Tilburg University

New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity

Grijpink, J.H.A.M.; Prins, J.E.J.

Published in:
Digital Anonymity and the Law. Tensions and Dimensions

Publication date:
2003

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):
Grijpink, J. H. A. M., & Prins, J. E. J. (2003). New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity. In C. Nicoll, J. E. J. Prins, & M. J. M. van Dellen (Eds.), *Digital Anonymity and the Law. Tensions and Dimensions* (pp. 249-269). (Information Technology & Law Series; No. 2). T.M.C. Asser Press.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Chapter 11

NEW RULES FOR ANONYMOUS ELECTRONIC TRANSACTIONS?

AN EXPLORATION OF THE PRIVATE LAW IMPLICATIONS OF DIGITAL ANONYMITY*

Jan Grijpink and Corien Prins

1. BACKGROUND

Anonymous communication on the Internet has by now gained considerable attention. Developments discussed in the various chapters of this book show, for example, that companies are not entitled to learn the identities of “John Doe” defendants who have anonymously posted critical comments on message boards. Ongoing concerns of digital privacy stimulate the debates about possible ways to avoid being “profiled” on the Net and to 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 broader landscape of the legal consequences of anonymity? This chapter sets out the most important conclusions of the first stage of a study into the dimensions of digital anonymity. It is intended to elaborate the problem, to make people aware of the intricacies of the problem and thus to stimulate the debate on useful legal structures for anonymity. In doing so, the chapter focuses on private law, a legal domain that has so far not gained considerable attention in the anonymity discussion. Therefore, this chapter aims to address situations where consumers want to purchase anonymously on the Internet and are confronted with the question: to what extent does civil and consumer law allow anonymous transactions?

* This chapter is based on an earlier article published in *JILT*: J.H.A.M. Grijpink and J.E.J. Prins, ‘New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity’, 2001 (2) *Journal of Information, Law & Technology (JILT)* <<http://elj.warwick.ac.uk/jilt/01-2/grijpink.html>>, and on J.H.A.M. Grijpink and J.E.J. Prins, ‘Digital anonymity on the Internet’, *Computer Law and Security Report*, Vol. 17 No. 6 (2001), pp. 379-388.

The discussion is put in an international perspective. Our 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. Given the present developments, both in the European Union and at an international level, it is to be expected that individual countries' margins for domestic policy-making are likely to diminish to an increasing extent. The current cross-border dimensions of ICT applications demonstrate the erosion of national policy autonomy. This explains why new consumer protection rules and private law dimensions regarding anonymous communication and transaction, need to be considered from an international angle.

However, when discussing the introduction of new rules at the international level, it should not be forgotten that the affected legal cultures of national countries may vary. Also, legal cultures could play a significant role in the possible need to amend rules or to introduce new provisions. For example, certain legal cultures could be characterised more than others by the urge to remove the cause of risks. Other legal cultures prefer to control risks by splitting up the damage over a larger group of people. For example, by the provision of insurance schemes against excessive damage from anonymous transactions. 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 sharing it out, disproportionate risks must sooner lead to extra protection for weaker parties and, therefore, to new rules.

Although this chapter addresses private law implications of anonymous transactions from an international perspective, the Dutch legal system serves as a provocative illustration. The Dutch legal culture has a strong preference for prevention which contrasts nicely with the claim and insurance-oriented Anglo-American legal cultures.

This chapter proceeds with paragraph 2 on dimensions of anonymity. Anonymity is a concept that is subject to multiple interpretations. The key questions regarding digital anonymity are only worth addressing if absolutely anonymous electronic legal transactions are technically feasible and practically significant. We will set forth that case in paragraph 3. Paragraph 4 outlines the status of an absolutely anonymous contract under contract law and property law. This provides an idea of the leeway that current private law regimes offer for anonymous legal transactions. This is a good starting point for answering the question whether such regimes will be adequate when it comes to widespread anonymous transactions. In paragraph 5 we look in the same way into the legal status of less absolute forms of anonymity in legal transactions (semi-anonymity). To answer the next question concerning the desired legal development, in paragraph 6, we assess the role the law has to play if anonymous electronic legal transactions threaten to dislocate vulnerable legal relationships. We will then examine two alternatives for the development of new law: based on national law (in this chapter: Dutch law) or derived from foreign law. These considerations lead in par-

graph 7 to conclusions regarding the extent to which the risks of anonymous electronic legal transactions will in the future require the introduction of new legal rules in Dutch law.

2. 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 discover 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 in evaluating the legal implications. For this purpose we make a distinction between:

1. Absolutely anonymous legal transactions. Here, whether or not a self-chosen pseudonym is used, no traces are left that make it possible to establish identity.
2. Spontaneous, semi-anonymous legal transactions. Here, whether or not a self-chosen pseudonym is used, there are some traces that make it possible to establish identity.
3. Organized, semi-anonymous legal transactions. Here, a pseudonym is used that is issued by a third party who knows the identity of the user.
4. Spontaneous, personalized transactions. Here unverified or unverifiable identifying personal details are used.
5. Organized, personalized transactions. Here identifying personal details accurately verified by an authorized third party are used.

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.¹ 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 a 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 questions 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.² 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.

¹ 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 and 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*, No. 8, Samson, Alphen aan den Rijn, 1997; 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.

² 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 retrospectively by means of verification because, for instance, the suspect can no longer be located or because the available data are contradictory. 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.

The outer extreme of the classification described *above* is therefore formed by absolute anonymity. When acting absolutely anonymously it is not possible to trace a legal transaction back 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 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.³ We will argue underneath that organized semi-anonymous communications and transactions, for example by using an independent third party, may solve various of the present problems and dilemmas raised in balancing such interests as the need for law enforcement agencies to trace the authors of criminal deeds, on the one hand, and the freedom of communication and privacy of Internet users, on the other. Also, organized semi-anonymous communication could be an option in balancing interests between parties that transact by means of anonymous electronic communication.

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

³ 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.

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.

3. THE TECHNICAL FEASIBILITY AND 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 concerned whether those processing personal details are complying with the privacy laws. Therefore, privacy is being protected by, amongst other things, anonymity.⁴ 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.

The final reason why people want to transact anonymously is because they are involved in criminal activity or tax evasion and do not want to leave a trail of their dealings.

Having thus explained the social significance 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 deposit cash in order to load the card with the value of that cash amount. The cash goes to a float account (e.g., Interpay). Once A has

⁴ For a discussion of this link between privacy protection and anonymity, reference is made to J.H.A.M. Grijpink, 'Chain-computerisation for better privacy protection', in *Information Infrastructure and Policy* 6 (1997-1999), IOS Press Amsterdam. This article is based on J.H.A.M. Grijpink, *Werken met keteninformatisering* [Working with chain-computerisation], Sdu Uitgevers, The Hague, 1999 [Section III Privacy and anonymity], pp. 133 ff.

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's 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 feasible. The conditions are: (a) an anonymous chip card that people can use to remit payment and (b) public terminals at which the cards can be charged or used to remit payment without their numbers being registered.

A further example to illustrate the technical feasibility of anonymous digital communication is the Internet café. One can purchase a certain amount of on-line time – e.g., in an Internet café or a public library – and anonymously get an e-mail address. If the user buys 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.⁵ The person concerned remains anonymous, and receives the purchased goods if he produces 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 cardholder is the same person as the one from whose account the amount must be deducted, and then executes the payment transaction. Provided the Internet Service Provider (ISP) is able to establish the true identity of the subscriber in question, this category of semi-anonymity also includes the ability to surf, send and receive e-mails and to chat on the Internet – all the time using a pseudonym. But the subscriber does not necessarily have to be registered under his own name. In practice, the identity of a subscriber is seldom verified. In the Netherlands an ISP may not ask for proof of identity other than on a voluntary basis. Neither is he legally or practically able to verify the validity of information he has been given on a voluntary basis because he lacks legal authority and is obstructed by the nature of the technical infrastructure.

4. 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

⁵ Goods can already be collected at 7-11 shops of this type in Japan.

means whatsoever, even via a pseudonym. Hence, 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 50 euro-cents 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 deprive the contract of its legal force: this agreement results in a legally binding contract. Problems tend only to arise if the subject of the sale 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? 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. 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.

4.1 Absolute anonymity under contract law

Does contract law permit 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 the first motivating factor in the formulation of new legal rules for digital anonymity.

4.1.1 *The Formation of an Absolutely Anonymous Electronic Contract*

The key principle of our contract law is that contracts can in principle be entered into without a prescribed form as Article 3:37, paragraph 1, of the Dutch Civil Code provides: “unless stipulated to the contrary, declarations, including notifications, can be given in any form and can be incorporated in one or more treaties”. 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 done with absolute anonymity and, hence, makes possible absolutely anonymous, electronic legal transactions.

There are, however, some 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 Dutch Civil Code). The parties cannot deviate from them by agreement. Justifying these mandatory formal requirements are the protection of a weaker party (e.g., against excessive haste or the ascendancy of the other party) and the promotion of legal certainty. Apart from these specific cases, the true identity of the parties is not laid down as a formal requirement, bearing a nullity sanction, anywhere else in contract law.
- In the consumer field it is important to be able to identify the capacity of the parties to a contract. By virtue of Article 6:236 of the Dutch Civil Code, certain stipulations in contracts with consumers are deemed to be unreasonably onerous and nullity is attached as a sanction (the “blacklist”).
- The criterion is that the seller acts in pursuit of a profession or business and the buyer is a natural person who is not acting in pursuit of a profession or is not a 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 is usually known. However, even where a person acts using a pseudonym, his capacity may still be clear without his identity being disclosed. In such a case the anonymous contract will be valid.
- Sometimes, knowing a person’s identity is necessary 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*)⁶ the boundaries of contractual freedom are, among other things, determined by certain circumstances under which both parties negotiate: the parties are bound by trust and their legal relationship is determined by the justifiable interests of both parties. This could mean that under certain circumstances, the contracting parties are obliged to disclose their identity or at least to disclose their identity to a certain degree.

- Copyright law is another example where anonymity may be relevant. If a completely anonymous document is distributed on the Internet, there may be difficulties in ascertaining the extent to which the work can be freely used because its author cannot be traced.
- Otherwise Dutch legislation, case law⁷ and legal doctrine⁸ barely address the nature and the status of (absolute) anonymity under private law. We can take it from this that the question whether an absolutely anonymous contract is legally valid can be answered affirmatively provided there is certainty as to its terms and, in the specific circumstances adumbrated *above*, there are no mandatory legal provisions which, as a practical matter, require the identification of the contracting parties with, at the very least, a pseudonym which is traceable back to the right person.

4.1.2 *The Implementation of an Absolutely Anonymous Contract*

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

⁶ HR (Supreme Court) 15 November 1957, *NJ* 1958, 67.

⁷ See however HR (Supreme Court) 24 January 1997, *NJ* 1997, 339. The Supreme Court ruled that the provisions of Art. 2:93, para. 1 and Art. 203, para. 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 squatters.

⁸ See however G. Ballon, 'Ik gaf mijzelf geen naam' [I gave myself no name], *Tijdschrift voor Privaatrecht*, No. 3 1981, pp. 557-592.

- 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 request the 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 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.

4.2 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 the 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, 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 to be valid under Dutch property law. Therefore, absolutely anonymous contracts are not possible under Dutch property law.

5. 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 paragraph 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 bankcard can trace that consumer in its administrative records if fraud relating to his chip card has been committed. This is an example of organised semi-anonymity.

In this paragraph 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 organised 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.

5.1 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.

5.1.1 *Semi-anonymous contracts*

We explained *above* 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 a 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 the 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 the circumstances relevant to the agreement. The Dutch Supreme Court ruled in the already mentioned case of *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.⁹ This could lead to situations where it is expected from a party that he reveals his true identity.

- Under certain circumstances, 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 a 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 the contracting parties to use their true names on penalty of the contract being declared null and void.

5.1.2 *Problems concerning the implementation of the semi-anonymous contract*

An electronic contract under a pseudonym is 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 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 adverse consequences. 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 indicate clearly the capacity in which he is acting, he cannot later claim nullification of a stipulation from the grey list or a reversal of the burden of proof in relation to it.

⁹ See HR (Supreme Court) 15 November 1957, *NJ* 1958, 67.

- Organized semi-anonymity can render relevant the acts or omissions of a third party, for example, the issuer of the pseudonym by the use of which a semi-anonymous legal transaction is purportedly made. The consumer who 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.¹⁰ 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.¹¹ 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 can in some cases provide a practical barrier both with respect to the validity of contracts and to their implementation and enforcement.

5.2 Semi-anonymity under property law

As discussed in paragraph 4.2, 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.

¹⁰ 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).

¹¹ COM (1999) 626 def.

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

6. ARE NEW LEGAL STRUCTURES FOR DIGITAL ANONYMITY DESIRABLE?

In this paragraph we examine the role that the law should play in our legal culture if digital anonymity disrupts the existing balance of power in vulnerable legal relationships. In this context we will also take account of how legal cultures adopt a different approach to tackling anonymous legal transactions. Three strategic choices must be made by any legislator to determine whether action should be taken to counterbalance the negative effects of digital anonymity.

6.1 Legal culture: the choice between prevention or damage control

The role that the law in Dutch legal culture will have to play in an information society without geographical borders cannot easily be determined.¹² In the third scenario of strong international legal and administrative dependence described in paragraph 2, in the year 2010 the Netherlands might occupy a subordinate position among a large number of international legal communities and interest groups. The role of the European Union within this scenario remains limited owing to mutual discord between the growing number of Member States. Because electronic legal transactions have a cross-border 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 even under those circumstances, new legal rules for digital anonymity will preferably have to be of an international character.

Thus, the question of which new legal rules for digital anonymity are desirable depends in the first place on differences in legal cultures in our world. For our exploratory study, it is especially important that in the Dutch legal culture the law primarily sets out to work by preventing certain problems from arising. Other legal cultures prefer to try to reduce any risks by damage control and by spreading the consequences over a larger group of people, thus limiting the amount of damage any individual can suffer. In keeping with the extent to which more importance is attached to preventing losses as a result of digital anonymity than to spreading them over a larger group, within the Dutch legal system disproportionate risks will lead to new rules for the protection of weaker parties.

¹² See also the report of the Netherlands Scientific Council for Government Policy (WRR), *Staat zonder Land* [Governments Losing Ground], No. 54, The Hague 1998; the cabinet paper *Internationalisering en recht in de informatiemaatschappij* [Internationalisation and law in the information society] *Kamerstukken II* 1999/2000, 25 880, No. 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>.

Only the future will reveal whether sufficient space for policy-making remains available to the Dutch legislator to tackle anonymity by limiting the possible use of anonymity and putting in place facilities that guarantee traceability, thus enabling domestic law to retain its prevention character. If not, given the global dimension of electronic communication, we must take into account that in the information society of the future there will be more rather than less room 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 be 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 legally matters 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 such conditions anonymous legal transactions are possible. But can legal systems of this nature simply be incorporated in our Dutch law?

6.2 The function of the law: the choice between legislation or self-regulation

In addition to the legal culture, the prevailing views on the function of the law also determine whether the legislator 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 approach of the Dutch government with regard 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 has 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 transactions have not yet crystallized and require more experimentation. Furthermore, developing practice could provide an onset for new legal standards in respect of anonymous or semi-anonymous transactions.

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 on the other side of the coin, there is the risk that self-regulation insufficiently safeguards the interests of the consumer as the weaker party to the contract. 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 effects of the legal concepts of fairness and equity. But these remedies

only provide for a correction mechanism afterwards. An exception to this is the provision of Article 6:240 of the Dutch Civil Code. This enables interest groups to submit in advance general terms and conditions to the court for testing in abstracto. This provision is not explicitly laid down for codes of behaviour and private sector related enforcement mechanisms but may become a necessary part of a fully developed regulatory system.

With current low-scale use, self-regulation provides adequate legal conditions for semi-anonymous legal transactions. But it remains to be seen whether this will remain the appropriate response when the use of semi-anonymous and even absolutely anonymous legal transactions becomes widespread. In this case, we could see greater risks, more legal uncertainty and a clear deterioration of the legal position of the weaker parties involved. For instance, a consumer who takes part in an absolutely anonymous contract without the parties being present will not be able to prove afterwards that he was a party to the contract. An adjustment of the legal framework will also be necessary if the suppliers' risks can no longer be insured.

6.3 Developing new rules: the choice between renovation or building from scratch

If adjustment of the legal framework is necessary with regard to digital anonymity, there are two methods available to the legislator:

First, existing regulations could be amended. This could involve the mandatory use of certain technical facilities to tackle the possible problematic consequences of anonymity, particularly with a view to strengthening the legal position of the anonymous consumer. This form of adjustment is better done at the international level – in the European context by the European legislator. 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. Extra consumer protection against disproportionate risks of anonymous transactions would be a logical step within this policy. Further agreements with the United States could be made at the European level.

Meanwhile, development of Dutch domestic law could consist of further extending the legal infrastructure for organised semi-anonymity that we have developed using a wide range of instruments under administrative law (such as compulsory identification, the obligation to provide proof of identity and regulations that provide authority properly to verify submitted proof of identity using data that are not available to the public).

Secondly, a completely new regulatory framework could be constructed. The challenges posed by absolutely anonymous transactions are likely to be the main motivation for new rules. This is because they necessitate a concrete system of

rights and obligations in depersonalized legal relationships. We observe some beginnings of this in contract law although not under the law of property.

In this light it is important to ascertain the extent to which other legal systems provide for useful legal structures to regulate (digital) anonymity. 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 remains unknown (the unidentified principal). Also, a contract may be made by an agent even without the vendor knowing 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 absolutely anonymous or spontaneously semi-anonymous transactions, while retaining the envisaged protection of privacy. The risks can be covered by collaterals and insurance schemes and thus be made independent of the parties directly 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 reliable anonymous legal transactions.

In the light of the global character of the problem of digital anonymity, it is desirable to keep an open mind to solutions developed within other legal systems. In the scenario of increasing global interdependency between nations, it is likely that the various national legislators will all have insufficient margin for the development of new legal rules for digital anonymity from their own domestic law. For as long as truly international solutions are unavailable, domestic solutions derived from foreign law will need to suffice.

7. CONCLUSION

In this section we formulate our preliminary conclusion. The questions were:

- (a) Will the risks of anonymous electronic legal transactions in the future necessitate new private law structures?
- (b) What form are these structures likely to take? and
- (c) What direction is the law concerning digital anonymity likely to take in the future?

In our Dutch legal culture prevention of the causes of loss takes priority over the distribution of damage and risk after the event. Consequently, we expect that this policy will be carried through into the area of digital anonymity resulting in close regulation to prevent risks materialising in the first place. We have noted that in Dutch law the space for absolutely anonymous and semi-anonymous contracts 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 any adverse consequences. 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. These consequences are acceptable provided people act semi-anonymously only to a modest extent. 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 remains to be seen. We think that widespread anonymous transactions 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 organised semi-anonymity could also be extended (e.g., under property law), so that it will be possible to break through a person's anonymity afterwards if necessitated by a court order or by the law. Organised 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 organised 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 organise.¹³

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

¹³ J.H.A.M. Grijpink, *Werken met keteninformatisering* [Working with chain-computerisation], pp. 133 ff.

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 proof 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 great deal 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 organised 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 worldwide. By way of making a first move in that direction, we feel it is desirable to look into the extent to which already existing foreign legal structures such as 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 is trust in anonymous electronic transactions, consumer protection, combating identity fraud and, let us not forget, the issue of legal certainty when cross-border 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 an 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 conduct research into the directions proposed here, paying attention to the effect that derivation from foreign law has on the key principles of a private (civil) law system.