Contracting for liability limitation

7

Contracting for liability limitation

LUCAS BERGKAMP AND MICHAEL FAURE

It has been suggested[1] that the market for security services does not function well because security providers cannot negotiate and obtain adequate limitation of liability. Due to competition by small firms that are not concerned about their liability exposure, the larger firms are effectively forced to assume full liability under the law for damages caused by their malperformance. In addition, government agencies contract for security services in accordance with the legal provisions governing public procurement, and this process does not accommodate negotiations for limitation of liability of the security provider. Consequently, there could be a market failure as a result of which security firms are effectively forced to accept the complete lack of any liability limitations.

This chapter analyses this issue. The first part discusses practices in other sectors of industry that are exposed to analogous risks of potentially catastrophic damage to determine whether and, if so, to what extent they limit their liability exposure by contract or other risk management mechanisms. In the second part, we turn to risk mitigation strategies that are or could be employed by the economic actors in the security chain or by other operators exposed to terrorism-related risk. We assess the effectiveness of risk mitigation mechanisms in potentially reducing exposure of economic actors in the security chain and other operators to third-party liability. This analysis seeks to determine which of the mechanisms used in other sectors could effectively reduce exposure to liability for terrorism-related risk. To answer this question, the basic structure of the security industry and other relevant industries are compared with the basic structure of the industry sectors discussed in the first part. We attempt to identify potential restrictions on the possibility to contract for liability limitation and pay attention to public procurement for security products and services, which may not accommodate contracting for liability limitation. The last section presents our conclusions.

[1] Bergkamp, Faure, Hinteregger and Philipsen (eds.) 2013, 268.

7.1. Industry practices with respect to limitation of liability

7.1.1. Analysis of three specific sectors

In this section, the use of contractual protections (general terms and conditions, etc.) against unlimited liability vis-à-vis third parties in industry sectors other than the security industry is analysed. Practices in the following three sectors are reviewed:

- software, in particular cybersecurity software;
- pharmaceutical industry; and
- meteorological forecasting.

Risks and practices in each commercial sector will be analysed and presented in accordance with the following structure:

(1) Nature of potential exposure to risks of large-scale damage (including scope and historical exposure).
(2) Current industry practices to limit exposure contractually (liability limitation used in contracts; risk sharing and mutualisation pools; liability capping and exclusion schemes; and availability, prevalence and nature of any insurance contracts used).

The sectors of industry analysed in this chapter are exposed to potentially major liability for damages such as property damage, personal injury, including medical expenses and disability, pain and suffering (in some jurisdictions called "moral damage"), environmental damage and economic losses (also referred to as "lost profits"). In theory, each sector could be exposed to claims for each type of damage. Unsafe, defective or ineffective pharmaceutical products may result in a flood of claims for personal injury, which could lead to medical expenses, loss of income, pain and suffering, etc. Defective or ineffective security software could result in the unavailability of e-commerce websites, resulting in massive loss of income, or it could provide gateways for "hacking" into computer systems for managing critical infrastructure, such as nuclear power plants, which, in turn, could cause a nuclear accident with many casualties, massive property damage, environmental contamination and enormous loss of income. Likewise, incorrect meteorological reports could cause mischief for air, maritime and road traffic and result in accidents, personal injury, property damage, medical expenses and loss of income. Thus, in terms of the potential for exposure to massive liabilities, the pharmaceutical, software and meteorological industry may be in a position similar

to the security industry and other operators exposed to terrorism-related risk. There may be significant differences, however, in terms of the probability of the risk of actual incidents and the risk of incurring liability therefore.

With respect to accidents leading to potential liability exposure, the level of regulation of an industry sector may play a role. Of the sectors analysed in this chapter, the pharmaceutical industry is the most heavily regulated, while the other sectors are regulated to a lesser extent. The level of regulation of the economic actors in the security chain would appear to be somewhere between the pharmaceutical industry and the other sectors, although the security-related industry is such a broad category that the level of regulation very much depends on the specific area. As discussed in Chapter 2, the level of regulation may have a positive or negative influence on liability exposure. Extensive regulation does not necessarily imply reduced liability exposure; regulation may have this effect if it is effective in reducing the actual risk of accidents. Conversely, it is also conceivable that onerous but ineffective regulatory standards could result in increased exposure, where plaintiffs can invoke non-compliance in support of claims based on negligence.

The actual risk of terrorism is a function of many variables, such as the political situation, the attractiveness of a target, the level of protection at the target, the sophistication and specialisation of the terrorists, etc.[2] The level of regulation is not likely to be an independent factor but more likely to reflect the actual or perceived risk of terrorism. If, in deciding where and when to attack, terrorists conduct a rational cost-benefit analysis, their decisions would be predictable. Past experience has shown that attacks targeting means of transportation (airlines, subways, etc.) are fairly common and tend to occur in large metropolitan centres (e.g., capital cities). Cyber-attacks, on the other hand, do not appear to have resulted in the kind of damage at which terrorists aim. Due to this and other factors, actual risk levels differ substantially from one sector to another.

Whether companies in a particular sector are able to negotiate contractual liability limitations and indemnification obligations is a function of the structure of the market, the main types of customers, their bargaining power, customs and other factors. There may be substantial differences between sectors of industry and between individual companies in this regard. For instance, small companies providing security services may

[2] Ibid., 189.

be willing to accept large liability exposure; large public entities that are purchasing security goods or services may be in a position to reject any limitation of liability, etc. The applicable law may also restrict the use of liability limitation; for example, the Unfair Contract Terms Directive[3] does not permit blanket liability limitations that unfairly bias contracts against consumers. While an exhaustive assessment of these factors is beyond the scope of this book, some observations on these issues are made in passing.

7.1.2. Industry practices in other sectors

The actual liability exposure of companies in different sectors of industry varies due to factors such as the nature of their activities, the physical risk associated with such activities and, secondarily, the law and regulations applying to their activities, including the rules on liability. Another relevant factor is industry practice with respect to risk management. The relevance of these practices to operators and security providers exposed to terrorism-related risk is considered below. One of the primary considerations in attempting to draw useful parallels is the extent to which the mechanisms employed by the sectors of industry surveyed can be said to effectively limit liability within these sectors (i.e. software, pharmaceutical and meteorological industries).

To limit or exclude liability, the software industry has deployed contractual clauses set forth in an "End User Licensing Agreements" (EULA), also called "clickwrap agreements". These clauses effectively limit liability exposure and deter claims, but they are not enforceable in the European Union to the extent that they seek to limit consumers' choice of forum or court,[4] nor to the extent to which they seek to impose a limitation on liability for personal injury or death and any incidental or consequential damages arising therefrom under the Unfair Contract Terms Directive.[5] The Unfair Contract Terms Directive provides that "[a] contractual term which has not been individually negotiated shall be regarded as unfair if,

[3] Council Directive 93/13/EEC on unfair terms in consumer contracts [1993], OJ L095/29, (Unfair Contract Terms Directive).

[4] Ibid., Article 6 states: "Member States shall take the necessary measures to ensure that the consumer does not lose protection granted by this Directive by virtue of the choice of the law of a non-Member country as the law applicable to the contract if the latter has a close connection with the territory of a Member State."

[5] Ibid., Annex, sections 1(a) and (b).

contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer."[6]

Clickwrap agreements fall within the ambit of "not individually negotiated agreements", a term used in the following provision of the Unfair Contract Terms Directive: "A term shall always be regarded as not individually negotiated where it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, particularly in the context of pre-formulated standard contracts."[7] The Directive requires that such contracts do not contain terms that are "unfair" to the consumer. An illustrative list of terms considered unfair[8] includes those terms which have the object or effect of:

– excluding or limiting the legal liability of a seller or supplier in the event of the death of a consumer or personal injury to the latter resulting from an act or omission of that seller or supplier; . . .
– excluding or hindering the consumer's right to take legal action or exercise any other legal remedy.[9]

Many EULAs do not explicitly acknowledge that liability limitations may not apply in the EU. Some EULAs, however, acknowledge generally the non-universality of such limitations. For example, a cybersecurity firm's limited liability clause excluding "all damages whatsoever" is followed by an exception stating that "[b]ecause some States do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you."

Where jurisdictions restrict the ability of EULAs to limit liability for personal injury and incidental or consequential damages, or to specify a specific court for claims, software companies are effectively forced to accept the liability exposure or avoid the jurisdiction altogether. The industry's current practices to limit exposure, however, to a large extent remain untested by the courts, and their actual legal effects are in many cases a matter of speculation. Moreover, where the insurance policies of software companies provide coverage for damages that are excluded by EULAs, there is a second layer of protection against potential future claims.

The question should be asked how it is possible that the software industry has been able to impose liability-limiting contracts on its customers

[6] Ibid., Article 3(1). [7] Ibid., Article 3(2). [8] Ibid., Annex 1.
[9] Ibid., Annex 1, para 1(a) and (q).

on an apparently large scale. In this regards, the software industry may be in a unique position. There are a number of reasons that may help explain this situation:

(1) Software cannot be held to any objective "safety" or "security" standards beyond the standard set by its manufacturer. Manifest manufacturing defects or design defects may render it obviously unusable and reasonable consumers expect that even well-functioning software contains some "bugs". It thus is hard to specify objectively what constitutes a failure of software, or lack of care in developing software, given the dynamic nature of the industry and the constantly evolving security threats to which it must respond. It is indicative that under the Product Liability Directive, which may or may not apply to software,[10] a producer cannot be held liable where he can demonstrate that "the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be detected."[11]
(2) The method of sale and delivery of software, which increasingly is done over the internet, allows for the utilisation of so-called "shrink" or clickwrap agreements. Linked to this is the respective bargaining power of both parties. Moreover, it is likely that the price of software would be dramatically different if software companies could not disclaim implied statutory warranties (like functionality and security) and limit the scope of their prospective liability. All firms in the software market are in the same position in this regard and all providers therefore include liability limitations in their EULAs, thereby normalising the use of these contractual terms and precluding consumers from acquiring these products without acquiescing to these terms.
(3) The position of contract software service providers may be different, however. With regard to the provision of bespoke security services for critical infrastructure, the generalised use of exoneration from liability is unlikely, since it would contradict the specific performance objectives agreed between the parties. Although, due to the sensitive nature of cybersecurity services for critical infrastructure, very little information is publicly available, security software providers may well have cyber liability insurance policies, which offer protection where direct liability limitation is not possible. Moreover,

[10] Stapleton 1994, 334. [11] Unfair Contract Terms Directive, Article 7(e).

> some of the most vulnerable industries are jointly operated with State agents, which may shield private contractors from sole liability, or bring them within the scope of sovereign immunity where available.

In Europe, the pharmaceutical industry, to a large extent, remains exposed to potential third-party liability claims. Strict regulation and pharmacovigilance procedures and the structure of the civil liability system (no class actions, etc.), however, may well work to reduce the number of claims against pharmaceutical companies. Note that regulation in the area of security does not necessarily produce the same effects. Unlike economic actors in the security chain, pharmaceutical companies have had a long history of facing claims and thus developed mechanisms to protect against such claims, without resorting to exoneration and other contractual liability limitations.

Again, the nature of the product concerned is key to understanding the industry's liability exposure. Pharmaceutical products are regarded as "inherently" risky; i.e., it is generally acknowledged that the products pose a certain degree of risk to the user and that the risks may well vary as a function of the disease to be treated and the physical condition or susceptibility of the user. The extent to which companies are exposed when it comes to such risks depends also on the Member State in question. Germany,for example, imposes strict liability for any risks that are not pre-identified and cause personal injury to the plaintiff.[12] Disclosure of the risks (specifically, the performance limits) of security products and services, by contrast, is often either impossible or undesirable. Although the public understands that these products and services cannot be effective against each and every attempted terrorist attack, the expectations are high. If and where security fails and terrorists are able to carry out their plans, the ensuing damage is not characterised as an "unfortunate side effect" in the same way as in the case of pharmaceutical products.

With regard to the general user who uses publicly available weather information, free of charge, the liability-limiting disclaimers employed by the meteorological industry, in general, are effective in limiting exposure. Alternatively, the meteorological industry can reduce its liability exposure by carefully describing the services rendered or the standard that applies to its forecast (e.g., forecasts are provided "as is", and may not be accurate, since they are based on predictions based on models). In cases in which such devices were not deployed by a company, however,

[12] German Pharmaceuticals Act (*Arzneimittelgesetz*; AMG).

the general standard of care (and, as a related matter, the public's understanding of the unpredictability of the weather and the inherent limits of weather reports), the lack of foreseeability of harm in a specific case, the doctrine of risk assumption, the requisite proximate causal link between the weather report and the plaintiff's damage and the plaintiff's burden of proof would help to protect the company concerned against liability.

Although the same standards of liability apply to the economic actors in the security chain in the event of a terrorist attack, the results may well be different. The doctrine of risk assumption, for example, is highly dependent on the specific situation, and victims of a terrorist attack on an aeroplane may not be deemed to have accepted the risk of scanning equipment malfunction. The nature of the risk in the meteorological industry is a natural risk, independent of individual human activity, while the risk in the security industry is a risk arising from intentional human behaviour. This difference may well translate into a different level of exposure of economic actors in the security chain.

To be sure, there are areas and circumstances in which the meteorological industry remains vulnerable to liability exposure. Because the meteorological industry predicts event in the future, however, it can invoke the limits of available models and scientific processes to argue that incorrect reports are not the result of any fault or negligence. While the ever-evolving meteorological forecasting modelling may enhance the ability to predict, at the same time the weather itself may become less predictable. Moreover, accuracy is increasingly guaranteed by advertised services in the context of contractual relationships with particular customers.[13] In this sense, an analogy could be drawn with the security industry.

7.1.3. Relevance for the security industry

Each of the three commercial sectors surveyed above exhibits certain specific characteristics that have influenced the nature of both its liability exposure and the instruments deployed to limit liability (and their effectiveness). The findings therefore cannot be generalised or extrapolated to the security industry, which operates in different markets and in different regulatory and economic contexts. In theory, however, the contractual mechanisms deployed in these three commercial sectors could be relevant to the economic actors in the security chain. Whether, in practice, contractual liability limitations can play a significant role is a function of

[13] Millington 1987, 238.

whether such limitations will be accepted by the business partners of the economic actors in the security chain, and to what extent such limitations are effective vis-à-vis third parties that have not agreed to them. This, in turn, is a function of market structure, relative bargaining power, specific laws and regulations, etc. (Similar reasoning applies also to the possible deployment of other instruments such as mutual risk pools, which are discussed in 8.2.) In theory, these arrangements could help, but whether, in fact, they can be established by and for the benefit of the economic actors in the security chain given the industry's specificities and the market structure, requires further analysis. Potentially relevant factors may be whether the industry's business partners are willing to accept liability limitations; whether there is sufficient standardisation across the industry to enable a general standard to be determined; whether the political and legal context in which the economic actors in the security chain operate would support liability limitations; which specific structures are most fitting to the industry; and whether other means, or a combination of them, could achieve the same effect in a more effective, cost-efficient or otherwise more desirable manner. In short, the analysis of industry practices in other commercial sectors provides useful insights into how liability risks can be managed. It demonstrates the respective strengths and weaknesses of each approach for the relevant industry and highlights the extent to which particular industry practices in this regard are a product of the particular needs and experiences of the industry in question.

In the security industry, however, there may be an additional complication that deserves attention. Contractual mechanisms may be difficult for the economic actors in the security chain to secure, to the extent contracts are awarded by public procurement based on contracts that are not negotiable. Public procurement is regulated extensively[14] to ensure fair opportunities and competition, but this law does not require that contractors assume full liability under the law. Of course, where a standard contract proposed by a purchaser does not provide liability limitations and a specific bidder insists on such limitations, its chances to be awarded the contract may be adversely affected (see further under 7.2.2., below). Sector-wide liability limitations and related mechanisms, in theory, would

[14] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC, OJ [2014] L 94/65 and Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC , OJ [2014] L 94/243.

be an option, but they raise issues under competition law and there is as yet no evidence of any such attempt in the security industry. It remains to be seen whether and, if so, how specific tools could be relevant and workable for economic actors in the security chain in light of industry practice and market structure, procurement practices and the like.

7.2. Risk mitigation strategies

The analysis presented in previous sections suggests that, when compared to other sectors, security providers may be less capable of deploying risk mitigation measures to limit their liability. The reasons for their reduced ability to limit their liability include the following. First, economic actors in the security chain, in particular service providers, have argued that they have been unable to negotiate contractual limitations of their liability. Contractual liability limitations can involve (1) narrow descriptions of primary obligations and limited representations and warranties; (2) exoneration for certain types of damages, for all damage caused by negligence, or for other types of exposure; (3) liability limitations in the form of financial caps or similar mechanisms; (4) indemnities; and (5) hybrid provisions, combinations of or variations on the above. The customers of the economic actors in the security chain appear to have been able to impose their terms and conditions on their providers, which has resulted in a lack of contractual protection for the security providers.[15]

Second, as discussed, the customers of the security industry are often public or semi-public authorities, which buy products and services through a regulated and standardised public procurement process. This may mean that these customers impose their terms and conditions, which tend to favour them and that non-acceptance of such terms may disqualify the bidder. Where this is so, security providers must either accept unlimited liability or the risk of being excluded or disfavoured by purchasers. For economic and business reasons, companies may not want to forego this market and thus accept the terms offered.

Third, security providers may not have been able to contract adequate insurance at a reasonable price to cover the liability risks associated with terrorism-related risks. Where this is so, they are not insured or underinsured for the liability exposure associated with terrorist attacks.

Beyond these considerations, there are broader public policy issues associated with the civil liability exposure of the security providers. For

[15] Bergkamp, Faure, Hinteregger and Philipsen (eds.) 2013, 300.

instance, should we encourage innovation in security and if so, should we do so through liability limitations? In light of the differences between security providers and other economic actors, these policy questions deserve further consideration (see Chapter 11).

The position of the security industry in public procurement is not unique, and other sectors of industry that sell much of their output to governments may be in a similar position. Nevertheless, the issue requires further analysis, because security providers may be exposed to larger liability risks than other sectors and the lack of liability limitations may thus become a problem.

There is no reliable and representative research on the extent to which security providers are unable to negotiate limitations on their liability in contracts with the Member State's public authorities and governmental agencies in public procurement for security products and services. It has been reported, however, that Member State public authorities insist that security providers remain fully liable under the applicable law.[16] Because there are often one or more bidders willing to accept these conditions (in particular, smaller companies whose assets are much smaller than the potential liabilities), all other companies are effectively forced to go along or they must accept that their chance of being awarded the contract decrease significantly. In some cases, individual companies have decided not to participate in bidding because they are not willing to assume the liability risks.[17] It has been reported that companies willing to accept full liability exposure in the maritime security area are more likely to offer sub-standard products or services, or have limited assets.[18] If, due to their reluctance to accept unlimited liability risks, financially strong security providers offering high quality products and services were consistently losing business to financially weak providers offering sub-standard products and services, this would be a concern. In itself, this would not necessarily justify a legislative liability limitation, however. In lieu of a liability limitation, it could possibly provide an argument in favour of the regulation of security providers, or another measure targeting financially weak companies.[19] In the absence of problems of underdeterrence of financially weak companies and the "judgment-proof" problem,[20] if

[16] Ibid., 300. [17] Ibid., 300. [18] Ibid., 300.

[19] Such a measure could involve a solvency guarantee in order to avoid externalisation of insolvency risk.

[20] Shavell 1986. This problem arises where the amounts of potential liabilities exceed the assets of the potentially liable person, so that, to that extent, liability does not create any financial incentives to prevent harm.

and to the extent that security providers are "forced" to accept contracts that do not set any limits to their liability, such contract clauses could merely reflect the preferences of the Member State governments. Viewed in this light, any legislative intervention might have adverse consequences. Under these circumstances, the EU or a national legislature would have a hard time supporting contractual liability protection for the security industry, because that would appear to be diametrically opposed to the Member State governments' explicit preference for full liability exposure.

The practice of the Member State public authorities to refuse to grant liability limitations could be consistent with a well-functioning market, in which security providers decide whether to bid for a specific project according to the totality of the proposed transaction, including their liability exposure. There does not appear to be any documentary evidence of a structural problem that requires legislative intervention in the market. In the absence of such a problem, the market may simply be competitive in relation to the ability and willingness of providers to assume liability risks. In that case, a liability limitation would eliminate competition in this regard and thus encourage excessive risk-taking, which would result in higher risk levels.

7.3. Conclusions

The analysis presented in this chapter shows that security providers, unlike companies in other sectors such as software, may not be able to negotiate limitations on their liability in contracts with their customers. This appears to be true in particular where the government or public agencies purchase security services or products in a public procurement process governed by public procurement legislation.

Although no individual factor discussed above, such as the lack of contractual liability limitation or adequate insurance coverage, may place security providers in a unique position with respect to their liability exposure, it is possible that the combination of factors is unique to the economic actors in the security chain. For instance, software companies are potentially exposed to catastrophic liabilities, but they are able to limit their exposure by contract and to contract adequate insurance, while security providers are also exposed to catastrophic liabilities, but are unable to limit their exposure by contract and to contract adequate insurance. The combination of the exposure to large liabilities (even if it is based solely on fault) and the inability to limit such exposure by contract (and to obtain adequate insurance coverage, which, by definition,

is subject to financial limits) might render security providers uniquely vulnerable to such liabilities. As noted, none of this means that liability exposure must therefore be directly limited, but it may mean that there is possibly exceptional liability exposure that may require policymakers' attention.

In addressing the liability of the security providers, it is important to consider not only the difficulties that they may face, but also the objectives of the liability system. Where liability exposure is excluded or limited, the realisation of these objectives may be impeded. Accordingly, there must be important policy reasons to justify an exclusion or limitation of liability, given the potentially negative effects of such a measure in terms of deterrence (prevention), risk allocation and loss-spreading. Moreover, there are differences between jurisdictions with respect to both liability exposure and the ability to deploy mitigation strategies; some of the arguments in favour of a liability limitation apply to the liability exposure of the US security industry and have not the same force in the European liability environment. In most EU Member States, specific direct compensation solutions have been worked out to cover damage resulting from terrorist activities. Indeed, a representative of a large reinsurer said that he was unaware of any problems with respect to the insurability of the liability exposure of the security industry in Europe.[21] This cautions against the adoption of any direct measures involving an exclusion or limitation of the liability of security providers. Measures such as direct State-provided compensation of damage caused by terrorists, of course, may result in a de facto limitation of their liability exposure.

[21] Bergkamp, Faure, Hinteregger and Philipsen (eds.) 2013, 306.