DIGITAL ANONYMITY ON THE INTERNET

NEW RULES FOR ANONYMOUS ELECTRONIC TRANSACTIONS?

AN EXPLORATION OF THE PRIVATE LAW IMPLICATIONS OF DIGITAL ANONYMITY[1]

Jan Grijpink and Corien Prins

This article sets out the most important conclusions of the first stage of a study into the dimensions of digital anonymity. It is intended to set out the problem, make people aware of the intricacies of the problem and thus stimulate the debate on useful legal structures for anonymity. The article focuses on Holland's private law dimensions, addressing situations where consumers want to purchase anonymously on the Internet.

1. BACKGROUND

Lately, anonymous communications on the Internet have gained considerable attention. A New Jersey state court judge ruled in November 2000 that a software company is not entitled to learn the identities of two "John Doe" defendants who anonymously posted critical comments on a Yahoo message board.[2] In the Fall 2000, Ian Avrum Goldberg's dissertation on *A Pseudonymous Communications Infrastructure for the Internet* received world-wide publicity.[3] Ongoing concerns of digital privacy stimulate the debates about possible ways to avoid being 'profiled' on the Net and communicate anonymously.

Anonymous communication raises various (legal) questions. What exactly do we mean by anonymity? Why would people want to communicate and transact on an anonymous basis? What are the practical and legal restraints upon anonymity when communicating and transacting with others? In other words: aside from the ad-hoc problems that now arise under case law, what is the larger landscape of the legal consequences of anonymity? With the purpose of directing the key question towards future developments in information technology, the study is based on a picture of the future in which the large scale use of anonymous electronic transactions occupies an important position. We hereby take the chip card as an illustrative example and focus on the Dutch legal situation. Finally, it should be mentioned that this study forms part of a broader search for sustainable legal and organizational transformation processes arising from new information and communication technology.[4]

The article is laid out as follows. Section 2 provides an outline of the key questions concerning a new law for digital anonymity and some background information. Anonymity is a concept that is subject to multiple interpretations, an issue that is discussed in section 3. The key question is only worth addressing if absolutely anonymous electronic legal transactions are technically feasible, and we can put forward a plausible case supporting the practical significance of anonymity in electronic legal transactions. We will set forth that case in section 4. Section 5 outlines the status of an absolutely anonymous contract under private law, contract law and property law. This provides an idea of the room that current private law offers for anonymous legal transactions, which is a good starting point for answering the question of whether these provisions will be adequate when it comes to the widespread anonymous use of chip cards. In section 6 we look into the legal status of less absolute forms of anonymity in legal transactions (semi-anonymity). To answer the question concerning the desired legal development, in section 7 we address the role that the law will have to play if a situation arises in which anonymous electronic legal transactions dislocate vulnerable legal relationships. We will then examine two alternatives for the development of new law: based on our own Dutch law or derived from foreign law. These considerations lead in section 8 to conclusions regarding the extent to which the risks of anonymous electronic legal transactions will in the future necessitate the introduction of new legal rules.

Given that legal development takes so much more time than the introduction and distribution of new technology, it is of great importance to gain early insight into the direction in which the law can best develop in response to new technology. That is the underlying motive behind this part of the overall study and the justification for directly reporting on the first preliminary results, in the hope that this will set in motion a

ISSN 0267 3649/01/$20.00

discussion that offers prospects for timely legislation should the need arise.

2 KEY QUESTION

The key question to be addressed in this article is the following: Do the specific implications of border-transgressing anonymous electronic legal transactions form a reason for the legislature to proclaim new legal structure under private law? Is it possible to foresee the areas in which this could be done, and if so, how (domestic legal development or derivation)? To answer this question we concentrate mainly on private law with an initial approach from the perspective of the bilateral consumer transaction under the obligatory contract. This is where the idea of protection is most pronounced, so that the need for new legal rules in this context will perhaps be the most striking.

The chip card, and the multifunctional smart card in particular, makes it possible to place the new information and communication technology literally in the hands of the user. A portable, intelligent means of actively participating in electronic legal transactions. It is safe to assume that the chip card will in the future become an important instrument for joining and exiting the information superhighway (e.g. to remit payment) and will play a crucial role in electronic legal transactions.

The chip card also enables the user to participate in legal transactions anonymously. This can even be done very safely, by using anonymous biometrics.[5] The ability to participate with absolute anonymity in legal transactions gives rise to various normative and concrete legal questions. What is the legal effect of an anonymous electronic contract or an anonymous claim arising from an anonymous electronic contract? To what extent can an anonymous suspect be prosecuted? To respond to this and other questions, it is expected that solutions will be developed that give anonymous electronic legal transactions a place in the legal system. The anonymous legal transaction is not as such a new phenomenon. But the application of ICT in anonymous legal transactions creates new risks in social and economic life, or moves the goalposts of risks that are already present. This could disrupt the traditional balance in the (legal) relationship between parties. To give these ideas concrete form, we will start out from a picture of the future with the widespread use of anonymous chip cards, but other forms of anonymous electronic legal transactions may also give rise to the need for new legal rules (there are already various anonymity applications on the Internet that function separately from a chip card).

The law is typically time and place related, electronic communication is not. This is illustrated by the existence of rules governing national jurisdiction and of principles relating to the scope of national law. There is a fundamental field of tension between the border-transgressing alternatives of technological applications such as chip cards and the Internet on the one hand, and the scope of legal rules and their enforcement on the other.[6]

Individual countries' margins for domestic policymaking are likely to diminish to an increasing extent. It is therefore important to evaluate in advance the efforts in the area of the legal infrastructure in the light of possible scenarios relating to (international) administrative and legal relationships. In 1998 the Dutch Ministry of Justice published three scenarios that could be used for that purpose.[7] In the most radical scenario, in the year 2010 the Netherlands occupies a subordinate position in a large number of international legal communities and interest groups. In a totality of mutually-competing, world-encompassing legal communities and interest groups, the role of a European Union with 25 or more member states could prove much more modest that many people presently assume. The current border-transgressing dimensions of ICT applications demonstrate that we are already seeing an erosion of national policy autonomy. This explains why new rules regarding the implications of the anonymous use of chip cards will increasingly have (or need to have) an international character.

In this respect it is important to bear in mind that in parts of the world with other legal traditions and cultures there prevail completely different views on legal transactions and their implications. The function that the law in the Dutch legal culture will have to fulfil in an information society without geographical boundaries is by no means certain.[8] The legal culture plays a significant role in the need for rules. The one legal culture is characterized more than the other by the urge to remove the cause of risks. Other legal cultures prefer to reduce risks by dividing the consequences over a larger group of people. It then becomes possible to insure oneself against risks of this nature. The consequences are spread out, but are not avoided. For as long as more importance is attached to preventing the damage caused by digital anonymity than to dividing it, disproportionate risks must sooner lead to extra protection for weaker parties and, therefore, to new rules.

3. ANONYMITY: A QUESTION OF DEGREE

Anonymity is not a fixed characteristic of a person. I am not anonymous to myself, and neither am I to people who have known me since I was a child. Anonymity is therefore in the eye of the beholder. I am anonymous to somebody who cannot find out who I am, or would only be able to do so by making a disproportionate amount of effort. We describe legal transactions as anonymous if it is not possible to establish the true identity of an acting party because he has left no traces behind whatsoever, or has disguised all traces using a pseudonym from which his real name cannot be derived. If, for example, something goes wrong with the formation or implementation of a contract and this situation causes one of the parties to the contract or a third party to suffer losses, it is not possible to recover those losses from the party that caused them.

Although most people do not make a distinction between various degrees of anonymity, such a distinction is important to evaluating the legal implications. For this purpose we make a distinction between:

- absolutely anonymous legal transactions, whether or not with the use of a *self-chosen* pseudonym (no traces that make it possible to establish someone's identity);
- spontaneous semi-anonymous legal transactions, whether or not with the use of a *self-chosen* pseudonym (there are traces that make it possible to establish someone's identity);
- organized semi-anonymous legal transactions with the use of a pseudonym *issued by a third party*;

- spontaneous personalized transactions using unverified or unverifiable identifying personal details;
- organized personalized transactions with the use of identifying personal details which have been accurately verified by an authorized third party.

The determinative factor of this division is first and foremost the use of a pseudonym that does or does not leave traces that make it possible to establish who is using the pseudonym. A pseudonym is a distinguishing mark with which a certain transaction or act can be traced back to a certain existing or fictitious person.

That distinguishing mark can be anything: a password, a pseudonym, a personal number, an electronic signature, a pin code or a biometric number.[9] Secondly, it is important to know whether the pseudonym was spontaneously selected by the person using it or organized. 'Organized' means that the pseudonym was issued by a private or public authority such as a supervisory body or an intermediary, or by a third party involved in a contract situation, such as the bank of a party to a contract who remits payment by means of a PIN payment.

To properly understand the concept of various forms of anonymity in legal transactions it is important to grasp the difference between establishing someone's identity (identification) and verifying someone's identity (verification). Identification sets out to establish someone's *true* identity. Verification merely establishes whether two details relate to *the same* person. In practice, people rarely set out to establish the true identity of others, but generally settle for establishing that someone is the person they expect them to be. Unfortunately, people are often unaware of the limitations of the customary forms of personal identification, so that verification is often placed on par with identification. Even if a person can be compared on the spot with a photograph on an identity card, this one-off and isolated verification can never provide certainty that the person in question is actually who he says he is. For many legal transactions a personal identification along the lines of 'he is *the same* as ….' is however sufficient.[10] A verification of this nature can be made using a pseudonym.

The most important reason to take actions and conduct transactions under a pseudonym is that the person using the pseudonym can make him or herself recognizable without revealing their real name. To give an example, a person can participate in discussion groups and be recognized by his 'nick'. A person can also present himself by means of a chip card PIN code as the legal holder of the PIN card.

The outer extreme of the classification described above is therefore formed by absolute anonymity. When acting *absolutely* anonymously it is not possible trace back a legal transaction to a person because no lead is available. The telephone box is a well-known example of the absolute anonymity of the caller. If at least one party knows or can find out exactly who the acting party is, we no longer speak of anonymity but of semi-anonymity. In a semi-anonymous legal transaction certain bodies or intermediaries can establish the identity of the people involved if there is good cause to do so. Internet remailing services on the Internet are a good example of semi-anonymous actions. P.O. Boxes, car registration numbers and the ability to bid anonymously at an auction are examples of semi-anonymity. Further details about the true identity of the user, holder or client can be obtained from at least one body (under more or less strict conditions and sometimes for a fee). We can distinguish two variants of semi-anonymity: spontaneous and organized semi-anonymity. Examples of spontaneous semi-anonymity with self-chosen pseudonyms are stage names and pen names. In other cases we can distinguish organized semi-anonymity with a pseudonym issued by a third party rather than being chosen by the user himself. The PIN code for a chip card is an example of an organized pseudonym that facilitates organized semi-anonymity.[11]

If someone's true identity is known or can easily be determined by means of traces or identifying personal details, we speak of a personalized legal transaction. The most reliable form involves an authorized third party verifying the accuracy of the identifying personal details. This third party could be a private or public body, such as a civil-law notary, a registrar of births, deaths and marriages, or a private organization that has obtained TTP (Trusted Third Party) status. In the case of spontaneously personalized transactions there usually remains uncertainty about who the other party actually is.

A pseudonym therefore makes it possible to remain anonymous to one party and to be completely known to another. If a bank issues a PIN code, the bank can establish when issuing the PIN card who the holder actually is. If a person later uses the PIN card to make payment, he can remain anonymous to the other party to the transaction, using the PIN code as a pseudo identity (pseudonym) and the PIN card as a pseudo-identity card. The shopkeeper who receives payment by way of the PIN payment knows that the client is the legal holder of the PIN card according to the bank, without the bank having to tell him the precise identity of the client. This double effect makes it possible to arrange anonymity in legal transactions in such a way that the desired legal certainty is created.

4. THE SOCIAL SIGNIFICANCE OF ANONYMITY

If anonymity is to little social avail, or if absolute anonymity in an electronic environment is technically impossible, the bottom falls out of our research into new legal rules in response to anonymity. In this paragraph we will therefore discuss these two elements that determine the relevance of our research.

As mentioned in the introduction, the desire for anonymity is clearly increasing in practice. Witness, for instance, the popularity of prepaid telephones without subscriptions and anonymous access to the Internet, explicitly offered as such. One of the underlying reasons why people are drawn more and more towards anonymous electronic legal transactions is that they are becoming increasingly concerned about how much privacy will remain in an information society. After all, those who participate anonymously in legal transactions are no longer dependent on the question of whether those processing personal details are complying with the privacy laws. The protection of privacy is being brought about via anonymity.[12] In addition to privacy considerations, people may wish to remain anonymous for purposes of freedom of speech. It is clear that in various parts of the world, people may have an interest in not being identified and thus connected to certain published

views and opinions. Due to the international character of the Internet, the freedom of expression-related reasons for anonymous communications may gain new dimensions. Finally, arguments why people would want to transact anonymously could be because they are involved in criminal activity and do not want to leave a trail of their dealings or because they want to evade tax.

Having thus explained the social usefulness of anonymity, we subsequently test the technical feasibility of digital anonymity. Somebody holds a chip card that can (only) be used to remit payment. The card contains a form of counter system so that the holder can keep track of the card's balance. There are (public) terminals where people can input cash in order to load the card to the value of that cash amount. The cash goes to a float account (e.g. Interpay). Once person A has loaded his card, he goes to a shop and pays for his goods using his chip card. The amount to be paid is then deducted from the card without the card number being recorded. The shopkeeper can then cash the amount paid at Interpay. Unless the shopkeeper knows who the buyer is because he spontaneously recognizes him, the customer has in this case paid for his goods absolutely anonymously. Absolutely anonymous payment using an (anonymous) chip card is therefore already feasible. The conditions are an anonymous chip card that people can use to remit payment and public terminals at which coins and banknotes can be used to increase the balance of the anonymous card without the card number being registered when loading the card and remitting payment.

There are also conceivable applications in which the user has purchased a certain amount of online time - e.g. in an Internet café or a public library - and has anonymously been given an E-mail address. If the user has bought any goods in this manner, he can collect them anonymously at a (variant of the) 7-11 shop, where his right to collect the goods is verified by means of a code on the chip card with which the online payment was made.[13] The person concerned remains anonymous, and is given the purchased goods if he holds the same chip card with the correct code.

Although we see that absolute anonymity is already technically feasible, most of the transactions that are presently described as anonymous are not absolutely anonymous. These transactions are virtually always semi-anonymous. A semi-anonymous transaction that we are now all familiar with is payment using a PIN code. Although the shopkeeper does not have to know who the PIN payer is, the bank does have that information. The bank uses the PIN code to establish that the card holder is *the same* person as the one from whose account the amount must be deducted, and then executes the payment transaction. This category also includes the ability to surf, send and receive e-mails and chat on the Internet anonymously. The Internet Service Provider (ISP) is often able to establish the identity of the subscriber in question by way of traces.[14]

5. THE LEGAL IMPLICATIONS OF ABSOLUTE ANONYMITY UNDER PRIVATE LAW

In the case of absolute anonymity it is not possible to trace back a legal transaction to a person. The identity of the acting person cannot be determined by any means whatsoever, even via a pseudonym. So what are the legal implications for the parties involved?

The first point to note is that there are of course already various everyday legal transactions in which one of the parties remains anonymous because he pays in cash on the spot for a product or service. When a person inserts a guilder into a coffee machine for a cup of coffee, a legal contract is entered into, although it will probably not occur to him or her to regard it as such. In formal legal terms, an obligatory contract is formed in a consensus between the parties concerning certain obligations. The fact that the parties reach agreement without knowing each other's identity does not rob the contract of its legal force: this agreement too results in principle in a legally binding contract. Problems first arise if the result of the contract is not forthcoming or if the contract is not complied with for other reasons.

So what does the electronic dimension add to the phenomenon of acting absolutely anonymously? Our position is that the initial difference is the fact that the anonymous electronic transaction is made at a distance without any physical contact between the parties to the contract, either directly or indirectly (owner of a coffee machine). It will therefore, for example, be more difficult for the supplier offering his products or services by electronic means to establish the capacity in which his anonymous opposite party is acting. A second difference is that the parties will want to participate anonymously in electronic legal transactions on a much bigger scale. Based on the assumption of simple, widespread and global anonymous legal transactions in the longer term, the time has now come for us to pose the question of what the implications of anonymous transactions will be under private law. Do the legal instruments that determine the content of the relationship between the parties participating in electronic legal transactions permit absolutely anonymous transactions, and to what extent can the consequences of absolutely anonymous actions be cushioned by the existing legal framework? We will address these questions first from the perspective of contract law and then in relation to the law of property.

5.1 Absolute anonymity under contract law

Does contract law permits anonymous electronic contracts? To answer this question we must take a separate look at their formation and implementation. Given our interest in the need for new rules governing electronic legal transactions, we will concentrate on bilateral, absolutely anonymous contracts because the protection of vulnerable parties will probably be first to give rise to new legal rules for digital anonymity.

Absolutely anonymous electronic contracts

The key principle of our contract law is that contracts can in principle be entered into without prescribed form: 'unless stipulated to the contrary, declarations, including notifications, can be given in any form and can be incorporated in one or more treaties', reads article 3:37, paragraph 1, of the Dutch Civil Code. Unless opposed by imperative law, the parties are free to incorporate in the contract the obligation that their mutual identity is laid down. But the key principle is that the parties themselves determine the method used to declare their intent. This could therefore be an absolutely

anonymous one. This makes absolutely anonymous electronic legal transactions possible.

There are, however, limitations:

- First, formal requirements can bar legally valid anonymous contracts. The law contains mandatory formal requirements only in specific cases. Legal transactions that are not performed in compliance with mandatory formal requirements are in principle null and void (article 3:39 of the Dutch Civil Code). The parties cannot deviate from them by agreement. Underlying these mandatory formal requirements can be the protection of a weaker party (e.g. against excessive haste or the ascendancy of the other party) or the promotion of legal certainty. We have established that - for the time being - the true identity of the parties is not laid down as a formal requirement with a nullity sanction anywhere in contract law;
- Recognition proves to be important in various situations to the applicability of certain stipulations of the Dutch Civil Code. Examples include the limits set by the Civil Code regarding the contractual freedom of action of parties when one of the parties is a consumer. In article 6:236 of the Dutch Civil Code, certain stipulations in contracts with consumers are deemed to be unreasonably onerous, to which nullity is attached as a sanction (the 'blacklist'). The criterion is that the seller acts in the pursuit of a profession or business and the buyer is a natural person who is not acting in the pursuit of a profession or company (article 7:5, paragraph 1, Dutch Civil Code). This assumes knowledge of the capacity of the parties to the contract, for example whether a person enters into a contract as a consumer. If a person acts in his own name, the capacity of that party to the contract is usually known. However, also if a person acts using a pseudonym, the capacity of the anonymous party could in itself be clear without his identity having to be known. In that case the anonymous contract is in fact formed in a legally valid manner;
- Sometimes, knowing a person s identity can be of relevance to determine the relevance of a certain legal provision and therefore there can be no question of a person s total anonymity. The circumstance that a person acts anonymously can be a relevant factor in determining whether or not a contracting party could trust there to be valid offer to enter into an agreement. In this respect, attention should be given to the measures which can be anticipated by the contracting parties in order to prevent other parties from entering into agreements under false pretences. According to a ruling of the Dutch Supreme Court (Baris/Riezenkamp)[15] the boundaries of contractual freedom are among others determined by certain circumstances under which the negotiations by both parties: the parties are bound by trust and their legal relationships is determined by the justifiable interests of both parties. This could mean that under certain circumstances, contractual parties are obliged to disclose their identity or at least disclose their identity to a certain degree;
- The copyright system is another example of the legal implications which are involved in anonymity. For example, if a completely anonymous written document is distributed on the Internet, it is understood that everyone is in principle entitled to use this work. However, one cannot presume that this work is completely free legally because the author cannot be traced.

Dutch legislation, case law[16] and legal doctrine[17] othewise barely address the nature and the status of (absolute) anonymity under private law. This can be taken to mean that the question of whether absolutely anonymous contracts are legally valid can be answered affirmatively unless the content of an anonymous contractual obligation is not sufficiently determined, or mandatory legal provisions require to indicate the contracting parties with at least an pseudonym that can be traced back to the right person on penalty of the contract being declared null and void.

Problems concerning the implementation of an absolutely anonymous contract

In the absence of knowledge about the identity of the persons acting, legal problems can arise. The summary given below is not intended to be complete, but to give an impression of the multiplicity of legal consequences of absolute anonymity.

- First, formal requirements can give rise to implementation problems if a legally valid anonymous contract is formed. In certain cases the law prescribes formal requirements that can give retrospective grounds for nullifying the contract, or which place a party in a weaker position in terms of evidence if not met retrospectively. If it proves impossible to establish the identity of the other party owing to the lack of traces, the party affected is left picking up the pieces.
- Legal transactions performed by a party that is not competent to perform them are null and void or can be nullified. If, for example, a legal representative of a person not competent to perform a legal transaction wishes to nullify the contract, the identity of both parties will have to be known in order to demonstrate the minority or placing under guardianship of the person concerned in order to reverse the transaction. A creditor lodging a claim for damages will be left empty-handed if he is unable to establish the identity of the other party.
- Problems also arise in cases of late compliance, for which a notice of default is required. A requirement for a claim for damages is that the debtor is given notice of default. Article 6:82, paragraph 1, of the Dutch Civil Code stipulates that the default of a debtor comes into force if the debtor is held in default by a written notification.
- Article 6:237 of the Dutch Civil Code provides an overview of the stipulations in contracts with consumers that are legally suspected of being unreasonably onerous without the nullity of the contract being attached as a sanction (the 'grey list'). Contracts can in these cases be retrospectively nullified if the consumer makes a claim to that effect. In this case the other party could have known that the contracting party was acting in the capacity of a consumer. This is less clear if the consumer was anonymous to him. Moreover, the consumer must drop his anonymity as soon as he decides to appeal for nullification of the contract.
- The level of the parties' expertise is a relevant factor in assessing the liability of the parties and the duty of care arising from this. The rationale of a stipulation of this nature is jeopardized if the type of contracting party concerned is no longer clear.
- In the case of non-compliance, legal remedies such as the right of recovery (article 7:39 of the Dutch Civil Code)

and the ability to have a legal transaction nullified make it desirable that the identity of the non-complying party is known.

The summary given above shows that knowing the identity of the parties is not as such a legal condition for an obligatory contract under Dutch private law, but that its absence does limit the possibility of a legally valid anonymous contract, while the absence of knowledge about the identity and capacity of the parties results in problems in the implementation of the contract.

5.2 Absolute anonymity under the law of property

In the law of property we find a different situation. Under this law, the legislator invariably demands that the identity of the parties be known. After all, an entry in a register is a precondition for a large number of transactions under property law. Recognition is essential, not least for the protection of third parties. Article 3:260, paragraph 3, of the Dutch Civil Code, for instance, states that authority for granting a mortgage must be given by notarial deed. Put simply, in cases in which the law prescribes that a certain legal transaction must be performed by way of a notarial deed, the identity of the party or parties involved will have to be known in order to implement the rules for deeds of this nature, and knowledge of the identity of the parties will be a requirement with nullification as a legal consequence. Article 39, paragraph 1, of the Notaries Act of 1999 contains a statutory obligation for the civil-law notary to establish the true identity of the parties involved; paragraph 5 states that non-compliance with this obligation will result in the deed lacking authenticity and that he envisaged legal consequences will not be brought about.

In addition to prescribing the notarial deed, the Dutch Civil Code also requires that notification be made to certain parties. To give an example, for a legally valid transfer of a registered claim the law requires - in addition to the deed - that the debtor is notified of the transfer (article 3:94, paragraph 1, of the Dutch Civil Code). Put simply, absolute anonymity will not be possible in cases in which the law requires a mandatory notification to a certain party for a certain legal transaction being valid under Dutch property law. Therefore, absolutely anonymous contracts are not possible under Dutch property law.

6. SEMI-ANONYMITY

We explained before that anonymity is a question of degree: in addition to absolute anonymity there are also forms of semi-anonymity. In section 4 we noted that in virtually all cases where people speak of anonymity, what they really mean is semi-anonymity. After all, for certain bodies or intermediaries the electronic legal transactions can still be verified if necessitated by the law or by court order. When remitting payment with a chip card, the consumer, for instance, remains anonymous to the shopkeeper, but the bank that issued the bank card can trace that consumer in its administrative records if fraud relating to his chip card is committed. This is an example of organized semi-anonymity.

In this section we address the space provided by private law (contract law and property law) for semi-anonymity and its consequences. For the sake of simplicity, we will take as our starting point organized semi-anonymity, in which use is made of a pseudonym issued by a third party (such as a bank card or an IP address on the Internet). At least one body (the bank or the Internet Service Provider) is able to establish the identity of the user if necessitated by the law or the court.

6.1 Semi-anonymity under contract law

For contract law we will once again examine the bilateral electronic legal transaction, first from the perspective of the space provided by law for the legally valid formation of semi-anonymous contracts, followed by a discussion of the problems that can be caused by semi-anonymity regarding their implementation.

Semi-anonymous contracts

We explained in paragraph 5 that the Dutch Civil Code does in principle offer limited space for absolutely anonymous electronic contracts. We can extend this observation to electronic contracts on a semi-anonymous basis. On the grounds of the principle of freedom of action regarding contracts, parties are free to enter into a contract semi-anonymously, and an act of this nature can in principle result in the envisaged legal consequences:

- The Copyright Act is the best-known legal provision that allows the use of a pseudonym, but also limits the scope of the copyright as a result of its use. Article 25, paragraph 1, subsection b of the Copyright Act recognizes the right to semi-anonymity in the sense that the author can oppose the disclosure of his name if he has published the work under a pseudonym. But article 38, paragraph 1 of the Copyright Act limits the copyright to a term of 70 years from the first publication because the time of death of an unknown author cannot be established without breaching his semi-anonymity. An author working under a pseudonym can maintain the copyright on his work in accordance with article 9 of the Copyright Act via a third party such as publisher, who will usually know the author's real name but is not permitted to disclose it unless ordered to do so by the law or the court;
- In article 6:236 of the Dutch Civil Code certain stipulations in contracts with consumers are considered to be unreasonably onerous with nullity attached to them as a sanction (the 'blacklist'). This presupposes knowledge of the capacity of consumer. If a person acts under a pseudonym, the capacity of a semi-anonymous party could in itself be clear without anyone needing to know his identity. In that case, the semi-anonymous contract is legally formed, but otherwise it is not;
- Knowledge about the true identity of a certain person may also be of importance in other situations relevant under the Dutch Civil Code. Mention must be made at this point of the measures parties are expected to take in order to prevent that their contracting partner enters into the agreement while not being aware of all circumstances relevant to the agreement. The Dutch Supreme Court ruled in the already mentioned ruling Baris/Riezenkamp that the freedom of contract of a party may be limited due to the fact that this party has to take notice of the reasonable expectations of his contracting partner. [18] This

could lead to situations where it is expected from a party that they reveal his true identity;
- Under certain circumstances, the Dutch law works with formal requirements which cannot be set aside by the parties involved. Nullity is attached to them as a sanction. In case an individual acts under a pseudonym, he can, in principle, conform to these requirements provided that the semi-anonymity does not interfere with the formal requirement. Hence, a semi-anonymous written and signed employment contract for example is valid, provided the true identity can be traced if necessitated by law or court order.

As we mentioned before with regard to absolute anonymity, Dutch legislation, case law and legal doctrine barely address the nature and the status of a pseudonym. This can be taken to mean that the question of whether contracts under a pseudonym are legally valid under Dutch private law can again be answered affirmatively in situations where the use of a pseudonym is not contrary to mandatory legal provisions that require to use the contracting parties' true names on penalty of the contract being declared null and void.

Problems concerning the implementation of the semi-anonymous contract

An electronic contract under a pseudonym is in principle valid or subject to nullity in the same way as if the contract had been entered into with knowledge of the identity of the parties to the contract. The intent or knowledge of the acting parties is primarily relevant to the validity or the consequences of the semi-anonymous legal transaction. Also important here is the role of the pseudonym in the formation of and in relation to the content of the semi-anonymous contract. If problems arise concerning the implementation of the semi-anonymous contract, the usual questions regarding intent and good faith are invoked:
- A supplier who knowingly takes the risk of entering into a contract with a semi-anonymous party bears the risk of the adverse consequences of a shortcoming. If it actually proves impossible to establish the identity of the consumer, the supplier will face the same situation as he would in the physical world: he will receive neither what the consumer was obliged to provide, nor any compensation for damages;
- If it is not possible for the supplier to know the capacity under which the other party is acting (e.g. as a consumer) we feel that these consequences should in principle be attributed to the semi-anonymous party. If a consumer acting under a pseudonym fails to clearly indicate the capacity in which he is acting, he cannot later claim nullification of a stipulation from the grey list or reversal of the burden of proof in relation to it;
- Organized semi-anonymity also calls to the stage a third party, the issuer of the pseudonym using which a semi-anonymous legal transaction is subsequently made. The consumer that uses the services of an intermediary to obtain a pseudonym so that he can conduct semi-anonymous transactions on the Internet will generally enter into a contract with that intermediary, in which the various rights and obligations will invariably be laid down in the general terms and conditions. Can this third party be held liable for shortcomings in the semi-anonymous contract? A glance at the guarantee and exoneration clauses that are presently operated by operational anonymization services shows that they make ample use of the ability to limit their liability.[19] It is also important that the exoneration clause operated by the intermediary is not only effective against his opposing party - in this case the semi-anonymous consumer - but can also be invoked against others under certain circumstances on the grounds of the tenet of third party effect;
- If anonymization services are offered in combination with a certificate (e.g. for anonymous Internet payments), the liability position of the suppliers of these services will in the near future be fleshed out further by the European Directive on Electronic Signatures.[20] Article 6 of this Directive states that a certification service provider that offers qualified services to the public is liable for losses suffered by persons if those persons reasonably placed their faith in the certificates issued by the certification service provider. An exception is made to this liability if the certification service provider can demonstrate that the person in question acted negligently. An example of a situation in which the certification service provider is deemed liable is one in which the service provider fails to register the withdrawal of a qualified certificate and in which others wrongly place their faith in the certificate in question.

Our conclusion regarding absolute anonymity therefore applies mutatis mutandis to semi-anonymity. Knowledge of the identity of the parties is not as such a legal requirement for the formation of an obligatory contract under Dutch law, but its absence does limit the space for a legally valid semi-anonymous contract, while the lack of knowledge about the identity and capacity of the parties results in problems in the implementation of the contract.

6.2 Semi-anonymity under property law

As discussed in paragraph 5.2, absolute anonymity is not possible under property law. The provisions of the Notaries Act of 1999 referred to in that paragraph also rule out semi-anonymous contracts.

Therefore, we conclude that valid semi-anonymous contracts are not possible under the Dutch property law.

7. ARE NEW LEGAL STRUCTURES DESIRABLE?

In this paragraph we examine the role that the law should play in our legal culture if digital anonymity dislocates vulnerable legal relationships. In this context we will also take account of how legal cultures adopt a different approach to tackling anonymous legal transactions.

7.1 Prevention or cure

In the scenario of strong international legal and administrative dependence described in section 2, by the year 2010 the Netherlands occupies a subordinate position among a large number of international legal communities and interest groups, in which the role of the European Union remains limited owing to mutual discord. Because electronic legal transactions have a

border-transgressing character, there is in that scenario little space for autonomous policy in relation to the development of law for digital anonymity. To be able to operate effectively in the future under those circumstances, new legal rules for digital anonymity will preferably have to be given an international character.

The question of which new legal rules for digital anonymity are desirable therefore depends also on differences in legal cultures. For our exploratory study, it is especially important that in our legal culture the law primarily sets out to work preventatively by precluding certain problems from arising. On the other hand, other legal cultures, such as that in the United States, prefer to reduce risks by spreading their consequences over a large group of people. In keeping with the extent to which more importance is attached to preventing losses as a result of digital anonymity than to spreading them, disproportionate risks will sooner have to lead to new rules for the protection of weaker parties. The role that the law in Dutch legal culture will have to play in an information society without geographical borders cannot easily be determined.[21]

Only the future will reveal whether sufficient space for policy-making remains available to the Dutch legislature wishing to tackle anonymity by enabling domestic law to retain its characteristic preventative character by limiting the possible use of anonymity and putting in place facilities that guarantee traceability. With a view to the world-wide dimension of electronic communication, we must also take into account that in the future information society more rather than less room is needed for digital anonymity. Starting points are offered by foreign legal traditions that adopt a different approach to anonymity, such as American regulations which do not require that the identities of parties involved are known. We mention the English regulations regarding agencies which allow for their principals to remain unknown (undisclosed or unidentified). In a system in which relationships are completely separated from people it no longer makes any difference what exactly people intend to achieve by their actions, who they are, what capacity they are acting in or what the precise circumstances are.

Under these conditions anonymous legal transactions are possible. But can systems of this nature simply be incorporated in our Dutch legal system?

7.2 Legislation or self-regulation

In addition to the legal culture, the prevailing views on the function of the law also determine whether the legislature has to take action. After all, it is conceivable that the legislator leaves certain risks 'unregulated' and (for the time being) gives preference to self-regulation by market players. An approach of this nature is in line with the current position of the Dutch government with regard to the approach to ICT-related problems. It is precisely by deploying the self-regulation instrument that the government hopes to offer sufficient flexibility in an era in which technological and social turbulence have the upper hand. Regulation by market players could prove its worth during the period in which the technical developments relating to various forms of anonymous actions have not yet crystallized and there is a need to experiment. Furthermore, it is anticipated that the developing practical situation could provide an onset for the creation of new legal standards in respect of anonymous or semi-anonymous actions.

In the case of (semi) anonymous transactions, self-regulation would initially amount to a contractual solution. As well as the advantage of flexibility touched on above, the contract also provides for a broad range of tailor made solutions. But the other side of the coin is formed by the risk that the interests of the consumer as the weaker party to the contract will be insufficiently addressed in the case of self-regulation. Private law features various remedies that can compensate for the difference in the balance of power between the parties. Familiar remedies include article 6:231-247 of the Dutch Civil Code concerning general terms and conditions and article 6:248 of the Dutch Civil Code concerning the supplementing and limiting effect of fairness and equity. But these remedies only provide for a retrospective correction mechanism. An exception to this is the provision of article 6:240 of the Dutch Civil Code. This stipulation enables interest groups to submit general terms and conditions to the court for testing in abstracto. This is not explicitly laid down for codes of behaviour and private, sector-related enforcement mechanisms that are inherent to properly functioning self-regulation systems.

For the time being, self-regulation is sufficient in the current situation of the low-scale use of semi-anonymous legal transactions. But it remains to be seen whether this will also be the case when it comes to the widespread use of semi-anonymous and even absolutely anonymous legal transactions, using a chip card for example. A situation such as this will lead to greater risks, legal uncertainty and a deterioration of the legal position of the weaker parties involved. A consumer who enters into a contract absolutely anonymously at a distance cannot prove that he was a party to the contract, for instance. An adjustment of the legal framework will also be necessary if the risks to suppliers can no longer be covered by an insurance construction, or if the risk is not worth insuring for financial or business reasons.

7.3 Renovation or building from scratch

For the case in which the adjustment of the legal framework is actually necessary to digital anonymity, we will explore the two methods that are in principle available to the legislature for this purpose:

- the adjustment of existing regulations, such as the legally mandatory use of certain technical facilities to tackle the possible problematic consequences of anonymity (e.g. to strengthen the legal position of the anonymous consumer). Agreements of this nature should preferably be formed at international level. In any event, there is a task here for the European legislature. Recent policy initiatives show that the European Commission attaches great importance to an adequate level of protection for consumers who make use of electronic facilities.[22] Extra consumer protection with a view to disproportionate disadvantages as a consequence of anonymous transactions would be a logical step within this policy. Further agreements with the United States could also possibly be made on the basis of the European standards;
- the introduction of a completely new regulatory framework. Absolutely anonymous transactions could be the main reason for new rules, because they necessitate a concrete system of rights and obligations in depersonalized

legal relationships, for which we may have some starting points under contract law, but under the law of property there are none.

In the light of the border-transgressing character of the problem of digital anonymity, it is desirable to keep an open mind regarding the possible direction in which solutions can be sought based on other legal systems. The choice between renovation or building from scratch is part of the choice between the development of law from existing domestic legal rules or derivation from foreign law:

- Regarding development from domestic law consideration can be given to further extending the legal infrastructure for organized semi-anonymity that we have developed using a wide range of instruments under administrative law (such as compulsory identification, the obligation to give proof of identity and regulations that provide authority to properly verify submitted proof of identity using data that are not available to the public);
- Regarding derivation from foreign law it seems important to ascertain the extent to which other legal systems provide for useful legal structures. Mention should here be made of agency under English law . This can provide a framework for semi-anonymity. Using the agency structure, a contract may be made by an agent where the vendor knows the agent is acting for someone else but the identity of that person is unknown (the unidentified principal). Also, a contract may be made by an agent where the vendor does not know that the agent is acting for anyone else. In other words, as far as the vendor is concerned, his contract is with the agent and no one else (the undisclosed principal). It seems that in the case of a purchase over the Internet, the agent structure provides for a scheme to allow transactions on a semi-anonymous basis, using an intermediary (for example a Trusted Third Party or a Privacy Enhancing Medium - PEM) as an agent. It could thus be a useful weapon against a number of disadvantages of acting absolutely anonymously or spontaneously semi-anonymously, while retaining the envisaged protection of privacy. The risks can be covered by the provision of securities and division of liability under compulsory insurance schemes can thus be made independent of wishes or interests of the parties involved. Framework agreements and standard contracts will be important to regulate which party is liable for specific risks if an absolutely anonymous contract goes wrong, and how claims will be settled in the interest of trustworthy anonymous legal transactions.

In the scenario of increasing global interdependency between nations, it is likely that the various national legislators will all have insufficient margin for development of new legal rules for digital anonymity from their own domestic law. Then derivation from foreign law could provide for feasible solutions.

8. CONCLUSION

In this paragraph we formulate our preliminary response to the question of the extent to which the risks of anonymous electronic legal transactions will in the future necessitate new private law structures, what these structures will probably relate to and the direction in which this development of law could occur.

Our legal culture places prevention above a distribution of incurred losses, so that we anticipate that digital anonymity will be regulated as much as possible rather than compensated for in insurance constructions. In the case of absolutely anonymous and semi-anonymous contracts we have noted that the space for these legal transactions is limited (contract law), or is completely absent (property law). In a nutshell, it can be said that knowledge of a person's identity is not a legal requirement under contract law. Parties that knowingly take the risk of entering into a contract with an absolutely anonymous or semi-anonymous party bear the risk of the adverse consequences of a shortcoming. If the identity of the other party cannot be determined, the party in question will face the same situation as he would in the physical world: he will receive neither what the other party was obliged to provide, nor any compensation for damages. A consequence of this nature is acceptable and its implications are kept within reasonable limits if people only act semi-anonymously to a modest extent. The question remains, however, of whether this will be the case if widespread use is made of the possibility to surf, order and pay absolutely anonymously or spontaneously semi-anonymously in an electronic environment. We feel that widespread anonymous actions are accompanied by so many new risks to the various parties involved that this will lead to imbalances in the legal relationships, which will give the legislator cause to seek solutions to protect vulnerable parties and interests. Cases in point include suppliers demanding full payment in advance in an electronic contract entered into at a distance, stringent exoneration clauses and unfavourable proof stipulations.

With regard to the content of the possible new legal structures, it is likely that in our Dutch legal culture we will first be induced to search for ways of extending existing formal regulations that *limit* the possible use of absolute anonymity. In order to respond to a growing need for anonymity in legal transactions, the regulations for *organized* semi-anonymity could also be extended (e.g. under property law), so that it will be possible to break through a person's anonymity retrospectively if necessitated by court order or by the law. Organized semi-anonymity (or pseudonymity) in legal transactions is therefore a useful weapon against a number of disadvantages of acting absolutely anonymously or spontaneously semi-anonymously, while retaining the envisaged protection of privacy. It is only with the guarantee of this organized protection of a person's true identity without that being abused, that identity fraud can be kept under control and that pseudonyms can provide anonymity towards third parties without damaging the legal order. That is not to say that this form of anonymous legal transaction is easy to organize.[23] Beyond private law, it will require extra regulations under administrative law, such as an extension of the obligation of public and private bodies to check their clients' identity, of the duty of people to provide proof of identity and public-private co-operation in verifying people's identities and in testing the soundness of general and contractual proofs of identity. Apart from political and social issues that will have to be solved in an international context, bringing about the information infrastructure needed for this purpose will also take a lot of time and money. But balancing the interests of protecting privacy and the need for anonymity in the future information society on the one hand, and those of the legal order on the other, makes extending

organized semi-anonymity in our legal culture an attractive course to take for vulnerable transactions.

Because both of the above solution directions under Dutch law will reinforce already existing tendencies towards 'juridification' of our society without internationally achieving the envisaged legal protection under Dutch law, we feel that it is desirable to look into how more space can be created for reliable legal transactions on an absolutely anonymous basis, perhaps under our property law as well. This relates in the first place to absolutely anonymous transactions that are of less social importance and whose disadvantages can easily be insured. It also concerns socially important, vulnerable transactions that already tend to be settled on an absolutely anonymous basis world-wide. By way of making a first move in that direction, we feel that it seems in any event desirable to look into the extent to which already existing foreign legal structures such as the agency are suitable for this purpose, and whether this could be incorporated into legal systems that are not familiar with these structures, such as the Dutch legal system.

At issue here are the trust in anonymous electronic transactions, consumer protection, combating identity fraud and, let us not forget: the issue of legal certainty when border-transgressing anonymous transactions are involved. Given that the development of law takes so much more time than the introduction and distribution of new technology, it is of great importance to gain early insight into the direction in which Dutch law can best develop in response to more digital anonymity. The importance of new concepts and rules for digital anonymity in legal transactions makes it desirable to discuss and perform research into the directions proposed here, paying attention to the effect that derivation from foreign law has on the key principles of private law systems that are not familiar with such directions.

Dr *mr* J.H.A.M. Grijpink is Principal Adviser at the Dutch Ministry of Justice (jgrijpin@best-dep.minjus.nl). **Prof. dr J.E.J. Prins** is Professor of Law and Informatisation at Tilburg University, the Netherlands (J.E.J.Prins@kub.nl).

The authors are highly grateful for the contribution of **Chris Nicoll**, University of Auckland (New Zealand) to section 7.3.

FOOTNOTES

[1] The Dutch version of this article has been published in het Nederlands Tijdschrift voor Burgerlijk Recht [Dutch Journal of Private Law], NTBR 2001-4, Kluwer, Deventer

[2] The court's decision is available at: <http://www.citizen.org/litigation/briefs/dendrite.pdf>.

[3] Available at: <http://www.isaac.cs.berkeley.edu/~iang/thesis.pdf>.

[4] This research programme is an initiative of the Expertise Centre 'Globalization and sustainable development' at Tilburg University. The part of the research discussed here was conducted in collaboration between the Centre for Law, Public Administration and Informatisation at Tilburg University and the Directorate of Strategy Development of the Dutch Ministry of Justice.

[5] An isolated (without personal details) person-related biometric characteristic, from which one can derive that the person acting is the right one, but not precisely who he is. For a more detailed discussion of biometrics, reference is made to: R. van Kralingen, J.E.J. Prins, J.H.A.M. Grijpink, *Het lichaam als sleutel. Juridische beschouwingen over biometrie*, [The body as the key. Legal considerations on biometrics] in: Series IT and Law, section 8, Samson, Alphen aan de Rijn, 1997 and J.H.A.M. Grijpink, Biometrie als anonieme bewaker van uw identiteit, [Biometrics as an anonymous guard of your identity] in: Beveiliging, no. 5, May 1999, Keesing Bedrijfsinformatie BV, Amsterdam, pp. 22 ff.

[6] See: B. van Klink, J.E.J. Prins, W.J. Witteveen, *Het conceptuele tekort* [The conceptual gap], Infodrome, The Hague, autumn 2000 <http://www.infodrome.nl>.

[7] J.H.A.M. Grijpink, Justitiebrede scenario's voor het jaar 2010 [Scenarios for the Ministry of Justice in the year 2010], Ministerie van Justitie, Den Haag, April 1998

[8] See the report of the Scientific Council for Governmental policy 'Staat zonder Land', [State without Country] V 98, Den Haag 1998; the ministerial paper 'Internationalisering en recht in de informatiemaatschappij', [Internationalisation and law in the information society] TK '99-'00, 25880, no. 10, and the comparative study accompanying the ministerial paper into the views of various foreign governments on internationalisation and law B.J. Koops, J.E.J. Prins, H. Hijmans, *Internationalisation and ICT Law*, Kluwer Law International, The Hague/Boston, 2000. See also: <www.minjust.nl/c_actual/rapport/overcrbi.pdf>.

[9] A biometric number is a number that is derived using a formula from a physical characteristic (e.g. a fingerprint, the geometry of a finger or hand, or the characteristic movements when signing a document). A biometric number yields a person-*related* pseudonym. All sorts of other numbers and codes used to verify a person's identity are not person-related. Someone can give a PIN number to somebody else, for example; the electronic signature (code for encrypting data) is computer-related and can be used by another user of that computer. See: R. van Kralingen, J.E.J. Prins, J.H.A.M. Grijpink, *Het lichaam als sleutel. Juridische beschouwingen over biometrie*, [The body as the key. Legal considerations on biometrics] in: Series IT and Law, section 8, Samson, Alphen aan de Rijn, 1997and J.H.A.M. Grijpink, *Biometrie als anonieme bewaker van uw identiteit*, [Biometrics as an anonymous guard of your identity] in: Beveiliging, no. 5, May 1999, Keesing Bedrijfsinformatie BV, Amsterdam, pp. 22 ff., and J.H.A.M. Grijpink, Biometrics and Privacy, in: Computer Law and Security Report, March/April 2001, Elsevier Science Ltd, Oxford, UK.

[10] Verification is generally not sufficient for the application of criminal law. The police are therefore expected to irrevocably establish the identity of a suspect when investigating a criminal offence. If errors are made at this stage, the legal intervention will go wrong further on in the criminal law enforcement chain. After all, it will generally not be possible to rectify a faulty identification retro spectively by means of verification because, for instance, the suspect can no longer be located or because the available data are con tradictory. If the police have made a successful identification at the beginning of the criminal law enforcement chain, other partners in this chain will be able to make do with verifications further on in the legal proceedings.

[11] For examples of the various forms, see: J.E.J. Prins, *What's in a name? De juridische status van een recht op anonimiteit*, in: Privacy & Informatie 2000, [The legal status of a right to anonymity, in: Privacy & Information third volume] no. 5.

[12] For a discussion of this link between privacy protection and anonymity, reference is made to: J.H.A.M. Grijpink, Werken met keten informatisering, [Working with chain computerisation], Sdu Uitgevers, Den Haag, 1999, ISBN 90 5409 226 2, [Section III Privacy and anonymity], pp. 133 ff.

[13] Goods can already be collected at 7-11 shops of this type in Japan.

[14] This subscriber does not necessarily have to be registered under his own name. In practice, the identity of a subscriber is seldom verified, and in the Netherlands an ISP is not authorised to ask for proof of identity other than on a voluntary basis. Neither is he legally or practically able to verify the soundness and validity of a proof of identity because of the lack of authority and informationinfrastructure.

[15] Supreme Court, 15 November 1957, NJ 1958, 67.

[16] See however: HR 24 January 1997, NJ 1997, 339. The Supreme Court ruled that the provisions of article 2:93, paragraph 1 and article 203, paragraph 1 of the Dutch Civil Code concerning the possibility of the ratification by a company limited by shares or a private limited company, after its foundation, of legal transactions that were performed on behalf of the company being founded is applicable mutatis mutandis to other legal persons. See also HR 11 April 1997, NJ 1997, 583. See also the extensive case law on a subpoena for anonymous people that break into and occupy empty houses.

[17] See however: G. Ballon, 'Ik gaf mijzelf geen naam', [I gave myself no name] Tijdschrift voor Privaatrecht, no. 3 1981, pp. 557-592.

[18] See HR (Supreme Court) 15 November 1957, NJ 1998, 67.

[19] See for example: <http://www.anonymizer.com/3.0/services/agreement.shtml> (stipulations 9 and 11) and <http://www.xs4all.nl/freedom/ Freedom_files/content/voorwaarden.html> (stipulation 5.4).

[20] COM (1999) 626 def.

[21] See also the report of the Scientific Council for Government Policy, 'Staat zonder Land', [State without country] V 98, Den Haag 1998; the cabinet paper 'Internationalisering en recht in de informatiemaatschappij', [Internationalisation and law in the information society] TK '99-'00, 25880, nr. 10, and the study into the views of various foreign governments on internationalisation and law that accompanies the cabinet paper: www.minjust.nl/c_actual/rapport/overcrbi.pdf

[22] See the three proposed Directives, published on 12 July 2000, in which the importance of a high level of consumer protection is expressly put forward as a reason for introducing the new rules:

• Proposed Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector – COM(2000) 385;

• Directive on universal service and users' rights relating tot electronic communication networks and services – COM(2000) 392;

• Directive on a common regulatory framework for electronic communications networks and services – COM(2000) 393.

[23] J.H.A.M. Grijpink, *Werken met keteninformatisering* [Working with chain computerisation], Den Haag, p.133 ff. [Privacy and anonymity].

Book Review

Software Contracts

E-licences and Software Contracts – Law, Practice and Precedents, by Robert Bond, 2000, soft-cover, Butterworth, 285 pp., ISBN 0 406 91635 7

This text sets out to provide a overview of the issues relating to negotiating and drafting software licences in the digital age. It also offers an overview of UK law relating to computer contracts. Its rationale is that, as software licensing moves from traditional paper licences through to 'click-wrap' contracts, and as the "concept of licensing object code only is now replaced by open licensing", and as "the new licensing methods of the application service providers come to the fore", so these issues should be addressed and dealt with. The author intends that the work should complement academic works by providing a general explanation of the law whilst at the same time covering in more detail the practical and commercial aspects of computer contract negotiations.

There are five parts to the work, with Part 1 looking at the nature of software licensing and the different types of software licence agreements. Part 2 examines the laws and regulations affecting software contracts, the different types of intellectual property law and an overview of European Union law. Part 3 considers the issues of preparing for negotiations, negotiating principles, and the precautions that need to be considered for negotiations carried out by both suppliers and buyers. Part 4 looks at the issues involved in preparing the draft software licence agreements, the heads of agreements and memorandums of understanding, and a checklist of the contents of a typical software licence agreement. The final chapter in this section lists the key provisions of a licence. Finally, Part 5 explores some of the tactics and techniques of contract negotiation.

The book includes examples of different software agreements, including shrink wrap licences and licensing terms used in E-commerce. There is also a glossary of software of Web definitions, and it also accompanied by a CD-ROM containing the text.

Available from Butterworths, Halsbury House, 35 Chancery Lane, London, WC2A 1EL; Tel: +44 (20) 7400 2500; Internet: <www.butterworths.com>.