

## SUMMONS

Article 6:162 of the Dutch Civil Code, Article 10 of the ECHR, article 1 of the First Protocol to the ECHR, article 6.1 of the Authorisation Directive 2002/20/EC, articles 28 and 49 of the EC Treaty, principle of *égalité devants les charges publiques* [equality in bearing public burdens]

Today, the \_\_\_\_\_ of March, TWO THOUSAND AND FIVE,  
at the request of the private company with limited liability **XS4ALL Internet B.V.**, with its registered office in Amsterdam, the Netherlands, and its principal place of business at the address Eekholt 42 in (1112 XH) Diemen, the Netherlands, choosing as its address for service in this matter De Lairessestraat 111-115 in (1075 HH) Amsterdam, at the offices of Brinkhof, of which firm *mr* R. D. Chavannes is handling this matter, as well as at the address Noordeinde 33, in (2514 GC) The Hague, the Netherlands, at the offices of Houthoff Buruma Advocaten, of which firm *mr* P.J.M. von Schmidt auf Altenstadt is being appointed by my Petitioners as local counsel in this matter, and who shall act as such at law in the proceedings to be referred to below,

### HAVE SUMMONED:

The State of the Netherlands, more specifically, the Ministry of Economic Affairs, with its seat in The Hague, serving my writ there at the offices of the Procurator General to the Dutch Supreme Court, speaking with and leaving a copy hereof with:

### TO APPEAR:

not personally but represented by local counsel, on Wednesday, the twenty-third day of March, TWO THOUSAND AND FIVE, at 10.00 a.m., at the court session of the Hague District Court, which session shall be held then in the Law Courts at Prins Clauslaan 60 in The Hague;

### WITH EXPRESS NOTICE:

that if the Defendant does not appear or fails to appoint local counsel on the initial cause-list date or a cause-list date in the proceedings to be set later by the Court, and the required time periods and formalities have been observed, the Court shall enter a default judgment against it and shall grant the claims, unless the Court deems this to be unlawful or unfounded;

## IN ORDER TO:

hear it respectfully claimed and moved on behalf of my Petitioner as the Claimant as follows:

<b>1</b>	<b>FACTUAL BASES</b> .....	<b>2</b>
1.1	<i>Introduction</i> .....	2
1.2	<i>The Parties</i> .....	3
1.3	<i>History of the legislation on legal interception</i> .....	4
1.4	<i>The current scheme for enabling legal interception</i> .....	11
1.5	<i>Implementing legal interception capability</i> .....	12
1.6	<i>The costs of enabling legal interception</i> .....	18
<b>2</b>	<b>INTRODUCTION LEGAL BASES</b> .....	<b>22</b>
<b>3</b>	<b>CONFLICT WITH COMMUNITY LAW</b> .....	<b>22</b>
3.1	<i>Free movement of goods and services: the EC Treaty</i> .....	22
3.2	<i>Harmonisation to enhance free movement</i> .....	26
3.3	<i>Principles of Community law</i> .....	30
<b>4</b>	<b>CONFLICT WITH THE ECHR</b> .....	<b>36</b>
4.1	<i>First Protocol to the ECHR</i> .....	36
4.2	<i>Article 10 of the ECHR</i> .....	39
<b>5</b>	<b>FOREIGN CASE LAW</b> .....	<b>43</b>
5.1	<i>Austria</i> .....	43
5.2	<i>France</i> .....	44
<b>6</b>	<b>CLAIMS</b> .....	<b>45</b>
6.1	<i>Declaratory judgments</i> .....	45
6.2	<i>Damages</i> .....	46
<b>7</b>	<b>DEFENCE, EVIDENCE AND PROCEDURAL SUGGESTION</b> .....	<b>46</b>

## 1 FACTUAL BASIS

### 1.1 Introduction

- 1 At issue in these proceedings are the rules set out in the Telecommunications Act<sup>1</sup> regarding legal interception of telecommunications, more in particular the division of costs incurred in that regard. The costs of enabling legal interception are not borne

---

<sup>1</sup> *Bulletin of Acts and Decrees* 1998, 610, amended effective 1 September 2004 by the Act of 18 March 2004, *Bulletin of Acts and Decrees* 2004, 105.

by the State. Instead, they are shifted to telecom providers, even though the reason for enabling legal interception is solely to be found in the general public interests of criminal prosecution and national security.

- 2 Under Article 13.6(2) of the Telecommunications Act the administrative and personnel costs which directly arise from complying with a certain interception order are compensated by the State. However, Article 13.6(1) provides that the investment, operating and maintenance costs for technical facilities must be borne by the providers. These proceedings deal with Article 13.6(1) of the Telecommunications Act.
- 3 In this case, XS4ALL does not challenge in principle the need for legal interception. Nor does it ask the Court to depart from the case law of the Supreme Court regarding the review of enacted statutes against the Constitution or against unwritten principles of Dutch law. In these proceedings it argues that Article 13.6(1) violates European community law (the freedom of services, sector-specific directives and unwritten principles of community law) and the European Convention on Human Rights. Essentially, this involves the principles of equality in bearing public burdens, of proportionality, and of necessity, as embedded in that community law and Convention, given that the only justification for Article 13.6(1) of the Telecommunications Act is a wish to cut government expenditure. The relevant claims seek to have Article 13.6(1) of the Telecommunications Act declared non-binding or inoperative and to obtain compensation for the costs incurred in this regard in the past and still to be incurred in the future.
- 4 These grounds will be successively explained below. XS4ALL will do so at length and in detail, knowing that an enacted statute is not lightly set aside. Be that as it may, XS4ALL is convinced that Article 13.6(1) cannot be maintained.

## 1.2 The Parties

- 5 The Claimant (hereinafter: 'XS4ALL') has been active in the Netherlands since 1993 as an 'Internet service provider' (hereinafter: 'ISP'), a provider of Internet services to consumers and businesses. In 2003, it posted a turnover of approximately 51 million. It has about 285 employees and serves approximately 250,000 commercial and private customers. Given the services it provides, the Claimant can be considered a provider of public telecommunications services within the meaning of Article 1(ff) of the Telecommunications Act.
- 6 Under Article 15.1(1)(f) of the Telecommunications Act, the Ministry of Economic Affairs is the State Ministry which is responsible for monitoring compliance with the implementation of Chapter 13 of the Telecommunications Act.

## 1.3 History of the legislation on legal interception

7 The current Dutch policy on legal interception is based on a resolution of the European Council of 17 January 1995.<sup>2</sup> In this resolution, the Ministers of Justice and Home Affairs asked their telecom ministers to cooperate on introducing legislation mandating telecommunications infrastructure with legal interception capability. This non-binding resolution included an annex with requirements of the investigative services for being able to intercept telecommunications.

8 The resolution did not address the question of who would be responsible for the costs of making legal interception technically possible. Until 1995, the State had paid all these costs. During the phased liberalisation of the telecommunications market in the mid-1990s - in the course of which the incumbent state-owned company PTT was joined on the market by competing alternative communication networks and services (mobile telephony, Internet) - the first steps were taken to shift the costs of enabling legal interception to the market. The Mobile Telecommunications Act of 1994 stated that legal interception of the network of GSM providers had to be technically possible.<sup>3</sup> A bill was then introduced in 1995 which placed the burden of the costs for enabling legal interception of the GSM infrastructure on the licensees PTT and Libertel.<sup>4</sup> In the Minister's view, this cost apportionment between the State and providers was 'logical', because:

*[this] does not, after all, [pertain to] costs directly arising from the legal interception itself, but costs which the licensee must incur to be in compliance with the statutory requirements. [...] Budgetary considerations are also a factor. [...] Legal interception [...] increasingly entails costs for the State. This cost increase is due, on the one hand, to the fact that investigative authorities must use telephone interception as a tool to fight crime more often than they did in the past, and, on the other hand, to the fact that making it possible to intercept new forms of telecommunications always requires new investments. The State does not have any influence on technical developments relating to telecommunications, but is faced with the consequences of such developments, in the form of constantly increasing costs which the State must pay to legally intercept telecommunications.<sup>5</sup>*

9 The Minister felt that it was more logical for the GSM licensee, rather than the State, to bear the investment, operating and maintenance costs associated with making legal interception technically possible:

---

<sup>2</sup> OJ C 329 of 4 November 1996, p. 1.

<sup>3</sup> Article 13g of the Telecommunications Act 1988.

<sup>4</sup> GSM Legal Interception Act, *Bulletin of Acts and Decrees*, 1995, 594. An Article 64a was introduced in the Telecommunications Act 1988 which stated: "The investment, operating and maintenance costs for the technical facilities which have been incurred by a licensee regarding having third parties provide public mobile telecommunications (...) in order to comply with the provisions in Article 64 shall be borne by it."

<sup>5</sup> *Parliamentary Documents II 1994/1995*, 24108, No. 3, pp. 1-2.

*Specifically, the licensee is the one that enables use of the network, and should in that respect also bear the costs arising through the possible use of this network by criminal organisations.<sup>6</sup>*

- 10 It is clear that these arguments, the latter of which is circular, are barely supported and opportunistic in nature, and are almost entirely based on budgetary considerations. The State itself notes that the costs of enabling legal interception depend on the degree to which investigative authorities utilise legal interception, but does not attach to that the logical conclusion that the costs are prosecution costs and must therefore be borne by the State. If the costs of legal interception for the State are no longer counterbalanced by the benefits in terms of more effective criminal investigation, that is an indication that the authority to legally intercept must be used more sparingly, not an indication that the costs must be shifted to the providers.
- 11 The Council of State issued a negative recommendation on the proposed GSM Legal Interception Act, on grounds which XS4ALL which fully agrees with:<sup>7</sup>

*The Explanatory Memorandum states that legal interception increasingly entails substantial costs for the State, on the one hand, because investigative authorities must use telephone interception as a tool to fight crime more often than they did in the past, and, on the other hand, because making it possible to intercept new forms of telecommunications always requires new investments. A choice is made to put the burden on the licensee for the investment, operating and maintenance costs of the technical facilities for legal interception, because it enables use of the network. The justification for this, the Council of State finds, is apparently based on the notion that it is reasonable for the party – in this case, the licensee – which provides certain services to third parties commercially to contribute beforehand and structurally to the costs of investigating criminal offences of which these third parties might be suspected if information which may be relevant to the investigation can be derived from those services, whether or not through any artful devices. These investigative costs are therefore not borne entirely by the government, nor recovered from the persons convicted because of those criminal offences. This line of reasoning would, if also applied in other situations in which the government incurs costs in investigations, result in consequences which are hardly acceptable.*

*In principle, the Council does not consider it unreasonable for the government to require citizens to cooperate in a criminal investigation by furnishing the information or resources desired by the government. The starting assumption, however, must be that, exceptional cases notwithstanding, the costs related to providing such cooperation must normally*

---

<sup>6</sup> *Ibid.*

<sup>7</sup> *Parliamentary Documents II 1994/1995, 24108, No. A, pp. 1-2.*

*be borne by the government, given that investigation and prosecution of criminal offences is pre-eminently a task of the government. The Criminal Cases Fees Act (Bulletin of Acts and Decrees 1963, 130) is also based on this point of departure, as this Act provides for a system of fees for activities, for attendance as well as for related necessary costs, and for travel and accommodation costs incurred, insofar as these arise from a request or instruction from the Ministry of Justice in connection with, for instance, criminal cases (Article 1 of that Act). In the Council's opinion, an exceptional case as mentioned above is not present here, and the bill cannot be justified by purely budgetary reasons.*

- 12 During the plenary debate, the CDA [Christian Democratic Party] Parliamentary Party also pointed out three fundamental objections:

*For the CDA Parliamentary Party, there are three reasons to comment on this tiny bill, which actually does nothing else besides make the licensees, i.e., PTT and Libertel, pay for the costs which must be incurred to enable legal interception of GSM telephony. The first reason is related to the basic point that, in this manner, investigative costs, costs in connection with fighting crime, in the form of the facilities for legal interception are not borne in full by the government, as is ordinarily the case. The second reason is the fact that the business world was evidently not consulted regarding the financial and practical problems of these legal interception obligations. The third reason is the fact that, while a European standard is in the process of being formulated, that European standard still must be awaited. The question is how that is to be reconciled with the introduction of legal interception capability effective next 1 January.*

*I want to make clear that we are in agreement with the obligation imposed by law on the licensee to make legal interception of GSM telephony technically possible and to provide cooperation in that regard as part of a judicial investigation, even if that means that the licensee must furnish the technical facilities enabling this legal interception. Combating crime must continue to be possible after the introduction of new means of communication, such as GSM telephony. What we object to is that the specific costs of this obligation, which must be incurred by the operators and which result from what the government imposes on them, will be paid by a portion of society, in particular, the operators and, thus, probably the users of GSM telephony, and, hence, businesses. And this is so, even though the underlying idea with regard to fighting crime is that this serves the public interest and that the government must therefore be responsible for these costs. This is one of the government's core tasks. The flip side of that core-task notion is that the government therefore has a monopoly on investigating and prosecuting criminal offences. Taking everything into account, we think that the Minister's arguments for deviating from this essential principle are not convincing. The implicit idea that it is*

*apparently reasonable for a party which provides certain services to third parties commercially to contribute structurally beforehand to the costs of investigating criminal offences of which these third parties might be suspected if information which may be relevant to the investigation can be derived from those services is an idea we reject. We shudder at the prospect of a further expansion or extension of that idea. You can easily think of several ways in which this might be applied to road traffic. The fact that costs are increasingly going up, as the Minister states, because legal interception is becoming necessary more and more often does not in our view justify this unique step for GSM telephony. Indeed, the argument raises the question whether we will soon be going the same route for other means of telecommunication. After all, there, too, the government will have to conduct legal interception activities with increased frequency, given the rise in and nature of crime. The Minister's responses to a question by the CDA Parliamentary Party regarding whether we would in fact soon be going the same route for other means of telecommunication did not reassure us. She did not answer that at all, and I would indeed like to obtain clarity from the Minister on this at this time.*

*Mr Chairman! The fact that new forms of telecommunication always require new investments still does not in itself justify the violation in a specific case of the basic principle that the government bears the costs of investigation and prosecution. The fact that the cost apportionment includes a built-in incentive for the licensees to make legal interception possible in the most inexpensive manner seems reasonable and practical, but it is also not a convincing reason to violate this principle. In our opinion, the cost factors mentioned are precisely those types of aspects which the Minister could and should have discussed with the licensees, the business world, to find out whether an incentive could have been built in in other ways, so as to limit the costs as much as possible. That, too, is a point of criticism for us, Mr Chairman. What concerns us is that there was no consultation with businesses regarding the financial and practical problems of the legal interception obligation. Specifically, we have heard from various sources that this did not occur. Can the Minister state why she did not engage in such consultation and whether she still intends to pursue this?*

*Mr Chairman! As we see it, that consultation would also have been necessary to discuss with the business world the complicating factor of the European goal of making legal interception requirements uniform. This brings me to our third point of criticism.*

*Aren't businesses and operators now running the risk of making investments which, in time, must be supplemented again as a result of European uniformisation and, in the worst case, must be made once again? It would be to the Minister's credit – and I know the Minister as someone who takes such a remark to heart – if she could make agreements with*

*the business world on this point about the potential conflicting consequences of the Dutch steps with respect to the European measures. In short, Mr Chairman, it is a little proposal with, in the CDA Parliamentary Party's view, incalculable consequences regarding allocating investigative costs and the costs of combating crime. Thus, this is a fundamental violation of government responsibility, with an eye to fighting crime. For this reason, we cannot agree to the proposed regulation under the conditions stated in the legislative proposal.<sup>8</sup>*

- 13 The Minister's response was brief and not very convincing:

*As far as I am concerned, we are clearly talking about something different than the investigation itself, specifically, about enabling investigation and protecting state security. An extremely good comparison can be made, not with the car industry itself, but with the registration number system. It used to be the case that there were not many cars and registration numbers were unnecessary. If five cars, with different colours to boot, are on the streets in a village, it is exceptionally easy for the police to enforce the system. That was actually also so with the old telephone system. The police did not need very many tools to legally intercept telephone calls. Indeed, if someone telephones me in my car on ATF 3, the MPs can almost intercept the call themselves; hardly any equipment is needed. But technology doesn't stand still. A mass market is being created, for GSM as well, a highly complex technology, and the car industry has grown in the meantime. There aren't six cars in one village any more, but 6,000,000 in the Netherlands. As a result, it is no longer possible to enforce and investigate by eye. A registration number system has therefore been introduced, which is completely and entirely paid by motorists, and which is solely and purely designed to enable the government to exercise its investigative authority. In my opinion, this is the similarity with the current legislative proposal.*

*I believe that the government is entitled to ask companies investing in information infrastructure to include and pay for the technical options – including the maintenance costs – which enable the government to perform its tasks. Thus, I don't see any basic problem with this; indeed, I think it is very normal. I agree with the comment which Ms Roethof, among others, made in this respect. If increasingly complicated equipment makes performance of those tasks more and more difficult, it is very unfair to spread the costs among the taxpayers, when not every taxpayer has the option of then using it. One thing we can be certain of: those who are up to no good always use the most complicated equipment.*

---

<sup>8</sup> Official Verbatim Report II 1995/1996, No. 6, pp. 1120-1121.

- 14 A few conspicuous differences between registration numbers and enabling legal interception are the fact that the costs for registration numbers are low and predictable and occur only once, and the fact that a registration number is, of course, also useful for the owner (recognisability of the owner's own car). This is not so with enabling legal interception, a system in which the costs are high, continuous and (partly because of the government) unpredictable, and where the provider cannot, does not want to and may not utilise it for itself. The registration number system is a registration system which can better be compared to the one-off registration which all telecom providers are required to file with the regulatory agency *OPTA* (Independent Post and Telecommunications Authority), see Article 2.1 of the Telecommunications Act. In *XS4ALL*'s opinion, it is not in the least bit reasonable for only the users of a certain service or technology to pay for the costs of combating a criminal offence which is perhaps committed by a person who is also a user of that service or technology. Speed radar detectors along motorways and harbour/river police boats are also financed by people who walk. If a suspect is shadowed on foot, those staying inside also pay. The harm someone experiences from Internet crime does not depend on whether the person has his or her own connection; the entire society benefits when crime is combated and should indeed jointly pay for this.
- 15 Despite the negative recommendation by the Council of State and the opposition of several parliamentary parties, the Telecommunications Act was nonetheless adopted. This cost apportionment method was then, as had been feared by the Council of State and the CDA, expanded to cover all forms of telecommunication (networks and services) in the government's Envisaged Policy on Authorised Legal Interception of Telecommunications of 4 April 1996. Intention 5 read that the investment, operating and maintenance costs for the technical facilities in connection with legal interception and furnishing information as well as in connection with security should be borne by the network managers and the service providers.
- 16 This Envisaged Policy was justified in the same manner as the GSM Legal Interception Act, with it also being pointed out that this approach for GSM had become prevailing law in the meantime.<sup>9</sup> The Envisaged Policy provided for one-off compensation for costs for several existing networks and services.<sup>10</sup> The rationale was that the costs for enabling legal interception later will usually be much higher than if they are already taken into account when the telecommunications systems are developed.<sup>11</sup> The term 'internet' was still not mentioned anywhere in the Envisaged Policy. The question whether it should be possible to legally intercept internet services and, if so, who should pay for it, was therefore not addressed.
- 17 The Envisaged Policy on Authorised Legal Interception was fleshed out in the revision of the Telecommunications Act 1988 which ultimately resulted in the Telecommuni-

---

<sup>9</sup> *Parliamentary Documents II 1995/1996*, 24679, No. 1, pp. 9-11.

<sup>10</sup> See Policy Intention, Annex 4.

<sup>11</sup> *Parliamentary Documents II 1995/1996*, 24679, No. 1, p. 11.

cations Act 1998.<sup>12</sup> In the Explanatory Memorandum to proposed Article 13.6 of the Telecommunications Act, the Minister wrote:<sup>13</sup>

*When PTT was still a state-owned company, the costs which had to be incurred to make and keep legal interception of a telecommunications system possible were always paid by the State. The State has not been a network manager since 1989. Yet, the State still must be able to engage in legal interception. This is becoming more and more difficult due to the increasing technological complexity. The providers of public telecommunications networks and public services do not engage in legal interception themselves – this is reserved to the authorised agencies – but merely facilitate legal interception by taking timely organisational and technical measures based on statutory provisions. Costs must be incurred to comply with these statutory provisions. Thus, these costs arise from statutory obligations and do not relate to legal interception itself. From that standpoint, it is logical that these costs no longer be borne by the State, but by the providers.*

*Budgetary considerations are also a factor for the State. Legal interception of telecommunications is becoming an increasingly important, if not indispensable, tool in fighting organised crime in particular and protecting state security. It entails increasing costs for the State as well. This cost increase is due, on the one hand, to the fact that investigative authorities must use telephone interception as a tool to fight crime more often than they did in the past, and, on the other hand, to the fact that making it possible to legally intercept new forms of telecommunications also always requires new investments for the State. For instance, the rooms where legal interception takes place must be modified. In short, the State is faced with the consequences of technological developments relating to telecommunications in the form of constantly increasing costs to legally intercept telecommunications.*

*An additional benefit is that an incentive is therefore built in to accomplish legal interception capability in the most inexpensive manner, so that the increased costs caused by the facilities to be provided can remain limited. Moreover, making allowance for the costs incurred in business operations is a responsibility of the business.*

- 18 Critical questions by the House have not resulted in either further justification for or changes in the text.

---

<sup>12</sup> Bulletin of Acts and Decrees 1998, 610.

<sup>13</sup> *Parliamentary Documents II* 1996/1997, 25533, No. 3, pp. 125-126.

## 1.4 The current legal requirements on enabling legal interception

19 Article 13.1 of the Telecommunications Act reads as follows:

*1. Providers of public telecommunications networks and public telecommunications services shall only make their telecommunications networks and telecommunications services available to users if they can be legally intercepted.*

*2. Rules may be laid down by or pursuant to order in council regarding the technical capability to legally intercept public telecommunications networks and public telecommunications services.*

20 The requirements of legal interception capability were laid down further in the Decree on Legal Interception of Public Telecommunications Networks and Services, and further elaborated upon in a ministerial regulation.<sup>14</sup> Briefly stated, this entails an obligation for Internet providers to take such measures that they are immediately able to fulfil every specific order.

21 Article 13.2 of the Telecommunications Act states that providers of public telecommunications networks and services must cooperate in effecting a legal interception order. The Article reads as follows:

*1. Providers of public telecommunications networks must cooperate in effecting an order under the Code of Criminal Procedure or permission under the Intelligence and Security Services Act 2002 to legally intercept or record telecommunications which are completed over their telecommunications networks.*

*2. Providers of public telecommunications services must cooperate in effecting an order under the Code of Criminal Procedure or permission under the Intelligence and Security Services Act 2002 to legally intercept or record telecommunications provided by them.*

*3. Rules may be laid down by or pursuant to order in council regarding the organisational and personnel measures to be taken and the facilities to be provided regarding legal interception.*

22 Article 13.5 relates to security and reads as follows:

*1. Providers of public telecommunications networks and public telecommunications services must secure data with regard to a specific order or permission under the Intelligence and Security Services Act 2002 as re-*

---

<sup>14</sup> Decree of 10 November 1998, *Bulletin of Acts and Decrees* 1998, 642, most recently amended by a Decree of 16 December 2002, *Bulletin of Acts and Decrees* 2003, 22; Regulation on Legal Interception of Public Telecommunications Networks and Services, *Government Gazette* 2001, 107, p. 20.

*ferred to in Article 13.2 or a charge or request as referred to in Article 13.2a or Article 13.4, first or second paragraph, against disclosure to unauthorised persons as well as maintain the secrecy of these data.*

*2. Rules may be laid down by order in council regarding the measures to be taken in connection with the security as referred to in the first paragraph.*

23 Article 13.6 of the Telecommunications Act relates to costs and reads as follows:

*1. The investment, operating and maintenance costs for the technical facilities which have been or will be incurred by providers of public telecommunications networks and public telecommunications services to be able to comply with Articles 13.1, 13.4 and 13.5 shall be borne by them.*

*2. Providers of public telecommunications networks and public telecommunications services may claim compensation from the State Treasury for the administrative and personnel costs incurred by them which directly arise from complying with a specific order or permission under the Intelligence and Security Services Act 2002 as referred to in Article 13.2, first and second paragraphs, or a claim or request as referred to in Article 13.2a or Article 13.4, first or second paragraph.*

*3. Rules will be laid down by ministerial regulation regarding determining and compensating the costs referred to in the second paragraph.*

24 Article 13.8 provides for a potential exemption:

*In exceptional cases, Our Minister may grant an exemption from the obligations arising under this Chapter in agreement with Our Minister of the Interior and Kingdom Relations, Our Minister of Defence and Our Minister of Justice. An exemption may be granted subject to restrictions. Conditions may be attached to an exemption.*

## **1.5 Implementing legal interception capability**

25 Obviously, the fact that they were required to enable legal interception on their networks represented considerable costs to the providers. As the quoted articles demonstrate, however, much implementation of legal interception has been left to lower-level regulations and statutory instruments. The manner in which the implementation legislation designed by the State came about, as well as its contents and application, only served to further increase the costs providers had to make.

26 When the Telecommunications Act took effect on 15 December 1998, the Netherlands was far ahead of other European countries and the United States in terms of legal interception of Internet traffic. There were no national or international technical

standards, no detailed protocols for transferring the intercepted information between providers and investigative authorities and, hence, no equipment, either. Although the Council Resolution of 17 January 1995 referred to earlier was couched in very broad terms, such as ‘communications networks’, it was only applicable to voice telephony.<sup>15</sup>

- 27 The Dutch pioneering position and the manner in which the government further specified the statutory obligation into functional and technical requirements are extremely important in this case. Specifically, they illustrate that providers have had to incur much more costs to comply with their statutory obligations regarding enabling legal interception than if the Netherlands had waited until other countries had done the pioneering work and that, by very meticulously stating which functionality the providers had to offer and how they had to offer this, the State largely determined the costs of enabling legal interception itself. This is contrary to the assertion cited above<sup>16</sup>, used to justify shifting the costs to the providers, that the government had *no* influence on the technical or any other costs.
- 28 With the application of the possibility of an exemption in Article 13.8 of the Telecommunications Act, Dutch Internet providers were granted a reprieve until 15 April 2001 from the obligation to enable legal interception of all networks and services, in anticipation of agreement on a protocol, followed by invitations to potential suppliers to develop a system.<sup>17</sup> At the time this deadline expired, the practical details concerning the technical standards, norms and requirements for legally intercepting Internet traffic were either still being discussed or were absent completely. The organisational rules for legal interception were being examined by the Council of State for approval. It was not until 7 June 2001 that the final Regulation on Legal Interception of Public Telecommunications Networks and Services was published in the *Government Gazette*, which already went into effect on 15 June 2001.<sup>18</sup> By imposing immediate and complete legal interception capability, the State ignored the European (ETSI) standard for legal interception that was still being developed.
- 29 Thus, during the period 2000-2001, the State developed a standard that was entirely its own, laid down in two technical documents: the functional specifications of interception in WAI/GT/FuncSpecs, and the specifications of transfer of data flow to investigative authorities in the TIIT. In trying to move faster than the developments in an international context, the State forced providers in the Netherlands to incur substantial pioneering costs. It is a striking example of the way in which the State made choices that left others facing the financial consequences – choices which, most

---

<sup>15</sup> See, for example, Article 1.4: “Law enforcement agencies require access to call associated data such as: [...]”, showing that only telephone calls were covered. In 1995, the Internet was still only being used by a limited circle.

<sup>16</sup> See paragraph 8, final sentence quotation and paragraph 17, final sentence quotation.

<sup>17</sup> Policy Guidelines on Granting Exemptions on Enabling Legal Interception of Internet Services, 7 May 1999, *Government Gazette* 1999, 86, p. 9; Policy Guidelines on Granting Exemptions on Enabling Legal Interception of Internet Services 2000, 17 July 2000, *Government Gazette* 2000, 133, p. 37.

<sup>18</sup> Regulation on Legal Interception of Public Telecommunications Networks and Services, *Government Gazette* 2001, 107, p. 20.

likely, the State would not have made if those consequences had made a dent in its own budget.

## 1.5.1 *Functional specifications*

- 30 On 13 June 2000, under great pressure from the State, the ‘Internet Legal Interception Working Group’, a consultative body made up of representatives of the government (investigative authorities) and Internet providers, produced the first ‘official’ version of the document WAI/GT/FuncSpecs, in which the functional requirements were described for enabling legal interception of Internet services and Internet data transmission. ‘Functional requirements’ referred to the type of services and data which could be legally intercepted and retrieved. The Working Group was subsequently disbanded, but many questions remained unanswered, which, in practice, had to be resolved by the providers. The official WAI functional specifications published in the Government Gazette were incorrect. Those who built a system according to those specifications were guaranteed to end up with a non-functional solution. So, the legal interception equipment was developed on the basis of draft new versions of the WAI/GT. The WAI specifications continued to be highly detailed but, at the same time, the technical specifications were frequently unclear.<sup>19</sup>
- 31 Notably, then, it was the State which ultimately determined the details of the functional specifications that the providers had to meet. It did so in a manner that bred confusion, uncertainty and delay. In this way, the State not only largely determined which costs the providers would have to incur to comply with their statutory obligations but it also raised those costs unnecessarily.

## 1.5.2 *Technical specifications*

- 32 Another consultative body, the Legal Interception Sub-Group of the Post and Telecommunications Consultative Body, worked on a practical standard for transferring the legally intercepted data flows, the TIIT (Transport of Intercepted IP Traffic). The very first version of this protocol, version 0.1.2, came out in October 2000. It was not until September 2002, more than a year after the exemption period for Internet providers had expired, that the first official version of the TIIT was published by the Ministry of Economic Affairs, V1.0.0 (2002-09). During that period, internet providers had to be able to make legal interceptions but they did not know precisely how to do so, which again led to a great deal of uncertainty, consulting hours and costs.

---

<sup>19</sup> Many examples can be given, including: (1) unclear on how to deal with a customer who logs in twice at the same time (e.g. with a double ISDN connection or with an ADSL connection and telephone), (2) unclear on whether it should also be possible to legally intercept outgoing mail and whether that should be done, (3) secure key exchange: the WAI did not define the expiry date of the certificate, on account of which connections became invalid after a year and new certificates had to be created, (4) how to deal with a customer that moves during legal interception, (5) there was no portfolio of requests investigators were allowed to make, so eventually the providers made one, (6) on the one hand, they wanted it ‘all’, on the other hand, obviously, they did not want the viruses and spam that makes up most of the e-mail traffic.

- 33 The standard defines how the legally intercepted traffic must be provided to the State in a secure manner. TIIT provides that two types of nodes be installed in the provider's network: a 'recording system' (S1, also called a 'sniffer') which records Internet traffic and a transmission system (S2) which creates a secure connection between the provider and the particular investigative authority for transmitting the intercepted data. The government works with two nodes as well: a receiving system (T1) which receives the data from the provider's transmission system and a storage system (T2) which stores the data. Working with different nodes prevents a central security problem from arising and avoids the situation in which the failure of one system may compromise the integrity and security of the other systems. Only encrypted data is exchanged between the provider's transmission system and the investigative authorities' receiving system. Any failure in this communication will not affect recording of a suspect's data by the recording system, nor will it affect the data already stored in the storage system at the investigative authorities' location.
- 34 The standard also makes a distinction between the pure data flow and the related traffic information. According to this document, providers must separately record and provide the related traffic information (the 'IRI', Interception Related Information). For technical reasons, most providers cannot suffice with one S1 recording system, but must install several of these expensive systems in their networks (which are complex and not easily adjustable), in order to be certain that all the traffic of a specific suspect is received.
- 35 Despite the repeated insistence of the NLIP, the State refused to give an indication of the number of simultaneous wiretaps that providers could expect at most. The aforementioned Council Resolution of 17 January 1995 assumed a maximum number of simultaneous intercepts that could be processed:

*8. Law enforcement agencies require network operators/service providers to make provisions for implementing a number of simultaneous intercepts. [...] The maximum number of simultaneous interceptions for a given subscriber population will be determined in accordance with national requirements.*

- 36 Initially, the Netherlands did not apply a maximum, but an opposite requirement, a permillage of the total number of customers that could be legally intercepted simultaneously. This permillage requirement was done away with, however, in 2001, at the time ISPs had to be able to offer legal interception capability. This change was explained as follows:

*First, as a result of the elimination of the 'permillage requirement' in Article 2 of the Legal Interception Decree, the specific details regarding the various networks and services in this Regulation have ceased to have effect. Now, the only requirement regarding the various networks and services is that they be designed in such a manner that every specific order can be effected immediately. Consequently, in the new system, the pro-*

*viders themselves determine how much capacity for legal interception they wish to reserve in order to be able to immediately effect the specific orders provided to them. This freedom for providers also entails extra responsibility; if the provider unfortunately cannot meet the requirement that a specific order be effected immediately, it cannot be claimed that the legal interception capability requirement under Article 13.1 of the Telecommunications Act was implemented in an incorrect or deficient manner. Regarding the precise background for elimination of the legal interception permillages, reference is made for brevity's sake to Section 2 of the Explanatory Memorandum to the Decree Amending the Decree on Legal Interception of Public Telecommunications Networks and Services.*

- 37 The result is that providers must be able to effect every legal interception order, regardless of how many they already have in progress. In other words, the providers no longer have any guidance whatsoever and must balance the amount of the investment against the chance that, at a certain peak time, they will not have any lines available for legal interception, thereby committing a crime by being unable to comply with an interception order. Providers are forced to purchase several S1 systems in advance and install them in their network.
- 38 XS4ALL started looking for a supplier in August 2001, in other words, even while the TIIT was still busily being developed. The NLIP had organised a suppliers' day in The Hague. XS4ALL then went through a complete process with four different suppliers, with an American company that had developed an interception box based on the American Carnivore requirements, with Accuris from Ireland, with the Dutch company Pine and with the Israeli company Comverse (from which the government also purchased the equipment). In the end, XS4ALL opted for the new Dutch solution to be developed by Pine. Intensive development began in November/December 2001.

### 1.5.3 Problems in implementation

- 39 The most significant initial and current problems in implementing legal interception capability can be described as follows:
- As the Netherlands was very far ahead in mandating that it be possible to legally intercept Internet services, providers were compelled to go through a complicated order process to find a supplier which could meet these requirements. Suppliers charge considerable development costs for new technology.
  - As it was very unclear for a long time what the final specifications would be, and as each provider's network is different, clear price comparisons could not be made. XS4ALL went through four order processes with four different suppliers before a clear choice could be made concerning the costs of the purchase and permanent maintenance and licensing costs. The first three suppliers with which XS4ALL negotiated, the American company, Comverse and Accuris, quoted amounts which were more than ten times as much as the solution ul-

timately chosen. By collaborating with the Dutch company Pine on the legal interception solution developed at that point, called 'EVE', XS4ALL opted for equipment costs which, relatively speaking, were extremely low, but, at the same time, for a development process which was relatively labour-intensive.

- The State exerted a great deal of pressure on providers in 2000 and 2001 to provide legal interception capability for services and networks as quickly as possible, but was itself seriously deficient in addressing several points – first, through impracticable secrecy rituals concerning the functional specifications and, second, as a result of the fact that the investigative authorities' receiving system was not ready technically or administratively (and still is not). XS4ALL has the impression that it was one of the first parties in the Netherlands to ultimately have a working solution. However, to make it so, XS4ALL had to engage in many additional discussions with all interested parties in 2001-2003 regarding 'whether it worked yet', including test days, with test data being sent to the investigative and security services. To this day, both the investigative and security services regularly make technically infeasible requests, forcing XS4ALL's technical experts to explain how the network operates technically and why the requested information cannot be provided in the desired manner.
- Due to this imbalance in know-how – which was exacerbated by a steady growth of the number of parties authorised to give orders pursuant to Chapter 13 of the Telecommunications Act - XS4ALL (and other providers) are in practice forced to educate the investigative authorities on dealing with encrypted communications, certificates and storage of data flows which are so large that the investigative authorities, too, lack sufficient reliable storage capacity to receive and analyse the intercepted information securely.
- Due to a lack of knowledge and coordination, investigators often turn out in practice to be unable to handle the technical requirements. They request - and therefore receive – much more data than they can process and thus frequently impose new requirements on providers regarding 'partial legal interception capability' of specific Internet protocols.<sup>20</sup> Although, from the investigators' perspective, the desire for filtered traffic, for example, was not new, Parliament chose to legitimise only a full intercept or an incoming e-mail intercept. Internet providers have always explained that partial legal interception capability per Internet protocol is not technically possible, but that the provider would then have to employ a full intercept and itself filter the desired information from this, and that this would, *inter alia*, constitute an unacceptable intrusion on the secrecy of communications. In practice, under the threat of, for example, seizure of equipment, providers are in fact compelled nevertheless to only furnish that information which the investigative authorities can process themselves.

---

<sup>20</sup> In principle, the legal interception obligation pertains to legally intercepting all the Internet traffic of the party concerned. It is up to the investigative authorities to distil the desired information from that data flow.

- While the legal interception specifications were being developed, XS4ALL had to negotiate with suppliers. At the same time, the bandwidth in the network increased sharply, making it necessary to constantly adjust the legal interception facilities. From a couple 100Mbit/s connections in 2000, XS4ALL grew to 8Gbit/s in 2004. Currently, XS4ALL is growing again towards another step, towards 10Gbit/s. Keeping this continuous growth in line with the legal interception facilities as well constantly takes a lot of time and thought, both at management level and from a purely technical standpoint, in terms of installing and maintaining facilities.
- 40 The following picture emerges. The State laid down in the law that all costs of enabling legal interception are to be borne by providers and that it was allowed to detail the obligation to enable legal interception in lower-level regulations. Next, the State imposed highly detailed, complex and therefore costly demands on legal interception facilities and unnecessarily inflated the costs for providers by issuing unclear, untimely and incomplete regulations.

## 1.6 The costs of enabling legal interception

- 41 The costs of enabling legal interception can only be influenced by the providers themselves to a very limited extent. The delegated regulations promulgated by the State under Articles 13.1(2) and 13.2(3) of the Telecommunications Act contain very specific provisions concerning the facilities which the providers must have available. Hence, the State requires providers not only to make unlimited legal interception of their networks and services possible in the abstract, but also requires them in concrete terms to take numerous specific measures and thereby make considerable, additional investments. Because the specifications are driven by the desires of the investigative system and the investigative system desires the best possible facilities, Article 13.6(1) of the Telecommunications Act, in combination with the other provisions of Chapter 13 of the Telecommunications Act, means that the providers have had to put a 'state of the art' legal interception infrastructure in place at their own expense for the government's benefit. The State gave itself carte blanche and it is using it to the fullest extent.

### 1.6.1 Costs incurred by XS4ALL

- 42 In order to acquire insight into the costs it incurred in implementing and maintaining the capability for legal interception – costs it must bear itself pursuant to Article 13.6(1) of the Telecommunications Act – XS4ALL called in Ernst & Young, an accounting firm, to conduct an investigation. Ernst & Young's report is submitted as **EXHIBIT E-1**. It shows that, in the period 2001-2004, XS4ALL spent EUR 489,293 to meet the demands of Chapter 13 of the Telecommunications Act.
- 43 The costs XS4ALL incurred mainly related to investments in the purchase of equipment, costs of external project management and personnel costs. The person-

nel costs, in particular, were very high indeed due to the complex nature and lack of clarity about the technical and functional specifications the system had to satisfy.

## 1.6.2 Situation in other Member States

- 44 The scheme for regulating the costs of enabling legal interception in the Netherlands based on budgetary considerations is fairly exceptional. Although accurate information is scarce, a recent study into legal interception capability in the G-7 countries reveals that they all – with the exception of Germany – pay some compensation to their telecom providers for these costs.<sup>21</sup> The study is submitted as **EXHIBIT E-2** and provides the following picture:

**France:** *Due to a ruling of the French Council of State (see below, paragraph 132 et seq.), providers are generously compensated for the costs of enabling legal interception, as a result of which providers have not protested that much against enabling legal interception. Businesses are compensated for their actual costs. Investments in technical equipment are recovered from the government. The criticism mainly has to do with the fact that the cost compensation process is slow and cumbersome.*

**Italy:** *In Italy, too, the costs for enabling legal interception are compensated generously. The official list introduced with the Decree of 26 April 2001 proposes a step-by-step notion, in which businesses may recover investment, maintenance and personnel costs from the government. Initially, the businesses are responsible for the costs of transferring data, with the businesses receiving compensation from the municipal government. Settlement occurs locally or by the court which imposed implementation of the control measure. Recent press exposure<sup>22</sup> shows that Italy pays about EUR 300 million annually by way of compensation to telecom providers.*

**United Kingdom:** *The RIPA (Regulation of Investigatory Powers Act) requires the Ministry of Home Affairs to provide financial compensation. The government released around GBP 20 million for those payments for 2001-2004. This is expected to almost cover the costs incurred. It cannot be said yet exactly which costs will be reimbursed in the calculation (hardware, software, personal costs). To prevent providers from making a profit on implementing legal interception capability, there are no set price lists in connection with the costs to be incurred by the businesses.*

**United States:** *Congress has allocated around USD 500 million to pay compensation for installation of the technology required of the providers. The TCCF (Telecommunication Carrier Compliance Fund) was created to*

---

<sup>21</sup> F. Büllingen & A. Hillebrand, Sicherstellung der Überwachbarkeit der Telekommunikation. Ein Vergleich der Regelungen in den G7-Staaten, Wissenschaftliches Institut für Kommunikationsdienste, 2003.

<sup>22</sup> Economist, 3 March 2005.

*settle the payments (USC § 1020). . The authorised government agencies deposit a certain amount in this Fund. Under USC § 1020, payments are made from the fund to compensate providers for the costs they incur to have their systems satisfy statutory legal interception requirements. Costs incurred to adjust equipment and networks that were created prior to 1995 are eligible for more and faster compensation.*

*The Criminal Code provides the businesses with full compensation for the costs of implementing measures: "Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefore by the applicant for reasonable expenses incurred in providing such facilities or assistance."*

**Canada:** *Under a current bill, providers having to adjust existing systems to make legal interception of them possible would not have to pay the related costs themselves. New systems would have to include a 'basic intercept capability'.*

**Japan:** *The government has indicated that it is prepared to assume a large portion of the development costs. Debates are going on in Parliament regarding the cooperation expected from the providers. In anticipation of this discussion, the Ministry of Justice explicitly stressed in a statement to Parliament that, if the requirements laid down by the government exceed the capabilities of the businesses' equipment and technology, or seriously disrupt their performance, the providers will have legitimate grounds for refusing to cooperate.*

- 45 The Finnish Telecommunications Act specifically provides that the costs of investing in legal interception capability are compensated in full<sup>23</sup>. In Austria, the same situation has applied since the *Verfassungsgericht* rendered a judgment, which will be discussed below (§ 127)

### 1.6.3 Impeding innovation

- 46 The Dutch legal interception legislation has also led to considerable non-financial costs. Lack of clarity about the demands the government will impose on legal interception capability and the high and uncertain costs involved in the development and implementation of legal interception capability form a considerable impediment for the development and availability of new services. A number of examples will illustrate this.

- **VPN** – Although there is great corporate demand for secure internet connections (so-called VPN-services), XS4ALL does not provide them itself. Rather, it

---

<sup>23</sup> See Article 98 of the Communications Market Act (unofficial English translation at [http://www.mintc.fi/www/sivut/english/tele/telecommunications/communications\\_market\\_act.pdf](http://www.mintc.fi/www/sivut/english/tele/telecommunications/communications_market_act.pdf)).

has resellers do this. They are not public telecom providers in the sense of the Telecommunications Act so they are not required to offer legal interception capability. If XS4ALL were to offer VPN-services itself, it would also have to be able to remove the security from the connection in case of legal interception itself. That is impossible without fundamentally affecting the security of the connection and it would render the service unmarketable.

- **IPv6** - The functional and technical specifications are based on version 4 of the Internet protocol (IPv4). There are no functional or technical specifications for the legal interception of IP version 6. Functionally, however, IPv6 is a major innovation, because IPv4 has a very limited number of IP-numbers and sorely needs expanding. In addition, IPv6 offers various security improvements because it allows better safeguarding of connections against hacking, attacks and other risks. IPv6 cannot be legally intercepted, or only with the greatest difficulty, and furthermore the State's policy in this regard is unknown. It is this uncertainty that keeps XS4ALL from investing heavily in IPv6 and, consequently, this innovative service is hardly being used at this time.
  - **VoIP** - XS4ALL does not itself offer voice over IP (VoIP, telephone calls via the Internet) but customers can use it. If a legally intercepted customer is using VoIP, the voice communications are also intercepted, but not in a readable format because of encryption. There are no technical or functional specifications for legally intercepting VoIP. It is highly unclear whether, and if so, how VoIP must be legally intercepted. This keeps XS4ALL from investing in this technology - a technology that national and international governments agree is important for the development of competition in the telephony market.<sup>24</sup>
  - **WiFi** - XS4ALL does not offer so-called hotspots (public access points for wireless internet access) itself because the costs of individual legal interception capability are so high that a profitable business case is out of the question. Under great pressure from the government, KPN developed legal interception capability in the hotspots itself with its HubHop, something which XS4ALL cannot afford.
- 47 In general it is not practically possible for XS4ALL to invest in new security services because, being a provider of public telecom services, it is subject to the legal interception obligation. Uncertainty about the requirements and costs of legal interception

---

<sup>24</sup> See in this respect the recent press release of the European Commission, 'EU regulators favour pro-competitive approach to Internet telephony', IP/05/167 of 11 February 2005, in which Commissioner Reding is quoted as follows: "I expect Voice over IP to lead to more diverse and innovative services in the market which may well have an even bigger impact on consumers and businesses than email. And Voice over IP is just the tip of the iceberg. IP-based networks and services will be the basis for a whole new range of communications services, not only benefiting consumers directly, but feeding through directly to the whole economy. I am convinced that, as the market develops, the European Commission and national regulators will jointly ensure that throughout the EU, the roll-out of new IP-based services will not be hindered by regulatory hurdles."

tion capability render the service infeasible businesswise, or at any rate considerably slows down the introduction of such services.

- 48 This is all the more objectionable because said services can be offered without any legal interception capability by market players that cannot be considered to be providers of public telecommunication networks or services within the meaning of the law. For example, internet users can build a VPN-connection or make VoIP calls by using software applications. The Skype program is a good example of a VoIP-application that enables non-interceptable telephone calls. Providing a software application is not covered by the legal definition of providing a public telecommunication service. In other words, XS4ALL bears the burden of a facility in the public interest that does not fully safeguard such public interest.

## **2 INTRODUCTION LEGAL BASIS**

- 49 This concludes the background to and implementation of the statutory obligations in relation to legal interception and the costs incurred in the process. Below, XS4ALL will explain, in support of its claims, why Article 13.6(1) of the Telecommunications Act is non-binding. The following subjects will be discussed: the primary and secondary European Community law, the principle of *égalité devant les charges publiques*, and the European Convention on Human Rights.

## **3 CONFLICT WITH COMMUNITY LAW**

- 50 Article 13.6(1) of the Telecommunications Act and the further regulations to implement this provision conflict with European Community law. The Dutch regulations are not reconcilable with the rules regarding the free movement of goods and services within the Community.
- 51 The free movement rules are set forth in the EC Treaty itself, but the underlying principles of Community law were further developed with regard to the electronic communications sector in a series of sector-specific harmonisation directives from 1997, which were thoroughly revised in 2002. The advancing harmonisation limits the Member States' freedom to further introduce or maintain national regulations for the communications sector.
- 52 The free movement rules in general will be discussed below first, followed by the additional content which has been given to these rules for the electronic communications sector.

### **3.1 Free movement of goods and services: the EC Treaty**

- 53 Article 49 of the EC Treaty prohibits restrictions on the freedom to provide services within the Community. The prohibition relates both to discriminatory measures and

to any restriction which makes the activities of a provider of services which is located in another Member State and provides services there lawfully less attractive.<sup>25</sup> That such a measure applies without distinction to domestic service providers and service providers from other Member States – and, hence, does not discriminate in that sense – does not change the fact that such a measure may impede entry into that Member State’s market, thereby constituting a restriction on the free movement of services within the meaning of Article 49 of the EC Treaty.

- 54 It almost goes without saying that provision of Internet services is by definition a cross-border activity and that measures that restrict the freedom to provide services have, by definition, a cross-border impact. After all, internet traffic can be always available on the other side of a state border.<sup>26</sup> Moreover, XS4ALL has around 1650 customers that are located in other Member States besides the Netherlands and that purchase services from it which can be legally intercepted.
- 55 Article 13.6(1) of the Telecommunications Act and the further regulations to implement that provision constitute a restriction on the free movement of services within the meaning of Article 49 of the EC Treaty. As described above, the requirement of enabling legal interception of the equipment at the providers’ own expense and the further regulations regarding the manner in which this must occur keep businesses from becoming active in the Dutch market. The provision of Internet services by businesses which provide similar services in other Member States becomes less attractive. This does not involve a mere theoretical barrier to access, given the substantial costs – explained above – which a starting company wishing to provide Internet services in the Netherlands will also have to incur. Every statutory or other obligation imposed by Member States on businesses to pay a fee or incur costs makes providing services less attractive, thereby restricting the free movement of services.<sup>27</sup>
- 56 That a barrier to providing telephony and Internet services constitutes an impediment to trade between Member States is also obvious for the following reasons. Internet access is partly provided by international companies which are active in several Member States. XS4ALL is a subsidiary of KPN Telecom, which is active in such countries as Belgium and Germany. Moreover, Internet access is becoming an increasingly important medium for conducting inter-State trade. Electronic trade is considered a vital engine for economic growth by the EU and is the subject of a Community har-

---

<sup>25</sup> See, *inter alia*, European Court of Justice, 28 March 1996, Case C-272/94, *Jur.* 1996, p. I-1905, *Guiot*, Finding 15, and European Court of Justice, 29 November 2001, Case C-17/00, *Jur.* 2001, p. I-9445, *Cosster*, Finding 29.

<sup>26</sup> Hijmans recently summarised the case law trend of the European Court of Justice to the effect, as far as internet traffic is concerned, there is no such thing as a purely internal affair of which all relevant aspects take place in a single member state: H. Hijmans, ‘De Europese Unie, verdwijnende grenzen en elektronische diensten’, *SEW* 2004, 52, p. 353. He also explicitly supports the position that internet traffic should always be supposed to involve a relationship with the internal market.

<sup>27</sup> See recently, for example, the judgment of the European Court of Justice of 13 June 2002 in the consolidated cases C-430 and 431/99, *Jur.* 2002, p. I-5235, *Sea Land Service*, Finding 38.

monisation directive.<sup>28</sup> As is well-known, Internet traffic has no concern for national boundaries and traverses the European Union.

- 57 As a fundamental treaty principle, the free movement of services can only be restricted by regulations which are justified by the compelling public interest reasons recognised in the case law of the European Court of Justice and which apply to all persons or businesses engaging in an activity in the territory of the Member State of receipt. A national rule which restricts free movement is, however, only justified if it secures realisation of the stated objective and if the chosen regulation restricting free movement is necessary to realise the stated public interest objective.<sup>29</sup>
- 58 Protecting essential security interests and guaranteeing public order and public security have been recognised in the case law as compelling public interest objectives which may justify a restriction on free movement.<sup>30</sup> XS4ALL recognises that national regulations mandating that providers of electronic communications services make it possible to legally intercept the equipment used may as such fall under the exceptions recognised by the Court of Justice which justify a restriction on free movement. Imposing an obligation on all providers of electronic communications services to make it possible to legally intercept the equipment used may also be necessary for the public interest pursued, and perhaps it is the measure which restricts free movement to the least extent possible. Due to a lack of knowledge regarding the background concerning the Dutch Parliament's choice to impose the obligation and due to a lack of insight into the usefulness which can be expected from alternatives to a complete obligation to enable legal interception, XS4ALL disputes that this obligation is consistent with the proportionality principle. In any event, this applies to the manner in which the State has implemented the obligation in practice. As explained above, alternatives to the further regulations to implement Chapter 13 of the Telecommunications Act exist (more restricted, more transparent, more timely alternatives) which can achieve the public interest objective pursued while demanding a smaller investment by the businesses concerned and therefore restricting free movement less than the current regulations.
- 59 There is, however, no ground for justification recognised in the European Court of Justice's case law for the Dutch Parliament's choice to make the providers of electronic communications services pay for the costs of enabling legal interception as laid down in Article 13.6(1) of the Telecommunications Act. On the contrary, the Court of Justice has repeatedly stated that purely financial considerations of Member States cannot justify a restriction on free movement.<sup>31</sup> In this connection, reference can be

---

<sup>28</sup> Directive 2000/31/EC.

<sup>29</sup> Cf. Kapteyn/VerLoren van Themaat, *Het recht van de Europese Unie en van de Europese Gemeenschappen* [European Union and European Community law], 6th edition, Deventer, the Netherlands, 2003, p. 546; Oliver, *Free Movement of Goods in the European Community*, 4th edition, London 2003, § 8.01.

<sup>30</sup> See, for example, the ruling in the *Sea Land Service* case, cited above, Finding 41, and the references in it.

<sup>31</sup> See European Court of Justice, 3 October 2002, Case C-136/00, *Jur.* 2002, p. I-8147, Finding 56; European Court of Justice, 16 July 1998, Case C-264/96, *Jur.* 1998 p. I-4695, Finding 28; European Court of

made to the following finding of the Court regarding application of the former Article 36 of the EC Treaty (now Article 30 of the Treaty, which states which exceptions Member States may make to the free movement of goods):

*In particular, Article 36 cannot be relied on to justify rules or practices which, even though they are beneficial, contain restrictions which are explained primarily by a concern to lighten the administration's burden or reduce public expenditure, unless, in the absence of the said rules or practices, this burden or expenditure clearly would exceed the limits of what can reasonably be required.<sup>32</sup>*

- 60 The Explanatory Memorandum to Article 13.6(1) of the Telecommunications Act and the GSM Legal Interception Act shows that the shifting of investment, operating and maintenance costs for legal interception is solely based on the concern of limiting government expenditure. A public interest need or reason is not stated as to why the costs could not be borne by the State. None of the recognised exceptions to the prohibition on restrictions on free movement of services may therefore serve to justify Article 13.6(1) of the Telecommunications Act. For that matter, the State has never asserted, let alone demonstrated, that the amount of the costs which it would have to bear in repealing Article 13.6(1) of the Telecommunications Act clearly would exceed the limits of what can reasonably be expected. After all, what can reasonably be required, in the State's view, of a few providers of public telecommunications services can in any event be expected from the State itself as well.
- 61 Even if, with regard to shifting costs related to facilitating legal interception, the State could invoke an exception recognised by Community law which justifies a restriction on free movement – which, as explained, is not the case – the scheme still must otherwise be proportionate. The provision that the costs of enabling legal interception must be paid fully by the providers concerned and the further regulations to implement that provision are, however, neither necessary to achieve the objective pursued (creating the possibility of legal interception), nor are they the measures which restrict free movement the least.
- 62 The envisaged legitimate objective in this case is to enable investigation of criminal offences, not reduce the budget deficit. The envisaged objective can be achieved with a measure which restricts free movement less: if the State pays the costs of enabling legal interception, the interest pursued (enabling legal interception) will not be undermined at all, while entry into the Dutch market will no longer be impeded for providers.

---

Justice, 6 June 2000, Case C-35/98, *Jur.* 2000, p. I-4071, *Verkooijen*; European Court of Justice, 21 November 2002, Case C-436/00, *Jur.* 2002, p. I-10829, *X and Y*; and *Zennati and Gambelli*.

<sup>32</sup> European Court of Justice, 20 May 1976, Case 104/75, *Jur.* 1976, p. 613, *De Peijper*, repeated in, *inter alia*, European Court of Justice, 12 July 1990, Case C-128/89, *Jur.* 1990, p. I-3239, *Commission/Italy*.

## 3.2 Harmonisation to enhance free movement

63 The general rules regarding free movement have been fleshed out further with regard to the electronic communications sector based on harmonisation measures. The measures take into account the public interests pursued by Member States, including facilitating criminal investigation based on legal interception of communications, by indicating within which limits Member States may supplement the harmonised regulations for the sector – which also guarantee free movement within the Community and establish a ‘level playing field’ for service providers in the Community – through adoption of regulations to protect those interests.

### 3.2.1 Authorization Directive 1997<sup>33</sup>

64 The fourth paragraph in the Preamble to the Authorization Decree 1997 read:

*Whereas conditions attached to authorizations are necessary in order to attain public interest objectives to the benefit of telecommunications users; whereas under Articles 52 and 59 of the Treaty, the regulatory regime in the field of telecommunications should be compatible and consistent with the principles of freedom of establishment and freedom to provide services and should take into account the need to facilitate the introduction of new services as well as the widespread application of technological improvements; whereas, therefore, general authorization and individual licensing systems should provide for the lightest possible regulation compatible with the fulfilment of applicable requirements; whereas Member States should not be required to introduce or maintain authorization schemes, in particular where the provision of telecommunications services or the establishment and/or operation of telecommunications networks is not subject to an authorization scheme at the date of entry into force of this Directive.*

65 Article 3.2 provided that authorizations could only include the conditions stated in the Annex. These applied, however, “without prejudice to [...] measures taken by Member States in accordance with public interest requirements recognized by the Treaty, in particular Articles [30] and [46], specifically in relation to public morality, public security, including the investigation of criminal activities, and public policy.”

66 Thus, with regard to the permissibility of restrictions on free movement, as developed further in the Authorization Directive 1997, reference was made back to primary Community law during the period that the Authorization Directive was applicable. As explained above, Article 13.6(1) of the Telecommunications Act and the further regulations based on it are not consistent with the Treaty rules concerning free movement of services.

---

<sup>33</sup> Directive 97/13/EC of the European Parliament and of the Council of 10 April 1997 on a common framework for general authorizations and individual licences in the field of telecommunication services, OJ L 117/15.

### 3.2.2 Authorisation Directive 2002<sup>34</sup>

67 The Authorization Directive 1997 was replaced by the Authorisation Directive 2002. According to the third paragraph of the Preamble, the Authorisation Directive 2002 is intended to create a legal framework to ensure the freedom to provide electronic communications networks and services. The Directive provides that Member States must ensure the freedom of businesses to provide electronic communications services and networks. Article 3.2 states that provision of networks and services may not be made subject to a licence, but only to a general, usually statutory, authorisation.<sup>35</sup> Besides the conditions which are attached to this general authorisation, no other specific requirements may be imposed on providers of electronic communications networks and services.<sup>36</sup> In this manner, the Community legislation seeks to guarantee free movement in the electronic communications sector.

68 Article 6.1 of the Authorisation Directive 2002 provides as follows:

*The general authorisation for the provision of electronic communications networks or services and the rights of use for radio frequencies and rights of use for numbers may be subject only to the conditions listed respectively in parts A, B and C of the Annex. Such conditions shall be objectively justified in relation to the network or service concerned, non-discriminatory, proportionate and transparent. [underlining by attorney]*

69 The last sentence is explained in paragraph 15 of the Preamble:

*The conditions which may be attached to the general authorisation and to the specific rights of use should be limited to what is strictly necessary to ensure compliance with requirements and obligations under Community law and national law in accordance with Community law.*

70 Unlike the Authorization Directive 1997, the new Authorisation Directive 2002 includes an explicit reference to enabling legal interception as one of the conditions which may be attached to a general authorisation in accordance with Article 6.1. The list in part A of the Annex mentions under 11:

*Enabling of legal interception by competent national authorities in conformity with Directive 97/66/EC and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

---

<sup>34</sup> Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), OJ L 108/21.

<sup>35</sup> There are special rules, not applicable here, regarding rights of use for frequencies and numbers.

<sup>36</sup> Of course, requirements *can* be imposed which are imposed on all other companies as well, that is, which have nothing to do with the services provided.

- 71 Read together, these provisions make clear that the permissibility of Article 13.6(1) of the Telecommunications Act since the new Directive entered into force is no longer a matter of interpretation of primary Community law but of the interpretation of the Authorisation Directive 2002, specifically, Article 6.1 and Annex A, under 11. These mean that, without violating the Directive, Member States may impose the requirement that it be possible to legally intercept networks if and insofar as that requirement is objectively justified, as well as non-discriminatory, proportionate and transparent.
- 72 The Authorisation Directive 2002 moreover also provides for an exhaustive regulation of the financial conditions that may be imposed on providers. The Annex only mentions two conditions in that regard:
- Financial contributions to the funding of universal service in conformity with Directive 2002/22/EC (Universal Service Directive)
  - Administrative charges in accordance with Article 12 of the Directive.
- 73 Article 12 only deals with administrative charges in connection with regulatory activities.
- 74 Annex A does not mention as a possible requirement to be attached to the authorization that the costs of enabling legal interception be shifted to the providers. The condition cited under 11 also does not provide any latitude for this, because the cost shift under Article 13.6(1) does not satisfy the requirements of Article 6.1 of the Authorization Decree. Such a cost apportionment does not satisfy the demands of objective justification and proportionality. It impedes competition with providers from other member states and is therefore at odds with the objective of the Authorisation Directive, i.e. to bolster the free movement of electronic communication services by setting strict limitations in a harmonised manner on the conditions member states may impose on providers. With a policy that is aimed at creating as few barriers as possible to providing electronic communications services and only imposing conditions which are of the utmost necessity. This does not include the obligation that the providers themselves pay the costs of enabling legal interception. There is no objective justification, let alone necessity, for this.
- 75 The proportionality requirement has not been satisfied, as is evident from the mere fact that no consideration was ever given to the possibility of achieving the aim of legal interception capability without making the providers pay for all or part of the costs. It has been neither argued nor shown that Article 13.6(1) of the Telecommunications Act renders the investigation of criminal acts more effective, or that it in fact aims to achieve that.
- 76 Because the amount of the costs which providers must incur depends to a far-reaching extent on functional and technical specifications imposed in delegated regulations, Article 13.6(1) of the Telecommunications Act, as fleshed out further in

the implementation regulations, likewise does not meet the requirement of transparency. The costs cannot be estimated properly and are impossible to predict.

- 77 Thus, although the Authorisation Directive 2002 allows latitude for requiring providers to enable legal interception of their networks and services, the Directive does not allow this obligation to be paid for by those providers. Article 13.6(1) of the Telecommunications Act therefore violates the aim and the text of the Authorisation Directive 2002.
- 78 If the State were to take the position that the Authorisation Directive 2002 does provide latitude for Article 13.6(1) of the Telecommunications Act, then it would be wrong, because the Authorisation Directive itself would then be contrary to the free movement of services guaranteed by the EC Treaty. Specifically, secondary Community law must be interpreted and applied in accordance with primary Community law, which, after all, it fleshes out, *and* the Community legal principles to be discussed below.<sup>37</sup>
- 79 The entry into force of the Authorisation Directive 2002 not only meant another basis for the non-binding nature of Article 13.6(1) of the Telecommunications Act, but also a more stringent criterion against which the Dutch provision must be validated, because Article 6.1 of the Authorisation Directive 2002 curtails the existing exceptions under the EC Treaty.<sup>38</sup>
- 80 The Authorisation Directive 2002 is part of a package of harmonisation directives for the electronic communications sector that consists of a Framework Directive (2002/21/EC) and several specific Directives: the Access Directive (2002/19/EC), the Authorisation Directive (2002/20/EC), the Universal Service Directive (2002/22/EC) and the Privacy Directive (2002/58/EC).
- 81 The cited condition regarding legal interception from the Annex to the Authorisation Directive 2002 mirrors Article 15 of the Privacy Directive, which provides that restrictions on the scope of a number of provisions of the latter Directive are possible, provided they are embedded in law, ('Member States may adopt legislative measures') if they are necessary, appropriate and proportionate within a democratic society to safeguard a number of public interests which are then listed. What is done here in fact is that the review of Article 8 (2) of the ECHR is being introduced into European telecommunications law.

---

<sup>37</sup> European Court of Justice, 27 January 1994, Case C-98/91, *Jur.* 1994, p. I-223, *Herbrink*, and European Court of Justice, 10 July 1991, Case C-90/90, *Jur.* 1991, p. I-3617, *Neu*.

<sup>38</sup> Moreover, under Article 10 of the EC Treaty, as from the time it became clear to the Netherlands that the new Authorisation Directive would regulate this subject matter exhaustively, the Netherlands should have taken that into account and should have refrained from enacting conflicting measures. That point in time came on 12 July 2000, when the Commission draft of the new Authorisation Directive was published and it was clear that the new Authorisation Directive provided for complete harmonisation, with regard to legal interception as well. In any event, it was clear that Article 13.6(1) of the Telecommunications Act would conflict with the Authorisation Directive on 7 March 2002, when the Directive was adopted.

- 82 Accordingly, the question whether a Member State may attach a condition with regard to legal interception capability to a general authorisation not only depends on whether it satisfies the conditions of the Authorisation Directive (is mentioned in Annex A, objective justification in relation to the network or service in question, non-discriminatory, proportionate and transparent) but indirectly also on whether the condition satisfies the requirements in Article 8 (2) ECHR. If the condition does not satisfy the requirements of Article 15 of the Privacy Directive (Article 8 (2) ECHR), it cannot be attached to a general authorisation pursuant to the Authorisation Directive either. In that context it is relevant that Member States, pursuant to the Privacy Directive, must oblige providers to take certain measures to protect - briefly put - privacy, which to a certain extent corresponds with the positive obligation of the State under Article 8 ECHR to take measures that guarantee citizens right to respect for their private lives and correspondence (to be discussed below).
- 83 The question whether a restriction is permissible should not be assessed in the abstract but concretely. This requires a look at the effect the scheme as it actually phrased has on the rights and freedoms of citizens as mentioned in Article 8 ECHR, after which the general interest stipulated by the measure and the privacy interests of citizens must be balanced. In that balancing it is important, on the one hand, that the manner in which the burdens are apportioned means that the concrete scheme impedes XS4ALL in offering new and more secure services, while privacy on the internet is, as everybody knows, vulnerable (which sets the internet apart from other communication services and networks) and under the Privacy Directive and Article 8 ECHR, the State is obliged to protect the privacy of citizens on the internet. On the other hand, the objective - legal interception to the extent necessary for prosecution and national security - is also feasible if the State assumes the costs of legal interception capability.

### 3.3 Principles of Community law

- 84 The cited, correct objections of the Council of State to shifting the costs of enabling legal interception to providers mainly related to the fact that providers are treated differently than other private persons, because they must bear the costs for being able to carry out a task which pre-eminently serves the public interest. With this cost apportionment, Article 13.6(1) of the Telecommunications Act also deviates from the principle applicable elsewhere in Dutch law that the costs for carrying out tasks which are pre-eminently a government matter (such as investigating and prosecuting criminal offences) should be paid for by the government and, as a result, from public resources. This rule is also referred to as the principle of *égalité devant les charges publiques*, or the principle of equality in bearing public burdens.
- 85 For example, it is established policy with regard to another government task par excellence, specifically, enforcement and supervision, that the government (as the representative of the public interest) must in principle pay the related costs itself, unless the costs are caused by a private person (for example, 'the polluter pays') or such person stands to benefit personally from the government's action.

### 3.3.1 Principles of Community law

- 86 Article 120 of the Constitution bars Article 13.6(1) of the Telecommunications Act from being reviewed directly against the Constitution or against general principles of Dutch law, like those of proportionality and equality, and more in particular *égalité devant les charges publiques*. Of course, the review prohibition does not apply to the implementation regulations in respect of Chapter 13 of the Telecommunications Act and in particular the additional costs caused by the technical and functional detailing of the obligations of Chapter 13 of the Telecommunications Act. Moreover, the effect of that review prohibition is negated by the fact that the enacted statute can and must be reviewed against other universally binding provisions of conventions and decisions of organisations under international law (e.g. the ECRH, see below) and against European community law (see above). Moreover, that community law includes the unwritten principles of community law, such as the *égalité* principle.
- 87 Principles of community law can be divided into legal principles of community origin and legal principles borrowed from the legal systems of Member States (the so-called *effet à rebours*) that subsequently found their way into community law. The principles of proportionality and equality belong to the former category, while the principles of legal certainty and, again, proportionality, belong to the latter.
- 88 To some extent the principles overlap; the *égalité* principle is derived from the principle of proportionality as well as from the principle of equality.<sup>39</sup> One of the manifestations of the equality principle is the rule that the disproportionately prejudicial consequences – i.e. consequences that are not regular general or business risks and that are borne only by a limited group of citizens or institutions – of a government act or government decision should not be borne by that limited group but should be distributed evenly across the community. This rule entails that afflicting such disproportionate damage with what is in itself a legal government act is unlawful towards the afflicted party.<sup>40</sup>
- 89 The European Court of Justice has explicitly recognised the principle of equality as one of the fundamental principles of community law, of which the various non-discrimination rules in the Convention are “merely a specific enunciation”.<sup>41</sup> The principle of equality in bearing public burdens is a form of the equality principle and the other face of the principle of proportionality: if the public authority shifts a certain disadvantage partly or fully to a certain individual or a limited group, that constitutes a disproportionate burden. Where the disadvantage relates to performing or cooperating with what is by definition a government duty, the *égalité* principle has been violated. Prechal and Heukels note that the *égalité* principle forms an important legal

---

<sup>39</sup> See, among others, S. Prechal and T. Heukels, ‘Algemene beginselen in het Nederlandse recht en het Europese recht: rechtsvergelijking en interactie. Nederlands rapport ten behoeve van het FIDE-congres 1986’, *SEW* 1986, pp. 287–331.

<sup>40</sup> C.f. HR 20 June 2003, *JB* 2003, 223 (*State/Harrida*).

<sup>41</sup> See, for example, ECoJ 21 June 1974, case 2/74, *Jur.* 1974, p. 631, *Reyners* or ECoJ 25 October 1978, case 125/77, *Jur.* 1978, p. 1991, *KSH*.

ground for compensation obligations of the government to the citizen not only in French, German and Dutch law<sup>42</sup>, but also in Community law<sup>43</sup>. Accordingly, the State must comply with that Community principle insofar as it concerns government acts in a field covered by Community law.

- 90 Other principles play a role here as well, such as the principle of proportionality in a narrower sense. Article 13.6(1) of the Telecommunications Act is out of proportion because the aim of the legal interception requirement is to be able to investigate punishable facts, while cost apportionment has nothing at all to do with that and is not necessary for it either. The only intention of Article 13.6(1) of the Telecommunications Act is to save costs. However, such a purely economic justification is not a legitimate aim, as we demonstrated.
- 91 As regards the lack of clarity about the question whether a certain service should be capable of being legally intercepted (and if so, how) Article 13.6 (1) of the Telecommunications Act also violates the principle of legal certainty, which, according to the European Court of Justice, “belongs to the general principles recognised in Community law”.<sup>44</sup>

### 3.3.2 Application of the *égalité* principle

- 92 Damage which falls outside the normal business risk and which burdens a limited group of citizens or institutions is therefore disproportionate. In other words, government acts which are lawful in themselves become unlawful when there is no compensation of costs for those specially affected. The same logic applies to Articles 13.1 and 13.6 of the Telecommunications Act: the requirement of enabling legal interception is perhaps itself not unlawful, but becomes so because the providers themselves must bear the costs according to Article 13.6(1) of the Telecommunications Act. The lack of a compensation scheme for disproportionate damage suffered by a limited group of companies is itself sufficient to constitute unlawfulness.
- 93 Article 13.6 of the Telecommunications Act is clearly damage falling on a limited group of companies, namely, providers of public telecommunications networks and services. That damage also falls outside the normal business risk of such a provider. Although the requirement of enabling legal interception can by definition only fall on the providers themselves, there is no justification or need for the fact that the costs only fall on those providers. As evidenced by the legislative history cited, the State has not formulated any other specific justification for Article 13.6(1) of the Telecommunications Act besides ‘budgetary considerations’, which, by law, cannot be a relevant justification. The disproportion of the disadvantage suffered by providers like XS4ALL is increased by the fact that they themselves do not benefit in any way from

---

<sup>42</sup> as well as in Austrian law (see below).

<sup>43</sup> Prechal and Heukels, ‘Algemene beginselen in het Nederlandse recht en het Europese recht’, *op. cit.*, p. 305.

<sup>44</sup> ECJ 13 January 2004, case C-453/00, *Kühne & Heitz*, AB 2004, 58, § 24.

their investments in legal interception capability, which concerns facilities that have no useful other function, nor benefit the market dynamic in any other way.

- 94 Relevant in this regard as well is that XS4ALL entered the market before the requirement of enabling legal interception (at the provider's own expense) was stated in the law. When it entered the market in 1993, there was no legal interception requirement in place for internet traffic and as regards telephony - which, conversely, had to be capable of being legally intercepted - the government paid the expense of legal interception. When XS4ALL entered the market, it did not know (and could not know) that it would have to provide legal interception capability for its service by 15 April 2001 at its own expense.
- 95 For that matter, it would be wrong to think that every provider that entered the market after the requirement of enabling legal interception had been introduced was aware of this requirement and, as a result, could not invoke the *égalité* principle. Under such reasoning, all damage caused by the State, however disproportionate and objectively unreasonable, would be lawful if it was merely announced ahead of time. The murder committed in García Márquez's novel *Chronicle of a Death Foretold* was no less punishable because it had been announced in advance.
- 96 An important distinction must be made between the costs of enabling legal interception and costs for *supervision* and *enforcement* which, under Chapter 16 of the Telecommunications Act, are also borne in part by the providers, because this is specifically based on the idea that the market participants themselves also have a real personal interest in - and often benefit from - such supervision. The same held true, for example, for the reorganisation of the pork sector<sup>45</sup> and fish sector,<sup>46</sup> intended to revitalise these industries. In the Explanatory Memorandum to Article 16.1 of the Telecommunications Act, the State puts it that:

*Passing on entrance and enforcement costs is - just as in the current legislation - of considerable importance with regard to implementation of the bill in question. An important argument favouring this is that a citizen or company may be expected to have a certain interest in or benefit from the entrance and enforcement activities to be carried out by the government.*

[...]

*Entrance and post-entrance costs may be charged to private persons, because there is an individual benefit which can be imputed. The proposed Article 16.1 assumes this as well. The picture is more complex in nature with respect to passing on 'preventive and repressive' enforcement costs. These costs should not in principle be charged to citizens and companies,*

---

<sup>45</sup> Supreme Court, 16 November 2001, *JB* 2002, 2, with Comment AWH and Supreme Court, 14 June 2002, *NJ* 2003, 689, with Comment HJS.

<sup>46</sup> European Court of Justice, 10 July 2003, Case C-20/00, *Jur.* 2003, p. I-7411, *Booker*, *NJ* 2004, 147, with Comment MRM.

*particularly not because enforcement cannot be imputed individually and the individual benefit is difficult to determine. Under the circumstances indicated in the working group's report, however, an exception can be made to this principle. The circumstances referred to in the report are present with regard to the telecommunications legislation, especially given the fact that there is in principle a limited number of parties which have a benefit specifically imputable to them from the enforcement activities carried out by the government. In any event, it is indicative that the telecommunications legislation can indeed be characterised above all as regulation intended to organise markets.<sup>47</sup>*

- 97 This text is remarkable, as it provides the context in which the facts were weighed – the same context that is abandoned so spectacularly in Article 13.6(1) of the Telecommunications Act. Making legal interception capability mandatory is not a market-organising provision but a prosecution and security tool. Article 13.6(1) of the Telecommunications Act is all the more remarkable in the light of the Further Memorandum of Reply, in which the Minister, in response to questions from the Upper House concerning Article 16.1 of the Telecommunications Act, emphasised that costs incurred in connection with repressive criminal enforcement are, without exception, not to be passed on to market parties. According to the Minister, such costs fell outside the scope of the proposed compensation regime and were therefore to be financed from public resources.<sup>48</sup> These considerations cannot be reconciled with the justification cited, from the same Explanatory Memorandum, for Article 13.6(1) of the Telecommunications Act (budgetary discretion). After all, providers obtain *no* individually imputable benefit from enabling legal interception. They have absolutely no interest of their own, besides the public interest in security which the rest of society has, too. The associated “costs should not in principle be charged to citizens and companies, particularly not because enforcement [of criminal law] cannot be imputed individually and the individual benefit is difficult to determine.”

### 3.3.3 Review of enacted statutes against principles of Community law

- 98 One of the functions of the Community legal principles is as a supplemental standard for validating the *de facto* or legislative acts of the Community itself. Thus, Article 5, paragraph 3, of the EC Treaty articulates as the proportionality principle that the action by the Community must not go beyond what is necessary to achieve the objectives of the Treaty.
- 99 Another function of the Community legal principles which is especially relevant here concerns standardising the content and manner of applying national statutory measures.<sup>49</sup> In applying Community law, the national court must review the enacted stat-

<sup>47</sup> *Parliamentary Documents II*, 25533, No. 3, pp. 132-133.

<sup>48</sup> *Parliamentary Documents II*, 25533, No. 309d, pp. 20-21.

<sup>49</sup> See S. Prechal and T. Heukels, ‘*Algemene beginselen van gemeenschapsrecht als toetssteen voor nationale wetgeving* [General Principles of Community law as Touchstone for National Legislation]’, *RegelMaat* 1987, pp. 15-21.

ute against unwritten principles of Community law. This means, *inter alia*, a review under unwritten Community law, notwithstanding Article 94 of the Dutch Constitution. According to the Dutch Supreme Court, that provision prohibits a review against unwritten principles of international law, but, not against unwritten principles of Community law. Articles 93 and 94 of the Constitution play no role in the event of violation of Community law.<sup>50</sup>

- 100 In this manner, too, Article 120 of the Constitution, which would prevent review of enacted statutes against general legal principles, is left out of the picture. All of this is a consequence of the supremacy of Community law.<sup>51</sup> In the Belgian VAT case *Belgocodex*, the European Court of Justice found:

*26. It must be recalled in this regard that the principle of protection of legitimate expectations and the principle of legal certainty form part of the Community legal order and must be observed by the Member States when they exercise the powers conferred on them by Community directives. However, in the specific circumstances of the present case, it is not for this Court but for the national court to determine whether a breach of those principles has been committed by the retroactive repeal of a law in respect of which the implementing decree was never adopted. [underlining by attorney]<sup>52</sup>*

- 101 The requirement of reviewing national measures against the written and unwritten principles of Community law also follows from the Community allegiance obligation under Article 10 of the EC Treaty: a national measure, whether it be an administrative act, judicial decision or legislation, which is inconsistent with a Community legal principle cannot be maintained.<sup>53</sup>
- 102 The principles apply to the Member States when they act within the scope of application of Community law. This is obvious when they act to effect or apply Com-

<sup>50</sup> See HR 2 November 2004, LJN no. AR1797 and Tom Barkhuysen, Henk Griffioen & Wim Voermans, 'Artikelen 93 en 94 Grondwet volgens Hoge Raad niet van belang voor doorwerking EG-recht', *NJB* 2004 no. 44.

<sup>51</sup> See Prechal and Heukels, 'General Principles of Community law as Touchstone for National Legislation', p. 21, and J. H. Jans, R. de Lange, S. Prechal and R. J. G. M. Widdershoven, *Inleiding tot het Europees bestuursrecht* [Introduction to European Administrative Law], AAe Libri, Nijmegen, the Netherlands, 2nd edition (2002), p. 159. Cited with approval by Advocate General Wattel in his Advisory Opinion to the Supreme Court, 28 February 2001, *BNB* 2001, 198c, with Comment Kavelaars. For validation of Enacted statutes against Community legal principles by the administrative court, see, *inter alia*, Judicial Division of the Council of State, 4 December 1990, *AB* 1991, 687, with Comment Sewandono. With regard to the supremacy of Community law over the national law of the Member States, see C. A. J. M. Kortmann, *Constitutioneel recht* [Constitutional Law], 4th edition, Deventer 2001, p. 120, and the sources referred to there, including European Court of Justice, 15 June 1964, Case 6/64, *Jur.* 1964, p. 1141, *Costa/ENEL*. The supremacy principle is codified in Article 1-6 of the Treaty establishing a Constitution for Europe to be signed in October 2004 (unofficial consolidated text available via <http://ue.eu.int/igcpdf/nl/04/cg00/cg00087.nlo4.pdf>).

<sup>52</sup> European Court of Justice, 3 December 1998, Case C-381/97, *Jur.* 1998, p. I-8153, *Belgocodex*, *BNB* 1999/29, with Advisory Opinion Alber and Comment Van Hilten, *FED* 1999/559, with Note Verver; repeated in European Court of Justice, 8 June 2000, Case C-396/98, *Jur.* 2000, p. I-4279, *Schlossstrasse*.

<sup>53</sup> See, *inter alia*, Prechal and Heukels, 'General Principles of Community law as Touchstone for National Legislation', p. 21.

munity law, for example, in implementing a directive or applying a regulation.<sup>54</sup> Member States also act within the scope of application, however, when they take a measure which impedes free movement and is defended by the Member State with a Community-based ground for justification such as, in this case, protecting essential security interests and guaranteeing public order and public security.<sup>55</sup> The latter situation applies, so that Article 13.6(1) of the Telecommunications Act also must be validated against those principles. The result of that validation, as stated before, is that this provision is invalid.

## 4 CONFLICT WITH THE ECHR

### 4.1 First Protocol to the ECHR

103 Article 1 of the First Protocol to the ECHR states:

*Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.*

*The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties.*

#### 4.1.1 Possessions

104 ‘Possessions’ within the meaning of Article 1 of the First Protocol has an autonomous meaning which is not limited to possession of physical goods: other rights and interests constituting benefits can also be viewed as rights of possession.<sup>56</sup> The criteria are that the right or interest has economic value, that it can be determined objectively and, further, that the existence of the right or interest can be proven convincingly. The investments at issue here are mandatory, so the possessions in question pertain to money.

105 According to the case law of the European Court of Human Rights, Article 1 of the First Protocol includes three rules which are related to each other. The first rule entails a person’s right to “peaceful enjoyment of his possessions”. The second rule protects against deprivation of possessions, except if this is in the public interest and satisfies the conditions provided for by law and the general principles of international

---

<sup>54</sup> See the sources in Jans *et al*, *op. cit.*, p. 159, Comment 22.

<sup>55</sup> See European Court of Justice, 18 June 1991, Case C-260/89, *Jur.* 1991, p. I-2925, *ERT*, and European Court of Justice, 4 October 1990, Case C-159/90, *Jur.* 1991, p. I-4685, *Grogan*.

<sup>56</sup> European Court of Human Rights, 23 February 1995, Series A 306-B (*Gasus Dosier- und Fördertechnik*); European Court of Human Rights, 16 September 1996, *RJ&D* 1996-IV, Vol. 14 (*Matos e Silva*).

law. These two rules are included in Article 1, first paragraph, of the Protocol. The third rule, set forth in Article 1, second paragraph, of the Protocol, recognises that the Member States are entitled to control the use of property in the general interest.

106 From the connection between the rules in paragraph 1 and the rule in paragraph 2, the European Court of Human Rights has inferred that the statutory rules controlling the use of property must satisfy the requirement of proportionality between the objective of the regulation and the damage attached to the restriction placed on the use of the property. The second rule provides that deprivation of rights of possession will only be possible in exchange for compensation assured ahead of time, leaving aside exceptions. As interpreted by the European Court of Human Rights the third rule can also necessitate granting compensation, so as to create a ‘fair balance’ in this way. The ‘fair balance’ requirement demands the existence of a reasonable measure of proportionality between the means used and the objective pursued, or in other words, between the interests of society and those of protecting the fundamental rights of the individual. That requirement is not met in the case of an individual burden which is excessive for the person concerned.<sup>57</sup>

#### *4.1.2 Disproportionate regulation of the use of possessions*

107 Article 13.6(1) of the Telecommunications Act must be regarded as an individual and exceptional burden. Specifically, in connection with the requirement of enabling legal interception in Article 13.1 of the Telecommunications Act, Article 13.6(1) of the Telecommunications Act requires providers such as XS4ALL to invest and keep investing at their own expense in technical facilities used solely for the public interest. That obligation encompasses a required use of property (the providers’ own financial resources) to develop, purchase, install, staff and maintain technical legal interception systems as well as a restriction on the use of the technical facilities which XS4ALL possesses and of which the facilities for providing legal interception capability are a mandatory part.

108 Article 13.6(1) is not proportionate. There is no reason, aside from a budgetary one, why the providers should pay for making it possible to legally intercept their facilities. They do not benefit from legal interception capability, nor are they guilty of a problem for which enabling legal interception is a remedy. The ‘fair balance’ can only exist if the providers, though required to enable legal interception of their facilities in the public interest, nevertheless receive compensation for all the costs incurred by them in this respect.

#### *4.1.3 Deprivation of possessions*

109 Article 13.6(1) of the Telecommunications Act should not only be regarded as an unjustified regulation of property, but even as a deprivation of possessions. After all,

---

<sup>57</sup> As summarised in Supreme Court, 16 November 2001, *NJ* 2002, 469; *JB* 2002, 2, with Comment AWH, Legal Finding 6.2.2, and the case law of the European Court of Human Rights cited there.

providers are required to spend a substantial portion of the capital available to them on enabling legal interception, something on which they would not spend that capital on their own initiative. The mandatory expenditure of one's own money on something which is only desired by someone else and is only used by that other person is equivalent to handing over one's own money to that person. According to Article 1 EP, deprivation of possessions is only permitted if and when (1) in the public interest, (2) proportionate and (3) by or pursuant to the law.

- 110 That legal interception capability can serve the public interest is not being disputed here. What is being disputed is the cost scheme of Article 13.6(1) of the Telecommunications Act. The public interest is not served by providers of telecommunication services and networks bearing the costs of legal interception measures to be taken in the public interest themselves. The mere fact that such a scheme benefits the Treasury financially is not an argument. Parliamentary records show, however, that no other argument exists.
- 111 As regards proportionality and the requisite 'fair balance' in case of deprivation of possessions, the ECHR has always made quite clear that compensation is, in principle, required.

*Compensation terms under the relevant legislation are material to the assessment whether the contested measure respects the requisite fair balance and, notably, whether it does not impose a disproportionate burden on the applicants. In this connection, the taking of property without payment of an amount reasonably related to its value will normally constitute a disproportionate interference and a total lack of compensation can be considered justifiable under Article 1 only in exceptional circumstances. Article 1 does not, however, guarantee a right to full compensation in all circumstances, since legitimate objectives of "public interest" may call for less than reimbursement of the full market value.<sup>58</sup>*

- 112 In this case, providers receive no compensation whatsoever for their required investments. There are no exceptional circumstances justifying such a deprivation of possessions. The small payments which providers receive under Article 13.6(2) of the Telecommunications Act for carrying out individual burdens cover only the individual costs and are not, therefore, compensation for the required investments. Even if they should be regarded as such, no "legitimate objectives of public interest" have been asserted or are present which would necessitate compensating less than the full market value of the possessions that were taken away, given that such objectives, according to the ECHR, pertain to economic reform or measures against social inequality<sup>59</sup>.

---

<sup>58</sup> ECHR 9 December 1994, Series A no. 301-A, Holy Monasteries/Greece, § 71.

<sup>59</sup> See, for example, ECHR 21 February 1986, Series A no. 98, James and ECHR 8 July 1986, Series A no. 102, Lithgow.

113 A recent application of Article 1 of the First Protocol with respect to the validation of an Act of the Dutch Parliament concerned a case regarding the authority of shipping brokers. In that ruling, the Dutch Supreme Court found that, insofar as there is a deprivation of property, the State's right to control the use of property does not change the fact that such a deprivation without compensation violates the right guaranteed in Article 1 of the Protocol to natural and legal persons to peacefully enjoy their possessions, if there is no reasonable balance between the impairment of that right and the objective envisaged with the deprivation measure.<sup>60</sup> It has already been noted with respect to the situation at hand that the objective envisaged with the deprivation measure is nothing more and nothing less than saving tax money. That is not even a legitimate objective in itself, while the small positive effect that Article 13.6(1) of the Telecommunications Act has on State finances is disproportionate to the extremely high costs which providers must incur to satisfy the requirements for enabling legal interception under the Telecommunications Act.

#### 4.2 Article 10 of the ECHR

114 It has already been argued above (§ 46 et seq.) that various services that could enhance the reliability and confidentiality of communications are being delayed or not offered at all because of the high and uncertain costs of legal interception capability, which costs are borne by the providers according to Article 13.6(1) of the Telecommunications Act.

115 Article 10 ECHR provides:

*1 Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*

*2 The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

116 It may be assumed that XS4ALL may derive rights from Article 10 ECHR in the context of its professional activities. Internet services seem without any question to be means for freedom of expression within the meaning of Article 10 ECHR. The ECHR's

---

<sup>60</sup> Supreme Court, 14 April 2000, AB 2001, 135, with Comment T. A. van Kampen, JB 2000, 196, with Comment B. van den Berg (*Kooren Maritiem/State*). The Supreme Court referred to the European Court of Human Rights, 9 December 1994, Series A, No. 301-A, *Holy Monasteries/Greece*, § 70-71.

judgments in *Lentia* and *Autronic* show that the protection of Article 10 ECHR is not confined to the content and use of information, but also covers the access to and use of means of communication, including telecommunication. In the *Autronic* judgment, the ECHR found that:

*Article 10 applies not only to the content of information, but also applies to the means of transmission or reception since any restriction on the means necessarily interferes with the right to receive and impart information.*<sup>61</sup> [underlining attorney]

- 117 In the *Antelecom* judgment, the Dutch Supreme Court extrapolated the consequences of the technological developments – which are causing the traditional distinction between broadcasting and telecommunications to disappear – and considered Article 10 ECHR to apply to access to the telephony network.<sup>62</sup> This leads to the conclusion that internet services, including internet access services, constitute means for freedom of expression and that an internet provider like XS4ALL may derive rights from Article 10 ECHR in the context of its professional activities.
- 118 These rights are affected directly by Article 13.6(1) of the Telecommunications Act. The effect of the obligation of legal interception capability, in combination with the obligation to bear the related costs, is that confidential and reliable communication technologies are not made available or less quickly. The ECHR looks straight through outward appearances and formalities to the real position of the individual citizen.<sup>63</sup> According to established case law of the ECHR, rights pursuant conventions must be construed such that they give the citizen practical and effective guarantees. “Hindrance in fact can contravene the Convention just like a legal impediment.”<sup>64</sup>
- 119 As the effect of Article 13.6(1) is to impede access, the scheme should also reviewed under the requirements of the second paragraph of Article 10 ECHR. In that regard, the ECHR assumes a fixed review framework comparable to that of Article 8 ECHR: provided by law, necessary in a democratic society, to safeguard certain public interests. In the present case, the main question is whether the scheme as it has been given shape concretely and as it is being applied to XS4ALL is necessary in a democratic society. It should be established in that context whether there is a ‘pressing social need’ and whether the measure is proportionate.<sup>65</sup> The State has not argued – nor is it likely – that it is necessary in a democratic society for providers of telecommunication networks and services to bear the costs of legal interception capability themselves. This is evident, among other things, from the fact that the State did bear the costs of legal interception capability of the telephony network for decades.

---

<sup>61</sup> ECHR 22 May 1990, NJ 1991, 740 (*Autronic*); ECHR 24 November 1993, NJ 1994, 559 (*Lentia*).

<sup>62</sup> HR 26 February 1999, NJ 1999, 716 with comment EJC (*Antelecom*)

<sup>63</sup> Van Dijk & Van Hoof 1998, p. 74.

<sup>64</sup> ECHR 9 October 1979, NJ 1980, 376, with comment E.A. Alkema (*Airey*)

<sup>65</sup> ECHR 26 April 1979, Series A 30 (*Sunday Times*).

- 120 In the context of the proportionality review several issues play a role. The State must make an acceptable case for the necessity of the restriction (i.e. it should adduce 'relevant and sufficient reasons'). With respect to the argument of a reduction of the budgetary burden to justify a restriction, reference is made to a judgment of the Dutch Supreme Court of September 2002 regarding the Antillean broadcasting monopoly. In that judgment, the Supreme Court held that financial considerations as such do not suffice to restrict fundamental rights.<sup>66</sup>
- 121 Pursuant to the ECHR, the State not only has negative obligations but also positive obligations to do what is necessary to protect the freedoms of its citizens. The ECHR derived positive obligations not only from Article 8 ECHR,<sup>67</sup> but also from Article 10 ECHR<sup>68</sup>. Both articles are relevant to this case. On the basis of the ECHR case law regarding Article 8 ECHR, it may be concluded that the state has the positive obligation to guarantee the confidentiality of citizens' communications on the internet. On the basis of Article 10 ECHR, the state has a positive obligation to guarantee the availability of means of communication.
- 122 In the context of reviewing whether a restriction is necessary in a democratic society, these positive obligations play a significant role.<sup>69</sup> 'The Convention must be interpreted as a whole.' The fact that internet communications are vulnerable from the point of view of privacy means that the state's positive obligations to take measures to protect the privacy, or at any rate to support the measures taken by parties like XS4ALL to protect privacy in the shape of newer, more secure services, should be given more significance when weighing the interests involved. The availability of such technologies stimulates the freedom of expression because it allows people who would otherwise be silent for fear of repression to communicate. Besides, on the basis of Article 10 ECHR the State should, in principle, facilitate the freedom of expression, inter alia by making it possible to introduce new services.
- 123 Basically, then, this case is about the following. By in fact impeding the introduction of new services, the State restricts the freedom of expression that XS4ALL, as a provider of communication services, is entitled to derive rights from. In the context of the necessity issue, the burden the current scheme represents for XS4ALL and the prejudicial effect of the current scheme for the freedoms of citizens (Articles 8 and 10 ECHR) for which the State is responsible must be weighed against the State's financial interest. The conclusion is that Article 13.6(1) of the Telecommunications Act does not survive such a review because a) financial considerations in and of themselves cannot justify a restriction; b) with the current scheme, the State ignores its

---

<sup>66</sup> HR 20 September 2002, NJ 2004, 148.

<sup>67</sup> ECHR 13 June 1979, Series A. 31 (*Marckx*); NJ 1980, 463, with comment E.A.A. ECHR 9 October 1979, Series A. 32 (*Airey*) ECHR 7 July 1989, Series A. 160, NJ 1991, 659, with comment E.J. Dommering (*Gas-kin*). ECHR 26 March 1985, Series A. 91 (*X & Y v. Nederland*). ECHR 9 December 1994, Series A. 303-C (*Lopez Ostra*); ECHR 24 June 2004, *Mediaforum* 2004-7/8, no. 24, with comment G.A.I. Schuijt (*Caroline von Hannover*). ECHR 19 February 1998, RJ&D 1998-1 (*Guerra*).

<sup>68</sup> ECHR 16 March 2000, RJ&D 2000-III (*Ozgur Gundem*).

<sup>69</sup> See also ECHR 21 June 1988, Series A 139 (*Plattform Ärzte für das Leben*) where positive obligations of the state in weighing the interests of the second paragraph are included.

responsibilities pursuant Articles 8 and 10 ECHR while in fact there is a need on the internet for more secure services and, at the same time, the costs for XS4ALL (and its customers) form an unreasonable burden, due to the high amount of those costs, their unpredictability, and the fact that interception of communications is in the interest of society as a whole (rather than XS4ALL or its customers) and should therefore be paid out of state funds.

### 4.3 ECHR and Community law

124 The violation of Article 1 of the First Protocol and Article 10 ECHR that Article 13.6(1) of the Telecommunications Act represents also plays an important role in reviewing Article 13.6(1) of the Telecommunications Act under primary, secondary and unwritten Community law, in addition to what has already been argued in this respect earlier. According to the established case law of the European Court of Justice, the consequences of fundamental rights make themselves felt in European Community law. In this regard, the ECHR has special significance.<sup>79</sup> Article 6.2 of the EU Treaty explicitly characterises the fundamental rights as principles of Community law. Hence, in applying legislation based on European directives, the Member States are not exempted from the obligation in the Community legal structure to respect the fundamental rights. In a ruling from 2003 concerning deprivation of property by seizing fish produced, the European Court of Justice set forth the standard for reviewing a measure arising under primary or secondary Community law against property rights. It found:

*68. However, fundamental rights are not absolute rights but must be considered in relation to their social function. Consequently, restrictions may be imposed on the exercise of those rights, in particular in the context of a common organisation of the markets, provided that those restrictions in fact correspond to objectives of general interest pursued by the Community and do not constitute, with regard to the aim pursued, a disproportionate and intolerable interference, impairing the very substance of those rights.*

125 The crucial difference between this fish case and the case at hand regarding the costs of enabling legal interception has to do with the fact that, in the European Court of Justice's view, the fishermen suffered relatively little damage and, moreover, also benefited from the challenged measure, because it resulted in less disease among the fish and in enabling fishing again in the affected area as soon as possible. In contrast, the providers do not benefit at all from enabling legal interception, or at least no more than any other citizen, to the extent it were to indirectly result in a safer society.

---

<sup>79</sup> European Court of Justice, 10 July 2003, Case C-20/00, *Jur.* 2003, p. I-7411, *Booker, NJ* 2004, 147, with Comment MRM, Legal Finding 65.

## 5 FOREIGN CASE LAW

126 The current action is not the first in which the lawfulness of an obligation on the part of providers to pay for the costs of enabling legal interception themselves is at issue. Because, as already described, the laws of most industrialised nations provide for compensation of these costs, such an action has not been necessary in those countries. Very similar decisions of the highest courts in Austria and France are noted here. A similar case is now pending in Germany.<sup>71</sup>

### 5.1 Austria

127 The Austrian *Verfassungsgerichtshof* determined in its decision of 27 February 2003 (**EXHIBIT E-3**) that the Austrian scheme regarding the costs of enabling legal interception, which is virtually identical to the Dutch one, was unconstitutional. Although the Austrian Constitution is not the same as the Dutch Constitution and the Netherlands does not have a system of constitutional case law, the Austrian decision is based on the same principles of necessity and proportionality which the Dutch court must follow according to Community law and the ECHR.

128 The Austrian Court found that the total exclusion of any form of compensation for the costs of making it possible to legally intercept a network or service was contrary to the equality principle for two reasons. In earlier case law regarding the equality principle, the *Verfassungsgerichtshof* had already determined that, while the mandatory use of private persons to fulfil public-law duties was not in principle objectionable, this did not justify being able to impose obligations to cooperate of whatever nature and intensity, irrespective of quality or scope. The Court then found that intercepting telecommunications in connection with prosecution or national security is essentially a public task. The State must in principle also bear the costs itself and cannot in principle shift these to citizens. The State must have good arguments to do this, with these restrictions being able to survive scrutiny under the equality principle.

129 The Court found that the legislature must observe the proportionality principle (*Verhältnismässigkeitsgrundsatz*) if it wishes to shift burdens which are public (costs of enabling legal interception) to the shoulders of private persons (telecommunications providers). Thus, the legislature must balance interests. In this balancing of interests, it must, on the one hand, take into account the costs faced by the private provider. On the other hand, it must determine specific criteria regarding why this/these private person(s) in particular should have to bear the costs. According to the Court, these criteria may, *inter alia*, consist of the determinability and, therefore, specifically, financial predictability of the performance to be rendered by private parties, the economic reasonableness of the distribution of burdens for the individual proprietor, the interest to be served (which must also be an interest of the proprietors concerned)

---

<sup>71</sup> See <http://www.tkg-verfassungsbeschwerde.de.vu/>. The arguments regarding costs can be found, with sources, via [http://www.tkg-verfassungsbeschwerde.de.vu/beschwerdeschrift\\_tk.pdf](http://www.tkg-verfassungsbeschwerde.de.vu/beschwerdeschrift_tk.pdf), § 3.1.1.2.

and the dangers particularly associated with the proprietor's activities which will be neutralised by the desired cooperation.

- 130 The Court validated the scheme against these points of departure and concluded that the scheme did not withstand validation. The Court attached importance to the fact that the financial burdens for the businesses concerned were very high. It observed that the scope and, hence, costs of the Austrian obligation to provide legal interception capability (just like the Dutch one) could not be determined, because they were not limited by law, but could always be adjusted to the state of the art by the Minister through a regulation (compare the Legal Interception Decree and Legal Interception Regulation in the Netherlands).
- 131 Finally, the Court determined as a matter of principle (and following the points of departure of Community law as outlined above) that budgetary considerations in themselves and by themselves could not provide a sufficient objective justification for the cost apportionment scheme enacted by the legislature here.

## 5.2 France

- 132 In France, a statutory provision comparable to Article 13.6(1) of the Telecommunications Act was introduced in 2000. Article 48 of *de Loi de finances rectificative pour 2000* – the name itself indicates that it was a law aimed at saving costs – provided that providers “*mettent en place et assurent la mise en oeuvre des moyens nécessaires aux interceptions justifiées par les nécessités de la sécurité publique. Les investissements réalisés à cette fin sont à leur charge.*” The law did include an unclear scheme for partial compensation of operating costs: “*L’Etat participe au financement des charges d’exploitation supportées par les opérateurs pour la mise en oeuvre des moyens nécessaires dans des conditions déterminées par décret en Conseil d’Etat.*”
- 133 This provision was declared unconstitutional by the *Cour Constitutionnel* in a ruling on 28 December 2000 (**EXHIBIT E-4**), because it violated the principle of *égalité devant les charges publiques*:

*40. Considérant qu’il est fait grief à cet article par les deux saisines de mettre à la charge des opérateurs la totalité du coût des investissements nécessaires à la pratique des interceptions, ainsi qu’une partie des charges d’exploitation correspondantes; que, selon les requérants, ces dispositions rompent l’égalité devant les charges publiques;*

*41. Considérant que, s’il est loisible au législateur, dans le respect des libertés constitutionnellement garanties, d’imposer aux opérateurs de réseaux de télécommunications de mettre en place et de faire fonctionner les dispositifs techniques permettant les interceptions justifiées par les nécessités de la sécurité publique, le concours ainsi apporté à la sauvegarde de l’ordre public, dans l’intérêt général de la population, est étranger à l’exploitation des réseaux de télécommunications; que les dépenses en ré-*

sultant ne sauraient dès lors, en raison de leur nature, incomber directement aux opérateurs; [underlining by attorney]

- 134 The *Cour Constitutionnel's* reasoning was consistent with what XS4ALL is essentially arguing in this case: although it is understandable that the State desires cooperation from providers regarding legal interception of their network and service, there is no justification for shifting the costs to them. Investigating criminal offences is reserved to the State; it should pay the costs, also if they are incurred by others pursuant to law.

## 6 CLAIMS

### 6.1 Declaratory judgments

- 135 Community law bars a Member State from invoking statutory provisions against citizens which violate Community law. This likewise applies to the ECHR under Articles 93 and 94 of the Constitution.
- 136 As Article 13.6(1) of the Telecommunications Act is inconsistent with primary, secondary and unwritten Community law and with the ECHR, it must be declared non-binding or at least not be applied. Article 6.1 of the Authorisation Decree has been implemented incorrectly by the State, as Article 13.6(1) of the Telecommunications Act was not removed or amended during implementation. Interpretation of Article 13.6(2) of the Telecommunications Act in line with the Directive, such that it also included investment, operating and maintenance costs, might eliminate the inconsistency described, but may not be an obvious step, as it would presumably require an interpretation *contra legem*. Many believe that is not possible, because it would violate the principle of legal certainty<sup>72</sup> or give Directives the effect of Regulations.<sup>73</sup>
- 137 The first declaratory judgment claimed seeks to have Article 13.6(1) of the Telecommunications Act declared non-binding or in any event declared inoperative with respect to XS4ALL. The second declaratory judgment relates to the State's liability. Article 13.6(1) of the Telecommunications Act must be considered unlawful legislation. The State bears liability, including strict liability, in this regard. As a result, XS4ALL is entitled to compensation of the costs which it has incurred in the past and will incur in the future to comply with the requirements in Chapter 13 of the Telecommunications Act.

---

<sup>72</sup> See, inter alia, S. Prechal, *Directives in European Community law*, Oxford 1995, p. 348.

<sup>73</sup> See, *inter alia*, President of The Hague District Court, 7 July 1995, *IER* 1995, 30 (*Novell/America Direct*), Legal Finding 16, and Hague Court of Appeal, 1 June 1995, (*Pink Floyd*), Legal Finding 16.

## 6.2 Damages

138 XS4ALL seeks compensation in these proceedings for the damage it has already suffered and damage it will suffer until Article 13.6(1) of the Telecommunications Act has been repealed, or at least until the law provides for an adequate scheme of compensation for the costs of enabling legal interception. The amount of the damage suffered has already been explained.

## 7 DEFENCE, EVIDENCE AND PROCEDURAL SUGGESTION

139 The State's defence to XS4ALL's specific claims is not known. Recent statements made by Minister Donner to the effect that the costs of implementing the proposed obligation for telecom providers to store traffic data for a period or one or more years should be borne by the providers shows that the State has not changed its position since the introduction of Article 13.6(1) of the Telecommunications Act. Insofar as the State's presumed defence can be inferred from the Parliamentary Documents, such defence has been mentioned and rebutted above.

140 The question whether Article 13.6(1) of the Telecommunications Act violates primary, secondary and unwritten Community law and the ECHR is a question of law, for which it is difficult to put forward evidence. Given that Article 13.6(1) of the Telecommunications Act is a restriction on the EC Treaty's basic assumption of freedom of services, as specifically harmonised in the Authorisation Directive, as well as a restriction on the right of possession as protected by the First Protocol to the ECHR, the State bears the burden of proving the assertion that this restriction is nevertheless permissible.<sup>74</sup> Insofar as required by law and useful, XS4ALL is prepared to furnish evidence for all its assertions, including, in particular, its assertions with respect to the state of affairs concerning the technical and functional implementation of providing legal interception capability and the amount of the investment, operating and maintenance costs for the technical facilities which it has incurred and will incur to comply with Articles 13.1, 13.4 and 13.5 of the Telecommunications Act.

141 Given that the case concerns a fundamental question and that XS4ALL is unaware of the State's specific defence, while that defence can be expected to perhaps be legally complex, XS4ALL suggests to forego a post-defence statement hearing and to first give the parties the opportunity to file a reply and rejoinder.

### IN CONSEQUENCE WHEREOF:

May it please the District Court, by judgment, insofar as possible with immediate effect notwithstanding appeal,

---

<sup>74</sup> Cf. Oliver, *op. cit.*, § 8.11 and European Court of Justice, 8 November 1979, Case 251/78, *Jur.* 1979, p. 3369, *Denkavit Futtermittel II*; European Court of Justice, 19 February 1981, Case 130/80, *Jur.* 1981, p. 527, *Kelderman*.

1. to issue a declaratory judgment that Article 13.6(1) of the Telecommunications Act is non-binding or at least inapplicable, because it violates primary, and/or secondary and/or unwritten Community law and/or the ECHR, more specifically, one or more of the following provisions: Article 6.1 of Directive 2002/20/EC, Article 49 of the EC Treaty, unwritten Community law, Article 1 of the First Protocol to the ECHR, Article 10 ECHR, Article 8 ECHR;
2. to issue a declaratory judgment that the State is liable for the investment, operating and maintenance costs for technical facilities which XS4ALL has incurred and will incur to comply with the obligations of Chapter 13 of the Telecommunications Act;
3. to order the State to pay XS4ALL an amount of EUR 489,293 (in words: four hundred eighty-nine thousand two hundred ninety-three euro) plus statutory interest as from the day this amount becomes due and payable until the date of full payment;
4. to order the Defendant to pay the costs of these proceedings.

The costs for me, bailiff, are

Bailiff

## EXHIBITS

	Date	Description
Exhibit E-1	3 March 2005	Ernst & Young's report regarding the costs incurred by XS4ALL in connection with legal interception
Exhibit E-2	July 2003	Wik Report regarding enabling legal interception in G-7 Countries
Exhibit E-3	27 February 2003	Decision of the Austrian <i>Verfassungsgerichtshof</i> (violation of the proportionality and equality principles)
Exhibit E-4	28 December 2000	Ruling of the French <i>Cour constitutionnel</i> (violation of the <i>égalité</i> principle)