BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

Internal distribution code:
(A) [ ] Publication in OJ
(B) [X] To Chairmen and Members
(C) [ ] To Chairmen
(D) [ ] No distribution

Datasheet for the decision of 12 March 2012

Case Number: T 0002/09 - 3.5.04

Application Number: 02077838.7

Publication Number: 1263240

IPC: H04N 9/16

Language of the proceedings: EN

Title of invention:
Display device

Patentee:
Koninklijke Philips Electronics N.V.

Opponent:
DSM IP Assets B.V.

Headword:
Public availability of an e-mail transmitted via the Internet/PHILIPS

Relevant legal provisions:
ECHR Art. 8
Directive 97/66/EC, Art. 5, 14, 15
RPBA Art. 13(1)

Relevant legal provisions (EPC 1973):
EPC Art. 54(2), 99(1), 100(a)
EPC R. 55(a), 56(1), 76(2)

Keyword:
"Admissibility of a contrived opposition test case (yes)"
"Novelty and inventive step (yes - no public availability of an e-mail transmitted via the Internet)"

Decisions cited:
G 0009/91, G 0010/91, G 0001/92, G 0009/93, G 0003/97, J 0020/85, T 0084/83, T 0328/87, T 0830/90, T 0472/92, T 0952/92, T 0809/95, T 0055/01, T 1081/01, T 1134/06, T 1553/06, T 1875/06, T 1309/07, T 1465/07, T 0426/08
Société Colas Est and others v. France (ECHR, no. 37971/97)
Liberty and Others v. The United Kingdom (ECHR, no. 58243/00)
Von Hannover v. Germany (no. 2) (ECHR, nos. 40660/08 and 60641/08)

Headnote:

1. An opposition filed within the framework of a test case is not inadmissible for that sole reason, provided that the prosecution of the proceedings thereby instituted is contentious because the parties defend mainly opposing positions. (See point 1.3.3)

2. The content of an e-mail did not become available to the public within the meaning of Article 54(2) EPC 1973 for the sole reason that the e-mail was transmitted via the Internet before the filing date of 1 February 2000. (See points 4.6 to 4.8)

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0002/09 **-** 3.5.04

D E C I S I O N
of the Technical Board of Appeal 3.5.04
of 12 March 2012

Appellant: (Opponent)
DSM IP Assets B.V.
P.O. Box 9
6160 MA Geleen (NL)

Representative:
Mooij, Johannes Jacobus
DSM Intellectual Property
P.O. Box 9
6160 MA Geleen (NL)

Respondent: (Patent Proprietor)
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven (NL)

Representative:
Cohen, Julius Simon
Philips
Intellectual Property & Standards
P.O. Box 220
5600 AE Eindhoven (NL)

Decision under appeal:
Decision of the Opposition Division of the European Patent Office posted 24 October 2008 rejecting the opposition filed against European patent No. 1263240 pursuant to Article 101(2) EPC.

Composition of the Board:

Chairman: F. Edlinger
Members: B. Müller
M. Paci
C. Kunzelmann
C. Vallet

Summary of Facts and Submissions

I. The opponent DSM IP Assets B.V. has appealed against the decision of the opposition division rejecting the opposition filed against European patent No. 1 263 240. Mention of the grant of the patent was published on 8 March 2006. That patent, which comprises claims 1 to 3, originated from European patent application No. 02077838.7 filed on 11 July 2002 and published on 4 December 2002. This application was a divisional application of parent application No. 00200326.7 for the subject-matter of claims 5 to 7 removed from the parent application. Pursuant to Article 76(1) EPC 1973, the divisional application and the patent granted from it are deemed to have been filed on the filing date of the parent application, i.e. on 1 February 2000 (hereinafter also referred to as "the filing date"). The title of the invention is "Display device".

II. The parent application was granted as European patent No. 1 006 733. In opposition proceedings that patent was maintained in amended form on the basis of a sole claim which, according to the division, "contains in combination the features of granted claims 1 and 4". Mention of the grant of the patent was published on 16 October 2002. Both parties have appealed against that decision of the opposition division. The reference number of that appeal case before the present board is T 1553/06.

III. An opposition against the patent granted on the divisional application was filed on 6 December 2006. It was based on the ground of lack of inventive step (Article 100(a) EPC 1973) of the subject-matter of each

of claims 1 to 3 in view of certain combinations of prior-art documents I2, C3 (originally labelled C7) and C5. These documents, together with a notarial record pertaining to I2 and referred to as A2, were submitted together with the notice of opposition. Originals of documents I2, C3 and C5 were supplied in the oral proceedings before the board, complemented by originals of notarial records pertaining to these documents. Details of the documents are provided below. New references (starting with the letter T), which the opponent provided in the oral proceedings before the board for the sake of clarification (see table "NEW REF" attached to the minutes), are indicated in brackets.

I2 (T11)
Webpage entitled "Display Device" allegedly found at URL http://www.gironet.nl/home/morozov/CIE/DISPLAY_DEVICE on 12 January 2000, on the basis of the keyword string "THREE CATHODES and PHOSPHOR SCREEN and CONVERGENCE" entered in the AltaVista search engine as a webpage dated "12-1-00" (**T11**), as certified in notarial record **A2** dated 13 January 2000 at the request of DSM N.V. (DSM Patents & Trademarks).

C5
E-mail from Mr. de Vries of AkzoNobel to Mr. Mooij acting for the opponent, sent unencrypted (except, as alleged, for the name of the sender) on 25 January 2000 at 21:44, as certified in a notarial record dated 31 January 2000 at the request of DSM N.V. (DSM Patents & Trademarks).

C3 (originally labelled **C7**)
E-mail from Mr. de Vries (AkzoNobel) to Mr. Mooij (opponent), sent encrypted on 17 January 2000 at 20:45, as certified in a notarial record dated 18 January 2000 at the request of DSM N.V. (DSM Patents & Trademarks).

The documents I2, C5 and C3 were referred to for the first time during the proceedings up to grant of the parent application. During these proceedings the document referred to as I2 above had already been relied on in a letter of 6 October 2000 by DSM N.V. (DSM Patents & Trademarks). That letter had been submitted as third-party observations under Article 115 EPC 1973. I2 was furnished subsequently, on 4 March 2002. Furthermore, in a letter of 10 October 2000, the **applicant** itself had indicated that the subject-matter of both claims 5 and 7 of the application as filed, corresponding to claims 1 and 3 of the divisional application, respectively, had been communicated over the Internet by e-mails C5 and C3 on 25 and 17 January 2000, respectively.

With a letter of 11 March 2011, the opponent also filed non-patent documents O1 to O9 in support of its submissions.

IV. By decision of 24 October 2008 the opposition division rejected the opposition. The division held that out of the documents that the opponent had submitted, i.e. I2, C5 and C3, document I2 was the only available prior art and did not disclose the additional feature of claim 1 or render it obvious. Claims 2 and 3 were dependent on claim 1 and therefore shared its fate. The printout of I2 and the copy of the record of the notary proved that I2 could "even" be found via the search engine AltaVista

and was accessible for a time and in a manner enabling the finder to download and print the document. In contrast, e-mail C5 did not form part of the state of the art. It had not been shown how C5 could be found on the Internet. Furthermore, it could not be concluded from the adoption of Directive 2002/58/EC in 2002 that previous e-mail communication had not been viewed as confidential, especially if the message contained a confidentiality warning as in the present case. For the same reasons the opposition division considered that PGP-encrypted e-mail C3 did not form part of the state of the art. The division also pointed out that public availability of C3 would additionally require that, at the relevant date, the finder could have gained knowledge of its content with the means available to him, which could not be equated with the means at the disposal of the U.S. intelligence service to which the opponent had referred.

V. The board issued a communication pursuant to Article 15(1) of the Rules of Procedure of the Boards of Appeal (RPBA), annexed to a summons to oral proceedings dated 27 December 2010.

Admissibility of the opposition

The board concurred with the conclusion of the opposition division in the decision under appeal that the requirements of Rule 76(2)(c) EPC, in particular an indication of the facts and evidence presented in support of the grounds on which the opposition was based, were met.

The board raised the issue of admissibility of the opposition of its own motion under a different aspect. The board pointed out that the Enlarged Board of Appeal considered opposition proceedings to be contentious in nature. According to the Enlarged Board's ruling in case G 3/97 (OJ 1999, 245) an opposition was inadmissible if the involvement of the opponent was to be regarded as circumventing the law by abuse of process. Such a circumvention of the law arose, in particular, if the opponent was acting on behalf of the patent proprietor.

On the basis of a number of facts arising from the file, the board wondered in parallel appeal case T 1553/06 whether the proprietor and the opponent, possibly in conjunction with one or several other persons, e.g. one Mr. de Vries, professional representative before the EPO, had worked together at the request of the study committee for intellectual property of VNO/NCW (Confederation of Netherlands Industry and Employers) to create a test case regarding the question of whether and, if so, under which conditions, documents placed on the Internet constituted prior art within the meaning of Article 54(2) EPC 1973. In the affirmative, the board said that the contentious nature of the proceedings, being a condition for an opposition to be admissible, might be in doubt.

From certain facts relating to two e-mails C5 and C3 by which the subject-matter of claims 5 and 7 of the application as filed had allegedly been communicated over the Internet, the board concluded that a possible (single) test case might originally have been intended to also encompass the question of whether e-mails transmitted via the Internet constituted prior art

within the meaning of Article 54(2) EPC 1973. This particular issue was being dealt with in the present appeal proceedings.

Substance

The board considered it to be critical for the assessment of novelty and/or inventive step of the subject-matter of the claims at issue to determine whether or not any of documents I2, C3 and C5 allegedly all submitted to the Internet (I2) or transmitted via the Internet (C3 and C5) before the filing date of the patent, constituted prior art within the meaning of Article 54(2) EPC 1973.

The board expressed the view that a document indexed in a public web search engine was, in principle, available to the public. The board tended to acknowledge that I2 was publicly available before the filing date of the patent.

As for C3 and C5, the board invited the opponent to show that e-mail C5 was routed via one or several territories in which it was lawful to intercept it and to disclose its content. The board considered it conceivable to conclude that information that was legally prohibited from being accessed, let alone disclosed, was not publicly available, unless it had actually been disclosed before the filing date. In respect of the allegedly encrypted e-mail C3, the board indicated that, if the opponent believed it could show the above, proof was also required that the 128-bit decryption key was available to the public.

VI. In the oral proceedings held before the board on 11 and 12 April 2011 (during which the parallel appeal case T 1553/06 was also discussed) the parties made the following requests:

The opponent requested that the opposition be declared admissible, that the decision under appeal be set aside and that the patent in suit be revoked. If the opposition and the appeal "are not admitted", the three questions already on file in case T 1553/06 should be referred to the EBA [Enlarged Board of Appeal] and the board's discretion be used to refund the opposition and appeal fees to the opponent. Those questions are attached to the minutes of the oral proceedings in each of the two cases.

The patentee requested that the opposition be rejected as inadmissible, that the appeal be dismissed and the patent maintained in its entirety.

At the end of the oral proceedings the chairman closed the debate and announced that a decision would be given in writing.

VII. The claims of the patent as granted and upheld by the opposition division are as follows.

"1. A display device comprising
- a cathode system (3) including a grid (29) and three cathodes for emitting three separate electron beams (231,232,233), each cathode having an individual electron source (21,22,23),
- a phosphor screen (4) placed opposite the cathodes,

- an electro-magnetic deflection system (6) for scanning at least a part of the phosphor screen (4) with the electron beams (231,232,233) and arranged such that the electro-magnetic deflection system (6) converges the three electron beams (231,232,233) to a single moveable spot on the phosphor screen (4),
- a cathode modulator (5) having a signal input (50) for receiving an analogue electrical video signal and having an output for applying separate modulation voltages to the respective electron sources (21,22,23) of the cathodes (3) relative to the grid (29),

characterised in that

- the cathode modulator (5) is provided with three regulable analogue amplifiers (11,12,13),
- each regulable analogue amplifier (11,12,13) having a signal input for receiving the same analogue electrical video signal,
- each regulable analogue amplifier (11,12,13) having a signal output for supplying one of said modulation voltages,
- each regulable analogue amplifier (11,12,13) having a control input, the amplification ratio of each regulable analogue amplifier being regulable on the basis of a regulating signal applied to the control input of said analogue amplifier (11,12,13) and **in that**
- the cathode modulator (5) is provided with an integrator circuit (17) having an input for receiving the analogue electrical video signal and having an output for supplying said three regulating signals, the integrator circuit (17) being arranged to derive an integrated video signal from the analogue electrical

video signal and to derive the three regulating signals from the integrated video signal
- the integrator circuit (17) having its output coupled to the respective control inputs of the three regulable analogue amplifiers (11,12,13) so as to apply the respective regulating signals to the respective control inputs of the individual regulable analogue amplifiers (11,12,13) and
- the cathode modulator (5) is provided with three regulable voltage supplies (14,15,16), each regulable voltage supply being electrically connected to one of the electron sources (21,22,23) of one of the cathodes (3), each regulable voltage supply having a voltage control input, each regulable voltage supply (14,15,16) being arranged to supply a DC voltage having an adjustable voltage level, each of said voltage levels being dependent on respective voltage control signals applied to the respective voltage control inputs of said respective regulable voltage supply and **in that,**
- the cathode modulator is provided with a DC regulator (18) having an input electrically connected to the output of the integrator circuit (17) and having an output electrically connected to each individual regulable voltage supply (14,15,16),
- the DC regulator (18) being arranged to derive said three voltage control signals from the integrated video signal and that
- the cathode modulator is arranged such that
- the light output (L) at the moveable spot on the phosphor screen corresponds to the signal level (V) of the electrical video signal according to

$$L = (a + bV)^{\gamma}$$

- with γ in the range 3.35 to 4.09, in particular γ having the value 3.72 for at least a first and a second selected value of the signal level of the analogue electronic video signal.

2. A display device as claimed in Claim 1, **characterised in that**
- the first selected value of the signal level of the analogue electronic video signal is in the range between 180mV and 220mV, preferably being equal to 200mV, and
- the second selected value of the signal level of the analogue electronic video signal is in the range between 360mV and 440mV, preferably being equal to 400mV.

3. Use of a display device as claimed in any one of the preceding Claims for inspection of small details with low contrast in monochrome medical images for prolonged periods of time of at least 2 hours."

VIII. The arguments of the appellant/**opponent** are summarised as follows.

Arguments submitted in the statement of grounds of appeal

Claim 1 not inventive in view of I2 and C5

The difference between claim 1 and I2 was the final feature of the claim dealing with the relation between the light output L and the signal level V.

The problem solved by that feature was to provide a display which yielded a brightness distribution that was very comfortable for studying images on the screen (column 7, lines 39-41). The problem of how to improve

comfort of viewing images on a display device was mentioned in C5. C5 described the relationship between the light output L and the signal level V, which for a person skilled in the art of monochromic displays was known as the γ-curve. C5 disclosed that a γ in the range between 3.35 and 4.09 was "very pleasant for a human to watch". The problem, as well as the solution thereto by the final feature of claim 1, was thus disclosed in C5. Accordingly, in order to solve the problem of improving the comfort of viewing, the skilled person would use the gamma curve mentioned in C5 in the display device known from I2. Therefore the subject-matter of claim 1 was not inventive in view of I2 and C5.

Claim 1: public availability of I2 and C5

The remaining questions were whether I2 and C5 were publicly available. Regarding I2, the opposition division had concluded that this document was available to the public before the filing date of the patent in suit based on the facts and arguments given in the opposition.

C5 had been sent by e-mail before the filing date of the patent in suit. The e-mail had been sent over the Internet which was outside the control of both sender and receiver. It was well known that Internet-based mail could, already in 2000, easily have been intercepted. To support this statement, the opponent filed documents D1 through D4, D1 to D3 with the statement of grounds of appeal and D4 shortly thereafter. The documents are as follows:

D1: WildID LLC, Top 10 Places Your Email Can Be Intercepted, 2000, http://security.ngoinabox.org/Documentation/Misc/top10intercept.pdf

D2: AnonIC.org, Data Interception, 2004, http://www.anonic.org/online-security.html

D3: AnonIC.org, Email Security and Anonymity, 2004, http://www.anonic.org/email-security.html

D4: Zwenne, Gerrit-Jan, The Netherlands, Trouble for new Dutch public transport chipcard, Bird & Bird Privacy & Data Protection Update, Issue 15 - March 2008 (extract), http://mail.twobirds.com/ve/ZZ867058NjN7172uD77v/stype=print

The opponent summarised the content of documents D1 to D3 as follows:

- D1 described 10 places where e-mail could be intercepted and that at least a million people in the world had the technical knowledge to intercept Internet-based e-mail.
- D2 explained how data interception could be performed.
- D3 showed one example of how easily e-mail privacy could be compromised. Someone interested in the subject of the invention could easily have selected C5 from the mass of e-mails by using a few keywords, as e-mail traffic could be rated according to keywords.

(As for the content of D4, see end of the present section "Arguments submitted in the statement of grounds of appeal".)

Although publications D1 to D4 might be of a later date than C3 and C5, it was well known that security of the Internet had been even worse in 2000 than it was at the date when the statement of grounds was filed (i.e. on 25 February 2009), as many security updates had been issued since 2000 to avoid interception of e-mail and hacking of computers.

Decision T 444/88 stated that

it is sufficient that the document was in fact available to the public before the priority date of the patent in suit, whether or not this was known by any member of the public, and whether or not any member of the public actually inspected the document.

In determining whether C5 had been made available to the public the question was therefore not whether this particular e-mail C5 had been intercepted, but whether it could have been read. At least one million people could have intercepted C5. The warning that the information was confidential could not be considered as keeping C5 out of public availability, when at least one million persons, not bound by confidentiality, could have intercepted C5.

C5 had therefore to be considered as publicly available.

Claim 2 not inventive in view of I2 and C5

The additional feature of claim 2 was related to the choice of the signal levels of the video signal required for the light output of the phosphor on the screen.

As there was no disclosure in the patent in suit that the extra feature of claim 2 was linked to any particular technical effect over claim 1 and 200 mV and

400 mV were well-known values for signal levels of an analogue electronic video signal, variations around these values represented a routine adaptation which could be expected from an expert without any inventive skill. Claim 2 was therefore obvious in view of I2 and C5.

Independent claim 3 not inventive in view of C5, I2 and C3

Independent claim 3 claimed the use of a display device as claimed in any one of the preceding claims for inspection of small details with low contrast in monochrome medical images for prolonged periods of time of at least two hours.

The opponent claimed that, starting from C5 that described a monitor with three cathodes and a particular γ-value and his general knowledge to find suitable values of the analogue electronic video signal levels of claim 2, the man skilled in the art faced with the problem of constructing such a monitor would find I2, describing the essential elements of the construction. Once having the monitor of claim 2, a second problem, independent of the first problem, was in what field such a monitor, having an adjustable relationship between light output intensity to an input signal level, could be applied. Faced with this problem, the person skilled in the art would combine the teaching of C3 with the disclosure of I2 and C5.

Given the fact that e-mail C3 could be intercepted from the Internet for the same reason as described for e-mail C5, the remaining question was whether the encryption of

the text by PGP formed a bar to the public availability of C3.

PGP, whose last version had been released in 2002, was a publicly available encryption program. In 2000 PGP was available with a key length of not more than 128 characters, because that was the limit that could still be broken by computer power of the U.S. intelligence service.

As there was no limitation to the effort that was required without inventive skills to obtain information in order for that information to be considered publicly available, C3 became publicly available on the day the e-mail was sent.

Claim 3 was therefore not inventive in view of C5, I2 and C3.

Independent claim 3 not inventive in view of I2, C5 and C3

Starting from I2, faced with the problem of adapting this monitor such that it was very pleasant for a human to watch, according to the teaching of C5, the person skilled in the art would give the γ-curve a value of γ in the range between 3.35 and 4.09. With his general knowledge he would be able to find suitable values of the analogue electronic video signal levels of claim 2 without any inventive skills. Moreover, it was common workshop practice to adjust a monitor to a desired γ-curve with a very good approximation by making the adjustment for a limited number of points on that curve.

Once having the monitor of claim 2, a second problem, independent of the first problem, was in what field such a monitor, having an adjustable relationship between light output intensity to an input signal level, could be applied. Faced with this problem, the person skilled in the art would combine the teaching of C3 with the disclosure of I2 and C5.

The availability of C3 had been discussed in relation to the previous section (C5, I2, C3). On top of the public availability, the opposition division had raised the question as to whether means required to decrypt C3, at the disposal of the U.S. intelligence service, were also available to the public. The opponent stated that there was no reason to assume that decryption by PGP was a privilege confined to the U.S. intelligence service, as public availability was not limited by a budget. To illustrate this point the opponent referred to D4. This document described how easy it had been for a few students to hack into a new Dutch public transport chip card, the development of which had cost more than €200 million and in which the data were certainly encrypted.

C3 should thus be considered as publicly available and claim 3 was therefore not inventive in view of I2, C5 and C3.

Arguments submitted in the letter of 11 March 2011 (i.e. after the board's communication setting out its provisional opinion)

Admissibility of the opposition

The opposition was admissible in particular for the following reasons all relating to the admissibility issue raised by the board of its own motion:
- that oppositions were "contentious proceedings" was not a general principle,
- the parties satisfied the criteria for "contentious proceedings",
- VNO-NCW (the Confederation of Netherlands Industry and Employers) did not control either party,
- co-operation between parties' representatives did not make proceedings non-contentious,
- there would be undesirable consequences from a ruling of inadmissibility.

More specifically, as stated in the paragraph bridging pages 6 and 7 of the opponent's letter of 11 March 2011 (emphasis added):

Various representatives of the Parties have on multiple occasions ... discussed this case with officials at the EPO to explain that this is a test case that arose out of informal discussion in the forum of "Studiecommissie Intellectueel Eigendom van VNO/NCW" [study committee for intellectual property of VNO/NCW]. **The facts set out by TBA** [the present technical board of appeal] **in the Remarks** [the communication annexed to the summons] **are admitted** by the Appellant and there has never been any intend [sic] to deceive the EPO. The conduct of the Parties and their professional representatives shows there has neither been abuse nor any intent to circumvent the law.

Issues of proof

The opponent pointed out that
- one should not discriminate against a particular disclosure merely because of the form in which it was made, i.e. written documents in electronic form (whether on the Internet or in e-mail) had to be assessed in the same manner as analogous printed paper documents;
- for publication it was sufficient that someone *could* have read the content of a document, not that someone *did* actually read it (citing T 381/87, OJ 1990, 213);
- as for the standard of proof, earlier decisions of the boards of appeal were wrong to treat Internet disclosures like prior use. Web and e-mail disclosures were potentially available to all and so should be treated in evidence the same way as (allegedly) published paper documents would be. Accordingly, the "balance of probabilities" standard should be applied to all written documents irrespective of the form in which they were published (paper, Internet, or e-mail). Any concern about the reliability of Internet or e-mail evidence should impact on the weight attached to a particular document and should not affect the threshold of standard of proof. The decisions in cases T 1134/06 and T 1875/06 could be distinguished on their facts. In the alternative, insofar as they suggested that the "up to the hilt" test should be applied to all Internet disclosures, they were incorrect.

E-mails C5 and C3 (C7)

The opponent referred to the following invitation by the board made in its communication annexed to the summons (at point 3.2.4, on page 29):

The opponent is invited to show that email C5 was routed via one or several territories in which it was lawful to intercept it and to disclose its contents.

For the following reasons the opponent submitted that this "test" was neither reasonable nor necessary.

(1) "Test" is unreasonable

The "test" proposed by the board was a new requirement that the opponent could not have foreseen and therefore taken steps to retain the suggested information. Document O5[1] (written contemporaneously with the time the e-mails were sent), filed with the opponent's letter of 11 March 2011, discussed the difficulty and reliability of extracting e-mail transit information from extended headers. But although in theory e-mail transit information might have been available from the extended header of an e-mail (normally hidden from the user), this information was not always available. Transit information was much more difficult to obtain eleven years after the date the e-mail was sent. In the present case electronic copies of the e-mails were no longer available.

(2) "Test" is not necessary

The opponent submitted that the "suggested test" was both impractical and unnecessary.

For publication it was sufficient that someone *could have* read the content of a document, not that they *did* actually read it (e.g. T 381/87, OJ 1990, 213). For an

[1] A3C Connection issue Oct-Nov-Dec 2000

e-mail the probability that a party could read its content was high.

Even at the time an e-mail was sent the sender did not know and could not control the servers through which the message would be routed. Sending an e-mail was like throwing a piece of paper over a wall. You had no idea who would read it. The fact was that unless context imposed a duty of confidence on a reader it was highly likely that an e-mail would be read in transit by someone (whether lawfully or unlawfully). Transit information merely showed that a sender might have been "lucky" that in a particular instance an e-mail passed through states which prevented unlawful interception (though this did not mean non-publication). Sending an e-mail meant it could have been routed via servers where no legal protections existed and so could have been read.

As submitted, the correct standard of proof to apply was balance of probabilities. Elaborate technical tests were not needed, as the opponent only had to show that public access to information in the e-mail was more likely than not. This was based on several factors, such as who was likely to read its content in transit and on receipt and what duties of confidence could be shown or assumed for such readers (real or potential).

According to a report to the U.S. Congress (O2[2]), filed with the opponent's letter of 11 March 2011, unknown parties diverted significant volumes (15%) of Internet

[2] 2010 Report to Congress of the U.S.-China Economic and Security Review Commission, 111th Congress, 2nd Session, November 2010; Chapter 5, Section 2: External Implications of China's Internet-Related Activities (see pages 241 & 243-244)

traffic to China in April 2010. There was every reason to assume that some party in China could have accessed the content of this traffic and would have been free to publish it in China. A similar diversion could have happened in 2000 when the relevant e-mails were sent.

Nor could transit through the Netherlands alone be assumed for e-mails sent from one Dutch computer to another as traffic was routed to find the fastest not geographically shortest route. In fact in 2000 it was extremely likely that an e-mail sent from the Netherlands travelled outside the E.U., probably via the U.S. Document O8 (filed with the opponent's letter of 11 March 2011), a map of the inter-regional Internet backbone of September 2000 (based on data from TeleGeography Inc., Global Backbone Database), showed that at that date the majority of bandwidth had been located between the E.U. and the U.S. and therefore the fastest routes had also been likely to be outside the E.U.

The opponent also noted that in the present case, as the e-mail addresses for AkzoNobel and DSM had a top level domain ".com" and both entities were large multinational companies, there was no certainty that the e-mails from and to these addresses were sent externally (i.e. left the relevant company intranets) from a company server located in the Netherlands. It was quite possible that they could have been sent first via fast dedicated intranet connections within each company's internal network to any location in the world where that company had a server and thence externally from that country depending on the quickest path available. This was independent of the actual location of Mr. de Vries and

Mr. Mooij when they sent or received the e-mails or of the location of the headquarters of either company.

So, on the balance of probabilities, it was more likely than not that the e-mail messages in question had passed at some point outside the E.U., but even if they had not this did not mean confidentiality could be assumed.

(3) Interception does not preclude legitimate access

That interception was a criminal offence did not imply that nobody could read an e-mail in transit for legitimate reasons. It could not then be assumed that such legitimate readers had an absolute duty to keep secret the content of every e-mail they read (or could have read). Whether a duty of confidentiality could be imposed on these readers depended on the law of confidentiality and the content of the e-mail.

(4) Determining general principles for e-mail disclosure

Whether the content of an e-mail could be deemed public had to be considered at several stages: (i) at the sender, (ii) during message transmission and (iii) at the recipient. If at any one of these stages at least one reader *could* have accessed (not *did* access) its content and had a reasonable belief that he was free to repeat its content to another person, then the content of the e-mail had to be deemed available to the public.

(i) *The sender stage: intent*

Factors that might be used to determine whether a sender intended to keep information in an e-mail secret included some or all of the following:

- content and nature and number of addressees; and/or
- whether others had access to the e-mail account or could send e-mails on the sender's behalf.

Thus a reader in transit, i.e. a person who *could* have accessed (not *did* access) the content during transmission on the balance of probabilities, or a recipient could reasonably believe no confidentiality had been intended for the content of a message sent from a company e-mail "generalenquiries@company.com" to every person in an address book or for a message sent from a general computer used by everyone in the department.

General e-mail disclaimers asserting among other things confidentiality of the content and that the content was intended for the recipient only had almost no value and provided little guide as to the sender's intent. Firstly, they were almost always added indiscriminately to all e-mails, whether confidential or not, usually automatically. Secondly, such disclaimers could not unilaterally impose a duty of confidence on a reader who might not agree with them.

(ii) *At message transmission stage (readers in transit)*

A reader in transit could be acting lawfully or unlawfully.

(a) Unlawful ("hacking")

A reader reading an e-mail by unlawful interception (hacking) might reasonably assume its content was, in principle, confidential.

However a disclosure that was made unlawfully was still a disclosure. While this might create a remedy for damages, it could not undo the effects of publication.

Article 5 of the Directive 97/66/EC prohibited interception within the E.U. "except when legally authorised". The opponent also noted the last date for implementation of this Directive had been 24 October 2000, almost nine months after the e-mails C5 and C3 had been sent. So while it had been prohibited to (unlawfully) intercept these e-mails at servers based in the Netherlands, this did not show even a strong probability of confidentiality of their contents during transit.

(b) Lawful (ISP's activities)

Even if one equated unlawful interception with confidentiality, then the fact that even a large class of people would be prevented from lawfully intercepting e-mail under this Directive did not mean that one could assume that those who were “legally authorized” to access the contents of e-mails while in transit automatically had to be subject to the same obligation of confidentiality.

It was highly likely that at least one person would have lawful access to an e-mail in transit. For example,

administrators at an Internet Service Provider (ISP) would routinely access random e-mails to check that ISP policies were being complied with or to address technical issues or comply with government requests. Typical terms and conditions in an ISP contract might also require that customers permitted such activities. Thus, interception by the ISP would then not be prohibited by Article 5 of the aforementioned Directive as it would not be "without the consent of the users".

ISPs were required by many E.U. governments to monitor e-mails. For instance, in the U.K., the Regulation of Investigatory Powers Act (RIPA) 2000 required large ISPs to install technical systems to assist law enforcement agencies with interception activity. There had also been widespread criticism that too many U.K. agencies had the ability to use RIPA powers. Document O9[3] (filed with the opponent's letter of 11 March 2011) discussed the implications of RIPA for e-commerce. A comment highlighted one of the concerns of the British Chamber of Commerce (BCC) as being "public disclosure of critical company information". Thus, notwithstanding interception under RIPA having been lawful (permitted by Directive 97/66/EC), the BCC nevertheless believed that information still *could* be published.

Thus the number of individuals, whether employed by the private sector (ISP) or public sector, that fell outside Article 5 of Directive 97/66/EC and could have lawfully accessed e-mails in transit within E.U. Member States was surprisingly high, and not just limited to

[3] Hosein, Ian, Whitley, Edgar A., The regulation of electronic commerce: learning from the UK's RIP act, Journal of Strategic Information Systems 11 (2002)31-58

traditional law-enforcement or security-service personnel where confidentiality of their activities might be readily assumed.

Both the board and the patentee assumed that because access to an e-mail was lawful its content had also to be kept confidential by that person. The opponent disagreed that such a universal duty of confidence could be assumed or imposed on lawful readers in transit.

Several examples showed that a rule assuming universal confidentiality in content of an e-mail read lawfully in transit could not be supported.

An ISP administrator who might lawfully read an e-mail that mentioned the current football score or the weather in his home town, or that was marked as a press release, could reasonably expect no prohibition on passing this information to a friend.

By contrast, a message sent from a managing director to his board of directors (at home, i.e. not via a company network) which included financial information about the company and a request to store paper copies in a locked cabinet would, because of its context, self-evidently be deemed confidential by a lawful reader in transit, whether or not the message explicitly mentioned confidentiality or contained a standard e-mail disclaimer.

So the opponent submitted that both the nature and context of the information transmitted had to be assessed (using only the information in the e-mail) before a lawful reader in transit could decide whether

the content of an e-mail was deemed confidential and so to be treated as such.

Generic e-mail disclaimers were not useful in assessing whether a message was confidential. Instead, the lawful reader in transit had to decide for himself based on the e-mail as a whole whether or not it was reasonable for him to keep its content secret.

The opponent submitted that an assessment had to be made whether it was likely on the balance of probabilities that at least one reader in transit was free, or could reasonably assume that he was free, to disclose the content of a message he *could* have (not *did*) read. The obligations on such a reader had to be derivable from the content and context of the e-mail alone, as the reader had no other background information.

Factors which might suggest to a "lawful reader in transit" that the content was to be deemed confidential could be any of the following:

- content inside a password-protected attachment (Word document or the like);
- encrypted e-mail;
- certain subject-matter (financial information, business strategies, anything labelled trade secret, details of a process for making a commercial product, personal or health information);
- the roles of sender and recipient and their relationship (doctor - patient, lawyer - client, patent attorney - inventor, priest - parishioner).

Conversely, absence of these factors might lead a reader to conclude reasonably that the information was deemed unimportant and non-confidential.

Factors such as

- sending information in an open e-mail neither encrypted nor password-protected,
- sending an e-mail to a large number of addressees,
- copying an e-mail to an addressee who was clearly inappropriate (e.g. family member or friend)

could lead the reader to the same conclusion of absence of confidentiality.
Certain subject-matter per se, such as non-embargoed press releases, could also be considered to be inherently not confidential.

(iii) *At recipient stage (obligations agreed to by the intended recipient)*

The patentee asserted that there was a non-disclosure agreement (NDA) between Mr. de Vries and Mr. Mooij. However an NDA might not be enough to guarantee confidentiality of an e-mail because, while it bound sender and recipient to some extent, it could not bind a third party such as a reader in transit. How the recipient treated the information after receipt might also be important to judge whether the e-mail content had been treated at the time as being confidential. For example, could anyone else access either of the recipient's two e-mail accounts to which C5 and C3 were sent? If so, who? Would such persons be expected to have a duty to keep such e-mails secret by virtue of their position? The subject-matter that was included in the scope of the NDA was also important.

(iv) *Encryption*

Encryption showed a common intent on the part of both the sender and recipient to exchange information of a confidential nature, as previously encryption/decryption keys had to be exchanged (so it was not a unilateral act). As such it was probably sufficient that on the balance of probabilities any reader in transit (whether lawful or not) would then assume confidentiality of the content of an encrypted e-mail. Access to encrypted e-mail could not be assumed to be impossible. In this context, the opponent referred to document O9 discussing the operation of RIPA in the U.K., which required users to supply their encryption keys to certain authorities if lawfully asked to do so.

However, as discussed, encryption did not prove how the information was treated by a recipient after arrival. Nor could one assume that all the content of an encrypted e-mail was intended to be kept secret merely because some information in it might be so intended.

A sender could not impose a unilateral obligation on a recipient (or reader in transit) and exchanging encryption keys between persons A and B did not imply that B had to keep all communications from A secret. It might be that only certain messages or parts of a message were sensitive, or that the information was sensitive for a certain time only. In other words, encryption alone was insufficient to show the extent of confidentiality in message content; further context was required.

For example, the sender and recipient might have an NDA covering the field of car parts. If the sender then sent an unsolicited encrypted e-mail about displays, this would not be covered by the NDA and the recipient would be free to disclose it.

(v) *Summary of factors to consider for assessing whether an e-mail was public*

The test for "made available to the public" was a "could access" not a "did access" test, i.e. whether, on the balance of probabilities, it was reasonable to assume that a person could have obtained information. It did not matter whether anyone made use of this possibility.

The technical means by which information was delivered was less significant than the obligations on the sender and recipient and any message carrier who might reasonably be expected to have contact with the message and have lawful or unlawful access to read its content.

One should apply the same principles to e-mail as to a letter, i.e. there should be no discrimination as to the technical means of delivery. So, for example, an unencrypted e-mail was like a postcard viewable by all, whereas an encrypted e-mail was more like a letter in an envelope. Whether or not a person in transit had a duty to keep the content of an e-mail secret could not be assumed on the basis of whether interception was lawful or not. Rather, it was fact-specific and depended both on the content and context of the e-mail.

It was useful to apply commonly accepted principles to test whether information should be regarded as confidential.

If treated in a cavalier manner, a sender could not rely on a document being secret.

If the recipient did not agree to keep something secret, secrecy could not be imposed unilaterally (e.g. a blanket footer asserting "confidentiality" in all e-mails from the sender was not enough).

The actions of the sender/recipient were more instructive than a label: how they treated the information told you whether it was really intended to be confidential.

The nature of the relationship might be relevant to whether a third party reasonably knew the message was secret.

Arguably, any third party who lawfully (e.g. an employee of an ISP) read an e-mail had no duty to keep it secret, unless shown otherwise (i.e. the burden of proof was reversed). If a party was reckless, the burden of proof was reversed, so the sender had to show that there was no real possibility of publication.

(5) Applying these general principles to the current facts

(i) *E-mail C5 (sent unencrypted from Mr. de Vries (of AkzoNobel) to Mr. Mooij (acting for the opponent) on 25 January 2000 at 21:44)*

E-mail C5 contained a two-part disclaimer at the end of the message. The first paragraph was more personal to the sender. It included the text portion "Confidential information may only be sent to me by email if your email mailbox is within the akzonobel.com server." The second paragraph, on the other hand, had the style typical of a corporate e-mail disclaimer added automatically to every e-mail from AkzoNobel (or perhaps its legal department) that could not be removed or edited.

This two-part disclaimer was not internally consistent. The first paragraph stated that e-mail might not be a safe method of sending confidential information. Yet the second paragraph nevertheless tried to assert this confidentiality. As the content only "might" be confidential etc., a reader was left none the wiser; presumably, then, the content might also not be. The disclaimer asserted that "retention, dissemination, distribution or copying" of the e-mail by anyone who was not the recipient was prohibited. Yet these were the very activities that a lawful "reader in transit", such as an engineer or administrator at an ISP or server, was required to perform in order to do his job! So such a person could not accept the terms of this disclaimer (which in any event was not a contract) and they could not be imposed unilaterally on him.

The e-mail was unencrypted. So a lawful reader in transit could have accessed its content. While not being decisive for establishing lack of confidentiality, lack of encryption was one factor suggesting that the sender did not intend to keep the content secret.

A lawful reader in transit would assume from reading this e-mail alone (especially the second part asserting confidentiality) that the disclaimer had probably been indiscriminately added to all AkzoNobel e-mails and therefore could (and indeed had to) be effectively ignored.

Furthermore, whether or not there was an NDA between Mr. de Vries and Mr. Mooij was irrelevant to a lawful reader in transit, as due to privity of contract he was not bound by such an NDA. Existence of an NDA might provide context for a reader to infer confidentiality in a message. However, there was nothing in the e-mail to indicate to a reader that such an NDA existed. So a reader of the e-mail only had the content and context of the e-mail to make this assessment.

In this context, Mr. de Vries' admission in the first part of his e-mail disclaimer that e-mails containing confidential information should be sent via a server at akzonobel.com and his actions in sending information to Mr. Mooij via e-mails to two servers not located at akzonobel.com would lead a reasonable person to infer that the message could not contain confidential information and that Mr. de Vries did not intend to keep the content of this message secret.

Nothing, either in the titles of the sender and recipient or in the content or context of the message, provided any information about the relationship between Mr. de Vries and Mr. Mooij or suggested, due to the nature of their relationship (e.g. lawyer and client, patent attorney and inventor), implicit confidentiality for a reader in transit. There was no indication inherent in the e-mail that Mr. Mooij had to keep its content secret. He was not an inventor, and was employed not by AkzoNobel but by DSM. There was no indication that the e-mail was sent in the course of seeking legal or patent advice (where it would be reasonable to assume confidentiality unless otherwise indicated).

Nor was there anything inherent in the nature of the content which might suggest confidentiality (technical information could not be assumed to be confidential merely because it was technical, whereas for example financial information might be). The e-mail described the display device as "new and improved" but this on its own did not suggest confidentiality, whereas a message referring to "patenting" or "an invention" might imply confidentiality to a reader.

Thus, as it was very highly probable that at least one reader in transit could have lawfully read this message (e.g. an administrator at any of the ISPs or servers through which the e-mail had had to pass) and since from the content and context of e-mail C5 no duty of confidence would be inferred by such a lawful reader, the content of e-mail message C5 had to be deemed made available to the public.

(ii) *E-mail C3 (sent encrypted by PGP from Mr. de Vries to Mr. Mooij on 17 January 2000 at 20:45)*

The confidentiality of encrypted e-mail C3 could not be assumed, even if an NDA existed at the time between Mr. de Vries and Mr. Mooij. As no blanket duty of confidence could be inferred from the context of their relationship and in the absence of a copy of the NDA, it still had to be assumed that Mr. Mooij had been free to disclose its content. This e-mail therefore formed part of the state of the art.

Arguments submitted during the oral proceedings

The board drew the opponent's attention to a discrepancy between the notarial record pertaining to e-mail C5 and that e-mail itself. While in the record it was said that the content of the e-mail message was "as stated on one page", the e-mail in reality consisted of two pages. The opponent considered that the indication in the notarial record was a mistake, but that the substantive content of the e-mail was indeed on one page.

The opponent agreed that Mr. Mooij was bound by a confidentiality agreement relating to the exchange of the e-mails C5 and C3, thereby clarifying what it had alleged in its latest letter of 11 March 2011. The question however was what the subject-matter of that agreement was.

As for the likely route that e-mail C5 took from its sender, Mr. de Vries, to its recipient, Mr. Mooij, the opponent referred to the network map submitted (document O8). According to that map, in September 2000,

the majority of Internet traffic had gone through the U.S. Therefore, on the balance of probabilities, it was highly likely that the e-mail had travelled via the U.S. Regarding the patentee's submission that e-mails were broken up in packets, sent along different routes and put together again at the point of reception, the opponent said that it was not clear where the message would be reassembled. But many ISPs had an obligation to keep records, so there was an obligation to assemble all the messages, and in practice that might happen. If ISP employees knew that they had to retrieve e-mails, then they would have the technical means to do so. ISPs could technically search very easily for particular information.

The e-mails could have been intercepted. If done lawfully, then there was no general obligation for the interceptor to keep the e-mails secret. As for persons authorized lawfully, one would probably have to apply the "proportionality" test, i.e. ask the following questions: What does the e-mail tell me about the content? Can I or can I not disclose it? (see written submission of 11 March 2011)

As for the question of when interception by ISPs was lawful, one had to distinguish between the situation in the E.U. and outside it, in particular in the U.S.

(1) E.U.

Directive 97/66/EC was the law. ISPs kept e-mails. There were exceptions for law enforcement in the Directive. Under usual circumstances, ISPs disclosed e-mail content

if required to do so by the police. The proportionality test applied to the prosecutor, not to ISP personnel.

(2) U.S.

U.S. law was less restrictive; it could not be expected that data could be kept confidential. ISPs could in principle do what they wanted.

There had been a substantial amount of dispute between the E.U. and the U.S. on the law on confidentiality. In July 2000 the "safe harbor" provisions had been approved. Before, there had been no protection concerning the handling of the data of European citizens in the U.S. Anyone had been free to look at e-mails.

These facts were shown by two documents[4] dealing with U.S. law on data protection and privacy and handed over by the opponent in the course of the oral proceedings. These documents will be referred to below as "Opinion 1/99" and "Data Protection". Hacking was clearly illegal under the U.S. Electronic Communications Privacy Act of 1986, but this was not the kind of access alleged by the opponent. The "proportionality" test applied to ISPs which had lawfully read e-mails.

[4] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government, adopted by the Working Party on 26 January 1999 (5092/98/EN/final WP 15); and Slemmons Stratford, Jean, Stratford, Juri, Data Protection and Privacy in the United States and Europe, Fall 1998.

C5 was not confidential, taking into account the second penultimate paragraph (i.e. the warning concerning confidential information). There was no indication that it had been sent for the purpose of advice, rather than as the result of two friends merely exchanging information. Anyone outside the E.U., e.g. in the U.S., would have been allowed to read the information.

(3) Worldwide

As to the legal situation worldwide, the board referred during the oral proceedings to point 11 of certain OECD Privacy Guidelines of 1980[5] entitled "Security Safeguards Principle". That point reads as follows:

Personal data should be protected by reasonable security safeguards against such risk as loss or unauthorised access, destruction, use, modification or disclosure of data.

The board mentioned that, among others, Australia, Canada, Japan and the U.S. had been members of the OECD at the filing date. The opponent answered that there was no presumption of worldwide illegality of interception. There was no evidence that those guidelines had been transposed into national legislation. In the U.S. in particular, they had not been.

Regarding specifically e-mail C3, the opponent conceded that, contrary to what it had alleged in the statement of grounds of appeal, whether PGP had been publicly available had no bearing on the present case. Instead,

[5] OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980; downloaded from http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html .

document O9 pertaining to the RIPA act (on interception by law enforcement agencies) was now most relevant.

Finally, the opponent confirmed that it was not alleging any specific instance of divulgation of any of e-mails C5 or C3.

Arguments submitted in the letter of 13 April 2011 (after the oral proceedings)

Further to the oral proceedings the opponent requested that the board use its discretion to reopen the discussion and admit the submission comprising remarks on a narrow issue that arose in those proceedings in relation to claim 3. The board had stated during the proceedings that the validity of use claim 3 did not need to be independently assessed. Indeed, if claim 1 was inventive then use claim 3 would also be inventive because it depended on claim 1. Alternatively, if claim 1 was obvious, then the opponent's request would be allowable, the decision of the opposition division overturned and the patent revoked, and there would be no need to go further and assess the validity of claim 3.

The opponent agreed that the board would normally be correct that a claim for the use of something inventive also had itself to be inventive, but exceptionally in this case this was not true for a number of reasons that the opponent gave in greater detail. The inventive steps of claims 1 and 3 were independent of each other and thus should be assessed separately with respect to the cited documents I2, C5 and C3/C7.

IX. The arguments of the respondent/**patentee** are summarised as follows.

Arguments submitted in the reply to the statement of grounds of appeal

Document I2

The patentee (at points 2.2 through 2.8) contended that I2 was not part of the state of the art at the filing date of the patent, relying in essence on the same arguments as those submitted in the statement of grounds of appeal in related case T 1553/06. A common thread to those arguments was the assertion that it constituted an "undue burden" as mentioned in G 1/92 (OJ 1993, 277) to find I2 on the Internet.

E-mail C5

From the opponent's argument that one million people could have had access to the communication, it could only be deduced that this concerned a minute fraction of the world population (less than 0.002%) and related only to an unspecified set of an enormous number of communications. That is, nothing was in fact said about whether communication C5 could have been intercepted. Thus, the opponent's argument showed nothing more than that, because communication C5 was an e-mail, there was a theoretical possibility that it could have been intercepted.

The opponent had not demonstrated (not even on the balance of all probabilities, let alone "up to the hilt") that communication C5 could have been intercepted by any

member of the general public. Hence, retrieving the information in communication C5 would put an undue burden on the skilled person. Notably, "hacking" was not commonly at the disposal of the skilled person in the field of display technology (i.e. the field of the present invention).

Further, the communication C5 had been marked confidential. It was noted that generally confidentially marked fax messages were not considered to be publicly available. As e-mail was at least more secure than fax messages, an e-mail marked confidential (such as C5) was not included in the state of the art.

E-mail C3

All arguments for communication C5 not being part of the state of the art also applied *a fortiori* to communication C3. Moreover, because communication C3 had been encrypted (by PGP) when it had been transferred over the Internet, the respondent noted that breaking PGP was not a tool normally available to the skilled person in the field of display technologies at the filing date. That breaking PGP had been available to the U.S. government was not tantamount to availability to the skilled person. There was only an indication that what was encrypted could be deciphered (which was presumably always the case). It did not imply that communication C3 could have been deciphered without undue burden to the skilled person.

Notably, document D2 (inadvertently referred to as D4 by the patentee) mentioned PGP as an adequate measure to secure e-mail (see D2, page 2, 2nd paragraph and the

paragraph bridging pages 2 and 3). Thus, document D2 confirmed that encryption, notably by PGP, would prevent the communication from being accessible to a member of the general public.

Directive 2002/58/EC

The patentee also pointed to Directive 2002/58/EC on electronic communication which was a confirmation of legal principles already applicable at the filing date of the opposed patent.

Admissibility of the opposition

In the light of the foregoing, the present opposition appeared to be based on documents several if not all of which were not included in the state of the art relative to the patent in suit. Accordingly, the patentee requested that the opposition be declared inadmissible.

Arguments submitted in the letter of 11 March 2011 (i.e. after the board's communication setting out its provisional opinion)

Admissibility of the opposition

Regarding admissibility of the opposition in respect of the issue of the contentious nature of the proceedings, the patentee replied:

The Board of Appeal has **correctly reconstructed** that in the present case there has been a **substantial level of co-operation between the parties and other professional representatives**. The purpose of the present patents (parent and divisional) was and is to assess if and to what extent disclosures via the Internet would fall under the prior art as defined in Art. 54 EPC.
...

Apart from this co-operation, however, there is no hierarchical relationship between the parties, nor has there been a hierarchical relationship between the parties and VNO-NCW. Notably, the opponent has not acted on behalf of the patent proprietor, but has been in contact with the patent proprietor in relation to the aim of establishing the status of disclosures via the Internet. The present opposition proceedings are contentious in that both sides have argued opposite views on the question at issue.

(quoted from the patentee's letter, page 1, second paragraph, and page 2, second paragraph, respectively, emphasis added)

Substance

As to the issue of confidentiality of the e-mail communications, the patentee observed that in the board's present view (expressed in the annex to the summons), the dividing line between public and non-public was strongly dependent on "technical issues how the e-mail was actually sent" and on a wealth of national legislation on e-mail privacy. Such a practice would never provide certainty to users of the European patent system and to the public at large. A more practical approach was to assess on the basis of the **intent** and reasonable expectations of sender and receiver of the e-mail communication. Thus, as was the case in the present opposition, an e-mail sent from one sender to only one or a few receivers and provided with a confidentiality clause would be considered to be intended for the (those) receivers only. Encryption would further strengthen the perception of sender and receiver’s intentions and expectations. On the other hand, an e-mail communication "broadcast" to a wide audience could not be considered as information which sender and receiver could reasonably expect had to be

kept confidential. Both communications C5 and C3, by their form and their nature, were clearly intended as bilateral communications between sender and receiver. Communication C5 was clearly not a broadcast in view of its confidentiality clause. The encryption of communication C3 only strengthened the fact that the bilateral communication had been intended by the sender for the "user" only.

Arguments submitted during the oral proceedings

As for the standard of proof, the patentee contended that the e-mails in suit were no longer retrievable. All information was under the control of the opponent and there was no way of independently verifying the sequence of events. Therefore, the standard was "up to the hilt", or at least higher than the balance of probabilities.

There was a confidentiality agreement between Messrs. de Vries and Mooij. Thus only readers in transit were relevant.

E-mail traffic was a one-to-one transmission of information that as such was personal, similar to a telephone conversation over public networks or voice over IP (VoIP). There were no search engines for e-mails. E-mails were broken up into packets and sent along different routes. At the point of receipt they were put together again. So even if there were a reader in transit, there would be no evidence that the person could have read the whole e-mail. If only a portion was read, one would not know which one and by whom.

In the present case, e-mails had been sent from one individual to another, not to a long list of individuals. Both e-mails had a confidentiality indication, and one of them was even encrypted.

So if an individual reader had intercepted an essential part, that would amount to eavesdropping. Thus the reader would be aware that it was not for him and was not to be disclosed.

An ISP employee reading e-mails only saw them for quality control. He was not interested in content, but only in the free flow of e-mail traffic.

Only the ISP transmitting the e-mail to a receiver got all the packets. Thus lots of service providers could be excluded from access to the whole e-mail. Only the last ISP might have a right to read but not to disclose it.

In the **E.U.**, any obligation of an ISP to hand over information to law-enforcement personnel did not include the total content of the server, but was limited to the information that had a bearing on the criminal offence they were investigating.

Regarding data protection in the **U.S.**, it was not known what portion of the e-mail had gone through the U.S. It was unknown whether any individual had legitimate grounds to look at the information. Even if an individual in the U.S. had legitimately had access to the essential part of the information, then that person would not have been free to disclose it to others.

The Internet site on U.S. law that the board referred to in the oral proceedings[6] showed that the exception for employees of ISPs related only to their official duties. Activities of ISP staff were limited to checks of a technical nature. ISPs could access technical content but not actual content.

Even if U.S. law were applicable, then the U.S. would not be the end point. Even if lawfully a service engineer were under no confidentiality obligation, the question remained whether all information of the e-mail would be available to him because the e-mail might have been broken up into packets and only reassembled at the end point.

Finally, even if access to C3 and C5 were judged to be established, essentially the same test as the one proposed by the opponent would be appropriate (i.e. what could be disclosed depended on the content, and in the present case account had to be taken of the confidentiality note).

Arguments submitted in reply to the opponent's letter of 13 April 2011

The board received no reply from the patentee to this letter.

[6] http://internetlaw.uslegal.com/privacy/

Reasons for the Decision

1. Admissibility of the opposition

1.1 Principle

At the outset, the board recalls that an opposition may be found inadmissible under Rule 56(1) EPC 1973 (Rule 77(1) EPC) at any stage of the proceedings, including appeal proceedings (see e.g. T 328/87, OJ 1992, 701, point 4 of the Reasons).

1.2 Compliance with Rule 76(2)(c) EPC

With regard to this issue, the board maintains its favourable preliminary findings set out in the communication annexed to the summons (at point 2.1), which are reflected e.g. in T 426/08 (at point 5.1.3). Further to a question by the board in the oral proceedings, the patentee affirmed its objection, without however furnishing any additional arguments. The board's findings that are now final are as follows:

The board concurs with the conclusion of the opposition division in the decision under appeal that the requirements of Rule 76(2)(c) EPC are met. The proprietor had argued that the opposition being based on documents that are not included in the state of the art, the opposition was not based on grounds which could prejudice novelty and /or inventive step of the patent. In this context the board draws attention to the wording of Rule 76(2)(c) EPC according to which the notice of opposition shall contain, *inter alia,* an indication of the facts and evidence presented in support of the grounds on which the opposition is based. The question as to whether or not that evidence is suitable for proving those facts is not a question of the admissibility of the opposition but a substantive one.

1.3 Whether the proceedings are contentious

1.3.1 The case law of the Enlarged Board of Appeal

For the board it follows from the decisions of the Enlarged Board of Appeal delivered in cases G 9/93 (OJ 1994, 891) and G 3/97 (OJ 1999, 245) that it is a condition for an opposition to be admissible that the opposition proceedings thereby instituted are **contentious**.

In G 9/93 (point 1 of the Reasons) the Enlarged Board said:

... [I]n G 9/91 and G 10/91 ... the Enlarged Board held that in view of their special post-grant character, opposition proceedings under the EPC are in principle to be considered as **contentious** proceedings between parties normally representing opposing interests. (Emphasis added)

Against this backdrop the Enlarged Board judged that:

the patent proprietor is not covered by the term "any person" in Article 99(1) EPC [1973] and is therefore not entitled to oppose his own patent under that provision. (See *ibid.*, at point 3 *in fine*).

The Enlarged Board's ruling in G 3/97 dealt *inter alia* with the question of whether an opposition filed by an indirect representative ("straw man") was admissible.

The Enlarged Board decided (see the Order) that:

1(a): An opposition is not inadmissible purely because the person named as opponent according to Rule 55(a) EPC [1973] is acting on behalf of a third party.
1(b): Such an opposition is, however, inadmissible if the involvement of the opponent is to be regarded as circumventing the law by **abuse of process**.
1(c): Such a circumvention of the law arises, in particular, if:
- the opponent is acting on behalf of the patent proprietor ...
(Emphasis added)

Under point 4.1 of G 3/97 the Enlarged Board explained in this respect that:

Attention has already been drawn to the decision in G 9/93 ... Here, it was decided that the patent proprietor is not entitled to oppose his own patent, since opposition proceedings are **contentious** and the opponent must therefore be a person other than the patent proprietor. This in itself requires no further comment. However, if the patent proprietor employs a straw man, then the latter, too, is representing the patent proprietor's interests. The identification of the straw man as opponent according to Rule 55(a) EPC [1973] does nothing to alter the fact that the person who is formally a party to the proceedings is on the patent proprietor's side. From this it follows that in this situation, too, the proceedings are not **contentious**. The employment of the straw man merely serves to conceal this circumstance and to circumvent the legal consequences arising from it. The action of the opponent on behalf of the patent proprietor therefore renders the opposition inadmissible. (Emphases added)

The present board cited the above case law of the Enlarged Board in its communication annexed to the summons to oral proceedings. It would add what the Enlarged Board said in G 3/97 on proof-related issues (see point 5 of the Reasons):

The burden of proof for a straw man objection is to be borne by the person raising the issue, ie the patent proprietor or, in the case of an objection by the Office of its own motion, the relevant EPO department.

Regarding the standard to be applied in assessing evidence, it must be remembered that any person is entitled to file an opposition. Withholding this legal entitlement from anyone requires a particular justification, which cannot be based on a mere balance of probabilities. Instead, before considering an opposition to be inadmissible, the deciding body has to be satisfied, on the basis of clear and convincing evidence, that the law has indeed been circumvented in an abusive manner by the employment of a straw man.

1.3.2 The opponent’s assertions

In its reply of 11 March 2011 to the board's communication, the opponent relied on the following arguments to establish the admissibility of the opposition (see section 1 of the reply):
- that oppositions were "contentious proceedings" was not a general principle,
- the parties satisfied the criteria for "contentious proceedings",
- VNO-NCW (the Confederation of Netherlands Industry and Employers) did not control either party,
- co-operation between parties' representatives did not make proceedings non-contentious,
- there would be undesirable consequences from a ruling of inadmissibility.

1.3.3 Analysis

On the basis of the parties' submissions, the board cannot find a circumvention of the law by abuse of process in the sense mentioned above, i.e. because the opponent acted on behalf of the patent proprietor.

In their submissions in reply to the board's communication annexed to the summons, both in writing and in the oral proceedings before the board, the parties admitted that they co-operated on a test case that arose out of a discussion in the study committee for intellectual property of VNO-NCW. It was only by these submissions that the parties informed the board of the test case. They may have conveyed pertinent information to the first instance as long ago as in 1998, as they contend. Yet the board, in its preparation of

the file for the oral proceedings, which is reflected in the communication annexed to the summons, found no hint of the parties having provided express information to the EPO that this was a test case. Rather, as follows from the facts enumerated in said communication under the section dealing with the admissibility of the opposition, the opposite would have to be concluded from the file as it stood at that time.

As for the prosecution of the test case, the parties agreed that the opponent was not bound by any instructions from either the patentee or the study committee. The board has no reason to cast doubt on these submissions. The fact that a test case was created does not necessarily imply that the various submissions made as part of it must have been under the control of one party (or of both parties jointly).

A further question is whether the opposition proceedings are not contentious because of the very fact that the parties defended their positions within the framework of a test case in order to obtain answers from the board to specific legal questions, i.e. whether and under what conditions disclosures via the Internet constitute prior art within the meaning of Article 54 EPC 1973.

The board is of the opinion that the prosecution of the opposition proceedings was contentious, as required by G 3/97, because the parties defended mainly opposing positions. The fact that the parties defended their positions within the framework of a test case and will obtain answers from the board to certain specific legal questions is immaterial in this regard. Therefore the opponent's challenge to the soundness of the requirement

of contentious proceedings established in G 3/97 need not be afforded any consideration.

From the above analysis the board concludes that the opposition is admissible. As a consequence, the parties' questions to the Enlarged Board are moot.

2. Admittance of documents

The opponent submitted the notarial records relating to e-mails C3 and C5, together with the originals of these two documents, only in the oral proceedings before the board. The board considers this submission as a non-complex reaction to its invitation in the communication annexed to the summons to prove the date and time of transmission and the contents of C3 and C5 and how they were accessed.

Non-patent documents D1 to D3 were filed together with the statement of grounds of appeal, D4 shortly thereafter, in order to support the opponent's statement that "it is well known that internet mail can and could in 2000 easily been [sic] intercepted" (see page 5). Their submission can be considered to be a non-complex reaction to the decision under appeal and they are relevant for establishing the factual basis of the present case.

For these reasons and because the patentee did not object to admittance of the aforementioned documents, the board admits those documents into the proceedings pursuant to Article 13(1) of the Rules of Procedure of the Boards of Appeal of the EPO (RPBA; OJ 2007, 536).

Non-patent documents O1 to O9 filed by the opponent with letter of 11 March 2011 were admitted into the proceedings (Article 13(1) RPBA) as far as the opponent had referred to them in writing. Their submission can be considered to be a non-complex reaction to the board's communication, and the patentee did not object to their admittance. O1, O3 and O4 relate to the admissibility of the oppositions in both appeal cases T 1553/06 and T 2/09, O6 and O7 concern the substance of the former case and the remaining documents O2, O5, O8 and O9 relate to the substance of the latter one.

The documents "Opinion 1/99" and "Data Protection" handed over in the oral proceedings before the board were likewise admitted (Article 13(1) RPBA) insofar as the opponent had referred to them in those oral proceedings (copies of these documents are annexed to the minutes of the oral proceedings). They are intended to corroborate submissions already made in the letter of 11 March 2011, and the patentee did not object to their admittance.

3. Issues of proof

3.1 Burden of proof

In opposition proceedings, the burden of proof lies with the opponent requesting revocation of a patent relying on a certain ground for opposition on the basis of asserted facts. It is for the opponent to establish such facts to the required standard of proof.

In the board’s view, this rule also applies, in principle, to establishing law outside of the EPC. Areas

of exceptions to this rule, where the board is supposed to know the law, include fundamental rights.

3.2 Standard of proof

As for the standard of proof, the board recalls that the EPO standard of proof is generally the "balance of probabilities" (see J 20/85, OJ 1987, 102, point 4 of the Reasons). However, especially in cases where only one party had access to information about an alleged public prior use, the case law has tended toward expecting that the public prior use be proved beyond any reasonable doubt or "up to the hilt" (see e.g. T 55/01, point 4.1 of the Reasons, and T 472/92, OJ 1998, 161, point 3.1 of the Reasons). The same strict standard was required for Internet disclosures in the decision in case T 1134/06 (see point 4.1 of the Reasons; affirmed in T 1875/06, points 7 to 9 of the Reasons). Conversely, it has been laid down in both the EPO Guidelines and the "Notice from the European Patent Office concerning internet citations" (OJ 2009, 456) that, in examination proceedings concerning Internet citations, the balance of probabilities will be used as the standard of proof for assessing the particular circumstances of a given case, and thus the probative value of the evidence in question. Proof beyond reasonable doubt ("up to the hilt") is not required (see Guidelines for Examination in the European Patent Office, Part C, Chapter IV, point 6.2.2, updated in April 2010, and "Notice from the European Patent Office concerning internet citations", point 3.2). The publication dates of Internet disclosures submitted by a party to opposition proceedings are assessed according to the same principles as are applied in examination proceedings

(see Guidelines, Part D, Chapter V, point 3.1.3, updated in April 2010, and "Notice from the European Patent Office concerning internet citations", point 4). In this context the board also refers to a more recent article about current French case law on affidavits drawn up by bailiffs detailing facts witnessed on the Internet ("Le constat d'huissier sur Internet"; see Attachment 3 to the annex to the summons). According to that article, French case law requires four technical precautions for finding an affidavit to be reliable: a precise description of the equipment used; a mention of the IP address of the connection; assurance that the connection operates without a proxy server; and the deletion of caches, temporary files and forms.

3.3 In particular the impact of the test nature on the standard of proof

It should be noted that the present contrived test case differs from a corresponding unplanned (real-life) test case, such as the (alleged) infringement of a patent further to which legal proceedings are initiated against only one of several parties which have all allegedly infringed the patent in the same jurisdiction. The present case differs insofar as the board, which has the duty to take into account all the facts pertaining to the case, must therefore also consider those facts that specifically relate to the contrived test nature of the case. This may have an impact on the standard of proof. For instance, if both parties agreed that a certain e-mail, such as C5 or C3, had been transmitted over the Internet and it were clear that this was a precondition for the test case to make sense, this might weigh in favour of this assertion and corroborate any notarial

declaration. In a corresponding real-life case, the board might arrive at a different conclusion.

Thus the outcome of a contrived test case such as the present one may, in those respects that differ from a real-life test case, be of limited use for parallel real-life situations. That is the risk that the parties incur when presenting a contrived test case.

4. Claim 1

4.1 Background

The opposition division, in the decision under appeal, held that, out of the documents that the opponent had submitted, i.e. I2, C3 and C5, document I2 was the only available prior art before the filing date of the patent in suit (hereinafter also referred to as "the filing date"). The division held that the subject-matter of claim 1 differed from the device of I2 (incorrectly referred to as D1) in that it included the (additional and final) feature dealing with the relationship between the light output L and the signal level V. The problem to be solved by the addition of this feature to the device known from I2 was regarded as to provide a display which yielded a brightness distribution that was very comfortable for studying images on the screen (patent specification, column 7, lines 39 to 41). I2 did not disclose this feature or render it obvious. The board notes that the content of e-mail C5 corresponds to the final feature of claim 1.

The opponent, in the statement of grounds of appeal, contended that the subject-matter of claim 1 was not

inventive in view of I2 and C5. The board will assume *arguendo* that the opposition division was right in considering I2 to be publicly available before the filing date and will assess below whether C5 was also made available to the public.

Pursuant to Article 54(2) EPC 1973:

The state of the art shall be held to comprise everything made available to the public by means of a written or oral description, by use, or in any other way, before the date of filing of the European patent application.

According to the case law of the boards of appeal, information is "available to the public" if only a single member of the public is in a position to gain **access** to it and understand it, and if said member of the public is under no obligation to maintain secrecy (see T 1081/01, point 5 of the Reasons, affirmed by T 1309/07, point 3.2.1 of the Reasons). Whether or not a member of the public has **actually** accessed the information is irrelevant (see T 84/83, point 2.4.2 of the Reasons).

4.2 The relevant facts and arguments submitted by the opponent

The opponent DSM IP Assets N.V. has modified its position in the course of the opposition proceedings before the board. The letter of 11 March 2011 and the oral submissions in the oral proceedings in part diverge from, and sometimes are incompatible with, earlier submissions. This is why, in case of doubt, the board will base the present decision on the latest expression of the opponent’s position, i.e. its remarks made in the oral proceedings before the board. Where earlier

submissions are in conflict, they may be disregarded, despite the opponent's blanket statement in its letter of 11 March 2011 according to which:

[i]n addition to the remarks in this letter, all previous arguments that the Appellant has submitted on file of both patents during examination (e.g. as third party observations [filed by DSM N.V. (DSM Patents & Trademarks)] during both oppositions (as opponent) and in both the above Appeal proceedings (as Appellant) are maintained. (See bottom of page 1.)

The opponent's latest position includes the following:

- the e-mail was routed inside the E.U. and possibly the U.S. (the opponent relied on Article 5 of Directive 97/66/EC and on a map of the inter-regional Internet backbone),
- at the filing date, it was in principle unlawful in both the E.U. and the U.S. to intercept e-mails,
- if, exceptionally, interception was done lawfully in the E.U. or the U.S., then there was no obligation to the interceptor to keep the content of an e-mail secret, provided that the interceptor recognised from its content and context that the e-mail was not confidential ("proportionality" test),
- in the E.U., interception was legally authorised for ISPs in particular for law-enforcement purposes (U.K.: see RIPA act),
- in the U.S., interception was legally authorised for ISPs without restrictions.

While in the oral proceedings the opponent's focus was on the above indents, the board considers that the opponent has not abandoned its view that the e-mail might also have been routed through territories other than the E.U. or the U.S., in particular through

territories where, at the filing date, it had not been unlawful to intercept e-mails.

4.3 Whether C5 forms prior art because it was communicated to the opponent's representative (recipient stage)

The parties admitted that there was a substantial level of co-operation between them and other professional representatives in order to create a test case. For the board, this explains why it was possible that e-mail C5 corresponding to the final feature of current claim 1, i.e. the feature of claim 5 of the parent application (just like C3 corresponding to current claim 3, i.e. the feature of claim 7 of the parent application), could be sent on 25 January 2000 (C3: 17 January 2000), i.e. before the filing date of the parent application on 1 February 2000, from Mr. de Vries of AkzoNobel to Mr. Mooij, the representative of the opponent DSM IP Assets B.V. and also of DSM N.V. (DSM Patents & Trademarks) on whose behalf notarial records were drawn up.

Access by Messrs. de Vries and Mooij to the information in e-mail C5 before the filing date, however, did not put this information into the public domain. This is because a non-disclosure agreement (NDA) not to divulge the respective information and binding on these two persons, among others, had been concluded. The then applicant mentioned in its letter of 10 October 2000 in the proceedings up to grant of the parent application, before the divisional application from which the patent in suit originated had been filed, that "both Mr. De Vries and Mr. Mooij were bound to a non-disclosure agreement pertaining to the subject-matter of the

present European Patent application" (see page 2, second full paragraph). In the oral proceedings before the board the opponent acknowledged that Mr. Mooij was bound by a confidentiality agreement relating to the exchange of the e-mail C5, but that the subject-matter of that agreement was not clear. In any case, the board must infer from the test-case nature of the present proceedings that disclosure of the content of e-mail C5 by either Mr. de Vries or Mr. Mooij was not permitted because otherwise the test case would have become largely moot.

4.4 Whether C5 was transmitted over the Internet

The board notes that the opponent, in support of its contention that C5 (like C3) was transmitted over the Internet, filed the original of a corresponding notarial record by a Dutch notary public at the oral proceedings (such original was also filed for C3). This record certifies that C5 (and another notarial record certifies that C3) was opened in his presence at a certain date and time. This original bears the signature and stamp of the notary public, and C5 and the attached notarial record were bound in one folder (idem for C3 and the further notarial record).

The discrepancy between the notarial record pertaining to e-mail C5 saying that the message was on one page and the fact that in reality the e-mail consisted of two pages is regarded by the board as an obvious mistake. What is decisive for the board is the fact that the substantive content of the e-mail was indeed on one page. The board considers the opponent’s statements to be credible given that this is a test case and transmission

of C5 (and C3) is a precondition for enabling the board to deal with the gist of the test case.

In the light of the foregoing, the board considers that the opponent has proven beyond reasonable doubt that C5 (like C3) was transmitted over the Internet at the date and time indicated in the notarial record. Given the agreement of the parties on this issue, the question as to the proper standard of proof (see point 3.2 above) need not be answered.

4.5 Whether C5 forms prior art because the notary saw it

As stated, it has been proven that a Dutch notary opened e-mail C5 (and C3). However, the board does not consider that the content of C5 (or C3) was divulged to the public by the fact that the notary public saw it before the filing date. This is because from the test nature of the present case it must be concluded that the notary was under a duty to keep this content confidential. Otherwise the test case would be largely moot.

4.6 Whether C5 forms prior art because it might have been intercepted from the Internet: in general

4.6.1 Disclosures via the Internet: the technical differences between webpages and e-mails

In its submission of 11 March 2011 the patentee said:

> The purpose of the present patents (parent and divisional) was and is to assess if and to what extent **disclosures via the Internet** would fall under the prior art as defined in Art. 54 EPC. (Emphasis added.)

At the outset the board draws the attention to a **basic factual difference** present at the filing date between

two types of "disclosures via the Internet", i.e. between content that exists on the World Wide Web (also referred to as "the Web"), a part of the Internet, on a **webpage** at a specific **URL** (Uniform Resource Locator) and content that is transmitted over the Internet by **e-mail**.

Content on the Web can, in principle, be accessed and read via its URL, which may have been found by the public at large with the help of a public search engine if the content in question has been indexed with keywords (electronic "pull type" technology, i.e. where the request for a transaction is initiated by the receiver).

An e-mail is a communication from a sender to one or several recipients (in case of a large number of recipients, sending is sometimes dubbed "broadcasting"). A (private) communication takes place between senders and receivers, who may be individuals or groups of persons, possibly members of the public (electronic "push type" technology, i.e. where the request for a given transaction is initiated by the sender). E-mails are not placed in an unrestricted area of the Internet, such as the Web. The board is not aware that they would be accessible by entering an address that may have been found with the help of keywords entered in a public search engine. An e-mail can only be read by a member of the public (who is not a recipient of the e-mail) if extraordinary measures, such as intercepting it on a computer network, are used. The opponent submitted that such interception was taking place in practice and that e-mails could be filtered according to keywords.

It should be added that e-mails transmitted over the Internet are generally divided into packets and later reassembled. Document D1 (at page 2, first and second full paragraphs), submitted by the opponent, explains e-mail transmission in greater detail as follows:

> ... given the dynamic nature of the Internet, it is impossible to absolutely predict exactly what path network traffic will follow. One e-mail message that you send could take an entirely different path to reach the recipient than another that you send to the same person. In fact, it is even worse than that: for the sake of efficiency, e-mail messages and other network traffic are typically broken down into smaller little chunks, or packets, before they are sent across the network, and automatically re-assembled on the other side. Each of these individual packets may in fact follow a different path to get to the recipient! (In actual practice, a given path tends to get reused until the operational parameters of that or other related paths have significantly changed.)
>
> The net result of all this is that your message, or at least little chunks of your message, travels through an indeterminate set of systems and network devices, each of which offers a point of interception.

4.6.2 Implications of the test for public availability of a document on the World Wide Web

In parallel case T 1553/06 the board developed a test for assessing the public availability of a document stored on the World Wide Web which could be found via a public web search engine on the basis of keywords. In devising this test the board started from its finding that the mere theoretical possibility of having access to a means of disclosure did not make it become available to the public within the meaning of Article 54(2) EPC 1973. What was required, rather, was a practical possibility of having access, i.e. the requirement of "direct and unambiguous access", set out in G 1/92 (OJ 1993, 277) and T 952/92 (OJ 1995, 755),

applied not only to access by the skilled person to information derivable from a means of disclosure, but also to access by a member of the public to the means of disclosure (see point 6.5.4 of T 1553/06). The test is as follows (see point 6.7.3 of T 1553/06):

If, before the filing or priority date of the patent or patent application, a document stored on the World Wide Web and accessible via a specific URL
(1) could be found with the help of a public web search engine by using one or more keywords **all** related to the essence of the content of that document and
(2) remained accessible at that URL for a period of time long enough for a member of the public, i.e. someone under no obligation to keep the content of the document secret, to have direct and unambiguous access to the document,
then the document was made available to the public in the sense of Article 54(2) EPC 1973.

The board in T 1553/06 also made clear that if any of conditions (1) and (2) is not met, the above test does not permit to conclude whether or not the document in question was made available to the public.

In case T 1553/06 the board analysed *inter alia* whether two webpages labelled I1 and I2 (the same I2 as in the present appeal) formed prior art. I1 and I2 were considered to have existed on the Web. Their contents were proven to have been found several times by a Dutch notary public after entering keywords in a public search engine. The opponent had furnished corresponding notarial records as evidence to that effect. The board held that the above test was complied with in relation to both these documents and therefore that both of them formed prior art. As for further document I3, for which no notarial record had been submitted, the board left the question as to whether that document existed on the Web unanswered. In any case, since the board found that I3 had neither been indexed by a web crawler nor could

be found by guessing its URL, the board arrived at the conclusion that there was no direct and unambiguous access to I3 and that it thus did not form prior art.

The board notes that in the present case even a superficial comparison between access to webpages and access to e-mails transmitted via the Internet before the filing date reveals marked differences, including the following:

- It is disputed between the parties whether illegal interception ("hacking") of e-mails was commonly possible for the skilled person in the field of the present invention.
- It is also disputed and there is no evidence that, before the filing date of the opposed patent, e-mails could be found on the basis of keywords with the help of a public search engine.
- Even assuming that it might have been possible, along the route that an e-mail takes, to retrieve it as a whole, i.e. that the packets into which it had been divided were reassembled at the point of interception, then, in the absence of an existing equivalent to a public web search engine, it would seem that the e-mail would have had to be searched for at a plethora of ISP mail servers and MX hosts (see D3, page 1, under the heading "How can an email message be intercepted?") all over the world and on the networks of a multitude of ISPs that were independent of one another. The opponent itself alleged that as the e-mail addresses for AkzoNobel (from which C5 was sent) and "DSM" (where it was received) had a top-level domain ".com" and both entities were large multinational companies there was no certainty that e-mails from and to these addresses were sent externally from a company server located in the

Netherlands. It was possible that they could have been sent first via an internal network (intranet) within each company to any location in the world where that company had a server and thence externally (via the Internet) from that country.

In addition, the opponent confirmed that it was not alleging any specific instance of disclosure to any third party of the e-mail C5 sent from Mr. de Vries of AkzoNobel to Mr. Mooij acting for the opponent. In contrast thereto it should be recalled that, in case T 1553/06, the fact that webpages I1 and I2 were retrieved from the Internet was certified by a Dutch notary public.

In the light of the above, the board has doubts as to whether public availability of e-mails transmitted via the Internet can reasonably be established at all if the technical conditions of the above test for public availability of webpages were to be applied *mutatis mutandis*, i.e. whether e-mails transmitted over the Internet could be accessed and searched in a way comparable to that of webpages, independent of whether or not access to and disclosure of the content of the e-mail were lawful. The board rather is of the opinion that the differences between webpages and such e-mails make a strong *prima facie* case against public availability of the latter.

The board however does not deem it necessary for purposes of the present case to embark on a more thorough enquiry into this issue. This is because it will be shown below that, on the basis of legal considerations relating to the lawfulness of access

and/or disclosure of e-mails sent over the Internet, e-mail C5 cannot be deemed to have been publicly available before the filing date. More specifically, the **legal** condition of the above test, applied *mutatis mutandis* to e-mail transmission via the Internet, of access by "a member of the public, i.e. someone under no obligation to keep the content of the document secret", is not complied with. Legal considerations outside the areas of European patent law and fundamental rights are based on the parties' submissions and may or may not reflect the actual state of the law at the relevant points in time.

In the following the board will assume *arguendo* that **technical** conditions of a test for public availability of e-mails transmitted via the Internet could still be devised that such e-mails could meet.

4.6.3 Breakdown of the legal analysis

The subsequent discussion is based on the board's understanding that the opponent, in essence, addresses the legal issues relating to the lawfulness of access and/or disclosure of e-mails sent over the Internet under two distinct hypotheses:
- an individual, i.e. a person to whom the task of monitoring e-mail traffic has not been entrusted, might have intercepted e-mail C5; and
- an ISP might have performed such an act, either for operational purposes or to comply with governmental requests.

Considering the distinction between individuals and ISPs to be expedient, the board will proceed with its analysis accordingly (see points 4.7 and 4.8 below). For

the reasons given in its analysis below, the board is of the view that
- in the case of an individual, the question is whether access and disclosure are lawful,
- in the case of ISPs, assuming access to be lawful under certain circumstances, the question is whether disclosure would then also be lawful.

For the sake of simplicity, the board will assume *arguendo,* apparently in line with the opponent's submissions, that any ISP through whose installations e-mail C5 was routed had the technical means to reassemble an e-mail if necessary.

4.7 Whether C5 forms prior art because an individual might have intercepted it from the Internet

4.7.1 Summary

Even under the assumption that **technical** conditions of a test for public availability of e-mails transmitted via the Internet could be devised that such e-mails could meet, however, e-mail transmission via the Internet would still not have rendered e-mail C5 publicly available for legal reasons connected with such interception. This follows from the considerations set out below.

4.7.2 Unlawfulness analogous to confidentiality agreement

In the communication annexed to the summons, the board considered that interception of e-mail C5 might have been unlawful in the relevant territories. The board

described the legal consequences of this possibility, drawn by analogy, as follows:

According to established case law, information covered by a confidentiality agreement is not considered to be publicly available, provided that it has been kept confidential. For the board, it might follow by analogy that information that is legally prohibited from being accessed, let alone disclosed, is not publicly available either, unless it has actually been disclosed before the filing date of the application. In the case of a confidentiality agreement a person is in *possession* of certain information but, because of that agreement, not allowed to *disclose* it. On the other hand, a legal prohibition of access does not permit a person to *obtain knowledge* of certain information. Should that person still obtain such knowledge in breach of the law, then the prohibition of access might also imply a prohibition of disclosure of that knowledge and the question of any legal impact of a confidentiality notice might be left unanswered.
(See paragraph bridging pages 25 and 26)

In the above communication the board mentioned a number of legal provisions according to which, at the filing date, intercepting e-mails might have been illegal both under Dutch (telecommunications and criminal) law and under the law of the then European Union, i.e. of the "E.U.-15" (the E.U., at that time, consisted of 15 Member States: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the United Kingdom). As for E.U. law, the board, more specifically, referred to Directive 97/66/EC.

As a consequence, the board issued the following invitation to the opponent:

The opponent is invited to show that email C5 was routed via one or several territories in which it was lawful to intercept it and to disclose its contents. (See point 3.3.2.4.)

In this context the statement by the opponent relating to the question of how to determine whether the content of an e-mail could be deemed public (see letter of 11 March 2011, at point 3.5) is also of relevance. According to the opponent, this question had to be considered at several stages: (i) at the sender, (ii) during message transmission and (iii) at the recipient. The opponent went on to say:

> If at any one of these stages at least one reader could (not did) have accessed its contents and had a reasonable belief that he was free to repeat its contents to another person then the contents of the email must be deemed made available to the public.

For the board it would follow that, under this view, if the reader held no such reasonable belief (based on the law of confidence), then the e-mail had to be deemed not made available to the public.

Moreover, the opponent argued that a reader reading an e-mail by unlawful interception (hacking) might reasonably assume its content was, in principle, confidential. For the board it would follow from this assumption that an e-mail that was intercepted unlawfully was, in principle, not publicly available either.

Thus the board considers that the opponent's assumptions also lead in principle to the board’s preliminary conclusion above regarding the analogous consequences of prohibition of access and disclosure by law and by contract (NDA). The board now confirms this conclusion.

4.7.3 The law in the territories through which C5 was routed

(a) Whether the territories are of legal significance

In reply to the board's communication annexed to the summons to oral proceedings, the patentee observed that, in the view expressed therein, the dividing line between public and non-public was strongly dependent on "technical issues how the e-mail was actually sent" and on a wealth of national legislation on e-mail privacy. Such a practice would never provide certainty to users of the European patent system and to the public at large.

The opponent, in its reply, considered the board’s invitation (reproduced above, at point 4.7.2), referred to as a "test" by the opponent, to be both unreasonable and unnecessary - only to, in essence, apply the letter of that "test" in that very reply, and later again during the oral proceedings. The opponent relied, in particular, on a map of the inter-regional Internet backbone (document O8) to show the likelihood that the e-mail was routed through the U.S.

Apparently, the opponent, like possibly the patentee as well (referring to "technical issues how the e-mail was actually sent"), considered that the board, in its invitation, was requesting the opponent to furnish e-mail header information. The board, however, had made no such express request. The fact that the opponent itself relies on the territories through which the e-mail was routed and attempts to establish that route (via the U.S.) on the basis of a map of the inter-regional Internet backbone (document O8) implies that, in the opponent's opinion, proof of the e-mail's route might be

established by means other than header information. (The board however does not mean to exclude the possibility that header information might constitute an appropriate means of evidence to that effect.)

In this context the board again notes the opponent's reference in the notice of opposition to Directive 2002/58/EC requiring E.U. Member States to bring into force the provisions necessary to comply with this Directive. At the patentee’s request, the opponent furnished a copy of the Directive, and the patentee, in the proceedings before the opposition division, discussed its implications (see letter of 15 May 2007, at page 2). Against this backdrop, the patentee’s latest stance denying the usefulness of taking (national) legislation into account amounts to an about-face.

The board considers that, in line with the parties' position before the opposition division and the opponent’s (at least implied) position before the board, the law in force in the territories through which an e-mail is routed naturally does play a role because all the activities on the territory of a sovereign state are, as a simple consequence of that sovereignty, subject to the state's laws, unless the state has lost its jurisdiction on certain subject-matter, in particular because it has transferred it e.g. to an international organisation. E-mail traffic being routed across the globe, such transfer would have had to be made on a global scale, e.g. by entrusting the corresponding tasks to a global international organisation. It has not been claimed by any party that this has taken place.

The conclusion that the law in force in the territories through which an e-mail was routed is of legal significance does not exclude, however, that interception by an individual may, across the whole world, not lead to public availability within the meaning of Article 54(2) EPC 1973 of the e-mail intercepted. This is because it might be possible to break down the world into territories in which interception was unlawful and territories in which interception was lawful but such lawfulness could not be taken into account for legal reasons. These questions are being dealt with in points (b) and (c) below, respectively.

(b) The legal significance of routing C5 within the E.U. and possibly the U.S.

While it was the opponent’s original assertion that C5 formed prior art for the sole reason that it was transmitted over the Internet, the opponent’s submissions in the oral proceedings, as already set out above, were focused on the allegation that e-mail C5 was routed within the then E.U.-15 and possibly the U.S. and that in both territories it was illegal for an individual (but not for an ISP) to intercept e-mails.

The board considers that it is the opponent's duty to state the facts and also, in principle, foreign or international law concerning its case (see above, point 3.1). The board therefore sees no reason to make enquiries of its own, especially given that the patentee made no objections to the opponent's submissions in this regard in the oral proceedings. The board notes that an e-mail transmitted over the Internet before the filing

date of 1 February 2000 in either the European Union (then comprising 15 Member States) or the United States was, according to the parties' submissions, prohibited from being intercepted, whatever the pertinent legal provisions may have been. In this respect the board refers to its analogy made in the communication annexed to the summons (see above at point 4.7.2), according to which information that is legally prohibited from being accessed, let alone disclosed, is not publicly available either, unless it has actually been disclosed before the filing date of the application. It follows from this analogy that transmission of e-mail C5 via the territories of the E.U. and possibly the U.S. does not, by itself, make the content of that e-mail publicly available. In other words, the legal condition of the test developed in T 1553/06 (see point 4.6.2 above), applied *mutatis mutandis* to e-mail transmission via the Internet, of access by "a member of the public, i.e. someone under no obligation to keep the content of the document secret", is not complied with.

Thus, the question as to whether the inter-regional Internet backbone map O8 alone, showing the situation as of September 2000, established that e-mail C5 was indeed routed via the U.S. need not be answered.

(c) The legal significance of any routing of C5 outside the E.U.-15 and the U.S.

However, even if e-mail C5 had been routed beyond the borders of the E.U.-15 and the U.S., the same result would ensue from the aforementioned analogy.

The opponent has made no specific indications as to any countries outside the E.U.-15 and the U.S. through which e-mail C5 might have been routed. The opponent relying on a certain report to the U.S. Congress as evidence (see footnote 2) only indicated that, in April 2010, a substantial amount of e-mail traffic was diverted from the U.S. to China, without, however, providing evidence that this was also the case before the filing date. For that reason alone, the allegation that e-mail C5 might also have been routed to China is pure speculation. In the absence of pertinent evidence, the question as to the standard of proof under which such evidence would have to be assessed does not arise.

Furthermore, the opponent alleged that it was possible that e-mail C5 sent by Mr. de Vries of AkzoNobel could have travelled first via AkzoNobel's internal network (intranet) to any location in the world where that company had a server and thence externally (via the Internet) from that country, depending on the quickest path available, again to any location in the world where the receiving company had a server. Yet, again, no evidence has been filed as to any specific circumstances under which e-mail C5 was thus routed. Thus, once more, these submissions as to a possible routing outside the E.U. and possibly the U.S. are mere speculation.

However, the board will still assume *arguendo* that e-mail C5 did traverse at least one territory outside the E.U. and the U.S. and that in that territory it was not unlawful to intercept C5. Even under this hypothesis the board would not accept any ensuing public availability of C5. This is because, in the board's view, the practical and effective protection of the fundamental

rights enshrined in Article 8 of the European Convention of Human Rights and Fundamental Freedoms (ECHR) would be jeopardised if information obtained in violation of this provision could be relied on to the detriment of those for whom the rights were designed.

The ECHR is relevant for the purposes of the EPC (see T 1465/07, point 8 of the Reasons and the cases cited there). Article 8 ECHR reads:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The European Court of Human Rights held in *Liberty and Others v. The United Kingdom* (no. 58243/00, 1 July 2008, paragraph 56):

Telephone, facsimile and e-mail communications are covered by the notions of "private life" and "correspondence" within the meaning of Article 8 (see *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 77, 29 June 2006, and the cases cited therein).

The Court has also consistently held that:

[w]hile the essential object of Article 8 is to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this negative undertaking, there may be **positive obligations** inherent in effective respect for private or family life. These obligations may involve the **adoption of measures** designed to secure respect for private life even in the sphere of the **relations of individuals between themselves** (see *X and Y v. the Netherlands*, 26 March 1985, § 23, Series A no. 91, and *Armonienė*, cited above [*Armonienė v. Lithuania*, no. 36919/02, 25 November 2008], § 36).

(See *Von Hannover v. Germany (no. 2)*, nos. 40660/08 and 60641/08), Grand Chamber, 7 February 2012, paragraph 98; emphases added.)

Against the backdrop of the above case law, it is the board's view that the right to the protection of private life and correspondence may be interpreted as requiring Member States of the Council of Europe to adopt measures prohibiting the violation of individuals' rights by the interception by other individuals of their e-mails sent over the Internet, subject to the exceptions mentioned in Article 8(2) ECHR.

As for the E.U.-15 the board, in this context, refers to Directive 97/66/EC that the opponent considered to be the law. Recital (2) of that Directive states:

... confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights (in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms) and the constitutions of the Member States.

Furthermore, Article 5 (and 14) of that Directive which the opponent also relied on (in the oral proceedings the opponent no longer insisted on the fact that, according to Article 15(1), the last implementation date of this article was 24 October 2000, i.e. after the filing date) read:

Article 5 - Confidentiality of the communications

1. Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with Article 14 (1).

Article 14 - Extension of the scope of application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in [Article 5] ..., when such restriction constitutes a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system, as referred to in Article 13(1) of Directive 95/46/EC.

The board thus considers that the E.U.-15 did adopt measures to protect individuals' rights against interception of their e-mails sent over the Internet, not only in respect of governmental requests to ISPs to monitor e-mails but also against violations by individuals, such as hackers, of the rights of other individuals, i.e. senders of e-mails.

The board notes in this respect that a distinction was made in recital 13 of the Directive between "the fundamental rights of natural persons" and "the legitimate interests of legal persons". As far as the protection of e-mails against interception is concerned, the board however believes that the obligation to grant protection by the law exists irrespective of whether e-mails are sent by a natural person or by such person on behalf of a legal person. This is because the rights of both natural and legal persons in respect of the secrecy of the content of their e-mails should be afforded equal weight. Interception must be prohibited indiscriminately, subject to exceptions such as those set out in Article 8(2) ECHR or in Article 14(1) of Directive 97/66/EC (both provisions were reproduced above).

(Regarding the right to "respect for ... his home" protected by Article 8(1) ECHR, the Court held in *Société Colas Est and others v. France* (no. 37971/97, 16 April 2002, paragraph 41) that:

in certain circumstances the rights guaranteed by Article 8 of the Convention may be construed as including the right to respect for a company's registered office, branches or other business premises.

It should be noted that on the filing date of 1 February 2000 not only the E.U.-15 but all EPC Contracting States were also Member States of the Council of Europe, with the exception of Monaco that joined the Council on 5 October 2004.

In the light of the above, the question as to any impact of e-mail diversion to China (see document O2) has become moot also because even if it had been lawful in China to intercept e-mails the board could not take that fact into account. It should also be noted that the opponent has offered no evidence to this effect, and indeed has not even expressly alleged any instance of lawful access.

(d) Conclusion

As a consequence, C5 does not form prior art because an individual might have intercepted it from the Internet, no matter in which territory of the world.

The opponent, in the oral proceedings, in any case focused more specifically on alleged lawful interception of e-mails by ISPs in the U.S., on the one hand, and of ISPs, as the case may be, in conjunction with law-enforcement personnel in the E.U. on the other hand. Accordingly, the board relying *arguendo* on such

lawfulness of interception will discuss the legal implications separately for each region below. In this context the board will assume, again favourably for the opponent, that it would be possible to devise technical conditions of a test that do not a priori exclude public availability of e-mails sent via the Internet and that ISPs were able, before the filing date, to intercept e-mails and search them on the basis of keywords (see the assertions under point VIII relating to document D3).

4.8 Whether C5 forms prior art because an ISP might have intercepted it from the Internet

4.8.1 The situation in the U.S.

(a) The opponent's proposed approach

Assuming lawfulness of interception of an e-mail by an ISP, the opponent proposed to assess the **content** of the information transmitted and its **context** in order to decide whether an e-mail should be deemed **confidential.** Such a finding would imply a duty, based on the law of confidence, for an ISP to keep the content of the e-mail secret, which, in turn, would rule out its public availability. The opponent's proposed approach is explained in greater detail below.

The opponent asserted in the oral proceedings that ISPs in the U.S. were, at the filing date of 1 February 2000, not required to keep data confidential because the E.U. "safe harbor" provisions had only been adopted in July 2000, i.e. after the filing date (under the Safe Harbor Agreement, U.S. signatories promise to handle the data of European citizens according to E.U. rules). The

supporting evidence for the legal situation before that date, which the opponent supplied in the oral proceedings, consists of the two documents "Opinion 1/99" and "Data Protection" (see footnote 4 above).

The "Data Protection" article of 1998 written by U.S.-based authors identifies a sharp contrast between privacy and data protection policies in the U.S. and in Europe. Where the U.S. approach had been to provide specific and narrowly applicable legislation, in Europe most countries had implemented unified supra-national policies with omnibus legislation. The article provides the following, more specific information:

The European legislation outlines a set of rights and principles for the treatment of personal data, without regard to whether the data is held in the public or private sector. In the United States, the legal tradition is much more concerned with regulating data collected by the federal government. (See page 17, second paragraph.)
...
The United States has largely avoided legislation governing the treatment of sensitive personal information in records systems held by sources other than the federal government. (See page 19, first paragraph.)

A European point of view is expressed in the paper "Opinion 1/99" by the "Working Party on the Protection of Individuals with regard to the Processing of Personal Data" (established by Article 29 of Directive 95/46/EC):

1. Privacy and data protection in the United States is found in a complex fabric of sectoral regulation, at both federal and state level, combined with industry self-regulation. Considerable efforts have been made during recent months to improve the credibility and enforceability of industry self-regulation, particularly in the context of the Internet and electronic commerce. Nevertheless, the Working Party takes the view that the current patchwork of narrowly-focussed sectoral laws and voluntary self-regulation cannot at present be relied

upon to provide adequate protection in all cases for personal data transferred from the European Union.

2. Given the complexity of the US system of privacy and data protection, the establishment in the US of an agreed “benchmark” standard of protection in the form of a set of "safe harbor” principles offered to all economic actors and US operators is a useful approach ...

One may conclude from the above two documents, especially the excerpts just quoted, that data protection and privacy standards in the U.S., apart from data collected by the U.S. Federal government, were less restrictive than in the E.U. when those documents were published, i.e. in 1998 and 1999 respectively, and thus before adoption of the Safe Harbor Agreement in July 2000. Nevertheless, it must be pointed out that these two documents do not expressly establish that ISPs in the U.S. were free to disclose data to which they had access; in fact they do not mention ISPs at all.

The opponent itself has anyway acknowledged that there were restrictions on an ISP's freedom to disclose the contents of e-mails read in transit imposed by the law of confidence, giving examples including the following:
- an ISP administrator could reasonably expect no prohibition on passing the information in a press release to a friend,
- but a message sent from a managing director to his board of directors which included financial information about the company and a request to store paper copies in a locked cabinet would be deemed confidential.
Accordingly, both the nature and context of the information transmitted had to be assessed before a lawful reader in transit (such as an ISP administrator) could decide whether the content of an e-mail was deemed confidential and so to be treated as such.

The following excerpt from document D1 submitted by the opponent makes it clear that, at the filing date, ISPs in the U.S. were indeed prohibited by law, even though no specific legal basis is indicated, from disclosing certain information that they can access to third parties:

Most ISPs are highly ethical and have the best interests of their customers at heart; however, there have been instances of less scrupulous ISPs taking advantage of the trust their users place in them. There was a case in San Francisco where an ISP was charged with multiple counts of intercepting email traffic between January and June 1998 from one of their business customers, namely Amazon.com, and forwarding the insider information contained therein to a competitor. They settled the case with prosecutors in November 1999. There have been other instances of this type of behavior, but these cases are frequently settled with relatively little press. This is not just limited to small ISPs however, in the case of a large ISP it is much more likely that it is a renegade employee intercepting messages than the ISP itself, but the ease of interception is just the same.

The question therefore is whether the board should draw upon the opponent's proposal to assess the **content** of the information transmitted and its **context** in order to decide whether an e-mail should be deemed **confidential**, thereby implying a duty, based on the law of confidence, for an ISP to keep its content secret (in the oral proceedings the parties said that breach of confidence might amount to a tort, but did not enter into greater detail). Where content and context of the information transmitted suggested no such duty, then the ISP would be free to pass it on to anybody (referred to by the opponent as the "proportionality" test; see below, under point (b)(i)). Then the information would have to be considered publicly available within the meaning of Article 54(2) EPC 1973. In dealing with this topic, the board, as stated, assumes *arguendo* that any ISP involved

in the transit of e-mail C5 was indeed able, at a relevant date before the filing date, to assemble the various e-mail packets into a complete e-mail and to search e-mails on the basis of keywords. The opponent's submissions obviously imply that it was generally not unlawful for U.S. ISPs to intercept e-mails, and the following analysis is based on this assumption.

(b) The board's position regarding the opponent's approach

The board is not convinced that the opponent's proposal reflects the right approach.

(i) The lack of relevance of intent

Content and context cannot be considered to be decisive for determining whether an e-mail is to be treated as confidential. Content and context thus cannot serve as a basis for drawing a distinction between e-mails with publicly available and non-available content. This follows from the considerations below.

The "proportionality" test suggested by the opponent is not convincing. In reality, this is a (binary) threshold test, i.e. whether the information attains a certain threshold of confidentiality, so the person reading it lawfully would decide that he was not permitted to disclose it. (Given that "proportionality" is the relationship of two variables whose ratio is constant, a genuine proportionality test would establish the degree of disclosure permitted to be made depending on the degree of confidentiality.) In determining whether that threshold has been reached, the **content and context**

would be decisive because they would make it possible to identify the sender's **intent** (see especially the opponent's submission as set out above, under section VIII entitled "(i) The sender stage: intent", and the summary under the subsequent point (v) of the same section). The patentee also expressly suggested relying on intent to assess confidentiality.

Consequently, this test involves a subjective element for determining whether an e-mail is to be treated as confidential and thus, under the law of confidence, in the parties' submissions, is prohibited from being disclosed. The decision of the Enlarged Board of Appeal in case G 1/92 (see point 2.1 of the Reasons), however, meant to exclude a subjective element from the assessment of novelty. Novelty thus implies an entirely objective assessment. This must take into account the nature of e-mail communication as point-to-point or point-to-multipoint transmission, not to the public at large, and the ISPs' role as transmission facilitators, not forwarders of single messages to indiscriminate addressees. For that reason alone the e-mails that ISPs can access must be treated as one single set of confidential messages. Given that, according to the opponent's submissions, the law of confidence (whatever the specific rules may be) prohibits their disclosure, the e-mails must all be deemed to be non-public, unless a specific instance of divulgation has been proven. Therefore, in this context, there is no need to assess any impact of disclaimers indicating confidentiality of e-mail content, no matter how they are phrased (e.g. whether personal to the sender or added automatically).

In addition, an intent-based approach would on balance not be more practical, as the patentee contends, than identifying the e-mail route and the law in the territories traversed. This is because such an approach would involve a large grey area where intent could not be readily identified. What about, for instance, company financial information presented like a press release, but confidential? Furthermore, a person lawfully reading an e-mail would have to know the applicable specific rules of the law of confidence in order to be able to decide whether or not disclosure of the content of a specific e-mail was lawful.

The board wishes to point out that the considerations under this point (i) not only apply to ISPs in the U.S. but also to individuals intercepting e-mail traffic lawfully anywhere in the world. This scenario has not been taken into consideration above in relation to the E.U.-15 and the U.S. because the parties considered that interception was prohibited in those territories (see point 4.7.3 (b) above). Thus, even if in the U.S. (or elsewhere in the world) it had been lawful for the public at large to intercept e-mails before the filing date, then they would have had to make the same assessment as ISPs to ascertain whether the e-mail in question had been intended by its author to be kept confidential. Because of this necessarily subjective element that G 1/92 had sought to exclude, e-mail traffic as a whole must be rated confidential. It is also for this reason, in addition to those given above, at point 4.7.3 (c), that C5 does not form prior art because an individual might have lawfully intercepted it from the Internet.

(ii) ISPs being in a situation analogous to that of an NDA

The board notes that, in exploring the issue of public prior use in T 809/95, the board deciding that case addressed the question of whether the persons who had tested the allegedly prior used product had had **an interest of their own in secrecy**. In this regard, the board relied on T 830/90 (OJ 1994, 713, point 3.2.2). The present board takes the view that, where such a party's own interest in secrecy can be established, then the situation will be analogous to that of a non-disclosure agreement between the parties involved.

In this respect, the board considers that, at the date of transmission of C5 (or C3) before the filing date of 1 February 2000, independent of any applicable data-protection and privacy or tort law, there generally was an expectation not only among e-mail users in the E.U., where, according to the opponent, stricter rules applied than in the U.S., but also among many e-mail users in the U.S., that not only e-mail messages which a lawful reader could rate as confidential, but also those that were clearly non-confidential would not be freely forwarded to third parties, irrespective of any legal prohibition against doing so.

As already mentioned, the two documents "Opinion 1/99" and "Data Protection" are silent as to ISPs' duties relating to data protection and privacy. Furthermore, the opponent, while referring to "typical terms and conditions in an ISP contract" has not provided any such boilerplate agreement. The opponent has therefore not established that, even assuming freedom to forward a

non-confidential e-mail to anybody for lack of prohibition under data-protection and privacy law, or tort law relating to confidence, an ISP was likewise allowed to pass on e-mails to third parties for lack of prohibition by contractual provisions. Nor has the opponent proven that, in the absence of such contractual provisions, there was also no general expectation on the part of e-mail users that ISPs would not forward e-mails. It would have been for the opponent to adduce appropriate evidence to that effect. Again, it is not for the board to make enquiries as to the state of the pertinent U.S. law and practice at the date of transmission of C5.

Given that forwarding e-mails to third parties might be detected, this might hurt the ISP's reputation, which in turn would bring about the danger of losing customers. The board therefore concludes that an ISP had a business interest of its own in keeping secret the e-mails to which it had access.

On the other hand, the board does not deny that there may have been several possible ways for ISPs to exploit e-mail content that might not have been frowned upon by many customers in the U.S. An example may be the use of e-mail content for drawing up profiles of the consumption habits of holders of e-mail accounts and selling those profiles to advertisers for targeting e-mail senders with advertising corresponding to those habits. Obviously, however, from such profiles no advertiser could derive the content of a specific e-mail such as C5.

In conclusion, applying the rationale derived from T 809/95 and T 830/90, the ISP's identified business interest in keeping e-mails secret creates a situation analogous to that of a non-disclosure agreement between the ISP and its customers. The fact that an ISP, through staff members instructed accordingly, might lawfully have read e-mails in transit has not therefore made those e-mails publicly available, independent of whether or not there were legal provisions (of data-protection and privacy law, or tort law) prohibiting the forwarding of those e-mails.

Regarding the role of ISP employees acting on their own behalf, the board notes the following. As indicated in the above quote from the document "Data Protection" there may be renegade ISP **employees** passing on e-mails to third parties. To that extent the considerations above relating to ISP companies apply *mutatis mutandis*. Employees also have a business interest in keeping the e-mails secret, because otherwise their companies and themselves might have to face severe consequences and thus ISP employees might lose their jobs. Nothing more need be said here, and nothing more can be said failing access to copies of typical employment contracts between ISPs and their employees which the opponent has not furnished.

(c) Conclusion

In the light of the above findings made under the assumption that U.S. ISPs were entitled to lawfully intercept e-mails transmitted over their networks, e-mail C5 has not become publicly available for that reason alone if it passed via the U.S. The opponent

would have had to prove a specific instance of disclosure of that e-mail.

4.8.2 The situation in the E.U.

(a) Disclosure by ISPs

As a preliminary matter the board notes that since lawful access to e-mails by U.S. ISPs at the filing date did not put e-mails into the public domain, this must be true *a fortiori* for the E.U. on the basis of the opponent's submissions, according to which U.S. ISPs had greater leeway than E.U. ISPs in dealing with e-mail content that had been lawfully intercepted. It is therefore only for the sake of completeness that the board will now discuss below the opponent's submissions on the E.U. situation.

The opponent argued that, as in the U.S., no general prohibition to intercept e-mail applied to ISPs in the E.U.-15 at the filing date of 1 February 2000. Article 5 of Directive 97/66/EC prohibited interception within the E.U. "except when legally authorised", i.e. in accordance with Article 14(1) of that Directive (the pertinent part of which is reproduced above, at point 4.7.3(c)). Administrators at an ISP would routinely access random e-mails to check that ISP policies were being complied with or address technical issues or comply with government requests. ISPs in the E.U.-15 were not generally allowed to disclose e-mail content. However, it was likely that at least one ISP administrator in the E.U. had not inferred any duty of confidence from the content and context of the e-mail C5.

Hence, the content of e-mail message C5 had to be deemed made available to the public.

The board has already dismissed the analogous reasoning in relation to U.S. ISPs above under points 4.8.1(b), which applies *mutatis mutandis*. As for the situation in the E.U.-15, the board in addition refers to its discussion of Article 8(1) ECHR in the context of interception by a member of the public, at point 4.7.3(c) above. There the board concluded that the right to the protection of private life and correspondence may be interpreted as requiring the adoption of measures prohibiting the violation of individuals' rights by other individuals by the interception of their e-mails sent over the Internet, subject to the exceptions mentioned in Article 8(2) ECHR. The board is of the opinion that Article 8(1) ECHR also requires the adoption of measures prohibiting the disclosure by ISPs, independent of content and context, of e-mails which, under these exceptions, they may have lawfully intercepted. In this context the board recalls that, pursuant to Article 5 of Directive 97/66/EC, E.U.-15 "Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services."

The board is of the opinion that ISP employees must generally be considered to be law-abiding, i.e. to heed legal prohibitions of disclosure of e-mails, until the opposite has been proven in a specific case. Under these circumstances, to establish disclosure of an e-mail to the public by ISPs in the E.U., the above-mentioned legal situation lends additional weight to the

conclusion that it would have been for the opponent to prove a specific instance of such disclosure.

(b) Disclosure by law-enforcement personnel

As for the situation in the E.U., the opponent not only relied on ISPs' lawful activities, but also on those of law-enforcement personnel. In the oral proceedings, the opponent focused on exceptions in Directive 97/66/EC for law enforcement, arguing that, in this respect, the "proportionality" test applied to the prosecutor issuing requests to an ISP, not to ISP personnel.

The opponent more specifically referred to the situation in the U.K. under the Regulation of Investigatory Powers Act (RIPA) concerning encryption. These submissions are based on document O9 (cited at footnote 3 above), where it was stated that the RIP Bill was introduced in particular “to comply with the new Human Rights Act” (see O9, second paragraph of section 7, at page 53). The British Chamber of Commerce (BCC) expressed concerns that interception under RIPA having been lawful (i.e. permitted by Directive 97/66/EC) there was a potential danger that critical company information *could* be published.

According to O9 (at point 7, first full paragraph), the regulatory intents regarding encryption were first mentioned in 1996, but Royal Assent to RIPA was given only in July 2000. The filing date of the patent in suit is 1 February 2000. The board therefore is at a loss to see how RIPA could conceivably be of relevance for the present case.

It is therefore needless to say that more than 10 years had passed since adoption of RIPA when the opponent first relied on RIPA in its submission of 11 March 2011, without providing any indication as to whether the BCC's misgivings were justified in the light of experience with interception on the basis of RIPA.

Favourably for the opponent, the board still supposes that law-enforcement authorities in both the U.K. and the other fourteen Member States of the E.U. on 1 February 2000, were, under certain circumstances, entitled to request ISPs to intercept non-encrypted information. In this respect, no evidence has been submitted as to which information would have been divulged in such circumstances. The board therefore considers that law-enforcement personnel must be presumed to have acted lawfully unless the opposite is proven in a specific case.

4.8.3 ISPs outside the U.S. and the E.U.-15

In the absence of pertinent submissions by the parties, the board assumes that the considerations made for U.S. ISPs apply *mutatis mutandis*.

4.8.4 Conclusion

E-mail C5 has not become publicly available for the sole reason that an ISP in the U.S., in the E.U.-15 or in other territories of the world may have lawfully intercepted it and that in the E.U.-15 law-enforcement personnel may have lawfully obtained access to intercepted e-mails at their request.

For a finding of public availability of e-mail C5 it would have been necessary for the opponent to establish that e-mail C5 had been disclosed by ISP or law-enforcement personnel to the public in at least one single instance. The opponent however expressly confirmed in the oral proceedings that it was not making such an assertion.

4.9 Overall conclusion regarding claim 1

Given the above findings, C5 does not form prior art, and from I2 alone the skilled person would not arrive at the subject-matter of claim 1 without an inventive step. The opponent has not based its challenge to inventive step on a combination other than I2 and C5. The subject-matter of claim 1 is thus inventive. The same applies to claim 2 which depends on claim 1.

5. Claim 3

The opponent maintains that claim 3 is not inventive in view of either the combination of C5, I2 and C3 (in that order) or I2, C5 and C3 (in that order) (see points 3 and 4 of the statement of grounds).

E-mail C3 was allegedly sent over the Internet after having been encrypted by PGP. Hence the board's considerations relating to non-encrypted e-mail C5 apply *a fortiori* to C3, as the patentee rightly pointed out. This means that its transmission over the Internet did not make it publicly available either.

The submissions relating to the encryption software PGP, which the opponent no longer maintained and replaced by

submissions on law-enforcement activities under RIPA, therefore need be given no consideration.

As the opponent relied on the above combinations of documents, including C3, in arguing that claim 3 was not inventive, the fact that neither C5 nor C3 constitute prior art inevitably deprives this reasoning of its basis. Hence the subject-matter of claim 3 is also inventive.

The question of whether claim 3, which is a claim for the use of the subject-matter of claim 1, shares the fate of claim 1 for that reason, or whether different considerations apply - as the opponent submitted in its letter of 14 March 2011 drafted after the oral proceedings before the board - need not be answered. The opponent has not alleged that on the basis of I2 alone the subject-matter of claim 3 did not involve an inventive step. Therefore the board exercised its discretion in not reopening the debate on claim 3.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

K. Boelicke F. Edlinger