express an intention to contract, from their words, writings and other circumstances.

Of course, there are several variations among legal systems, and these pure views are moderated by various additional concepts such as third party reliance or estoppel, good faith, misrepresentation and reasonableness. We will see the application of these below.

3.2.2 Application to agent-based provision of consent – the attribution of consent

The issue at hand is whether an electronic agent can intend or express intent. Taking the Civil Law view literally, it is obvious that an agent has no inner intent or state of mind (at the moment... again, one could argue that agents will evolve into devices that are self-determinate). The strictness of this view however is tempered at least in Germany, for example, where the objective view (based on the expression) will be taken to protect the recipient of any declaration of intent. This means that the party does not have to look behind the expression to determine whether the declarer actually intended the consent.

The objective view is of great assistance towards allowing software agents to contract: parties may rely on the outward expressions of the counterparties and do not have to look to their mental state. Electronic agents of course can express consent (offer or acceptance) by providing the appropriate electronic response to a request – e.g. the now traditional “I accept” message/click, but without the human action behind it. The validity of this consent is not determined on the basis of the inner mind, but determined on the basis of a test of reasonableness: would the reasonable counterparty believe that the declarer was giving his or her consent and intending to be bound. The consent only need be apparent, sufficient for the reasonable counterpart to base his response upon it (e.g. acceptance, performance or payment), so that the internal operation and programming of the electronic agent are irrelevant.

Problems may arise as to exactly whose consent is being expressed: the agent’s or the user’s? Insofar as the agent is merely a mediator like Agents A and B, and does not initiate a transaction without the intervention of the user,

²⁴ There are indications that this may be somewhat changing in France, for example. See E. Weitzenboeck, *op cit*.

then the consent in question must be considered to be that of the user. As we saw above, the agent can be considered a tool and the expression of consent is attributed to the user (either directly in relation to the transaction in question, or indirectly because the user knows that the agent is operating autonomously within certain parameters and entering into a series of transactions that tacitly the user agrees to). On the other hand, in relation to more advanced agents such as Agent C that can initiate a transaction without the knowledge of the user, the consent could seem to be technically that of the agent: the user is not aware of the transaction, so how can he/she give consent? In the end however, we contend that this consent will have to be deemed by the (reasonable) counterpart to be that of the user, unless certain circumstances indicate otherwise²⁵.

So it seems that this objective view, mainly prevalent in the Common Law jurisdictions, may assist courts in deciding affirmatively on the validity of an agent generated contract. The granting of this validity, attributing it to the user, would mean that contracts may be entered into by agents without the user(s) either knowing the terms of such agreements or even knowing that the agreement is taking place. Courts would have to rely on the initial parameterisation and operation of the devices to infer the general intent of the parties to enter into such agreements,

- either restrictively on the basis that the contract corresponds to the initial programming of the agent, and therefore the original intent of the user (closer to a subjective view of consent – the programming reflects the inner mind of the person); or
- more widely by enforcing contracts on the basis of the reliance of the counterpart upon the acts of the agent (pure objective view) – the user assenting to the means also assents to the consequences. Awareness of the time and terms are not relevant when considering the objective element of consent in the formation of contracts.

Again, it must be noted that the restrictive view may be difficult to use with more advanced agent technology. On the other hand, currently the more liberal interpretation may prove problematic even for common law courts and, until legislation is passed, require a fairly liberal interpretation of the law, as we discuss next.

²⁵ E.g. Trusted third party confirmation of limits of electronic agent's powers, or other intervening knowledge of the counterpart. If the consent could not be deemed to be that of the user, the answer to "whose consent is it?" is "no-one's": there is a mistake – somewhere along the line – that goes to the root of the contract and makes it void.

3.2.3 **Certain problems with the objective view – liability limitation and mistakes**

If we agree that the objective view of consent (and in the event of initiator agents, a liberal judge) will permit agent-based contracting, there will still be a fair amount of uncertainty and mistrust on the part of users if they know that they will be indiscriminately bound by any act of the agent. In relation to simple mediators, again we argue that there should be no problem for user confidence, except for problems of human or machine mistake or malignant intervention which would have to be dealt with. However autonomous and learning-functional agents may cause difficulties with unexpected acts and transactions that the user would not intend, foresee or authorise.

Accordingly, the following is a short list of reasons why persons (consumers especially but also merchants) may want to reject an agent-based contract, and without guarantees that this is possible, would hesitate to use these devices.

- a) Mistakes: human mistakes – either in programming or parameterisation.
- b) System failures: machine faults – power surges, etc., and external interference (viruses and other damaging acts).
- c) Unexpected acts: through agent learning and autonomy and bad deals (potentially involving bad faith on the part of the user).

These issues may be resolved by the application of certain traditional or more modern concepts of contract law which are discussed below. Otherwise legislation will be required (see section 4.4 below on recent legislation).

a) Mistakes:

In any transaction there can be a mistake, and contractual frameworks include underlying principles about the effect of mistakes on a transaction. In the end, the question of mistake is one of apportionment of risk: what to do when one party alleges agent mistakes (either agent itself or site-related mistakes in relation to an online merchant, such as has happened to Argos in the UK, or Kodak in the USA²⁶) in order to modify or annul a contract. There are three obvious parties to bear the risk:

- The innocent counterparty – seller or buyer – if the contract is cancelled.
- The mistaken user, if the contract is sustained with no modifications.
- The programmer/agent vendor in relation to defective agents (in relation to which, see also consumer protection issues below). In relation to programming errors, the user may have a remedy against the programmer or seller of the agent, whose liability may be limited, subject to mandatory law on exclusion of liability and consumer products.

²⁶ See “Kodak snaps under customer pressure”, ZDNet UK, 31.01.2002.

The effect on the principal contract between user and counterpart (seller, etc.) will be determined by basic principles of contract law, modified by any legislation that considers machine and/or human mistakes.

Generally speaking:

- A mistake made by one party that is known to the other will cancel a contract (the other party may not take advantage of the mistake, both under Civil Law duties of good faith in negotiations, and under Common Law principles of mistake).
- A mistake made by one party that is not necessarily known by the other, but which affects the contract to the extent that a reasonable counterpart would suspect an error, would also cancel the validity of a contract.
- A mistake made by one party that looks reasonable (see above, on reasonable consent) will probably bind the parties. On this basis the risk of an agent mistake would fall on the user of the agent.

Recent legislative attempts to deal with human errors are commented below, in section 4.4. One issue that will have to be determined is the question of adaptive agents that “learn”... possibly mistakenly. They may then enter into contracts that would never have been contemplated by the agent user, who may wish to plead mistake to avoid the contract. It will be a question of fact if the parameterisation or the adaptive functionalities of the agent were incorrect (the latter being something which may be very difficult to judge). The former may be a technical issue, though some form of recording of initial parameterisation should be kept.

On top of these issues, courts may wish to apply what has been called the “external aspects” of agency, limiting users’ liability to that which is reasonable – though this is yet to happen, and the effects fully understood.

b) System failures, exterior interference

We believe that the same principles should probably apply to system failures, certainly regarding mistakes that are so unreasonable as to affect the contract. An innocent party could also plead third party intervention (third party computer failures, power surges, etc.) to annul the contract. The same reasoning as above could be applied regarding the nature and extent of the mistaken terms in the eyes of the counterpart: if they are not unreasonable, the contract should be upheld and the user of the agent assumes the risk of using such technology.

Additionally there would be no recourse against the programmer, except if external interference such as interception or “spoofing” should have been foreseen and was not catered for (for which, the issue of agent security is essential using such technologies as encryption and digital signatures for secure contracting).

System failures and third party interventions such as denial of service attacks or viruses are a risk at all stages of online ecommerce, not just in agent based contracting. In section 4.4 below, we comment on how recent

legislation in the USA and Canada attempts to deal with these problems, either by providing clear guidelines as to contract validity or by providing procedures for the elucidation of real intent.

c) Unexpected acts and bad faith

This question is raised by agents that learn and adapt their beliefs, desires and intentions (possibly mistakenly, thereby distorting the user's intentions). They could then initiate new processes and enter into contracts that would never have been contemplated by the user.

First, the fact that users cannot foresee the agent decisions may not mean that they cannot be bound by them. Courts may wish to apply the previously mentioned “external aspects” of agency, limiting but also enforcing users' liability to that which is reasonable in the circumstances. Sartor argues for an intentional stance: contractual validity is based on the agent declarations and any default or malfunction would be construed as default of will removing consent and therefore invalidating the contract²⁷. In the event of any attempt to repudiate a deal on the basis of defects, it will be a question of fact if the initial parameterisation or the adaptive functionalities of the agent actually were incorrect, a technical issue which may be difficult to judge. Again, we argue that some form of record of initial parameterisation and user's intent could be kept. It must then be determined where the risk falls, in which case the rules of mistake should apply.

In addition, in some jurisdictions like Spain, for example, there may be a duty of good faith on the counter-party to correct or at least question an unexpected request or act in the course of negotiations, a duty which puts them in a difficult situation in deciding what to do. It may also not be commercially reasonable to hold an agent user liable for such unexpected acts which would normally be corrected in non-electronic or non-automated transactions. This issue is also complicated by consumer protections that allow consumers to cancel distance contracts within certain time periods, thus providing a consumer agent-user an advantage in relation to merchants.

3.3 Other issues

Now we have considered the fundamental or conceptual difficulties of agent-based contracting, we turn to some more practical or procedural problems that may be raised. This section looks in turn at the correct procedures for contracting (3.3.1), form and evidentiary requirements (3.3.2) the adequate incorporation of terms (3.3.3), whether software agents may provide legally binding or protected digital signatures (3.3.4) and the application of consumer rights in relation to contracts (3.3.5). After this, in

²⁷ G Sartor, *Agents in Cyberlaw* (2002).

Section 4 we turn to look at some legislative proposals that have been made (and some enacted) to deal with these issues.

3.3.1 Procedures – invitations and offers

The contracting framework regarding online contracting is still unclear within the European Union, especially as regards to the steps taken to form a contract (see above, general principles). The EC Ecommerce Directive left it up to Member States, in order to avoid upsetting national contract law frameworks.

As mentioned above, while a B2C site – and Agent A above, and maybe Agent B – may be considered by Common Law to be an invitation for a potential client to put in an offer for the goods on show which will then be accepted (or not) by the site, under Civil Law if the terms are sufficiently precise (they usually are, as they include description, price, delivery terms, etc. – and even more so if dialogues are standardised by the use of XML), the site will be considered an offer and the agent/user makes an acceptance – no further steps required. In practise, this is avoided by website terms of use that say that all consumer communications will be deemed offers, subject for example to availability and other criteria (payment authorisation, etc.).

When Agent B offers a special deal to the customer, is it really an offer, or would it be considered an invitation for the customer to make an offer to the store, and then store's systems decide whether there are sufficient units available to be able to accept it?

This means however that software agents may have to be programmed to take extra steps – more steps than may be really necessary – to comply with all national frameworks, which may vary from country to country. To add to this, the EC Ecommerce Directive requires electronic transactions to be acknowledged by Internet Service Providers (site owners). So this acknowledgement should also be incorporated into the programming, for compliance with procedural formation requirements. Extra processes will be required for Agent C, and maybe B, for them to satisfy these procedural requirements (please see the table at the end of this chapter, for a suggestion for Agent C).

The question is complicated however by the further requirement contained in the EC Ecommerce Directive regarding deemed reception: “when the data enter the recipient's information system”²⁸. If it is the agent who is collecting the relevant information/confirmation such as Agent C, it may be difficult to argue that the relevant data has been received by the consumer until the agent “returns to the fold” or sends the data on (back) to the user. Static agents resident in a user's computer or linked to a mobile phone (with instant access to data) would not pose much difficulty (provided

²⁸ Article 11 EC Ecommerce Directive.

the user can access the “state” or data contained in the agent at all times), however mobile agents, especially if they are more autonomous and don’t report back immediately after entering into an agreement, will cause serious difficulties with this. The transaction would not be deemed valid until the relevant acknowledgement was received, maybe days later, by the user. In fact, merchants may be disinclined to operate with agents as they will not be able to “presume” that the data is received by the user within a short period (like emails or SMSs). Programming specifications for agents could include a data field informing merchants when agents report back to Users (“immediate”, “within X period”, etc., or “by SMS”, etc.). Merchants could then perform the contract (software download, home delivery, etc.) accordingly.

Finally, consumer protection law provides certain procedural safeguards for consumers. These are briefly commented in section 3.3.5 below, and developed in chapter 4.

3.3.2 Form and Evidence

We now comment on whether the requirements for contracts to be made “in writing” can or have to be met in agent contracting, and how one can obtain and maintain evidence of an agent-formed contract.

As to the former, the requirement for contracts to be “in writing” that is established in certain jurisdictions and in respect of certain contracts is to be dealt with by national implementation of the EC Ecommerce Directive. Article 9 requires that: “Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means”²⁹. This has been understood to aim at allowing contracts to be made and evidenced in electronic form, with common exceptions for certain documents such as transfers of land. Most EU member states are adapting their legal frameworks to permit this³⁰.

The remaining question is a practical one of creating and storing evidence or proof of an agent-created contract, to provide higher levels of trust and certainty in agent based ecommerce. Similar to certain commercial sites that send email confirmations of sales (e.g. online air flight reservations or train bookings), software agents such as Agent C should be able to incorporate code to take advantage of these functionalities and even, for greater user comfort, refuse to deal with sites that don’t provide this feature. Whether this should be obligatory in ecommerce is debatable, as some

²⁹ Art 9 of the EC Ecommerce Directive.

³⁰ E.g. see Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico, for Spain.

offline transactions do not require documentary evidence, so why should online contracting be more burdensome? In the aim of providing certainty, transparency and predictability in ecommerce, some jurisdictions have required means to provide such documentary evidence. The EC Ecommerce Directive requires traders to provide recipients of a service a means for storing and reproduce contract terms, for example³¹. This may be all the more necessary – at least for the consumer – for agent contracting where the parties may not even be aware that such transactions are concluded.

This issue of form and evidence should also be linked to taxation requirements for invoicing, and electronic transaction record keeping. There does not seem to be any extra burden on companies in this area in relation to agent contracting. This issue should be dealt with by the internal programming of ecommerce merchant applications: appropriate invoices may be sent either by email or other communication system to purchasers. This issue is discussed further in section 3.3.5 below and Chapter 5 on Consumer Protection.

3.3.3 Terms

Agent contracting raises two questions regarding contract terms. Can we guarantee that all terms are properly incorporated into a contract? And, can the user have or be deemed to have knowledge of the terms?

One of the perennial problems of electronic contracting is the fact that contract law requires all terms applicable to the contract to be incorporated into the contract, otherwise they are not binding. Indeed, under consumer protection law the consumer must be notified of all these terms prior to conclusion of the deal (see below). In normal online contracting, the applicable terms are usually available to users and large notices (on good ecommerce sites) bring these terms to user attention. Ideally, the “I Accept” button presented by Agent B (which should often be “I Offer”!) is at the end of a scroll-down page that outlines all the applicable terms. Other now traditional procedures include adding the terms on a linked page (with the link next to the “I Accept” button). There are still debates about the validity of such links, but good website design should solve this issue. Additionally, if shoppers use agents to contract with the store that they are in, the log-on / registration system should provide an opportunity to give the general contracting terms to them.

As regards the question of attributing knowledge of the terms to the user, some questions that need to be considered are:

- a) If the user is not aware of the existence of a contract, how will he/she be deemed to be aware of the terms? This issue may be solved by the application of the attribution theory: the knowledge of the agent is

³¹ Art 10 of the EC Ecommerce Directive.

attributed to the user. As the user chooses to use an electronic agent, it is at the user's risk. This will have to be tempered by the application of mandatory consumer protection law (applicable according to the rules of Private International Law determined in the courts – usually – of the consumer's jurisdiction), for which, see below.

- b) What terms will be considered incorporated into the contract, and how? Again, this may be solved by technical means – but subject to consumer protections: a dialogue should occur between the merchant site and software agent like Agent C so that the appropriate terms are notified to the agent (and even sent on immediately to users, in some conditions), stored and transmitted back to user for reference and reproduction. It will be a question of the programming of the agent as to how many of the contractual terms (product characteristics, sellers, privacy rules, payment procedures, guarantees, expiration dates, jurisdiction and applicable law, conflict resolution procedures, etc.) are considered “variable criteria” that can be parameterised by the user, and therefore expressly accepted. Other items that are not included in an agent/site dialogue may be deemed implicitly accepted by the user (on the basis set out above) once the express items are accepted.

3.3.4 Signatures: can an agent provide a digital signature with binding effect?

The provision of consent to an agreement need not always be in writing and signed by a party. Persons not requiring high levels of security for their online contracting – authenticity, integrity, confidentiality, non repudiation – will not have a problem to agent contracting (in this respect), even if they cannot prove that one party or the other signed an agreement. The very fact that electronic commerce has been so successful despite the lack of use of digital signatures is witness to this.

However, one of the concepts that have been developed for secure electronic transactions is the digital signature. This form of signature has been proposed as a solution to problems of identification, integrity and repudiation, i.e. that the parties know who they are contracting with, that the document has not been tampered with, and that the signatory cannot turn round after the transaction and say: “I didn't sign that” and try to avoid any binding obligations. A court will normally uphold the obligation. Table 2.5 provides a brief outline of the key points regarding electronic and digital signatures.

*Table 2-5. Electronic and Digital Signatures in the EU Framework Directive*³²

³² Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

Electronic signatures: A definition of Electronic Signatures is: “means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”. This means data (signature) attached to other data (the document), that performs similar functions to a hand written signature. These can come in very many forms – e.g.: typed or scanned signature, electronic representation of a hand written signatures, a biological aspect, or a unique sequence of characters created by cryptographic means (providing better security).

Advanced electronic signatures: an “advanced signature” is one form of signature providing higher levels of security that has been given legal validity under the Digital Signature Framework Directive. It must be uniquely linked to the signatory and capable of identifying him/her, it is created using means that the signatory can maintain under his sole control and it enables data integrity. If it is backed by a “qualified certificate” (certificates that are produced (usually) by a trust service provider, whose obligations are outlined in the Directive) with a secure-signature creation device, like PKI software³³, it acquires legal validity as set out below. Only digital signatures using PKI currently fulfil the requirements.

Certificate providers: these constitute trusted third parties to ensure trust between trading parties, and are regulated by the EC Directive (and national implementation). They validate the linkage of the signature to its owner, issue certificates, generate keys or key pairs, and hold copies of keys.

The Digital Signatures Framework Directive: The Directive introduces a uniform standard for legal recognition of electronic signatures regardless of their origin in the EU, and facilitates the legal recognition of electronic writing. The legal effect of the Directive is that Member States must ensure that advanced electronic signatures satisfy the national legal requirements of a signature in relation to data in electronic form (in the same manner as a hand-written signature satisfies those requirements in relation to paper documents). Admissibility as evidence in legal proceedings can no longer be denied on the sole grounds that a signature is in electronic form, does not meet certain technical requirements or is not issued by an accredited issuer³⁴.

Advanced electronic signatures have not been taken up by the public, as they require obtaining a digital certificate from an authorised certificate authority and the process is cumbersome. As one may imagine, if these authorities are authenticating identity, they require proof of identity (ID cards, etc.) and other data from the user. This position may change, as governments promote the use of digital signatures for certainty and confidence in electronic commerce.

³³ There are some technical doubts about the strength of PKI, however this is the recognised standard, implemented in the original digital signature laws (Utah, Spain, etc.).

³⁴ National legislation is careful, however, not to provide definitive identification and admissibility through digital signatures, but aims to equate digital signatures and hand-written signatures in terms of evidence. There are times when a hand-written signature will not be admissible. Cf. for example, the UK Electronic Communications Act 2000 which will ensure that UK courts treat electronic signatures as producing the same evidential effects as physical signatures, but will not convert the document into a signed writing.

For our purposes it is relevant to see (1) if an electronic agent could incorporate digital signature technology (encryption and digital signature), which is a technical issue³⁵, and (2) if any digital signature issued by an agent would be a legally valid one.

The technical issue is not considered here – banks and other institutions are already incorporating digital signature technology in smart cards which can be inserted in computers or mobile phones, and we shall proceed on the basis that an electronic agent can technically issue a document with a digital signature attached.

What, then, are the legal effects? Are the conditions sufficient for the parties to benefit from the legal guarantees given by digital signatures? The construct relies on attribution. The basic assumption behind digital signatures is that if only one person has access to the private key and an encrypted document can only be decrypted using the corresponding public key then the encryption process must have occurred through the use of such private key, which means that it was the holder of the private key who encrypted the document. Consequently, the identity of the signatory of the electronic document has been revealed. But this does not mean that attribution has been achieved, because if the private key is stored in an electronic device such as an agent (or a smart card), then the agent can digitally sign a document. This means we are back in the situation where we have to see if a person can provide a signature through the mediation of an agent.

This question is similar to the debate on whether an agent may provide the relevant consent for a valid contract. We argue that there should be no problem with this, as owners of signatures have to use technological devices to insert a digital signature in a document anyway: why should the use of an agent prevent this?

There seems to be two basic issues, that of legal obligations and that of contractual obligations. First, does the law require that, assuming PKI technology is used for advanced digital signatures, a private key has to be used by a person (rather than a device)?

The UNCITRAL Model Law on Ecommerce allows data messages to be sent by an information system programmed by, or on behalf of, the originator to operate automatically (Article 13). However the Model Law on Digital Signatures adds some further requirements as to reliability (and therefore admissibility) of the signature:

³⁵ This involves an interface and communication with certification authorities, communications relating to private and public keys, storing private keys, etc. W3C is working on standards for XML solutions for Digital Signatures, which may be incorporated into agent technologies.

Article 6.b.3. “An electronic signature is considered to be reliable ... if the means of creating the electronic signature was, at the time of signing, under the control of the signatory and of no other person;...”

This (among other requirements) is also contained in the EC E-Signatures Framework Directive:

Article 2.2: “... an advanced digital signature will be effective if it is created using means that the signatory can maintain under his sole control ...”

The question therefore is whether the agent can be considered to be in the sole control of the signatory. This may be a question of technological fact that will be considered by the courts. The issue of who has the password or PIN required to activate the key would be considered. Storing this on the agent would be fairly risky (see below on user obligations), as the data is no longer “something that the user knows” but something that another person may acquire. This requirement, for example, would be even more problematic for mobile agents that can replicate themselves across the network in any hospitable server with the appropriate host environment. Are the keys then still in the control of the user? This issue may be solved by an agent that refers back to the mobile user (by SMS or other communication) for retrieval of the relevant data stored only in the user’s memory / control.

The EC Directive also provides that an advanced digital signature is to be satisfactory and admissible if it is “created using a secure-signature-creation device” (Art. 5). These devices are subject to various requirements set out in Annex III to the Directive³⁶, including secrecy and protection against use by others. This looks much less promising, as agent technology aims to provide autonomous devices. If we are therefore considering agents that are initiators rather than simple mediators, this would require the private key details to be included in the programming. In addition, the more the agent is autonomous, the less the user is going to know that the security has been compromised (as even warning procedures could be compromised too).

³⁶ The Annex states:

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
 - (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
 - (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
 - (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.
2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

The second question raised above is whether Certification Authorities, in their contractual rules with owners, require that owners have to keep the private key confidential and not record it in any way?

This will be a matter of contractual agreement (usually contained in a “Certification Authority Policy”) between the Certification Authority and user. For example, Identrus, the largest international network recently established for providing certification services, requires as follows:

“The Subscribing Customer:

Is obliged to protect its Private Key at all times, against loss, disclosure to any other party, modification and unauthorised use, in accordance with the Identrus Operating Rules and relevant contractual agreements and this CP.

Is personally and solely responsible for the confidentiality and integrity of its Private Key.

Is obligated to never store the PIN (Personal Identity Number) or pass phrase, used to protect unauthorised use of the Private Key, in the same location as the Private Key itself or next to its storage media, or otherwise in an unprotected manner without sufficient protection.”³⁷

For an agent such as Agent C to sign a message autonomously, it would need to hold both the PIN and Private Key, unless a separate repository could be safely implemented which the agent could consult to obtain one or the other (something that is not inconceivable). Keeping the two separate would seem to preclude the use of fully autonomous agents for digital signatures, as they would have to report back to the user for digital signature approval or generation, as mentioned above. The question of “sufficient protection” would have to be considered, of course as it may be possible to program agents or design a more complex system in a manner to achieve this level of security. Again, this will be a question of technology.

3.3.5 Consumer rights

Agent based contracting in the Research Scenario, as conceived in Agents A, B and C, involve consumers. So we must also consider how parties comply with legally imposed information, transparency and consent requirements when using agents for contracting. These include rights set out in the Consumer Protection Directives and the Ecommerce Directive of

³⁷ Identrus Certification Policy, Operating Rules and System Documentation Release 1.7 available at http://www.identrus.com/knowledge_center/library/certpolicies.html (visited 02/0512003).

2000, and the main issues are considered in Chapter 4 on Consumer Protection issues.

One particular comment should be made here about consumer protection in relation to contracting. It is unlikely that everyday consumers are informed and knowledgeable users of agents. Holding them liable for unexpected acts of the agents (and even mistake, third party intervention, or unexpected evolution) may be harsh and unfair, resulting in mistrust and rejection by consumers. Consumer protection law may protect them to some extent, especially regarding exclusion of liability by programmers and resellers and online merchants (see below). However it may be very difficult to establish technical criteria for standards (e.g. standards of reasonableness regarding agent functionalities) for this type of product. Alternative solutions include

- agent labelling, with third party approval of legal compliance, security, privacy etc, elements of any given agent; this could “enforce” the inclusion of levels of consumer protection in the internal programming of the agent (see below, under consumer protection – technical solutions), allowing consumers to indicate their required level of protection.
- insurance policies for agent transactions; or
- imposing strict liability on users or sites that deal with consumer-controlled agents.

Please see Chapter 4 on consumer rights for more comments in relation to this.

So far in this chapter, we have outlined and discussed some legal issues raised by agent based contracting, considering certain processes carried out by Agents A, B and C in the Research Scenario. We have noted that there are both conceptual and practical problems with agent contracting that will have to be solved if agent-based electronic commerce is to spread. In the next Section 4, we turn to look at certain proposals that have been initiated and enacted to deal (partially) with automated commercial transactions. After that, in Section 5 we will consider some final developments in this area, focusing on current technical solutions that are being proposed.

4. RECENT AND PROPOSED LEGISLATION AND DECISIONS

In this section, we will consider and comment certain legislative attempts have been made that may assist in overcoming some of the difficulties outlined above, and in promoting agent based contracting.

4.1 UNCITRAL Model Laws on Electronic Commerce and Digital Signatures

Although the UNCITRAL Model laws on Electronic Commerce³⁸ and Digital Signatures³⁹ is not applicable legislation, its provisions may be “applied” more and more through transposition into national laws (e.g. Brazil, Singapore, Thailand, etc.). This model law not only conceives of agent contracting, but also takes the approach of attributing the acts of an agent to the person that initiated the device: the “originator”. The two relevant articles are:

“Art. 2(c): “Originator” of a data message means a person by whom, *or on whose behalf*, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;” (*our emphasis*)

“Art. 13(2)(b): As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) *by an information system programmed by, or on behalf of, the originator to operate automatically.*” (*our emphasis again*)

The Model Law Remarks explain: “Data messages that are generated automatically by computers without direct human intervention should be regarded as “originating” from the legal entity on behalf of which the computer is operated.”⁴⁰

Conceptually this should deal with the issues of capacity and consent for contracting, as automated processes (data messages) are attributed to the legal or human person on whose behalf the agents is acting. It does not, however, deal with problems of mistake (machine) and other unexpected acts to which the user would not have consented and which would be attributed directly to the user (see above). Neither does this require participants to establish any procedure for error handling.

³⁸ See note 4 above.

³⁹ See note 5 above.

⁴⁰ UNCITRAL Model Law on Ecommerce, Article by Article Remarks, para 35.

4.2 UNCITRAL draft Model Law on Electronic Contracts

UNCITRAL has issued a discussion draft Model Law on Electronic Contracts, which was presented in March 2002 but will take a fair time before approval⁴¹.

The current draft directly considers agent contracting. The definition of “automated computer systems” involves a “computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a natural person at each time an action is initiated or a response is generated by the system” (Art. 5(e)).

As regards consent, the draft creates a presumption of the attribution of the action of the agent to the user of the software for the determination of the parties’ intent:

“Art. 9.2: In determining the intent of a party to be bound in case of acceptance, due consideration is to be given to all relevant circumstances of the case. Unless otherwise indicated by the offeror, the offer of goods or services through automated computer systems allowing the contract to be concluded automatically and without human intervention is presumed to indicate the intention of the offeror to be bound in case of acceptance.”

Article 12. provides directly for automated transactions:

“Art.12: 1. Unless otherwise agreed by the parties, a contract may be formed by the interaction of an automated computer system and a natural person or by the interaction of automated computer systems, even if no natural person reviewed each of the individual actions carried out by such systems or the resulting agreement.

2. Unless otherwise [expressly] agreed by the parties, a party offering goods or services through an automated computer system shall make available to the parties that use the system technical means allowing the parties to identify and correct errors prior to the conclusion of a contract. The technical means to be made available pursuant to this paragraph shall be appropriate, effective and accessible.

[3. A contract concluded by a natural person that accesses an automated computer system of another person has no legal effect and is not enforceable if the natural person made a material error in a data message and

⁴¹ A/CN.9/WG.IV/WP.95 - Electronic contracting: provisions for a draft convention at http://www.uncitral.org/english/workinggroups/wg_ec/index.htm

- (a) The automated computer system did not provide the natural person with an opportunity to prevent or correct the error;
- (b) The natural person notifies the other person of the error as soon as practicable when the natural person learns of it and indicates that he or she made an error in the data message;
- (c) The natural person takes reasonable steps, including steps that conform to the other person's instructions to return the goods or services received, if any, as a result of the error or, if instructed to do so, to destroy such goods or services; and
- (d) The natural person has not used or received any material benefit or value from the goods or services, if any, received from the other person.]”

Paragraph 2 of this Article 12 attempts to deal with the issue of errors in automated transactions. Inspired in article 11 of EC Ecommerce Directive, it creates an obligation for persons offering goods or services through automated computer systems, to offer means for correcting input errors. It leaves open what happens if there is no such correction mechanism (except see para. 3 quoted above). While online commerce platforms are improving their processes, including confirmation pages and final acceptance mechanisms for human users, for automated contracting like that conceived in Agent C there will be little opportunity for correction prior to concluding the contract (the error will only really be noticed on delivery or when the Agent reports to the user).

Paragraph 3 covers situations of material errors made by a natural person communicating with an automated computer system (i.e. would not cover agent-agent contracts, unless it is read that this applies to natural persons who contract through the use of their agents). In addition, we believe that this provision will probably only really be applicable for consumers, as repudiation rights are not common in commercial contracts. Unfortunately, the draft law has not included any provision for machine-made mistakes, such as computer crashes but also programming mistakes, which will certainly continue to occur.

4.3 The EC Ecommerce Directive

Unfortunately the EC Ecommerce Directive is of no real help regarding the conceptual difficulties for agent-based contracting. The closest one gets is Article 9, which provides that:

“Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in

particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.”

While this does not explicitly enable delegated or automated contracting, the preamble to the Directive includes agents as “electronic means”... which leaves the situation in the hands of national legislators and judges. National laws may indeed be more specific in implementation of the Directive, though this has yet to be seen. For example, this has not been the case of those countries who are writing new laws at the time of this work (UK, Germany, Spain), as we see next.

4.4 National legislation in the EU and third countries

So far, EU Member States are still discussing changes in national law required by this provision. Mainly governments are looking at issues of online contracting, i.e. without paper support or traditional signature. Several thoughts occur.

First, a variation among national regimes for electronic contracting will provide difficulties for the EU’s goal of harmonisation and levelling of the playing field for ecommerce. What does an Irish shopper do if agent contracting is supported in Ireland but not in Portugal? Should Agent C be limited to “Irish sites” (if that can be determined)? And what of a Portuguese shopper in the same circumstances? The purchase possibly may not be enforced in the home jurisdiction.

In addition, an uneven legal framework for automated contracting may cause technical procedural problems for different websites from companies in different countries. They may have to program different processes for different visitors, multiplying the complexity of commercial websites. This solution may only be valid if they can determine the “origin” of the visitors, and such variations are not considered discriminatory or contrary to the rules of the internal market. This interoperability point may be solved by more complex agents with processes that can deal with several jurisdictions – but who will pay for such applications?

A few examples of national attitudes in Europe include:

- **UK:** At the date of our research, the UK Government believes that no change is required to English contract law for valid electronic contracting. This would leave the question open until judicial comment or decision gave further precision⁴².

⁴² The Electronic Commerce (EC Directive) Regulations 2002 – and guidance: March 2002. At http://www.dti.gov.uk/cii/ecommerce/europeanpolicy/ecommerce_directive.shtml (visited 15/05/2002)

- **Spain:** The Spanish “Ley de los Servicios y Sociedad de la Información y Comercio Electrónico” (LEY 34/2002, of the 11th of July) reads

“Art. 23(1): Contracts concluded by electronic means will produce all the effects established under the legal system, when all the requisites for consent and other requirements for validity are satisfied”⁴³.

This may be no advance on the current situation, as the Spanish code seems to take a more subjectivist view of consent.

In the USA, contract law is left up to the individual states, however there is a centralised “uniform code” system that proposes model laws in order to harmonise contract law, mostly to prevent differences from upsetting inter-state trade. The uniform laws then have to be enacted into law by the states (by adoption). Two relevant model laws for electronic contracting, either online or through agents, are UETA and UCITA.

- **UETA: Uniform Electronic Transactions Act:** This act contemplates person-agent and agent-agent contracts, and takes the approach of attributing the acts of an agent to the person that initiated the device (Section 9), even if the person had no knowledge of the agreement or of its terms (section 14). This strict liability could be problematic from the user’s point of view, as he/she would not want to be bound by malfunctioning, unintended acts, errors or third party interventions, all the more so if the agent is intelligent and incorporates learning and adaptation. This act also deals with human mistake, providing for a correction mechanism, but not machine mistake (section 10).
- **UCITA: Uniform Computer Information Transaction Act:** This act recognises that contracts may be concluded by transmissions between agents and persons, “if the transaction demonstrates existence of an agreement between the parties using the agents” (section 202). In the USA the objective theory of consent would determine the validity of the transaction, subject to a reasonableness test which would temper the strict application of attributed liability. The Act aims to make clear the granting of assent, both by conduct and (somewhat unnecessarily) by electronic agents (section 112), applying the objective view (thereby allowing judges to take a more liberal view of consent mentioned above). What is more, the Act also indirectly provides for electronic mistakes, without specification, permitting courts to grant relief in certain cases (i.e. to annul the contract). This however applies only between agents and not between humans and agent: the latter would be left up to traditional concepts of mistake outlined above. To date, UCITA however is only

⁴³ Unofficial translation of the authors: “Art. 23(1): *Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurran el consentimiento y los demás requisitos necesarios para su validez*”.

enacted in two states. It has been rejected by most other States, as well as the American Bar Association, as unhelpful and unwieldy.

- **US jurisprudence:** A recent decision in the USA, *Specht v. Netscape Communications Corp*⁴⁴, emphasises that traditional rules of contract law will apply to e-commerce transactions: a federal district court concluded that no contract had been formed when a user downloaded software without first having to click through a license. This focuses on the need to incorporate terms in the contract and bring certain key terms to the purchaser's attention (an arbitration clause restricting the consumer's rights). Such rules may be difficult to comply with, for example with Agent C, without further specific negotiating and notification processes being incorporated into the agent's programming.

Canada is an interesting study, having had the benefit of the US and preliminary European experiences: the Uniform Electronic Commerce Act (UECA) was adopted in 1999⁴⁵. The act defines electronic agents, provides that contracts may be concluded by interaction between agents and humans and between such agents, and determines that persons are bound by the expression of consent by electronic means or by other electronic action (e.g. agent action) in a manner which is intended to express the consent, i.e. by conduct. Accordingly Canada would also apply an attribution rule and the objective test of consent, taking advantage of the reasonableness test to avoid excessive liability. There are rules for material errors made by persons when dealing with agents, but there is no rule for mistakes made by the agents themselves, through programming error or system failure for example.

5. MATCHING LAW AND TECHNOLOGY WITH A PROCESS VIEW

To establish legal validity and efficacy of automated contracts, several technical approaches have been suggested.

First, recent work on intelligent agents, especially mobile agents, is focussing on policy expressions for security. This involves establishing a set of documented information system security decisions defining the rules needed to be enforced by security mechanisms and controls of the underlying hardware and software comprising the agent system (e.g.

⁴⁴ *Specht v. Netscape Communications Corp.*, 150 F. Supp. 2d 585 (S.D.N.Y., July 5, 2001), *aff'd*, 306 F.3d 17 (2nd Cir. 2002).

⁴⁵ I Kerr, *Providing for Autonomous Electronic Devices in the Uniform Electronic Commerce Act* (2000).

privileges)⁴⁶. Work suggests these policies could be included in an external object, an “attribution certificate” and “policy certificate” governing the agent’s behaviour. This same principle can be extended to contracting (and consumer protection) issues, regarding definition of issuers and owners, authority, consent, definition of terms and conditions. Moreover, this trend towards expressing policies in objects can also be seen in relation to privacy, with the work on P3P dialogues. This is an issue which is commented on in Chapter 6, where we argue that one solution for incorporating these concepts of policies, rules and dependencies into the technical architecture is to use process modelling for higher level system design and interoperability.

Work is also being carried out in the area of commerce frameworks. As with EDI and B2B marketplace electronic commerce, electronic contracting (including agent contracting) would be more enforceable within a closed legal framework. Just as members of an EDI system or a B2B exchange agree to standard contract terms (including message validity and timing, jurisdiction, incorporation of certain terms – see UNCITRAL recommendation 31), agent users could agree to standard terms beforehand, through a registration mechanism, and then use the software agents for contracting within this framework. This may be applicable, for example, in the Research Scenario with agent contracting between the user and the store (Agents A and B), where there will be a registration / log-on process. This design precludes, however, open market contracting along the lines of Agent C (e.g. comparison shopping while the shopper is in the store)⁴⁷.

The question of open market trading raises the issue of the standardisation of shopping agents such as Agent C. This would entail agents being produced with a predetermined set of functionalities and processes recognised by merchants, who could agree to certain terms beforehand. This will subsequently provide more flexibility for agent contracting. The consequences of this include higher levels of consumer protection, the possibility of recourse to agreed dispute resolution mechanisms, and more certainty and trust in such dematerialised transactions. For example, standard processes for complying with the obligations of supplier information and error correction could be pre-established and incorporated into the technical architectures of affiliated merchants. This could also favour a standard for digital signatures among participants.

⁴⁶ See for example the National Institute for Standards and Technology Aroma project (www.itl.nist.gov/div897/ctg/aroma/home.html) and the IETF (<http://www.ietf.org/html.charters/mobileip-charter.html>) in the USA and in the EU, the PISA project (Privacy Incorporated Software Agent) online at <http://www.tno.nl/instit/fel/pisa/>.

⁴⁷ Unless such competitors and other merchants also participate in a wider architecture such as ebXML or other trading framework.

On the other hand, this type of “bound” agents does not necessarily provide the full benefits of ecommerce – with the Internet as a virtually endless supply of alternative products, terms and suppliers. For example, while there are current proposals for XML digital certificate standards within the W3C, which may ensure wide adoption, this is not yet the case for other elements of contracts, especially taking into consideration the differing contract regimes.

In our Research Scenario, we have only considered the concepts of electronic contracting between natural persons and agents, and between agents under the direct control of single entities or persons (the store, a web-merchant). Further complications will arise with complex agent platforms, and even more so mobile agents, where there may be a multiplicity of owners and actors intervening in the transaction: consumer, merchant, site host, agent host, trusted third parties, payment intermediaries, etc. In such complex scenarios, it will be important to analyse process by process each transaction and the parties involved for a proper analysis of responsibilities and obligations, including consumer, data and IPR protection.

Another solution that has been put forward is the question of registration and/or certification of Intelligent Agents, in a process that would be similar to corporate registration. This would be akin to – or would allow - giving legal identity to Software agents⁴⁸. It has been suggested that this would deal with some of the problems mentioned above: identification of the users, authority of the agent, mistake and proper functioning of the agents. Such a system, involving certification of the agents, including a security / authority classification which would determine what the limits of the agent’s activities are, would allow counterparties to check up on the agent it is dealing with (similar to digital certificates for advanced electronic signatures). This would increase certainty and reduce the scope for mistake.

Less formal would be a private system of “trustmarks” or private certification, similar to a labelling system, providing a private framework for the operation of the agents. This would include determining minimum standards, including privacy issues, establishing dispute resolution procedures and jurisdictional issues, and is rather similar to the idea of using agents within a more “closed” framework commented above. Both merchants and users would subscribe to the minimum standards required by the certification system. This is also a selling point for merchants (as all trustmark schemes may be), enabling higher levels of confidence.

The problem with these formal proposals is that they reduce the scope for innovation and creativity in the development and use of agents. Understandably they would only apply to more advanced “actor” agents that can incur contractual liabilities on behalf of the user – both merchants and consumers (as opposed to more simple search and compare agents, which

⁴⁸ A Karnow, *Liability for Distributed Artificial Intelligences* (1996).

are “observers”). On the other hand, especially from the consumer’s point of view, these schemes introduce an element of trust and confidence in agent trading. On the practical side, they would be fairly expensive to implement, involving registries, monitoring, standardising, verification processes which would incur a fair amount of time, effort and cost.

In the absence of immediate legal solutions to some of these problems facing agent contracting, we have argued that it may be possible to add certain technical features to software agents for enhancing the validity of any agent-based contract. The following list summarises suggestions made during the course of the analysis of Agents A, B and C in the previous sections.

- The identity of the user/principal (or at least, indicating that the software agent is a device and not a person) could be included in the coding, for the purpose of disclosing the existence of a principal and inferring apparent authority. This may run into problems of privacy (a user who doesn’t want to disclose his/her identity) which may be solved by a neutral indication that the software agent is only an electronic device. For example, a tag would indicate “nature = software agent” while “Id = XXX”.
- The nature of the user/principal could also be incorporated into the code: as business or consumer user (“nature of user = Consumer / Business”). This would provide the counterpart with some idea of its obligations, and the possibility or excluding certain consumer initialised agents if it only contracts (by law or by corporate policy) with businesses.
- Negotiation protocols should enable websites and agents to communicate regarding which party is making the offer, the acceptance and the acknowledgement required by the combination of national laws and the Ecommerce Directive.
- Run time errors and other unexpected events or state (e.g. after third party intervention) should be able to generate a “freeze/ refer or report back to user before proceeding” procedure – maybe with variable parameters to give the agent greater autonomy, parameters that could vary within even wider fixed limits as the agent learns, to reduce certain liabilities in the event of non-repudiable mistakes.
- Communications could be confirmed by email or SMS to users, for providing greater evidence of transactions, either encrypted (for security) or not.
- Agents should include functionalities for creating, transmitting and storing electronic evidence of transactions (emails, SMS, invoices).
- For adaptive/advanced agents, initial parameterisation should be stored as evidence of user intent, especially in the case of mistake or unexpected learning processes.

- Security features should be incorporated to minimise the risk of contracting after third party intervention (viruses, etc.) or system failure (power surges, etc.).
- Agents should withhold from contracting when in doubt, especially regarding terms of sale (exclusions of liability, etc.): a fall back procedure should allow the agent to report back to the user.
- Agents should include programming to send an Acknowledgement of Receipt back to (consumer) users as soon as possible (email or other data transmission – SMS etc.).

Below in Table 2.6, by way of example we present a summary of these legal and technical issues for electronic contracting that are presented by Agents C, the most complex of those set out above. Taking a process view, we attempt to establish the legal risks for each of the agent's processes. This enables us to determine further processes that may be either necessary (for compliance) or recommended (good practice, for greater confidence).

Table 2-6. Legal risks of Agent C's contracting processes

Principal Process	Legal issue (contract related)	Additional processes for compliance and/or certainty
Agent C determines a need to purchase specific item	None (internal process)	Registration of original agent programming / parameters (trigger events, contract conditions)
Agent C searches the network for various stores selling relevant products	Pre-contract issues: web-pages as advertising or offer Information requirements (consumer contracting issue)	Identification of data messages as advertisements or offers Forwarding of obligatory information to users.
Agent C negotiates with store(s) for the quantity, price and other terms of sale	Identification of parties – agent user identified as consumer Capacity of agent to negotiate Good faith and withdrawing from negotiation	Registration of negotiation steps (assistance to determine true intent) Session control and processes for system failures Well defined negotiation protocols
Agent C concludes purchase agreement	Capacity and Consent Mistake Incorporation of all terms	Certification of agent's "authority to conclude contracts" Process for retrieving and storing terms Process for error correction and confirmation Process for acknowledgement of receipt
Agent C provides delivery and payment details	Identification of parties	Digital signatures for payments (e.g. SET protocol) Reference to User for PIN
Agent C records transaction	Storage of evidence	Register of processes (but security level? – e.g. Encryption for integrity and confidentiality)

We argue in Chapter 6 that if these technical advertising, negotiation and contracting processes can be completed and modelled so that they become “universal” for the majority of B2C or B2B contracting processes (rather like a process protocol), we maybe able to create a legal architecture that can be applied to the technical processes for agent contracting. This legal modelling in turn will enable ecommerce software developers to legalise their technical models – thus creating a framework for compliant “contracting agent” engineering. This approach is developed more in Chapter 6.

Legal Programming

Designing Legally Compliant RFID and Software Agent
Architectures for Retail Processes and Beyond

Subirana, B.; Bain, M.

2005, XX, 314 p. With CD-ROM., Hardcover

ISBN: 978-0-387-23414-4