

Current problems and possible strategies for combating racism on the Internet

lic. iur. David Rosenthal²

Executive Summary

The Internet has become a powerful tool for many people, organizations and other groups. The Internet however today is also used for many objectionable if not illegal purposes. One such issue is the use of the Internet as a forum, a platform or a means of communication for *racism* in its various forms. There have been significant efforts to combat such abuses of the Internet, especially in the case of hate and racist speech on the Internet or the sale and exchange of goods such as Nazi memorabilia.

Those efforts to combat racism on the Internet have to date been successful only in part. This working paper looks into that matter by discussing in *part I* the legal and technical reasons which have made it so difficult to combat objectionable speech and activities on the Internet, even though it is illegal already in many countries to publish racist speech. This part of the report will also discuss the use of technological measures to fight racist content and hate speech on the Internet. The analysis of the current situation leads to the following conclusions:

- One should not expect any technology-only solutions to the problem of racist content on the Internet taking into account today's efforts. Technological solutions can nevertheless help to a) shield certain groups of users from a portion of objectionable and illegal material available on the Internet and b) identify the people offering such material.
- It is possible in several countries to take legal action against parties that are supporting racist content by providing the Internet infrastructure necessary to access or spread such illegal content. But such action against Internet providers is problematic for several reasons and should not be regarded as a viable, long-term solution unless it is focused against providers acting at the *source* of the illegal content (e.g. website hosting provider).
- In some countries, notably the United States of America (US), racist and hate speech is *protected* by the right of freedom of speech as guaranteed in the First Amendment to the United States Constitution and may therefore be freely published on the Internet. Although in many other countries, such as most of Europe, such contents often are regarded as a criminal offense, it is not possible for prosecutors in Europe and other countries to prosecute pub-

¹ Prepared for: Séminaire d'experts sur les procédures de recours ouvertes aux victimes d'actes de racisme, de discrimination raciale, de xénophobie et d'intolérance qui y es associée et sur les bonnes pratiques nationales dans ce domaine (to be held on February 16th to 18th 2000 in Geneva, United Nations High Commissioner For Human Rights); © by David Rosenthal.

² C/o Rosenthal – von Orelli, Information Technology Law, Hans Huber-Str. 15, P.O. Box 228, CH-4003 Basel, Switzerland, E-Mail: rosenthal@rvo.ch.

lishers of illegal online-content at its source in the US. As long as countries such as the US are actively protecting such content, this will be the case, even if members of US law enforcement or the current administration would personally support such prosecution. It remains to be seen what other legal or political possibilities exist.

- Any proposed self-regulatory schemes will not be able to stop any significant portions of racist contents on the Internet due to the decentralized structure of the Net unless the codes of conducts mentioned are accepted and strictly followed by all major and international providers, including those telecommunication companies providing Internet connectivity to rogue providers specialized on hosting racist websites.
- Self-regulation as such is really no solution to the problem, since the delicate decisions are only passed on to the industry. While it is true that privately owned companies are not under the same constitutional constraints as the government, the basic question remains the same: What level and quality of racist and hat speech should be tolerated? Also, self-regulation schemes have some serious drawbacks such as missing democratic justification, due process guarantees and supervision.
- Prohibition of racial discrimination seems to be possible in a wise, effective and constitutionally unproblematic way, even where the provisions in concern have been formulated quite vaguely.

Part II of the working paper will discuss possible and viable strategies for combating and prosecuting racism on the Internet at its source in regard to the current technological and legal obstacles.

Those strategies can be combined or pursued independently and in some cases offer the possibility for compromise on actions necessary to combat and eliminate racism on the Internet while respecting broad interpretations of freedom of speech rights. Since the US have been the main voice against banning racist content on the Internet because of the way it interprets the right of freedom of speech, this report will focus on the views on this issue as expressed in that country. This does not mean there is no problem with online racist speech in other countries, but in many cases there are legal remedies available there.

This working paper will discuss the following basic strategies for combating racist content on the Internet:

- Force effective self-regulation: Hosting and Internet connectivity providers in the US today in most cases are not legally obliged to provide their infrastructure to every customer wishing to use it. In fact, a notable number of providers today already prohibit customers the publishing of hate or racist speech using their infrastructure. Many other however do knowingly and willingly allow their systems to be used for racist websites and similar activities, since they do not have to fear prosecution until now.

Such action however *is* possible against them (company executives respectively) already today, although it would have to take place outside of the US, in Europe for example. It is foreseeable that such action could lead to an outcry and would put enormous pressure on such providers to comply since executives in charge might face serious criminal prosecutions on trips outside the US including even being arrested; this strategy could also lead to political

tensions between the countries involved, although one should note that the US is using the exactly same methods to stop (legal) foreign Internet offerings breaking US laws.

It would of course be possible to provide some sort of a «safe harbor» for providers actively taking part in such an effective self-regulation-scheme, which would shield them from legal action against them as long as they perform as defined by the relevant charter. The US government itself has proposed such schemes in other areas of law (e.g. data protection).

- Persuade providers for effective self-regulation: Besides taking legal steps against providers it is of course possible to try to convince providers to take part of a self-regulation-project in order to eliminate racist speech on the Internet. Large corporations and other institutions for example could be persuaded to require providers and carriers to obey a no-racism-policy in order to be considered as a supplier or contractor. Until now such schemes mostly have involved only *hosting* providers but not those access providers providing *connectivity* (Internet connections) or domain-name support for racist websites and other such activities.
- Support legal and political anti-hate-initiatives: Even in countries with a broad interpretation of free speech principles there have been and still are several initiatives pursuing a more restrictive view regarding racist content on the Internet. While racist speech in the US may only, if at all, be banned if it provokes the person to whom it is directed to violence or is part of a crime, a more relaxed interpretation of the First Amendment might be possible over time.

One strategy could be the active support of movements and organizations pursuing such a shift in interpretation. This would include various kinds of support such as providing funds, political pressure, platforms for divergent views on freedom of speech existing in the US already and more. This could include trying to shift the current discussion away from the freedom of speech issue towards the subject of *discrimination* as discrimination is the basic building block used for racist contents. Allowing racist speech basically is allowing public discrimination, while denying racist groups freedom of speech rights can be justified easily from a legal point of view.

Although a subtle strategy, changing established interpretations and viewpoints and even court decisions requires significant time and lobbying efforts. There are also open questions regarding international law if governmental institutions should carry out such a strategy, since it could be interpreted as a political interference in the matters of a foreign sovereign country.

- Limit racist speech geographically: A compromise solution could be to limit the access to racist speech from *outside* the US only. Providers could either be asked to voluntarily participate in such a scheme or could be forced to comply, as laid out in this paper.

It today is technologically possible to block the access to certain websites for international users. Vendors of encryption technology on the Internet have effectively practised this: Only people in the US or using US Internet access infrastructure were able to download software with strong encryption, while others were directed to software with weak encryption. Such a solution would not be difficult or expensive to implement technically, but would protect US

providers from prosecution, would limit access to racist websites much better than provider restrictions imposed on the end users side and it would honour the US right of freedom of speech, since racist speech would not be limited within the US.

- Effective content identification: Another compromise strategy could be to persuade the US government to regulate racist speech in a way to ease its detection and filtering wherever required. Although the US government may not outright ban racist speech it may impose reasonable restrictions.

Such procedures could be used to make easier for third parties, providers and foreign countries to identify and block racist speech. One could think of requiring providers of racist content to (visibly or invisibly) identify their contents to aid automatic filtering and blocking where such material is found illegal or undesirable. Although this method does not eliminate racist or hate speech, it could make it considerably easier to keep it under control, to identify the sources and to block export or import of such material. Such a scheme could be part of an efficient self-regulation regime.

- Civil action strategies: Although government authorities are not allowed to perform sovereign acts on another countries territory, they can use the legal system of such a country as a private person. This circumstance could actually be used for combating racist speech being spread through US servers. Representatives of a country could initiate civil proceedings against racist groups and their providers. One possible yet untested way could be the confiscation of the copyright of a racist manifesto depending on its origin.

This working paper will *not* make any suggestions as to which of the various strategies are desirable or politically most viable, if at all. Since any solution would have to satisfy diverging legal and possibly also diverging political standpoints, it in any case will be necessary to find a compromise and it is not clear, whether such is possible today. This paper, however, could provide some grounds for such a «solution». In any case, it will be important to study the effects of the methods described in-depth, since they could set some dangerous precedents or under some circumstances might be even abused by antidemocratic regimes for their own purpose. Freedom of speech on the Internet indeed is a very delicate issue, but certainly *not* an issue not to talk about when looking for ways to combat racism.

PART I

The Internet and the relevant players

The Internet is a global network consisting of many interconnected computer networks of any size. In countries with an established infrastructure it is basically possible for everybody to use the Internet for communications, information retrieval, trading and publishing purposes.

Although there are some governing organizations³ as well as standardized procedures and protocols for managing the Internet technically, there is no central author-

³ Such as the 1998 established Internet Corporation for Assigned Names and Numbers (ICANN), <http://www.icann.org>, responsible for address space allocation, protocol parameter assignment, domain name system management, and root server system management.

ity managing the use and the contents available online, not even for providing statistical information about the number of users⁴.

Of course, many market researchers offer their estimates and studies, based on various methodologies. Combining those numbers, as of September of 1999 there were about 201 million people online, whereas 112.4 million were found in Canada and USA, while Europe had about 47.15 online users, followed by the Asia/Pacific region with 33.61 million, Latin America with 5.29 million, Africa with 1.72 million and the Middle East with 0.88 million people⁵. According to other sources, about half of the North American users will have a private homepage by spring 2000⁶.

Access to the network is provided by *access providers*, which can either be commercial entities or non-commercial institutions such as universities or libraries. People with no computer or own Internet access can use Internet terminals offered to the public for free or for pay at many places. Once online, an Internet user can either use paid services for e-mail, facilities for publishing websites⁷ etc. or may take advantage of *free* e-mail- and website-services. Such offerings usually are backed by advertisements.

While for practical and cost reasons an Internet user will have to use an access provider, Internet-café, library etc. within his vicinity to get on the Internet, he has no such restrictions once he is online. The user may use a service offering provided by a local *service provider*⁸ with the same comfort, speed and cost as services offered by foreign service providers. In fact, many European Internet users today are making use of free e-mail- and website-services based in the US⁹.

A website can be accessed worldwide as soon as it is online. The user will not notice in which country the server actually resides unless told. Figure 1 gives an example: If a document is available on the web-server run by *Provider B*, this document can read by a customer of *Provider A* as well as a customer of any other provider. The *Reader* may also access all documents published by *Publisher 1* on the web-server run by *Provider C*. Because there is no direct connection between *Provider A* and *Provider C*, they will need one or several intermediary providers (*Provider ..*) for their exchange. This is the typical scenario on the Internet since access providers normally only have connections to a few other providers. They often will also make use of special interconnecting providers that run the main transit routes on the Internet. They are often called «backbone» providers.

The only thing the *Reader* needs to know about a website is its «URL»¹⁰, which in fact is its «Internet address» (for example <http://www.un.org/aroundworld/>). Using

⁴ Number of registered domains, nodes etc. do not provide accurate information on the number of Internet users or offerings.

⁵ Source: Nua Internet Surveys, http://www.nua.ie/surveys/how_many_online/index.html.

⁶ Source: NPD Group, <http://www.npd.com>.

⁷ A «homepage» normally is the main page of an World Wide Web offering, while the offering in whole is called a «website». The computer system where the website resides on is called the «web-server» or just «server». This computer system needs to be connected to the Internet permanently. The software used by users to look at websites is called «web browser».

⁸ This is the generic term for anyone offering «services» on the Internet. Likewise companies offering content are called *content providers*.

⁹ Such as provided by <http://www.yahoo.com>, <http://www.hotmail.com>, <http://www.altavista.com>, <http://www.lycos.com>.

¹⁰ Uniform Resource Locator.

this address it is possible to locate the appropriate web-server on the Internet as well as the requested folder and/or page stored on that particular server.

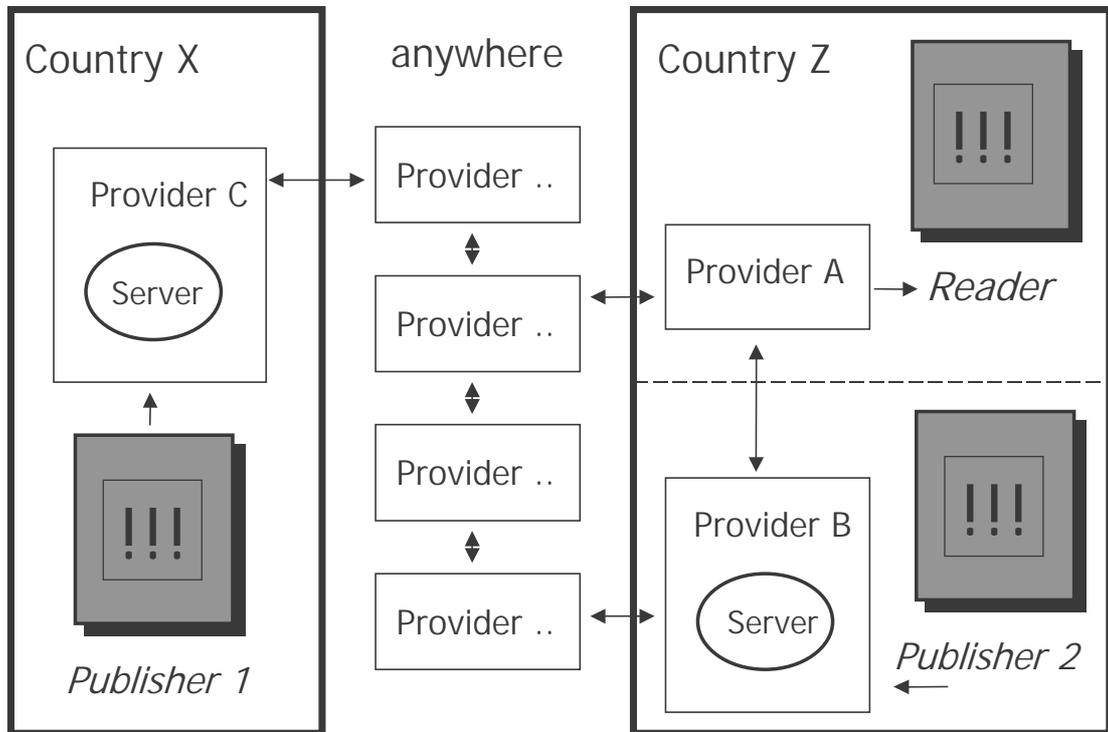


Fig. 1

= Internet

It is possible and fairly common to do web-publishing not with the same provider as the one used for accessing the Internet. In figure 1 *Publisher 2* for example might also choose *Provider C* as the host for his documents. A company offering its system to third parties for their publishing therefore is called a *hosting provider*. A hosting provider does not necessarily also has to provide Internet access services, although most access providers also are in the business as hosting providers for their access and other customers. From a technical standpoint it is neither difficult nor expensive to host websites.

access provider	Someone providing access to the Internet
service provider	Someone providing a service of any kind on the Internet, including access to the Internet
content provider	Someone providing online content (the «publisher»)
hosting provider	Someone providing the technical means for publishing content (the «printing office» and distribution)

backbone provider	Someone offering connections to a Internet transit network
connectivity provider	Anyone involved in offering Internet access, connections or transit

Although the Internet has no central command authority in place, every single part of it belongs to someone who pays for it and who maintains operations, security etc. In other words: There always is at least someone «responsible» and in charge for every part of the Internet. It therefore is (theoretically) possible to take down every part of the Internet and any website if the owner or operator wishes to do so. The operation of the Internet does not rely on every network and server to run; however, taking down important nodes or backbones may severely affect performance and access to certain offerings and may require the remaining networks and servers to be reconfigured.

Racism on the Internet

Racism occurs on the Internet in all forms known. The Internet yet has facilitated racism online in various ways. The most obvious form of racism on the Internet is racist and hate speech. It is today found on websites, within public discussion groups, as part of live online chats as well as within e-mail communications either between individuals or as part of a subscription mailing list¹¹.

A US report¹² published in March 1999 listed 1426 known Internet sites promoting racism, anti-Semitism, hate music, neo-Nazis and bomb-making. As of July 15th 1999 this number has skyrocketed to over 2100 sites. The increase has been significant over time: 1995 only one hate site existed on the World Wide Web according to the authors of the study. By the end of 1997 there already were 600. Other sources offer similar estimates. Some websites only contain hyperlinks to other offerings on the Internet; many other websites contain articles, pictures and even shops for memorabilia. Racist groups have also begun creating websites designed specifically to teach «racialist thinking» to young children¹³. Others are geared toward recruiting women, for example.

The Internet has also facilitated the trade of racist- and extreme-right-material such as Adolf Hitler's manifesto «Mein Kampf» or books denying the Holocaust, since US online retailers such as Amazon.com or Barnesandnoble.com have freely traded them to any country worldwide for some time. In other instances unsupervised online auction platforms¹⁴ were used in order to trade Nazi memorabilia.

According to law enforcement officials the Internet today is also used heavily for communications among members of racist and hate groups, either by e-mail or via online clubs not open to the public. According to several reports, the Internet is also frequently used for organizing and promoting meetings and conventions of extreme-right and racist groups.

The Internet is an attractive tool to spread of racism for three main reasons:

¹¹ For a more in-depth report see http://www.adl.org/frames/front_poisoning.html; see <http://www.hatewatch.org> for examples online.

¹² Source: Simon Wiesenthal Center, <http://www.wiesenthal.com>.

¹³ For example <http://www.wcotc.com/kids>.

¹⁴ For example <http://www.ebay.com>.

- Broad reach: The Internet provides an enormous, unmatched reach for recruiting followers. There is low or no financial investment required. Publishers of racist and hate sites therefore have praised the Internet on many occasions¹⁵. Although having a website by itself does not guarantee many visitors, but the efficiency for spreading racist opinions is much higher than using printed literature and leaflets or public meetings for example. According to published reports, the white supremacist website «Stormfront», located in West Palm Beach, Miami and Louisiana, receives 2000 to 2500 visitors per day.
- Protection from prosecution: Racist speech is prohibited by criminal law in many countries, such as most of Europe. Many countries have also joined an international treaty for the fight against any form of racism adopted on 21st December 1965 in New York. However, some countries – notably the US – still allow racist speech to be disseminated. Although the USA has ratified the aforementioned treaty as well, it has made reservations as it regards racist speech as protected by the right of freedom of speech as guaranteed in the First Amendment to the United States Constitution. An outright ban of speech from certain groups would also be viewed as contrary to a fundamental tenet of American democracy.

As a consequence to that, the US has developed into a «safe haven» for racists spreading their word worldwide by using the Internet. Not only people living in the US are taking advantage of this situation but also many Internet users from other countries: They are using US providers as a *relay* for their racist speech. Although it is difficult to act anonymously on the Internet, they are reasonably safe from identification (and therefore from prosecution) since foreign government authorities cannot force US providers to reveal the real identity of a person responsible for setting up a racist website because such publications are legal in the US. In this sense the US has taken a similar role as traditional «offshore»-countries do in regard of income taxes or legal gambling, for example. According to government sources in Europe¹⁶, today most racist and hate sites on the Internet are made available on the Internet from within or through the US. There have been also reports about servers located in Canada.

Legislative initiatives to combat racism on the Internet have been very limited in the US up to now. There few US laws in place¹⁷ or in the works¹⁸ against racism focus only on hate-related crime, but not on hate speech not connected to violence or other criminal offences.

- Difficult to trace: The vast amount of content available for Internet users and the legal limitations on extra-territorial investigations by foreign law enforcement authorities have made it difficult to identify and prosecute individuals in

¹⁵ «We reach tens of thousands of people, potentially millions. It's almost like having a TV network» («Net spawns Web of hate», Journal Star, November 8th 1999, <http://pjstar.com>); «I think it's the most important development in the history of mankind for the expression of dissident thought and opinion.»; «As far as recruiting, it's been the biggest breakthrough I've seen in the 30 years I've been involved in this.» (both from «Hate sets up shop on Internet», Denver Post, November 8th 1999, <http://www.denverpost.com>)

¹⁶ The Swiss Federal Police, for example.

¹⁷ Hate Crimes Statistics Act (HCSA).

¹⁸ Hate Crimes Prevention Act of 1999 (HCPA), S.622 / HR.1082.

connection with racist speech on the Internet, even if such speech is originating from outside the US. According to government sources, the Internet is also intensively being used for non-public communications among members of racist and hate groups. This form of communications not only is very efficient, but also is harder to intercept and, on certain occasions, to decipher since e-mail-messages may be encrypted as well. Another advantage of the Internet is the possibility to quickly move or copy content to new or mirror sites.

Because of those three reasons one should not expect racist and hate speech on the Internet and other forms of racism on the to slow down or even decrease any time soon. The Internet is a tool far too useful and interesting for racist and hate groups not to be used for their mission. There is also no sign of a mind change in the US regarding the fight against racist and hate speech.

Legal measures

From a legal standpoint there is no such thing as a law-free zone on the Internet. Actions on the Internet always have a «contact» to at least one jurisdiction since every action and offering on the Internet originates from somewhere and in most cases requires the use of at least one server.

Every sovereign country may define by itself what quality and quantity such contact must bear for the law of that country being applied to a particular online activity or offering. Normally an activity or offering on the Internet must have a «minimal» contact to a certain country to fall under its jurisdiction. Such contact can be established by doing business with a country as well as by accepting orders from residents of such a country. The use of a server located within a country often will be a sufficient contact as well, but does not necessarily have to be so in every situation. On the other hand the mere technical possibility to connect to a website from one country might not be enough for constituting a minimal contact between that country and the website mentioned.

As sovereign acts of law enforcement authorities can only take place within their territory, officials therefore are in general limited in their fight against crimes to their own country, unless another country is willing to assist them, mostly on grounds of similar laws.

In countries with laws against racist speech law enforcement will in general have no problem¹⁹ taking down any racist website on the server of a *domestic* provider²⁰ as well as identifying the person responsible for the content. The provider will be well advised to fully cooperate with the authorities, since it could be regarded as an accessory if knowingly and willingly assisting illegal speech²¹. The current and planned laws for limiting provider liability in Europe for example do not and most likely will not impede the prosecution of a *hosting* provider deliberately allowing racist speech

¹⁹ Of course law enforcement in many cases does not yet have the training, equipment or staff in order to effectively fight racism on the Internet.

²⁰ This could be the server of a hosting provider or a private server connected to the Internet by commercial access provider. In the second case taking down the website is done by cutting of the Internet feed to the server hosting the website.

²¹ Hosting providers usually are not obliged to know the all contents published on their servers and therefore are not liable until they had access to specific evidence of possible illegal contents on their servers. Such evidence often is given in the form of a notification by a proper authority.

on its server even after being notified by the authorities. Some countries explicitly require providers to assist law enforcement by supplying information about their customers. Such information can be vital for identification and collecting evidence.

Law enforcement will not be able to legally force the shutdown of a website hosted or fed by a *foreign* provider as long as no equipment is located physically in domestic territories. Authorities however could still prosecute individuals involved with such a website²². Such individuals could be taken into custody as soon as they enter domestic territories. In most countries it is possible to indict and sentence such people in absence once there is proper jurisdiction: Domestic prosecution of foreign individuals will in most cases only be possible if the alleged offender has directed its speech to an audience in the prosecuting country. Some further limitations may also apply.

Since many racist websites are out of reach for countries with laws against such contents some law enforcement authorities have tried to limit the reach of illegal websites by mandating access providers in their countries to block access to such contents. In other words: If a country for whatever reason can't eliminate the source of illegal information on the Internet it might want to try the other end – the provider serving the end-user. Such attempts to date have been unsuccessful²³, mainly because access providers face technical difficulties blocking selected websites on the Internet (see below).

Additionally there is legislation in effect or underway in several countries²⁴ in the world explicitly limiting the (criminal) responsibility of providers for illegal contents they carry, but do not (permanently) host on their server. It remains to be seen whether those laws also protect those carriers providing Internet connections to people hosting racist speech on their *own* servers²⁵. In other countries the legal situation for access providers is even less clear²⁶.

Technological measures

Racist speech being spread by using a provider within a country with laws against racism in place can – as shown – be countered effectively. The question in such cases will be whether law enforcement authorities will have sufficient training, resources, equipment and willingness to actually to put the law into action. The main problem however is combating racist and hate speech being spread or relayed us-

²² In many countries it normally is not possible to prosecute a company as such; prosecutors will usually focus on company executives and other individuals responsible instead.

²³ In a high profile case a German court in November 1999 overturned the conviction of a former manager of the German subsidiary of US service provider Compuserve on charges of aiding the distribution of child pornography. The court acknowledged the manager has not been in the position to block the sites himself and was only able to ask the companies U.S. headquarters to do so.

²⁴ The German «Telediensteegesetz» already has such provisions, while the European Union is preparing similar guidelines as part of its «Electronic Commerce» legislation; the remaining parts of the US «Communications Decency Act» (CDA) has also shielded providers from responsibility.

²⁵ Rules currently discussed in the European Union for example will only protect connectivity providers that (among other things) do not *select* the content they carry; it is unclear whether accepting and keeping a racist publication as a client already is considered as a «selection»; see article 12 of the proposed rules on electronic commerce, KOM(1999) 427.

²⁶ Switzerland, for example. One open question is what way of blocking access to certain websites is appropriate, if at all.

ing infrastructure (e.g. access or hosting providers) from countries with *no* laws or law enforcement against racist speech.

Technology could be one way to circumvent such problems in fighting the spread of racist speech online. Although this paper will focus on *legal* remedies against racist speech one should note that it also is technically possible to enforce the shutdown of a website in another country using hacking and sabotage techniques²⁷ fairly common and easily available on the Internet. It might be worth mentioning that there indeed are references of government officials publicly suggesting the use of such technology to combat websites supporting terrorist groups²⁸.

Legal technological measures however today mainly focus on preventing racist speech either from entering a country or being retrieved from users within that country. On first view, this might not seem very difficult since providers could simply be asked to install «filters» on their network to block out all racist pages. This in fact is possible, but not as easy and effective as one might believe.

Filtering can basically be done on three levels: Providers can ...

- a) prevent domain names of known racist contents to be resolved into usable network addresses²⁹,
- b) block any network connection to a server known to contain racist contents³⁰, or
- c) have customers use an intermediary webserver («proxy server») with built in filters for specific pages with known racist contents³¹.

These provider-level filtering techniques, however, have several, sometimes severe technical limitations:

- None of those techniques today are scalable, which means they will work with several thousand servers to be blocked at the best, but will not work with tens of thousands websites. If blocking racist websites would be considered as mandatory by law, providers of course would be obliged to block other illegal content as well, including websites with libellous content or content in-

²⁷ Sabotaging is often done by «denial-of-service»-attacks which – in simple words – consist of flooding the target system with data it can't handle anymore. Initiating such attacks does not require special knowledge but is considered illegal in most countries.

²⁸ In November 1997 a Spanish police official concerned about the presence of a Basque ETA separatist website on the Internet urged web users to thwart the ETA by saturating its website, but to be careful to do so anonymously (source: AFP, Nov. 22nd 1997).

²⁹ Since a domain name does not sufficiently specify the network node to be contacted once a user wants to call up a website, the browser has to retrieve the current network node address, called IP address, associated with the given domain name. This information is provided by domain name system (DNS) servers. Every access provider operates such servers for its customers; larger customers however often operate their own DNS servers.

³⁰ It is theoretically possible to filter out all data packets originating or targeting a specific IP address or an IP address range; this technique today is used within certain applications to prevent the receipt of unsolicited commercial e-mail.

³¹ All website requests have to be directed to such a proxy server which in turn retrieves the pages from the Internet on behalf of the user. Current browsers are equipped to make use of such proxy servers transparently. They today are used by providers for the purpose of reducing network traffic: Frequently requested pages can be held «in stock» locally. Proxy servers are also used by many companies either for security reasons or for restricting employees' access to the Internet. Most access providers, however, today do not mandate the use of proxy servers by their customers, except in countries where Internet access is not free.

fringing on intellectual property for example. Access providers most likely would soon be confronted with requests to block hundreds of thousands of websites – a task they today can't handle, even if the blocking list would be managed by a central office and supplied in a machine readable format.

- All blocking methods can easily be circumvented. The user could use special services to call up the websites indirectly through unsuspecting servers on the Internet. The publisher could copy or move his content to other servers not blocked (yet). Several racist websites today already are «mirrored» to several servers in different geographical regions in case one server should be blocked, sabotaged or go down for other reasons.
- Blocking method c) in most cases would only be effective for private customers, method a) would not work for users accessing the Internet from most companies with their own Internet infrastructure³².
- Mandating the use of intermediary systems described in blocking method c) would make it impossible to use many other services on the Internet that either are new³³ or do rely on a direct connection between the user and server. There is also a security risk associated with mandatory indirect connections since no end-to-end encryption could be possible anymore under certain circumstances. In other words: Mandating the use of intermediary systems would most likely severely hamper the free development of the Internet and electronic commerce, besides probably being unconstitutional even in countries with laws against racism.
- Blocking method a) will block every website using the same domain name as the racist website is using, while blocking method b) may block every website stored on the same server. Since a large portion of racist websites are placed public web servers containing many legitimate websites as well methods a) or b) do not seem appropriate since they would black out legitimate content as well.
- All of the blocking methods do only apply to websites containing racist speech. Neither blocking method described may prevent racist speech and other forms of racism within discussions groups, chat rooms, by e-mail or through online trade exchanges although new technology might be developed for such purpose.

From a legal standpoint there are some reservations as well. The main legal question to be answered is *who* should decide which websites should be blocked. Normally providers will either decide themselves or will follow suggestions made by law enforcement officials. Because only criminal courts are legally entitled to decide whether a specific website contains illegal speech, proactively blocking content involves a certain danger of censorship not covered by the law anymore and might affect due process rights of people limited by such provider or law enforcement «decisions» on the illegality of their content.

For those technical and legal reasons the blocking methods mentioned will only shield certain groups of users from a portion of objectionable and illegal material available on the Internet. It is basically a political question what tradeoff to the functionality, performance and cost of the Internet as well the right of unfiltered access to

³² With their own DNS server in particular.

³³ Intermediary systems in many cases would have to be updated to handle new services.

information should be made in order to block access to at least some racist websites.

The best and for many experts only viable solution from a technical and legal standpoint of view is to block such content at its *source* or as close to it as possible. Most experts today agree that blocking such content at the recipients' «end» of the Internet makes no sense in regard of its low effectiveness and the price to be paid – not only in financial terms. Since backbone and access providers already are or will be shielded from prosecution in many countries, there is also no legal basis for making such blocks mandatory.

Other measures

Of course providers could be asked to voluntarily block objectionable materials on the Internet. Many in fact do reserve the right to do so in their terms and conditions, which even allows them to take down a customer's website with legally acceptable contents. However, since the same technical limitations would apply, this approach today does not seem to be practicable on a systematic basis with a large number of websites, even if being coordinated by a central organization.

Most access providers today are in a «wait-and-see» mode. As soon as there is public pressure to block access to a particular web-server with material of undoubtedly racist nature many providers will block access to it as requested. Since such incidents have occurred in rather low numbers, this issue has not been really been a problem for them.

The same is true for providers hosting racist websites themselves. Many will take down such offerings because they oppose racism or fear negative consequences of any kind³⁴. Individuals wanting to publish racist speech of course can easily switch to other hosting providers without a policy against racist or hate speech. It of course would be very helpful if a large number of hosting providers worldwide would adopt such policies and would not tolerate racist or hate websites and other racist speech or action on their servers and services.

Since an increasing number of racist websites are stored on private servers run by hate groups themselves, self-regulation as described would have to include access providers providing Internet connections to such groups in order to be merely effective; the only way to stop such servers spreading their content would be to cut off their connection to the Internet. This issue to date has not been discussed widely, but based on passed experience one should not expect such connectivity providers to voluntarily participate in such action in significant numbers. This would require intense public pressure that today does not exist.

Another measure of course is the use of «filtering» software at the end-users premises. There today are many products available to computer users for blocking access to objectionable websites on their systems³⁵. Most of those programs are installed by parents, schools and public libraries to protect children or by employers at work. Since the user or employer himself decides what type of access should be blocked when, many of the aforementioned problems with filtering are not relevant in those cases. From a technical standpoint it is easier to block certain web-pages

³⁴ Major US hosting providers with a «no hate page policy» include America Online, Angelfire, AT&T Worldnet, Geocities, Tripod and Xoom.

³⁵ See <http://www.surfwatch.com>, <http://www.cyberpatrol.com>, <http://www.netnanny.com> for example.

on the users computer since such filtering solutions can intercept actions of the user more directly than if they would have to take place on a provider system. While still some drawbacks and limitations might exist with filtering, the user at any time can decide to turn of such filters.

The possibility to use private filtering software of course does neither stop the spread of racism on the Internet nor will it release law enforcement from its duty to combat such content in countries with laws against racist speech. The use of filtering software can only be viewed as an *additional* measure in order to shield certain groups from harmful contents.

The issue of «censoring» and «self-regulation»

Another thorny issue about racist speech is public and private «censoring». Since censoring is widely regarded as something undesirable one needs to differentiate carefully.

First of all, there is probably no country on earth where freedom of speech is unlimited. This is not even the case in the US. Speech in whatever form will only be tolerated up to a certain level or quality of «disturbance» of public order. In a democratic country the level and quality of acceptable unrestricted speech normally is defined by *law*. Censoring ordered by law thus in most cases is democratically legitimated. Law enforcement authorities enforcing those provisions therefore are not «censoring» Internet content; they are only enforcing what law censored already.

There are many different views on what level and quality of «disturbance» should be allowed for speech for democratic country to function and where to strike the balance between the public interest and the freedom of an individual. While today most countries consider for example speech consisting of child pornography as not tolerable³⁶ the opinions on racist speech not involving violence vary widely, as already noted before. Achieving a single, worldwide standard on defining what racist speech should be tolerated, if at all, seems to be a *political* process requiring a uniform understanding and assessment of the values involved. This paper of course cannot resolve that issue. It cannot even state that such a uniform, worldwide position on racist speech ever will be possible or does make sense.

Additionally, any filtering scheme in place and limitation of freedom of speech inherently carries the risk of being used in an unconstitutional way or even abused by antidemocratic regimes around the world for their own purpose. Under to cloak of combating racist speech such regimes may try to ban other content they find disturbing. This, of course, should not be tolerated.

Although frequently hailed, *self-regulation* as such is no solution to this particular problem either, since the delicate decisions are only passed on to the industry. While it is true that an alliance of service providers might not be bound by constitutional constraints regarding freedom of speech as government authorities often are, the basic question remains the same: What level and quality of racist and hat speech should be tolerated? In quite some cases where governments are calling for self-regulation this actually seems to happen just because those governments are

³⁶ Some differences remain: While in some countries child pornography is considered as illegal only if involving real children, other countries have outlawed all forms of child pornography, even when fully fictional (no real children depicted).

afraid of having to deal with thorny issues and do not want to take unpopular decisions themselves.

Resolving this issue is only one part of the problem. Self-regulation is popular in these days, but has some serious drawbacks. While European laws against racist speech, as an example, have democratic justification, any self-regulation scheme does not. This might not be viewed as a problem as long as the participants of such self-regulation schemes are taking their responsibility seriously. But there is no guarantee for that.

There are three main areas of problems to be considered:

- Self-regulation groups or individual companies normally are not under any supervision by the courts since they are operating as private entities.
- Self-regulation groups or individual companies do not have to observe due process rules and other basic rights, as the government has to do. While decisions and actions of such groups can seriously affect individuals or companies, there is normally no guarantee of fair, unbiased and sincere treatment by such groups – and no place persons concerned can complain. Although antitrust laws might provide some minimal protection against the power of self-regulation groups or powerful companies, such protection often is not within the reach of an individual.

The question to be answered is why should self-regulation groups not be required to obey similar rules, as the government would have to when using similar power? If they would, self-regulation probably would not make sense anymore, one answer could be. In other words: Self-regulation can be a very useful technique for eliminating basic rights such as freedom of speech. It therefore may indeed seem surprising that there is no other country endorsing both self-regulation and freedom of speech so intensely as the US does.

- Self-regulation groups and even to a lesser extent individual companies in general have no democratic justification. Therefore standards developed by them might not be representative with the general political consensus. While self-regulation groups may indeed be the only way to create an international standard in order to overcome varying views on the subject of racist speech, their rules may unfairly favour certain groups over-represented in the steering board of the self-regulation group in charge.

Those objections do not only apply to self-regulation groups. The power of individual companies should not be underestimated, since content-self-regulation schemes often rely only on a few companies providing the tools and intelligence necessary. Vendors offering filtering software for the Internet for example in some sense could very well be considered as private censors, as they define based on their own rules whether a website should be added to their different «black lists» of objectionable websites. Since their customers (parents, schools, libraries, employers, providers etc.) of course do not double-check those lists, those companies have significant power over what people can read on the Web and what not. This power can be abused, willingly or unwillingly – and of course errors can occur by mistake as well. In most cases, however, the owner of a website unjustly being blocked might find it very difficult to impossible to legally do anything against such companies or to recoup financial damage suffered in such a case.

Several such cases have been reported. Two examples³⁷:

- Cyber Patrol, a popular software package for filtering objectionable material, has defined several categories. The two categories selected by most, if not all customers are «FullNude» for pictures exposing any or all portions of the human genitalia and «SexActs» for sexual acts and/or lewd or lascivious behavior. The following websites, among many others, were found to qualify for both categories: MIT Project on Mathematics and Computation, National Academy of Clinical Biochemistry, Wetherinton Glass and Mirror (without even being online completely), Domain Services Network, Department of Computer Science, Queen Mary & Westfield College, The U.S. Army Corps of Engineers Construction Engineering Research Laboratories, a server at the University of Arizona and a website about local politics in the town of Ada, Michigan. In other words: Cyber Patrol considered all of those websites as pornography. The company itself states, «we cannot guarantee the accuracy or completeness of our screens and we assume no responsibility for errors or omissions.» Over 11 million people used the software by some estimates at that time.
- The Utah state government through its agency Utah Education Network³⁸ was or still is using a commercial software package to filter the Internet access of all of the 40 school districts and at least 8 of the 70 library districts in Utah. An examination in fall of 1998 found that many sites useful for educational and research purposes were blocked. Among the documents banned by the product: The U.S. Declaration of Independence, the United States Constitution, the Bible, the Book of Mormon, the Koran, the Adventures of Sherlock Holmes, the Canterbury Tales and all of Shakespeare's plays. A scholarly paper about Nazi Germany was banned as well as sites that *oppose* hate speech and racism. The company maintaining the filtering software states «as a rule, sites are not added to the Control List without first being viewed and approved by our staff.» The errors, however, suggest that the company used a computer keyword search for compiling the list only. Although the company offers the possibility to override bans, this was used only in very few cases; most errors go unnoticed.

Law enforcement authorities might also be in a position to de facto «censor» the Internet by warning hosting or access providers about content those authorities consider as illegal. Most providers will not offer resistance and will immediately remove such content, if possible. This involves a certain danger of material being blocked although no court order has ever been issued and the content concerned may be perfectly legal.

Those examples should make it clear that self-regulation is no silver bullet regarding the issue of racism on the Internet. One might be suspicious against government regulation, but the same objections apply to regulations by the private sector as well. Even more, self-regulation schemes normally do not provide any safeguards against abuse of power and similar developments.

Freedom of speech also should not be regarded as an issue to be regulated by the «market», as for example «business monopoly power» could be. Market pressure would primarily affect the behaviour of big market players, but people publishing

³⁷ Source: The «Censorware Project» at <http://www.censorware.org/>.

³⁸ See <http://www.uen.org>.

their ideas online are – thanks to the unique structure of the Internet – not dependent on any of those market players anymore to reach a broad audience³⁹. For that reason the market probably today will not be able hinder racist speech from being published even if the vast majority of all participants and Internet users would like to do so. In other words: Market self-regulation is too «wide-meshed» to stop racist speech. The market, of course, could develop new technological solutions to the problem and implement with governmental aid.

Laws against racial discrimination

This report cannot discuss the various laws and provisions against racial discrimination throughout the world and their effects. Yet, the experience made with such a provision in *Switzerland* is promising. In article 261^{bis} of the Swiss penal code, effective from January 1995, prohibits several forms of racial discrimination. Before coming into force the article has been criticised for being too vague and therefore unconstitutional. Such fears in fact are voiced quite often in connection with laws against racial discrimination and they might even be justified in certain cases. Nevertheless, judging upon the court decisions passed, the results have been very satisfactory in Switzerland, as it seems. According to the relevant literature, article 261^{bis} has been applied in a «wise» and «completely constitutional» way⁴⁰. Although some open questions remain and the doctrine might still need some refinements by the courts and through literature, there have been no insoluble problems regarding article 261^{bis} to date. This is also true for combating racist publications being hosted on servers within Switzerland, although the number of cases seems to be quite low.

PART II

Possible solutions

As part I of this working paper has shown to some extent, one should not expect too many results in combating racist speech on the Internet by relying solely on action at the receivers end, whether by self-regulation or government regulation. Action is necessary and should primarily be directed at the *source*. As long as there is no worldwide political consent on the issue of racist speech, there will be no easy or straightforward solution to racism on the Internet.

Nevertheless: Various alternatives exist, although some of them might not be politically viable. This part of the paper will list and explain some of the alternatives for fighting racist speech originating from countries not willing to stop such. The following basic strategies will be discussed:

- Force effective «self-regulation»
- Persuade providers for effective self-regulation
- Support legal and political anti-hate-initiatives
- Limit racist speech geographically

³⁹ America Online, the largest provider in the world, already today does not tolerate racist websites.

⁴⁰ See for example: «Rassendiskriminierung: Gerichtspraxis zu Art. 261^{bis} StGB; Analysen, Gutachten und Dokumentation der Gerichtspraxis 1995-1998», various authors, published by Gesellschaft Minderheiten in der Schweiz (GMS) and Stiftung gegen Rassismus und Antisemitismus (GRA), Zürich 1999.

- Effective content identification
- Civil action strategies

Those strategies can be combined or pursued independently and in some cases offer the possibility for compromise on actions necessary to combat and eliminate racism on the Internet while respecting broad interpretations of freedom of speech; since the US have been the main *voice* against banning racist content because of the right of freedom of speech, this report will refer to the views on this issue as expressed in that particular country in order to allow a discussion of the matter of great concern to many countries. Some of the strategies are new, some pick up existing concepts and most are discussed in the US already in some way or another. Since they may have broad consequences beyond combating racism, the effects imaginable should be studied very well (see below «Conclusion ...»).

The focus on the strategies for the US «market» also does *not* mean that there is no problem with racism on the Internet in Europe, Asia or other parts of the world. But the laws in Europe, for example, have made the fight against racist speech on the Internet much easier – at least from a technical and legal perspective; scarce law enforcement resources are another problem. Racist publishers on the Internet will of course always find ways to be one step ahead, but they can be effectively prosecuted in Europe. This is true even though many European providers soon might enjoy similar «immunity» as their US counterparts do.

Strategy 1: Force effective «self-regulation»

Freedom of speech in most democratic legal systems is a basic right of constitutional degree. As such it normally only protects individuals against restrictions or actions imposed by the *government*.

This is true in the US as well. Its local governments, with some exceptions, would have to tolerate a group of demonstrators marching through its streets. On the other hand, the First Amendment does not compel a privately owned publication, provider etc. to provide a platform or means for the dissemination of the opinions of racist groups⁴¹. Hosting and Internet connectivity providers in the US therefore in most cases are not legally obliged to provide their infrastructure to every customer that wishes to use it⁴². They basically can decide not to provide their system for specific content. In fact, already many hosting providers have declared that they will not allow their customers to publish hate or racist speech and they will remove such content as soon as they get informed about it. Another example is unsolicited bulk e-mail. Many providers today have a zero-tolerance policy for such communication. Senders of such e-mails have without success tried to contest such policies by insisting on freedom of speech rights.

Many providers however do not follow that path and actually do tolerate racist websites and similar activities. This is especially true for access providers offering Internet connectivity for people running web-servers dedicated to racist speech. Since those providers will not have to fear prosecution for doing so they believe not to have any reason to back off from assisting such customers in spreading their word.

⁴¹ There are exceptions. A privately owned institution under certain conditions could be considered being a public forum.

⁴² One exception for example are Internet servers provided by public universities and run by the school's administration itself.

Such prosecution however *is* possible, although it would have to take place outside the US. Once those providers and telecommunication carriers assisting in the spread of racist speech are identified, executives of such companies – under certain circumstances⁴³ – could be prosecuted in other countries affected by such speech as well. This of course would *not* affect executives working for subsidiaries of such providers since they have no responsibility for what is happening in the US in most cases. Such action would also only focus on those individuals knowingly deciding not to cut off support of racist speech although they could⁴⁴. Rules of international law of course also require that particular racist speech is in some way directed or intended for recipients in the country where the prosecution is taking place. Some open questions remain, though⁴⁵.

The strategy described here could therefore lead to a situation where executives of big US Internet service providers or telecommunication carriers would have to face prosecution in dozens of countries once countries with laws against racist speech start to coordinate their efforts and show willingness to enforce their laws. This is not the case today, although the law required to do so is in place already.

It is foreseeable that such action could lead to an outcry and would put enormous pressure on such providers to comply since executives in charge might face serious criminal prosecutions on trips outside the US including even being arrested; this strategy could also lead to political tensions between the countries involved, although one should note that the US is using exactly *the same methods* to stop foreign offerings on the Internet that are perfectly legal in the country of origin but not in the US⁴⁶.

Of course the reason for pressing criminal charges against executives of Internet providers and telecommunication carriers outside the US would not be their conviction. It would be a mere method of putting pressure on those companies to act against racist speech on the Internet; such action would not even require those companies to completely ban such content as long as they manage to prevent the export of such material (see below «Strategy 4 ...»). The «export» of racist speech could not be banned completely, but significant progress would be made.

This strategy has already worked in a number of cases⁴⁷, since a company doing business usually would not want to get in conflict with law, whether on its home territory nor in a foreign country it is doing business with. There is too much at stake

⁴³ Several requirements would have to be met. The executives responsible would have to be notified in advance about the nature of the content they are distributing in order to give a chance to act, for example.

⁴⁴ Hosting or access providers in general are not legally obliged to provide their services to private groups or for private purposes they do not wish to support. Existing provider contracts normally can be terminated with advance notice and normally contain escape clauses.

⁴⁵ There are different opinions on the qualification of racist speech as an offence by commission or as an objective crime, for example. Only the latter one would allow foreign prosecution.

⁴⁶ According to Australian press reports, the US Justice Department has confirmed that the chief executive of the first government-regulated Internet casino in the Northern territory of Australia is subject to prosecution in the US and could be jailed for up to two years because his company takes Internet bets from American citizens; the USA Wire Act of 1961 prohibits «assisting in placing bets or wagers on any sport event or contest» (Source: Computer Daily News, April 15th 1999).

⁴⁷ For example, the major online booksellers Amazon.com as well as Barnesandnoble.com in December 1999 have both agreed not to sell Adolf Hitler's manifesto «Mein Kampf» to Germany anymore at the request of German authorities (Source: various press and wire reports).

compared to the loss of business as a result of not dealing with publishers of racist content.

If such a strategy is to be chosen by a number of countries it would be in the best interest of all parties affected to provide some sort «safe harbor» for providers actively taking part of such an effective self-regulation-scheme. They would effectively be shielded from legal action against them as long as they perform as defined by the relevant *code of conduct*. The US government itself has proposed such schemes in other areas of law (e.g. data protection) and could assist in negotiating such an accord on the issue of racist speech with foreign countries or even international organizations as well. In any case, it would be very important to provide clear and practical guidelines to providers on what one expects them to do.

Strategy 2: Persuade providers for effective self-regulation

Besides taking legal steps against providers it is of course possible to try to convince providers without legal threatening to take part of a self-regulation-project in order to eliminate racist speech on the Internet. Until now such schemes mostly have involved only addressing *hosting* providers but not Internet providers or telecommunication carriers providing *connectivity* or domain-name support for racist websites and other such activities. It is important to include such providers as well because racist groups today do not have to rely on hosting providers for publishing their content, because they can run their own servers and thus only require connectivity, which they will easily be able to buy in most cases.

Of course there are many organizations⁴⁸, groups and even individuals petitioning various US providers and telecommunication providers to cease support to racist publications on the Internet. What seems to be missing, though, is some sort of coordinated line of action, which indeed makes it difficult to build up political and market pressure and as well as public awareness.

One strategy for an international organization or an alliance of countries with common goals regarding racism could be to assist and promote a more unified, more specific and more powerful lobbying of US providers and carriers, by either providing funds, public relations resources and opportunities or political support. It would also be necessary to single out non-compliant providers in order to attract media attention and increase public pressure.

Solely asking providers to combat racism on the Internet might not be enough. One might want to consider additional actions. One example could be creating a label given free-of-charge to providers actively participating in the fight against racism. This could be used as a marketing tool. Large corporations and maybe even some governmental or international organizations could be persuaded to require providers and carriers to acquire such a label in order to be considered as a supplier or contractor⁴⁹.

One might even consider persuading large providers⁵⁰ and carriers not to forward or receive any data from providers providing services to racist groups. A complete boycott may not even be required; it would already have significant effect if data traf-

⁴⁸ See <http://www.anti-racism.net/resource.html> or <http://www.hatewatch.org> for more details.

⁴⁹ Similar approaches have been used in other areas. Several private companies such as IBM and Microsoft have announced not to buy ads anymore from websites failing to publish adequate privacy promises to consumers.

⁵⁰ Such as America Online with over 20 Mio. members.

fic to and from such a provider would be slowed down artificially. It needs, however, to be closely examined whether and to what extent such behaviour would withstand antitrust and other laws.

Besides trying to persuade hosting and connectivity providers from refraining serving racist speech is to address the organizations responsible for the *domain name system*. Since most of those organizations are privately owned they are more or less autonomous in formulating rules for domain name registration and revocation. In many cases the lead lies with ICANN⁵¹, which has already adopted special rules that can lead to the (not court ordered) cancellation of a domain name found to infringe a trademark. The ICANN, under pressure, has demonstrated some willingness not only to regulate pure technical standards but to use its power to de facto setting rules for acceptable behaviour on the Internet as well⁵².

There are therefore at least some chances persuading the ICANN to set up rules against the use of domain names for racist purposes. Breaking such rules would in the end lead to the suspension or cancellation of the domain name in concern. Loosing a domain name technically does not exclude anybody from the Internet, but it makes it much more difficult for someone to be heard on the Internet⁵³. This concept is not totally new; Network Solutions, until recently the only official US domain name registry, did not allow the registration of the «Network Seven», the seven words that the major television networks will not air. Several racist domain names have also been blocked through registration by civil rights organizations⁵⁴.

One should be aware that the establishment of rules for domain name revocation in case of racist use will certainly draw a lot of criticism. Such criticism should be discussed thoroughly (see below «Conclusion ...»).

Strategy 3: Support legal and political anti-hate-initiatives

Even in countries with a widely accepted broad interpretation of free speech principles there have been and still are several initiatives pursuing a more restrictive view regarding racist contents on the Internet. While racist speech in the US may only, if at all, be banned if it provokes the person to whom it is directed to violence, a shift in interpretation of the First Amendment might be possible over time.

One strategy therefore could be the active support of movements and organizations pursuing such a shift in interpretation. This would include various kinds of support such as providing funds, political pressure, platforms for divergent views on the freedom of speech issue existing in the US already and more. It would also be important to constantly raise the issue of racism on as many occasions as possible. The fight against racism in all of its forms could be made a permanent issue on the

⁵¹ Internet Corporation for Assigned Names and Numbers (ICANN), <http://www.icann.org>, responsible for address space allocation, protocol parameter assignment, domain name system management, and root server system management.

⁵² This has lead to heavy criticism of the ICANN and its backers.

⁵³ Without a domain name, the well-known white supremacy website «Stormfront.org» could not be accessed by using its name anymore, for example. A user would have to know the correct network address 206.160.0.248, which will change every time a website publisher has to switch its provider.

⁵⁴ The domain name «nigger.com» has, for example, been registered by the National Association for the Advancement of Colored People (NAACP). The Anti-Defamation League Registered six domains with the word «kike».

political agenda whenever there is a possibility to do so. This includes putting pressure on the US government.

This strategy could and should include trying to shift the current discussion away from the freedom of speech issue towards the subject of *discrimination*. This isn't as far-fetched as it might seem on first view since discrimination is the basic building block used for racist contents. Since the US law is quite strict in preventing discrimination this strategy could be quite promising on the long run. It of course requires the US lawmakers and courts to understand that the main intent on publishing racist speech is to justify discrimination of certain groups of the population and to lay the foundation for such discrimination in peoples mind. Racism not only leads to hate, it *is* discrimination of other people based on their race, colour, religion or creed. In this sense, allowing racist speech basically equals to declaring discrimination as legal – just because there is no physical violence or financial damage associated with it.

Racist groups of course would claim to be «discriminated» themselves because of their belief once they would not be allowed to publish their ideas anymore. Looking at it with an isolated view one might even tend to agree, as many in the US do. The important point to understand however is that since racist groups use of speech to discriminate others basically should deprive them the right to be protected from discrimination by others in the same way. In other words: It is contradictory demanding to be allowed to discriminate others while asking not be discriminated oneself («venire contra factum proprium»). Racist speech as well often pursues fascistic ideas widely regarded as anti-democratic and therefore as well should not be protected by the right of freedom of speech. This would contradict the basic idea behind such right as a guarantee for democracy.

Therefore a country should not try to justify racist speech with the right of freedom of speech. Otherwise any effort towards eliminating discrimination might simply not be credible anymore.

The strategy described in this section should be carried out in a subtle manner. Changing established interpretations and viewpoints and even court decisions⁵⁵ nevertheless requires quite some time and lobbying effort. There are also open questions regarding international law should governmental institutions carry out such a strategy. This could be interpreted as a political interference in the matters of a sovereign country. The prospect of reaching consent on where speech indeed should be protected and where this is not desirable seems too inviting. One should also bear in mind that the strategy described is a very long-term effort requiring a lot of patience on all sides.

Strategy 4: Limit racist speech geographically

A compromise solution to the problem of racist speech on the Internet could be to limit the access to racist speech from *outside* the US only. While it not may be possible to convince the US to truly join the fight against racism on the Internet, it might be possible to prevent the spread of racist speech outside the US. Since the Internet

⁵⁵ In *Chaplinsky vs. New Hampshire*, 315 U.S. 568 (1942), the Supreme Court decided that so called «fighting words» are not protected by the First Amendment. Fighting words are words that will provoke the person to whom they are directed to violence. In *R.A.V. vs. City of St. Paul*, 505 U.S. 377 (1992), the Supreme Court however struck down a Minnesota statute against bias-motivated speech because it did criminalize only *race-based* fighting words instead of all. Since the selection was based on the contents of the words it would not withstand the First Amendment anymore, the Court ruled.

has made such dissemination easier than ever, one might be able to use technology to get the opposite effect as well.

This, again, is not a new strategy. At the time this report was written, US laws prohibited export of certain cryptographic products. Anyone offering strong encryption software on the Internet had to make sure no customers from outside the US would download such material. Since good encryption was available outside the US the ban was absolutely useless; it took the US government many years to realize that the only effect of their ban was to harm their own industry. But the ban has proven that export control on the Internet today technically is possible for commercial offerings, as long as such export control is done at the source.

The same scheme has been used on other occasions as well. An online lottery operating from the Principality of Liechtenstein, a neighbour country to Switzerland, has been using such techniques to effectively block out Swiss customers from using their system, since such service would be illegal in Switzerland. The online lottery nevertheless was offering their service through a Swiss access provider in the beginning.

Providers could either be asked to voluntarily participate in such a scheme or could be forced to comply, as laid out in this paper. Hosting providers not willing to refuse their services to racist groups could designate special servers for such content. Those servers could be programmed not to accept any connection from outside the US. Access providers not willing to give up serving racist groups as their customers could use similar methods. Using filtering techniques⁵⁶, they could effectively discard any incoming web traffic not originating from the US to such customers web servers.

Since every node on the Internet has a network address registered for use only within a specific part of the Internet, it is possible to determine the approximate geographic origin of a user. This system is not failsafe and of course can be circumvented⁵⁷, but would probably be effective for well over 90 percent of all non-US users. Those techniques are not too complicated to install or maintain and should not place a big burden for the provider community. Many large providers actually are already using information about the geographical origin of their visitors for marketing purposes.

Such a solution would allow US providers to continue offering racist speech on their networks without limitations to the US public, but would protect US providers from criminal prosecution abroad while not costing much. Maintenance of such a system also would not require constant updates since the filtering information is more or less static. Because such an action would take place at the root of the «problem», it would be quite effective in banning racist speech at least from a non-US perspective.

The big problem probably will be separating normal customers from those offering racist speech. Of course hosting and access providers could amend their terms and conditions with a clause requiring customers to identify racist content. They could even impose a contractual penalty on customers failing to do so, yet many of those

⁵⁶ Most routers (devices interconnecting two sub-networks on the Internet) and firewalls (security devices) can be programmed to filter data packets of certain types originating from within a certain IP address range.

⁵⁷ Users could for example try to masquerade by using a server located in the US as a relay.

customers still probably would not disclose their intentions in advance – and maybe not even their real identity. Many well-known hosting providers used for publishing racist websites today already have a no-hate-page policy, but still have to rely on hate watch organizations or individuals to inform them about abuses.

The strategy suggested in this section therefore should mainly be viewed as new way to deal with the well-known racist resources on the Internet using their own equipment or taking advantage of a provider not willing to completely ban racist contents of his servers and among his customers.

Strategy 5: Effective content identification

Another compromise strategy could be to persuade the US government to regulate racist speech in a way which will ease its detection and filtering wherever required by foreign laws but is in line with the First Amendment.

Although the US government may not outright ban racist speech it may impose reasonable restrictions such as requiring a *permit* or the observance of regulatory provisions for certain publications on the Internet⁵⁸. The purpose of such a permit would not be to prevent or hinder such speech from being published in any way, but it could be used to force publishers to *identify* their content in a machine readable and unique way either visibly or invisibly⁵⁹. The government could then legally stop publications not bearing such a «tag» for content identification without violating First Amendment. Such tags would make it easier for third parties, providers and foreign countries to identify and block racist content, but as well other content one might consider undesirable, illegal or problematic in other concerns.

In order not to violate the United States Constitution⁶⁰, such a scheme would have to treat equally every would-be-publisher and must not give too much discretion to the individual who grants the permit⁶¹. Therefore any statute requiring such a permit or ordering restrictions based upon the contents of the message or point of view to be expressed on the Internet probably would be unconstitutionally. Nevertheless it should be possible to find a paraphrase of potentially objectionable speech that neither is vague nor focused on racist or hate speech only – both would not be constitutional – nor does include *all* speech, since requiring permits or ordering restrictions for every publication on the Internet would be impractical and not make any sense.

A permit should not cost anything as well and it might not even be necessary to issue the permit on a one-on-one basis. The government could permit critical speech by issuing a «general permit» for everybody adding appropriate content rating tags. This would not put a burden on any publisher while allowing governmental legal action against individuals not observing the rules.

Although this method does not eliminate racist or hate speech, it could make it considerably easier to keep it under control, to identify the sources and to block export or import of such material. It would actually lead to the government assisting the industry in self-regulation by providing a legal framework for it to build up technical solutions to the problem. The online industry has been working on content rating

⁵⁸ See <http://www.adl.org/20faq/answers.html> for more information.

⁵⁹ Such content tagging should not require complicated programming nor should it cost anything.

⁶⁰ State constitutions might however provide greater protections for speech.

⁶¹ See *Interstate Circuit vs. Dallas*, 390 U.S. 676, 688-689 (1968), with further references.

schemes⁶² for some time now but has not made very significant progress yet. Government assistance could be helpful since it would force a number of publishers to identify their content which today have been reluctant in cooperating with self-regulation schemes.

Strategy 6: Civil action strategies

As described in this paper, law enforcement authorities normally are restricted to act within their country territory since extra-territory acts could be considered as violation of sovereignty of another country. This is however is true only for *sovereign* acts, as for example the prosecution of a crime. Government authorities normally are allowed to be active outside their home territory as long as they act as a *private* person.

This circumstance could actually be used for combating racist speech being spread from another country. One method for example could be to sue racist groups for their publications in front of a civil court. Although this probably never has been practised yet, one could think of several legal provisions on which grounds someone could take a publisher of racist speech to court. One such reason could of course be *discrimination*. Since racist opinions rarely are directed against a particular country as a whole, country authorities willing to fight against racism would have to join forces with a person suitable as a plaintiff. The government of such a country could finance such a complaint.

Another basis for entering into legal action could be *copyright*. Most forms of speech is protected by copyright. Therefore, the owner of the rights may order such material to be taken off the Internet. This would apply to racist speech as well. The government could get control of the copyright by it's own law: Some countries today have provisions in their criminal law permitting them to confiscate all kinds of assets if they are related or being produced by a crime. This in most cases does also include copyrights.

If, for example, a citizen of such a country is found to be using US servers for spreading racist manifestos, a court in the country of origin as a first step could «confiscate» the copyright on the illegal works of its citizen. Having obtained the copyright, the government could then effectively force any US provider to take down that content by using copyright law. It however remains unclear whether this new method would actually work in practice and could even be extended to works of citizens of other countries.

Conclusion & final remarks

This working paper cannot and will not make any suggestions as to which of the various strategies are politically most viable, if at all. Since any solution would have to satisfy diverging legal and possibly diverging political standpoints, it will be necessary to find a compromise.

This paper also should *not* be regarded as making any statement whether the various strategies presented are desirable. Several methods might indeed be tempting for use in the fight against racism on the Internet, because they seem simple and

⁶² The most important initiative seems to be the «Platform for Internet Content Selection» or PICS; see <http://www.w3.org/PICS/> for further information.

easy to be put into action. But such actions could also set dangerous precedents that have to be discussed thoroughly, since freedom of speech is a delicate issue.

While many people may agree using the methods described here in order to combat racism, actually using them without proper controls and definitions could lead to serious abuse for example. Other persons, groups or communities might successfully demand the use of such techniques to fight *other* online content they view as objectionable as well. If such «tools» for limiting speech on the Internet do not remain under control by truly democratic governments, organizations or international bodies, they one day might be misused by some antidemocratic groups or regimes for their purpose. This paper will not and cannot step into that debate but it can serve as a starting point for such a discussion.

Also, this paper should not only help to understand the technical and legal obstacles and different views regarding racism on the Internet. The «catalogue» of possible solutions and strategy, which of course cannot be considered as final, should make one thing clear: Despite diverging views on issues such as freedom of speech, there is potential for a «solution» to the problem which would satisfy all sides. But such a solution will of course require intense cooperation and many repeated efforts.

Racist groups on the other hand will continue to use the Internet as a perfect tool for recruiting new followers and for spreading their word.

(dr) (4.2) (14-APR-2000)

© 2000 David Rosenthal, Basel, Switzerland