W.H. van Boom, J.H.M. van Erp, Electronic Highways: on the road to liability, in: V. Bekkers e.a. (eds.), Emerging Electronic Highways, Kluwer Law International, the Hague 1996, pp. 153-164

12. ELECTRONIC HIGHWAYS: ON THE ROAD TO LIABILITY

A Case Study of the Internet

W.H. VAN BOOM AND J.H.M. VAN ERP*

1. Introduction

The study of Internet use from a liability perspective would require far more than only the brief analysis we can offer here. For this reason, it will be clear from the outset that this chapter will of necessity be more of an exploring nature than aimed at giving an overview of the law as it stands. Also we found — in part very much to our surprise — that this aspect of Internet use (or more generally, use of computer networks) did not attract the same amount of attention as liability questions do when it comes to, e.g., products liability. That is why the following thoughts are merely offered as a possible basis for further study. We will try to trace possible liability questions and at the same time attempt to develop an approach by which these questions can be dealt with in view of the specific nature of a worldwide information flow, which essentially the Internet is.[1]

A further preliminary remark concerns the sources of liability which will be discussed. From a private law perspective, liability can arise on several grounds: contract, tort (delict) and quasi-contract or quasi-tort. We will limit ourselves to contract and tort as possible liability sources, although it cannot be excluded that, e.g., a claim might arise on the basis of unjust enrichment.

To the private lawyer, the Internet does not have as much magic as it has for others. He sees it as a global physical network, aimed at information exchange, which is used for both commercial and non-commercial purposes by individuals and legal persons. It is this exchange of information which is the focus of liability questions. What happens if information gets distorted because of physical network failure or if the information was simply incorrect from the outset? Let us give some specific examples to be more concrete and show the almost limitless diversity of possible damages.

---

* Willem van Boom is Assistant Professor of Private Law at Tilburg University. Sjef van Erp is Associate Professor of Private Law and of Anglo-American Law at Tilburg University and during the fall of 1995 Visiting Professor at Cornell University, Ithaca, NY.

1 For an analysis of what the term "information" in this respect means, cf. Westerdijk, R.J.J., *Produktenaansprakelijkheid voor software, Beschouwingen over de aansprakelijkheid voor informatieprodukten*, Kluwer, Deventer, 1995, pp. 17 ff.

V. Bekkers et al. (eds.), Emerging Electronic Highways, 153–164.

- A businessman keeps track of stock-exchange figures on an Internet site. Every now and then he buys and sells stocks, relying on the information provided to him. One day a software failure on the provider's end leads to serious errors in the given data. The businessman however is unaware of the inaccuracies (these are of such a nature that it is not immediately clear that erroneous data are being published) and continues to deal relying on the information. As a result he suffers a substantial loss.
- When a scientist downloads a document from a network, he unknowingly downloads a virus as well. The virus could have been detected by the network, service, or information provider who negligently had not checked for the potential presence of viruses. As a result, the scientist's hard disk is erased: a year's work of research is lost. (We leave aside the question whether this is a case of contributory negligence, if it was normal practice to make backups.)
- An ftp-site contains an electronic booklet on edible mushrooms (complete with pictures). Someone relies on the booklet and prepares for himself mushroom soup. Unfortunately, the booklet is less reliable than expected: the soup turns out to be lethal.[2]
- A discharged computer analyst turns against his former employer and clogs the Internet with rather competitor-sensitive information on the employer's company. A moderator of a certain discussion list does not filter the information, though should have had reason to believe that the information might be harmful. As a result, the company in question loses a substantial market percentage, because of sudden public distrust of its products and services.

Before we can discuss a possible approach to these liability questions, we first have to consider in some more detail what the specific characteristics are of the Internet. This is necessary, as the Internet is a phenomenon which was unthinkable in the period in which classical contract and tort law were developed in the way we now know it, i.e., the end of the 19th century when the Industrial Revolution caused fundamental changes in the structure of western societies. It might very well be that Internet liability does not fit comfortably within our 19th-century concepts, which will then unavoidably force us to begin rethinking those concepts.

What, then, are those specific characteristics of the Internet? First of all, the use of the Internet creates worldwide liability problems, which tend to escape direct regulation by local (in particular, national) law. Information is made available on a network that connects computer systems all over the world. This information might be accessed from any point which gives a user a gateway to the Internet. Once the user is inside the net, it no longer matters whether the information is sought through, let us

2 Vandenberghe, G.P.V., 'European perspectives', in: Sieber, U. (ed.), *Liability for On-line Data Bank Services in the European Community*, Heymann, München, 1992, pp. 401-402.

say, a World Wide Web server in his own country or in a neighboring country, or even in a different continent. One possibility to limit the use of the Internet might be to somehow control the information that is made searchable for Internet users by a particular provider. An example could be the screening of information to detect, e.g., messages or images against the public moral. It is however doubtful whether this can be done in a really effective way. In most countries, more than one Internet provider is active. These providers can operate nationally (e.g., in the United States: America OnLine, CompuServe, and now also Microsoft), but can also operate — with growing frequency — merely on a local basis, limiting themselves to specific local markets (only targeting, e.g., a particular city or county, as can be seen in the United States). This results in a wide range of choices that can be made as to which Internet provider will be selected as a gateway. Simply changing your Internet provider might thus make it not too difficult to circumvent restrictions made by one provider. Furthermore, even if these restrictions were agreed upon on a nationwide basis, there would still be the possibility of an "innocent" WWW site giving links to less "innocent" sites. Given that each day on an average 500 new WWW sites are added to the Internet, it will be extremely difficult to police all the information provided by all sites wherever they are located. And, finally, if national checks and limitations somehow would prove to be effective, there is always the possibility of making a modem connection to an Internet provider abroad. Therefore, blocking access to certain information locally or nationally is ineffective, given the worldwide openness of the system. For the time being, the only really effective way to block information available on the Internet locally or nationally is to block Internet use altogether. We doubt, however, that even this is really possible. From a liability perspective, the globalization of information, with its inherent limitations on the control over information content, raises difficulties which are breathtaking, to say the very least.

Second, Internet use creates relations between an indeterminate number of institutions and people involved, the number of which can be pure accidental. Does one get the information through country A or perhaps also through country B and C, because the quest for information was rerouted for reasons of engaged lines? This aspect of indeterminacy applies to the physical side of the Internet, its software side, and, finally, its information side. E.g., if a file is being requested by ftp and the file contains information errors, this might be caused by physical (line) failure, transmitting software failure (either at the computer which sends, transmits, or receives the file), or might, finally, be caused by mistakes on the part of the information provider. And the latter may, in its turn, have both technical and non-technical causes.

Third, the status of the provider of information as well as the status of the user of the information can be that of a private person (who might or might not be paying for services), a private professional who uses the Internet for his work (again, this might be with or without remuneration for the provider), or an institution (either profit or non-profit). Here also, diversity is a key word.

2. Possible Starting Points for Analysis

Is postmodern chaos finally reaching areas of traditional private law analysis? We doubt it. It shall be clear that as the Internet creates a worldwide information flow, international regulation and supervision are required. National regulation and supervision will be less effective or perhaps even ineffective. The road to agreement on regulation and supervision will most certainly not be a road on which one travels with the speed of the superhighway itself. No doubt, for lawyers from the old and new world, "classical" freedoms (such as freedom of speech, freedom of the press) mean that regulation cannot mean overall censorship. But other countries might disagree and favor strict control over the flow of information. These differences, which are rooted in diverging constitutional provisions and differences in interpretation as to those freedoms, will reflect themselves in private law liability questions.

Given that global regulation (except for some voluntary self-regulation) for the time being is non-existent, first of all a solution has to be found for the problem which national law — if any — is to be applied here. Should one refer to a "lex informatica" and establish a separate set of rules specifically directed at relating Internet liability questions to a particular country or should one apply the current private international law rules on contract and tort? We think that developing a separate conflicts-of-law rule will be just as difficult as drafting global standards for regulation and supervision. For that reason there is no other option than to apply existing private international law.[3]

As to the application of substantive national law, the distinction which is traditionally made between contract and tort law seems to us a helpful tool in analyzing liability questions. We do, however, realize that these concepts are not as absolute as they might seem at first appearance. The boundary between the two areas may differ from one country to another, so what is considered a contractual problem in country A could at the same time be seen as a tort problem in country B. Also, there is a clear trend that contract and tort law show more and more overlap and sometimes are even merging.[4] Still, it can safely be said that a contract is the parties' self-imposed law and as such has a strong binding force.[5] If, e.g., a private customer of an Internet service provider does not get what she was promised and for which she paid, this is without any doubt a breach of contract and entitles her to the payment of damages. The same is true for universities which have a contract with, e.g., a national computer center that is responsible for their inter-university (national and/or worldwide) connections. Private law questions can be solved in this type of case in a fairly easy way, because the

3 Cf. Sieber, U., 'Haftung für Online-Datenbanken', *Computerrecht*, 1992, pp. 521-522.

4 See Erp, J.H.M. van, *Contract als rechtsbetrekking, Een rechtsvergelijkende studie*, Tjeenk Willink, Zwolle, 1990, pp. 15 ff.

5 Cf. Boss, H. and J.B. Ritter, *Electronic Data Interchange Agreements*, ICC, Paris, 1993, p. 10.

number of parties involved will be limited by the fact of the contractual nexus, the amount of possible damages can be established on the basis of the contract (which might include exemption clauses), and the contract most likely will point to one particular legal system (e.g., by an express choice of law clause).

This certainty and predictability is far less obvious in a tort context. Here it is not easy to determine which law will apply, who the relevant parties are and what the amount of damages will be. In fact, it seems that the starting point for legal analysis in this area will prove to be not the parties involved, but the existence of damages. "No damage, no parties" could become the new legal maxim. Thus it appears that the existence, type, and amount of damages will turn into the pivotal issue when it comes to solving Internet tort liability problems. We will further discuss this hypothesis in Section 4. But before we do so, it might be good to briefly analyze which parties can be involved in the worldwide flow of information.

3. Information Flow: Providers and Receivers

3.1. INFORMATION PROVIDERS

As mentioned in the introductory section, at the outset a distinction can be made between (1) the providers of the infrastructure (physical networks) and providers of services (e.g., software for the operation of information services, such as telnet, ftp, and novell software) and (2) the actual providers of information. The following distinctions only relate to the second group: the information providers.

The information providers can be classified in several categories. It may of course happen that these categories overlap and that a particular provider falls into two or even more categories.

Providing information can be done on a commercial and on a non-commercial basis, although — particularly in the world of WWW providers — some providers act in both categories. In the latter case, by giving "free" information they hope to get receivers of information interested in their services to such a degree that they might be willing to pay to obtain more information or other services. An example of a non-commercial provider is universities; commercial providers are, e.g., companies which maintain databases, such as Webcom, Westlaw, and Lexis; mixed providers can be financial institutions, such as banks and firms of accountancy consultants.

A second categorization which can be made is that between those giving information for a limited group of receivers (distribution lists, which in their turn may differ as to the requirements for participation) and those making information available "to the world at large" (publicly accessible databases, such as library catalogues). Limiting the group of receivers can be done in various ways. The list can be open for free subscription or only for previously controlled subscription. Then, it may also happen that, although the

list is limited, the data being sent become accessible to the public when they are stored in databases which can be freely accessed, e.g., through gopher. A further sub-categorization which can be made here is between moderated and non-moderated lists. If a list is moderated it means that the information given is, to a greater or lesser (usually: lesser) extent filtered before it is transmitted to the receivers.

A third categorization can be made between the providers of information at a primary and at a secondary level. The primary level consists of providers who give information that can be used without further accessing other sources. At the secondary level, providers can be found that only guide the receiver to the final (i.e., instantly usable) information. An example of the latter category is navigation services (gopher, archie, WWW).

3.2. INFORMATION RECEIVERS

As to the receivers of information, it seems to us that only one basic distinction can be made. That is between those who look for information on a commercial or a professional basis and those who do not do so (in private law terminology, "consumers"). Still, even this categorization is not without its problems. A receiver of information might be a consumer from the point of view that he is not involved in any commercial activity or acting in any professional capacity, but he may have gained so much experience that it would be questionable to still call this particular person a "consumer". A prime example here is a hacker. For that reason, it might be asked whether the above distinction between (to put it briefly) "professionals" on the one hand and "consumers" on the other hand should not be replaced by a distinction between those with experience ("professionals" and certain "consumers") and those without experience ("true consumers"), when it comes to legal questions in the area of computerized information.

4. Damage and Liability

4.1. THREE KINDS OF DAMAGES

Whenever information that has been released through the Internet turns out to be incorrect or incomplete and as a result someone has suffered damage, the question of liability arises. The problem in locating the actual mistake or hardware failure as well as pinpointing a person to whom these facts can be imputed is one thing. Quite another set of problems comes to mind when we think of the possible range of persons who suffer damage, as well as the type and amount of possible damage. We already offered some illustrations of what might happen in the introductory section.

Damages suffered as a result of incorrect or insufficient information can be divided into three categories: damage to the human body, damage to tangibles, and damage to purely economic interests. This division is classical and widely used. Although we already attempted to make clear that Internet liability questions have some specific characteristics which create liability problems of a very different nature compared to traditional areas of tort law, it seems to us that this division can also be applied to the risks of modern Internet traffic. There is a further classical distinction relating to damages which has to be considered here: intentionally inflicted damage as opposed to negligently inflicted damage. It is at the crossroads of these two distinctions (based on the nature of the damages and the state of mind of the person causing the damage) that further analysis can be done.

The widely accepted rule that whoever causes damage with the intent to harm is held liable[6] definitely applies to damage to the human body as well as to damage to tangibles. As far as negligently caused damage is concerned, in most legal systems the degree of protection through tort law depends on the damaged interest in a given case. Integrity of the human body is usually considered most worthy of protection; the degree of care to be taken whenever the possibility of bodily harm is involved, is set quite high. As a result, information that leads to injury of the body will fairly quickly be considered tortious. It is seen as an act of negligence to provide information with a possible lethal outcome whenever it is reasonably foreseeable that this result will ensue. A somewhat more lenient standard of protection is set for real and personal property.

The very moment a duty of care is assumed to prevent property from being damaged, liability arises whenever this duty is not performed. It is, however, not very clear in which cases this duty arises or should arise within an Internet context. Does an Internet user have the duty to warn others for a virus he knows is attached to a certain ftp file if the file was not placed on the ftp site by the user concerned? The question whether in such a case a duty of care exists is traditionally decided on the basis of the relationship between two persons. Here the specific nature of the Internet becomes an interfering factor in the decision-making process as it is normally used: if there is no particular "other" party that might suffer damage or perhaps has already suffered damage without even knowing it, what procedure should be followed to establish a duty of care? Should this be done in an abstract way (in other words: expect from this user what a reasonable bystander would have done) or does it simply mean that, because of the absence of a concrete relationship, no duty of care can arise?

This question leads to a different problem: can damage to something as intangible as an electronic document be considered damage to property? On this point no

---

6 Cf., e.g., Holmes, O.W., *The Common Law*, Boston, 1881, pp. 6-7; Keeton, W.P. *et al.*, *Prosser and Keeton on Torts*, St. Paul, 1984, pp. 33 ff; Brazier, M., *Street on Torts*, London, 1993, pp. 5-6, p. 24; Markesinis, B.S. and S.F. Deakin, *Tort Law*, Oxford, 1994, pp. 40-41.

unanimity exists. Some would interpret this as damage to a hard disk and thus as damage to property, while others would file this case under pure economic loss.[7]

In any case, two things are beyond dispute. First, damage inflicted with the intent to harm leads to liability. Second, in most cases negligently inflicted damage to the human body also leads to liability. More troublesome is the question how far the protection of purely economic interests reaches or should reach. As so often in law, it depends. Private lawyers through the centuries have been familiar with damage to reputation: actions for libel, slander, e tutti quanti have become very effective instruments for establishing liability and estimating the damage suffered here.[8] Of more recent origin is, e.g., the experience with damage suffered by losing out on a business deal or by closing the wrong deal, in other words, damage to business expectations. There is hardly uniformity in this field: some jurisdictions tend to treat loss suffered without an infringement on bodily rights or property as any other loss; other jurisdictions draw the line right there and in principle do not reimburse pure economic loss.

It is pure economic loss which, for tort lawyers, creates one of the major problem areas and it is exactly pure economic loss which is the most likely form of damages to be suffered in an Internet context. For that reason we will elaborate somewhat on the question whether, and if so to what degree, negligently inflicted pure economic loss should be reimbursed. We will not attempt to give a straightforward answer to this question, as we think that this would be too speculative, given the uncertainties involved. We do, however, feel that some criteria might be formulated, which might be of some help for further reflection upon this subject.

Which, then, could those criteria be? In most legal systems, a court would want to know whether (1) this specific damage was reasonably foreseeable for the information provider (the problem of the foreseeable plaintiff), (2) the receiver of the information had reason to rely on, e.g., the accuracy of the information, (3) a price was paid for access to the information,[9] and (4) there was a significant nexus between provider and receiver. In order to find a liable person it is further necessary to (5) ascertain that the provider could in an economically reasonable manner have prevented the accident from happening. If not, liability will not exist. In the following section we will discuss these criteria in some detail, focusing on (a) the reasonable plaintiff, (b) reliance by the receiver on the information received, and (c) the existence of a duty of care in a more

7 See Fuhrer, S., 'Computerviren und Haftung', *Schweizerische Juristen Zeitung*, 1991, pp. 130 ff.

8 Cf. Loundy, D.J., 'E-Law 2.0: Computer information systems law and system operator liability revisited', at Section V A, obtained from URL ftp://infolib.murdoch.edu.au/pub/subj/law/jnl/e-law/refereed/loundy.txt. See also Kahn, J.R., *Defamation Liability of Computerized Bulletinboard Operators and Problems of Proof*, CHTLJ Comment Computer Law Seminar, Upper Division Writing, February 1989.

9 Cf. Vandenberghe, *op.cit.*, note 2, p. 394.

objective sense: are there any standards to be found to which any user of the Internet should adhere, irrespective of the non-existence of a "counter-party"?

5. Pure Economic Loss and the Internet: Criteria to Be Used

5.1. THE FORESEEABLE PLAINTIFF

The drawback of widespread media like newspapers, television, and, recently, computer networks is that harmful information has an almost unlimited reach: it stretches itself unto every corner of the world. In a sense this makes it impossible to anticipate liability; whenever a provider hurls information into electronic space, he can only anticipate the unexpected to happen. This unforeseeability is — at least to some degree — out of question only when the provider willingly and knowingly provides information intended to hurt or destroy property, reputation, or goodwill.

Let us suppose a moderator is held liable for negligently failing to filter a libellous message sent through a moderated discussion list.[10] The reach of this list is unlimited: the message reached all parts of the globe and damaged the reputation of a worldwide-known and renowned organization. Should the moderator be held liable for all the harm, throughout the whole world, which is done to the reputation? One can indeed say that the damage in question is as such foreseeable for a moderator. The result of unlimited liability for all damage does however not sound appealing. It could possibly frustrate the flourishing of electronic media.

If we were to allow the reach of the causal chain to be infinite, it would be like opening the floodgates for unlimited liability of tortfeasors. Therefore an objective criterion should be formulated in order to contain the financial consequences of torts committed through the Internet. A few classical indicia may prove to be helpful, which leads us to the next criteria to be discussed.

5.2. WAS THE RECEIVER ENTITLED TO RELY UPON THE INFORMATION

If information is incorrect or insufficient, the question is whether the receiver was entitled to rely on the information. If not, there is no ground for liability. Apart from clearly nonsensical information not to be trusted, it is very hard to say that, as a matter of principle, information is generally to be relied upon. In our view, it would depend on a number of circumstances. Was there a direct contractual relationship between

10 See on this subject Schlachter, E., 'Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions', *Hastings Communications and Entertainment Law Journal*, 1994, pp. 87 ff. at Section III A 3.

provider and receiver? Was there a remuneration fixed? Was the information within a public or a private Internet space? What was the standing and reputation of the provider? All these circumstances are in our view relevant. At this point, attention should be given to the fact that contractual relationships tend to give rise to further-reaching justified reliance than non-contractual relationships. The closer the parties have come in their mutual dealings, the more trust and confidence between them will exist.

5.3. WAS THERE A DUTY OF CARE VIS-À-VIS THE RECEIVER

As mentioned before, the distribution of harmful information leads in any case to liability when the provider had the intention to harm the receiver. In all other cases the existence of a duty of care must be proven. Besides the difficulty as to who might be seen as the foreseeable plaintiff, which is of course of great importance in establishing a duty of care, it remains unclear when and to what extent such duties of care presently exist. Does every provider have the duty to moderate distribution lists? Does every provider have the duty to delete unsigned messages or is he allowed to forward them unaltered?

We submit that a comparison can be drawn between the present state of the Internet and the state of the industrial developments in the mid-19th century. As industry gradually developed, liability law was slow in keeping pace with the new types of hazards arising from the growth of industrial activity. It was more or less accepted that in order to stimulate technical evolution and therewith economic advancement, the industrial pioneers had to be given more or less free play. In doing so, industry-related casualties remained as a rule uncompensated. In the 20th century, liability law caught up with the industrial development and started to establish new forms of liability. These new forms provided clear incentives for protection of people involved in industrial activity from bodily injury and infringement of property. Nowadays, liability law has a strong grasp on industrial policy and development.[11]

5.4. SETTING THE STANDARDS

When we compare the development of industrial liability with liability for harmful information in an Internet environment, possibly the lesson to be learned is this. In order to stimulate further creation and growth of a fully matured network which is used worldwide, the standard of care should be set low for the time being. As soon as the Internet has reached a point at which the economic benefits are clearly discernable, one might consider stepping up the pace for liability law. Some basic standards however should apply immediately. The rule that intentionally inflicted damage leads to liability

11 Markesinis and Deakin, *op. cit.*, note 6, pp. 20-22.

is a rule which no doubt will also apply to harm done through the Internet. Very likely the same holds for intentionally inflicted bodily harm. What is uncertain is the great void in the area of liability for pure economic loss. Restraint rather than far-reaching, unlimited liability should be the course to be taken during, probably, the next decade.

5. Concluding Remarks

Traditional legal concepts as contract and tort seem to be useful tools in disentangling complicated liability questions that arise in the context of a worldwide information flow, which, in essence, the Internet is. Of course, the Internet with its physical and data networks creates problems unknown to lawyers some 25 years ago. But those problems are not so new that our "classical" (19th-century) concepts should be completely discarded. We tried to show to what extent those traditional concepts could still be used and where rethinking might be unavoidable.

Contracts have always been the prime source for creating a private order (in other words, self-regulation) and this is true even for new phenomena such as Electronic Data Interchange.[12] It is, however, clear that these contractual frameworks will only function when they are truly international in nature. The main problem here is the impact of rule-giving by national regulators trying to control the Internet. National regulation is on the one hand almost by definition ineffective because of the supranational nature of the net, but it can on the other hand be very compelling the moment problems arise and a national court is called upon to adjudicate, e.g., the validity of a contract. If the information flow is seen as floating around us in the air, the very moment things go wrong and information materializes in a certain place taking the shape of damages, suddenly the reality of local legislation can hit very hard.

If a contractual framework does not exist, or does not cover the case at hand, tort law becomes of foremost importance. From a tort perspective, the Internet is a meeting place for a diverse or (perhaps a better word) obscure group of information providers and a diverse (and obscure) group of information receivers. No nexus beforehand exists. Classical tort concepts, which presume the existence of an identifiable individual tort feasor and an identifiable individual "victim", were not developed for use in such a context which is characterized by involvement of innumerable and anonymous persons. In classical tort law, the nexus which leads to compensation of damages arises when two identifiable parties are being confronted with one another. Only then can questions arise such as: was there a duty of care of one party towards the other to avoid harmful behavior? Was one party's behavior the cause of the damage which the other party claims to have suffered? Modern tort law, on the contrary, shows a clear tendency away

12 See Chapter 11, 'Contracting in an On-line Marketplace'.

from this strictly individualistic view. The tendency towards abandoning the individualistic approach and at the same time focusing on objective criteria for establishing a legally relevant nexus between those who cause damage and those who suffer damage can already be found in the area of, e.g., products liability. A good example is the case of the DES hormone, that caused serious bodily harm to the daughters of women who had used that hormone during pregnancy. Mass production together with mass marketing of the DES hormone by several chemical industries, which led to a large unknown group of users, compelled the Dutch Supreme Court to critically reflect upon the traditional tort concept of causation. The main question was: does a causal connection between one specific "DES daughter" and one specific chemical industry have to be found or can this doctrine under the given circumstances be somewhat relaxed? The Supreme Court decided in favor of the plaintiffs as to the burden of proof of causation. This decision was one of the many changes that enable Dutch tort law to remain lenient enough to survive the problems of mass liability it faces as it enters the 21st century.[13]

By giving some criteria which might be considered relevant, we have tried to suggest in which direction a less strictly individualistic approach might lead where pure economic loss is concerned. In particular, we suggested that the existence and the type of damage should be used as material tracks to find the (group of) persons behind it. What we submit in this respect is therefore the reverse of what can be found in classical tort law. We move from damage suffered to the parties involved, not from the parties involved to the damage suffered.

To conclude, Internet liability questions can be solved in an adequate way through contract and tort law, as long as the supranational character of the Internet and its enormous diversity of providers and receivers are being taken into account. If regulation is considered necessary, it can only be done at an international level. Perhaps the most effective approach for the time being would be self-regulation, as it seems very much the case that only those actively involved in the expansion of the Internet realize both its positive and negative sides. A positive side is the resulting globalization of information and the resulting borderless society.[14] A negative side is that it can be extremely difficult to establish a legal nexus between those who suffer damages because of, e.g., libellous information and those who in the end are responsible for the dissemination of a libellous message. We hope that our explorative analysis may be a good starting point for rethinking liability questions concerning the Internet and, more in general, liability questions that arise through the emerging of electronic highways.

---

13 Dutch Supreme Court (Hoge Raad), October 9, 1992, *Nederlandse Jurisprudentie*, 1994, 535. Other examples are the recently enacted Class Action Act (Dutch Civil Code art. 3: 305a ff.) and strict liability for hazardous substances (Dutch Civil Code art. 6: 175 ff.).

14 This does not of necessity mean that it will also be a lawless society. Cf. Anderson, C., 'The Internet', *The Economist*, July 1, 1995, p. 17.