Fighting tomorrow's problems with yesterday's remedies

By Dr Hendrik Schöttle, Attorney-at-law at Hambach & Hambach LLP, Munich

Summary

There is no effective means for the government to block undesirable websites on the Internet from access from Germany. The currently extant methods can be set at naught with two mouse clicks without any special skills or additional hardware or software. In addition it cannot be technically excluded that the blockade likewise blocks out numerous contents that are not at all the target of the order requiring it. Where more than one or two websites are to be blocked a system is additionally required making regular automatic updating of the blocking lists possible.

In view of the immense financial and manpower expense, the high degree of collateral damage and evasion that can be accomplished simply by anyone, any blocking order fails the test of the proportionality principle and is thus contrary to law.

Discussions about the future of the German sports betting and gaming market continue unabated. The EU has recently also made it clear that it will not accept the planned revision of the Lottery State Treaty. The planned regulations are said to be contrary to freedom of services and are therefore against EU law, according to EU Internal Market Commissioner Charlie McCreevy in an interview with Spiegel. Nevertheless the German states still intend to stick to the draft treaty. On 13 December 2006 there are to be final deliberations on the State Treaty which, if the states get their way, will enter into force on 1 January 2008.

But whether it will ever get that far has by now become more than questionable. The State Treaty includes in its most recently revised version so many exceptions in favour of state providers that there can no longer be any talk of products „consistently geared to the goal of combating compulsive gambling.“ But this is precisely what the Federal Constitutional Court demanded in its sports betting ruling of 28 March 2006.

Blocking orders as a means to the end?

In order to displace numerous European online gaming providers from the German market thought has in the meanwhile been given to calling German Internet access providers to order as well. An example: In the German Bundestag’s sports committee consideration was given to whipping the German providers of Internet access into line in view of the many online programmes operated in other EU countries. At the final meeting of the Bundestag’s sports committee the matter was succinctly stated:

> *„When an unambiguous statutory prohibition is available for the future it will be enforced as well. Enforceability will affect the Internet providers on the one hand and the banks that handle payment traffic on the other one.“*[1]

In the current draft of the Lottery State Treaty as well, its justification therefore proceeds on the assumption that foreign websites will be blocked by the Internet providers.[2]

The proposal sounds as simple as it seems ingenious: The German providers of Internet access will be put under an obligation of blocking the websites of foreign gaming providers. With that prospective customers in Germany will no longer have the option of accessing those providers and the (financially painful) exodus from government providers to private and better competition will be stopped. Such demands

for control of the Internet are not new. The State Council in Düsseldorf has already attempted to cut off websites with rightwing extremist contents with blocking orders. In the debate that recently flared up again over a ban on „killer games“ demands were likewise heard „to issue regulations on limiting access to Internet sites with corresponding contents.“[/i][3].

But such a project suffers from two cardinal errors at one and the same time: A blocking order is first of all completely unsuitable from a technical point of view and therefore and secondly does not stand up to a legal test of proportionality. Such demands reveal a shocking misunderstanding of what is feasible and what is not feasible on the Internet. To clarify the technical issues it will be shown below here how it is possible with two mouse clicks to circumvent even the toughest form of website blocking, blocking of the IP address, without any additional software or special skills whatsoever. What ramifications that has for the legal reliability of blocking orders will then be examined in a second section.

Technical feasibility: all appearance, no essence

In order to illustrate why a blocking order is doomed to fail from a practical point of view, the technology behind the Internet must be considered in greater detail. The Internet was developed as a network whose strength is in particular that it is highly fail-safe; this fail-safe nature is in particular ensured by highly decentralised organisation. And precisely this strength is the great weakness of every attempt to filter out or block specific information flows.

DNS blocking

On the Internet, to provide addresses of computers, and thus for specific websites as well, the so-called domain name system (DNS) is used. It makes it possible to reach the website of the German Federal Constitutional Court in the

browser (e.g. in Firefox or Internet Explorer) at the address http://www.bverfg.de. A method of blocking websites that is also proposed[4] by government authorities consequently provides that Internet access providers (e.g. AOL, T-Online or Arcor) do not forward enquiries to specific websites. The user then gets an error message if he calls up the website in question.[5] Does it therefore suffice to fail to forward all enquiries that call for the homepage www.bverfg.de? By no means: Many websites do not just sail under one flag on the Internet but are also accessible via alternative domain names. In the case of the Federal Constitutional Court this is something like the address http://www.bundesverfassungsgericht.de/. Added to this, by the way, is the fact that in the case of the Federal Constitutional Court in both cases even the „www“ can be left out so that would already give us four alternatives. And this with a website that is not even out to circumvent potential blocking orders by means of different spellings. In Italy, however, such objections have not had any deterrence and a list of numerous foreign gaming providers has been presented that are to be blocked.[6] But no special skilled knowledge was revealed when the URL www2.sportwetten-gera.com was included. Most Internet users know what is at stake: It is frequently customary for large providers to distribute the server load (data traffic) amongst several computers. Thus an entry page under www.sportwetten-gera.com leads to the servers www1 to www4. If the Federal Constitutional Court were to apply the same technology we would already have twelve domain names that would have to be blocked in our example, and this for a single website!

Blocking of IP addresses

But is the website at least locked up behind bars if a blocking order encompasses all domain names? Anyone answering this in the affirmative outs himself as ignorant of basic technology. Every computer has its own IP address under which

it is reachable. In the case of the Federal Constitutional Court entering http://134.96.83.81/ in the address line of the browser also lets one reach this destination. So any protection that wants to be more than just a façade must also encompass the corresponding IP addresses.

Nevertheless, with such a heavy-handed approach frequently the wrong targets would get hit. Behind a single IP address there are often thousands of websites on a multi-domain server that have nothing to do with the one black sheep that is the target of the blocking order. It must also be kept in mind that Internet is not a static quantity of servers with unchangeable IP addresses: In this way four years ago numerous websites of Swiss universities were not reachable from Switzerland because the server on which the websites were operated was given an IP address under which a rightwing extremist portal formerly could be reached.[7] Since the blocking lists were not up-to-date the university homepages were also blocked although they shared neither their domain names with the rightwing extremists nor the latter's contents. Anyone imposing a blocking order would also have to regularly check the blocked websites to see that they were up-to-date. This is not just to protect innocent parties from blocking because the gambling providers will not be sleeping. For them it is easy within a few hours to add another domain name and another IP address. The blockade on the originally used website would thus have no effect. Therefore, a system would have to be set up making it possible to change blocking lists on a daily basis in order to pass these changes on to all providers. One need only keep in mind German „trailblazing projects" like the highway tolls and the electronic health card to imagine in what decade and at what cost such a system could be completed. And even still, other providers under the same IP address would still be unjustly blocked: Anyone wishing to block the IP address of a single illegal website on T-Online would be blocking practically all other websites on T-Online.

Circumventing a website block: a matter of two mouse clicks

But even if one accepted such collateral damage and such a cost explosion needed for daily updating of the blocking list and chose the strongest form of blocking, blocking of the IP address and the DNS entry, the „firewall“ for the average Internet user would be just as insurmountable as a red pedestrian stoplight. The users can circumvent such a shield with the simplest methods. As explained above, neither expensive software nor programmer skills are needed. On the contrary, the proof of what simple child’s play it is to be able to run such a blockade is only two clicks of the mouse away.

The following must be said in advance: The following „instructions“ do not constitute confidential insider skills taken from criminal Internet forums where hackers swap their latest discoveries. By no means, the government itself explains how the „censor“ can be thwarted and anyone can read it in the 26th Work Report for 2004 of the Independent State Centre for Data Privacy in Schleswig-Holstein (ULD);[8]:

> *„The Chinese government rigidly censors the Internet traffic of users in China so that numerous Internet programmes are blocked. This also affects German companies working in China. By means of AN.ON it is possible to circumvent this censor and to access Internet programmes that are not monitored by the government.“*

AN.ON is an anonymisation service, also called an anonymiser. An anonymiser functions as a proxy, in other words as an intermediary computer through which communication with the actual computer is cleared. Originally developed for the purpose of allowing anonymous surfing it can also be used to circumvent blocked websites as the State Data Privacy Centre in Schleswig-Holstein has demonstrated. The principle is amazingly simple: The user calls up the anonymiser in his

browser, enters the website that he wants to visit and that's it! In order not to disappoint any expectations, the proof will be shown here that the entire matter is one of two clicks of the mouse.

If the homepage http://showip.net/ is called up (first mouse click), you will see the IP address under which your computer can be reached on the Internet. At the same time the operating system used by your computer as well as your browser will be shown. If you then interpose an anonymiser by calling up the site http://anonymouse.org/cgi-bin/anon-www.cgi/http://showip.net (second mouse click) you will discover that your IP address has been changed. In addition your operating system and your browser type can no longer be recognised. With this second mouse click you have already successfully run all of your DNS and IP blockades. It goes without saying that instead of the website showip.net you can call up any other website you want[9] – including ones that are actually not supposed to be reachable in Germany.

Since most of these anonymisation services are operated outside of Germany you can access without any filter the websites that are blocked in Germany. Conclusion: Anyone really wanting to block a website must also control or block all anonymisers. But this means hundreds of computers spread out throughout the world and constantly accessible via shifting addresses; something that is impossible.

Professor Gerhard Schneider, a member of the board of governors of the German Research Network, has therefore reached the following unambiguous conclusion:

> *„In reality they [website blocks] are merely an attempt to prevent direct data exchange from one legal territory with a computer located outside of that territory. It has no impact on the indirect routes and as long as its own legal territory is small in relation to the expanse of the Internet*

> *innumerable indirect routes are available. The only way to really enforce a so-called total block is consequently to disengage completely from the Internet and from all other paths of communication (including the telephone).“*[10]

It should at this point also be obvious that it makes no difference what kind of websites are being blocked:

> *„Whether you wish to move against rightwing extremists or foreign gaming sites, the means are equally ineffective since the bits are the same,“ Schneider said in a telephone interview on 20 November 2006.*

After the little demonstration given above it should be clear that every average user can operate with an anonymiser. Beyond that there are enough efforts, including on the government’s part, to promote the use of anonymisers. The ULD mentioned above has already made this its objective with the AN.ON project (subsidised by the Federal Ministry of Economics). And even if freedom of speech should fall by the wayside in the process such projects should not have any future prospects according to current plans since the same technology could also be used to undermine the government gaming monopoly, at least financially. But even if the government no longer backs the gamblers up with explicit instructions, the corresponding tips are already circulating all over the Internet.

For the sake of completeness it should be remarked that the technique presented here is only one of numerous options for running the blockade. Whether by using a proxy, setting up a virtual private network (VPN) or simply by dialling into a foreign Internet provider there are any number of other possibilities for getting to the other side of the street in spite of the red pedestrian stoplight.

[i]Besides technology there is law: (dis)proportionality in the wider sense

As we have shown, even the toughest form of website blocking, blocking the IP address, constitutes an obstruction that can be overcome without any problems by any Internet user with two clicks of the mouse. That now raises the question of whether ordering such measures can be in conformity with law at all. The focus in our remarks below is solely the issue of whether blocking an IP address is a legally acceptable means to use against the illegal contents of a website under German law. Whether the website to be blocked provides rightwing extremist contents or sports betting, the underlying legal issues, highly controversial ones in the case of sports betting providers, shall not be of further interest here. For the sake of argument we can for once assume that a website includes illegal contents.

A blocking order providing for blocking of IP addresses is only lawful if it is also proportionate. That is actually the case when the purpose pursued by it stands in an appropriate relation to the interference with its targets, in other words, the access provider affected by the order. Proportionality thus obtains if the measure to achieve the objective is suitable, required and appropriate.

Dubious per se: its suitability

A means to an end is only suitable if the effect sought can be promoted by its assistance. It is not required that the effect is actually achieved in every single instance or that it is in any case achievable. The possibility of achieving the purpose suffices.[11] The Administrative Court of Düsseldorf that ultimately affirmed the legality of a blocking order, already had problems in establishing its suitability. Doubts about the effectiveness of the blocking methods proposed during the proceedings were so overwhelming that it was said to suffice if

„…the blocking constituted a 'step in the right direction."

> *Accordingly for the measure to be suitable it suffices that it makes access more difficult … for the average … user. This refers to a constituency that has not dealt with the technical details and has likewise either left configuration of its own hardware and software to others or preferably left it in the state configured by the manufacturer … For that constituency access becomes … at least ‚more blocked' and frequently even significantly impeded."*[12]

If we assume that the average user can operate a search engine then he can also use an anonymiser. It is hard to see how any significant impediment lies in the two required mouse clicks. If the Administrative Law Court of Düsseldorf goes as far as citing the Internet user with average intelligence then it should at least credit him with having average skills. Anyone who can send and read emails, buy things from eBay and order a train ticket online will not be stumped by an anonymiser. Not to mention the fact that for online gaming both the provider and the customer are driven by tangible financial interests. They will hardly be deterred by such an ineffective shield.

It is quite rightfully pointed out that only *„a small percentage of technically quite underaverage skilled users can be blocked out by such measures."*[13]

Necessity or the milder means

Besides suitability, there also has to be a necessity, that means there cannot be any milder means available that is just as effective. That this is the case under German law has been shown very vividly by the Administrative Court of Cologne using the DNS blocking discussed above as an example:

> *„All in all, it must be said that DNS blocking does not constitute any obstruction for technically sophisticated users and with normal users whether the block works depends on chance."*[14]

But the Cologne court still assumed that a blocking, whose effectiveness depended on chance, still constituted an effective means since there was said to be no proof that it *„practically does not prevent any access to the sites in question.“* Regardless of the question of whether in such a case any suitability can still be assumed at all, this method of blocking IP addresses should in any case be inferior since the latter’s effectiveness is at least not dependent on chance. Even beyond this, any milder means is not obvious and necessity must therefore be affirmed.

Appropriateness – how far can the government go?

Appropriateness is assumed, as the Federal Constitutional Court expresses it, *„if the measure is not out of proportion to the objective pursued. Those affected may not be overly or unreasonably inconvenienced. In any comprehensive weighing of the gravity of interference and the weight and urgency of the reasons justifying it the limit on what can reasonably be accepted must be maintained.“*[15]

In the framework of appropriateness the following arguments can be advanced:

First of all it must be borne in mind that blocking entails significant costs for Internet providers. If several hundred websites have to be blocked, as is currently under discussion in Germany with the gaming monopoly, then a way has to be found how this can be done in an automated manner. The automation cannot consist of what it consisted of in Italy where the authorities offered an in-house-produced PDF document for download on a website which is unsuitable for automatic evaluation simply because of its document format. Setting up such a procedure entails considerable costs. The Administrative Court of Cologne also recognised this issue with the panel therefore considering it possible that *„some day the point could be reached where the provider can no longer be reasonably expected to take the measure.“*.

Beyond that it must be taken into account that blocking an IP address frequently affects hundreds of accounts that are on the same server under another domain. On this the Düsseldorf Administrative Court tersely found:

> *„The fact that the blocking of an IP address due to the illegal nature of its contents can also simultaneously affect other (under certain circumstances, many other) perfectly legal ones does not render this method unsuitable for averting danger in the legal sense. In addition, separate domains for different programmes can very well provide the option of moving non-illegal contents to non-blocked IP addresses without changing the addresses used by the customers.“*[16]

The court was right to the extent that this does not eliminate the suitability but the appropriateness. In other respects this statement shockingly demonstrates how much the court overestimates itself. One thing should be clarified: The blocking order is directed at German Internet providers. The Düsseldorf Administrative Court nonetheless assumes that in this instance website operators all over the world will voluntarily and at their own expense actively seek to circumvent North Rhine-Westphalia’s blocking order. Do the judges really believe that an American website operator will move thousands of websites from one computer to another one with a non-blocked ip address, simply because a court far away in Düsseldorf denies users in North Rhine-Westphalia access to it? The reality will be quite different: Innumerable arbitrarily blocked websites, outdated lists with long since abandoned domain names and outdated IP addresses. And frustrated users. The latter will increasingly be using anonymisers and other techniques to be able to see the harmless contents blocked by this scatter-fire method. The IP blocking will in that case simply entail extra costs for all concerned and their effectiveness will be irrevocably

dissipated within a few months of their introduction.

Finally, in the context of what is appropriate, the most important thing to take into consideration is that the blocking method chosen does not constitute any serious hindrances as the Administrative Court of Cologne confirmed.[17] As demonstrated above, neither special technical skills nor any particular hardware or software are needed. The mere entry of an Internet address in a text input field must be mastered. In other words: Anyone who can enter an Internet address in the address bar of a browser can also enter it in the input field of an anonymiser. Anyone refusing to credit an Internet user with these skills is no longer dealing with the average user.

In summary: The high costs for setting up and administering an IP blocking, the necessity of daily updates for the blocked addresses, the risk of collateral damage in the form of blocks on numerous harmless websites cannot justify a „blockade“ that can be set at naught with two clicks of the mouse. Such a blocking order is therefore disproportionate and contrary to law.[18]

The Administrative Higher Court of Saxony-Anhalt has ruled in a similar manner when it overruled the obligation of a sports betting provider not to sign contracts with users from Saxony-Anhalt. The judges held the measure to be technically unenforceable.[19]

For the sake of completeness it should finally be pointed out that tacitly approving of the blocking of harmless websites violates the freedom of information of Internet users protected under article 5, paragraph 1, sentence 1 of the German Constitution.[20] To the extent that the providers of the blocked websites are additionally affected by this measure it also constitutes a violation of freedom of speech.

Conclusion

Just like it has been a matter of good taste, since the terrorist attacks, to demand the use of intercontinental ballistic missiles to pursue terrorists,[21] current events connected with the Internet lead increasingly to calls to suppress illegal, commercially unfavourable or simply unpopular contents on the Internet. The interests behind this may in some cases be understandable but this does not make the blocking any more feasible. Any one who still persists has not understood the basic structure of the Internet and is willing to be satisfied with a placebo effect achieved at great cost. A block on foreign online gaming providers in the EU would in addition be doing so on a basis that is incompatible with European law. But there are good grounds for hoping that the federal states will ultimately not abuse the uncensored Internet and thus sacrifice it to financial interests. It would constitute the absurd attempt to try to solve tomorrow's problems with yesterday's remedies.

(1) Karl-Heinz Hage from the office of the Berlin Senate, quoted according to the minutes of the 16th session of the sports committee held on 20 September 2006, at 27.

(2) See notes on the draft State Treaty on Gambling dated 25 October 2006, at 5.

(3) Spiegel Online (22 November 2006), http://www.spiegel.de/politik/deutschland/0,1518,449970,0.html .

(4) Thus in a blocking order by Düsseldorf District Court dated 6 February 2002, see http://odem.org/material/verfuegung/sperrungsverfuegung.pdf.

(5) Such a block can in addition itself be easily simulated. Under Windows XP a line for this must be added in the file C:\WINDOWS\system32\drivers\etc\hosts.

(6) The list can be downloaded from the website of the Amministrazione Autonoma dei Monopoli di Stato under http://www.aams.it/site.php?page=20060213093814964&on=download .

(7) See Telepolis report dated 5 April 2002, http://www.heise.de/tp/r4/artikel/12/12249/1.html.

(8) Retrievable at http://www.datenschutzzentrum.de/material/tb/tb26/kap15.htm.

(9) Anyone who does not wish to compose the URL himself can simply call up the German homepage under http://anonymouse.org/anonwww_de.html where the address to be called up can also be conveniently entered in an entry field.

(10) Schneider, „Sperren und Filtern im Internet," MMR 2004, at 18 (22).

(11) BVerfG, ruling of 18 July 2005, 2 BvF 2/01, BVerfGE 113, 167 et seq.

(12) VG Düsseldorf, ruling of 10 May 2005, 27 K 5968/02, MMR 2005, at 794. Cf. also OVG NRW, ruling of 19 March 2003, 8 B 2567/02, MMR 2003, at 348.

(13) Stadler, MMR 2003, at 209, note on VG Düsseldorf.

(14) VG Köln, ruling of 3 March 2005, 6 K 7603/02.

(15) BVerfG, ruling of 18 July 2005, 2 BvF 2/01, BVerfGE 113, 167 et seq.

(16) VG Düsseldorf, ruling of 10 May 2005, 27 K 5968/02, MMR 2005, at 794.

(17) VG Köln, ruling of 3 March 2005, 6 K 7603/02, sec 73.

(18) In the same vein Schmittmann in: Hoeren & Sieber, „Rechtsfragen des elektronischen Geschäftsverkehrs," 9, sec 144; Stadler, „Sperrungsverfügung gegen Access-Provider," MMR

2002, at 343, JurPC Web-Dok 16/2003, sec 28. Also on the subject of a blocking order against a host provider, OVG Sachsen-Anhalt, ruling of 27 February 2005, 1 M 320/05.

(19) OVG Sachsen-Anhalt, ruling of 27 February 2005, 1 M 320/05.

(20) In the same vein Rosenkranz, JurPC Web-Dok 16/2003, sec 28.

(21) „Rumsfeld: Mit Raketen gegen Terroristen“, Focus Online vom 28.06.2006, http://www.focus.de/politik/ausland/rumsfeld_nid_34375.html.

Hambach & Hambach
Rechtsanwälte | LLP
Haimhauser Straße 1
80802 München | Munich
Deutschland | Germany
info@ra-hambach.com
T +49 89 / 38 99 75 – 50
F +49 89 / 38 99 75 – 60
www.ra-hambach.com