The Registrar
European Court of Human Rights
Council of Europe
F–67075 STRASBOURG CEDEX

7 October 2008

Amicus curiae brief

concerning the application no. 2872/02
by K.U.
against Finland

1. Introduction

In the action mentioned above, the applicant complains that he had not had an effective remedy under national law to discover the identity of a person who put a defamatory text on the Internet in his name. According to his complaint Finnish legislation at the relevant time did not provide him with means to obtain redress or protection against the breach of privacy. The applicant was aged 13, and the advertisement read he was looking for a sexual relationship with another boy or man.

On 27 June 2006 the Court ruled that the complaints raise serious issues of fact and law under the Convention and are not manifestly ill-founded. As "friends of the Court", we would like to submit some remarks on the case as its outcome could have far-reaching effects on the privacy of all European Internet users and thus practically all citizens. A ruling requiring Contracting States to provide for the traceability of communications would have very serious consequences on user privacy which is itself protected by the Convention.

Article 36 par. 2 of the European Convention on Human Rights reads:

> *The President of the Court may, in the interest of the proper administration of justice, invite [...] any person concerned who is not the applicant to submit written comments or take part in hearings.*

Rule 44 par. 2 of the Rules of Procedure of the European Court of Human Rights specifies that not only may the President invite but also grant leave to any person concerned who is not the applicant, to submit written comments.

I therefore hereby ask the President to grant leave to the submission of the following written comments to the Court.

2. Requirement of an effective remedy

At the core of the present case lies a misrepresentation or identity theft – the perpetrator pretended to be the applicant when publishing the advertisement – as well as the publishing of illegal content on the Internet, constituting an act of calumny. This kind of behaviour is not specific to the Internet. The same advertisement could alternatively have been published on a public noticeboard or in a newspaper.

It makes sense to interpret the Convention as obliging its signatories to provide victims of such acts with an effective remedy. It would not be acceptable if a Contracting State did not provide for any redress whatsoever.

However, a wide margin of discretion must be granted to the Contracting States as to which remedies they provide. This margin of discretion has for long been recognised in the jurisprudence of the Court. Also, it is a general principle of law that human rights cannot impose duties the fulfilment of which would itself violate human rights. States can therefore not be required to impose disproportionate countermeasures.

3. Remedies against the publishing of illegal content on the internet

3.1 Removal of illegal content: Notice and take down procedures

The most effective remedy against illegal content on the Internet is a notice and take down procedure. The hosting provider is notified of the illegal content and obliged to take it down. This procedure corresponds to the removal of a notice on a public noticeboard in the "off-line world".

The Convention can be interpreted as requiring a notice and take down procedure in cases of illegal content being published on the Internet. A procedure of such kind appears to have been in place in Finland at the relevant time.

3.2 Blocking access to illegal content

Sometimes it is not possible to have content removed. This is mostly due to the fact that content which is illegal in one country may be legal in the country it is hosted in.

Some countries impose the use of filtering mechanisms on Internet access providers, most notoriously China ("great Chinese firewall"), but also European states such as Germany. These filters are not very effective, however, as any user with some technical knowledge can easily circumvent them. Publishers can also circumvent filters by re-publishing the content elsewhere. Also, filtering mechanisms are in practise commonly used to block access to politically controversial content. For example Turkish courts have repeatedly ordered the blocking of Internet media held to constitute a defamation of Turkdom. Finally, it needs to be kept in mind that the publication of content never directly and physically harms any person.

Article 8 of the Convention guarantees the right to privacy of communications. This provision protects citizens, in principle, from any control of the content of their communications, including the information they access via the Internet. Filtering mechanisms interfere with that right.

Article 10 of the Convention guarantees the right to access publicly available information. It is preferable that states agree on common standards regarding the legality of content, as has happened with the Additional Protocol to the Convention on cybercrime, and establish procedures to enable the international removal of such content rather than use ineffective blocking mechanisms to try and prevent citizens from accessing content which is legal in its country of origin. Principle 3 of the Council of Europe's Declaration on freedom of communication on the Internet reads: "*Public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers.*"[1]

The Convention should therefore not be interpreted as requiring the use of access filtering.

3.3 Criminal prosecution and identification of perpetrators

Publishing information on the Internet may infringe provisions of criminal law as in the present case.

It is doubtful whether the criminal prosecution of the publisher can be considered as a means of redress for the victim and whether the Convention should be interpreted as giving a citizen a right to criminal prosecution. Criminal prosecution is carried out in the general interest of justice, not in the interest of the victim. In modern states, public interest and the personal situation of the offender determine whether and how they are prosecuted, rather than the interests

1 Adopted by the Committee of Ministers on 28 May 2003, https://wcd.coe.int/ViewDoc.jsp?id=37031.

of the victim. Criminal prosecution is no longer an instrument of retribution but has become a preventive instrument. Criminology has continuously demonstrated that criminal prosecution needs to be used sparingly and with care if it is to benefit society.

Even if – despite the arguments set out above – the Convention was to be interpreted as requiring an effective system of criminal prosecution to be maintained, Contracting States would still enjoy a wide margin of discretion as to which acts they impose criminal sanctions on, which infringements they order to be prosecuted and which means of investigation they provide to the competent authorities.

In the present case, it was well within Finland's margin of discretion not to authorize access to traffic data for the purpose of identifying the author of the illegal advertisement. The following reasons shall be put forward for this opinion:

1. **Other means of redress are available** to victims of calumny that do not require the identification or criminal prosecution of the offender. For example, the offending content can be removed and the victim can be compensated.

2. Communications data allowing for the identification of the offender **should not have been available** in the first place. If the relevant content provider and the access provider had not retained the IP addresses of all of their users without any suspicion of wrongdoing (IP addresses are not needed for billing purposes), problems of access to the data would not have arisen. Both Article 10 of the Convention and relevant provisions of national constitutional law prohibit a blanket retention of information identifying the publishers of information on the Internet. The law of several Contracting States – for example paragraph 13 of the German "Telemediengesetz" – explicitly requires the provision of anonymous services. Freedom of expression (Article 10) would be disproportionally interfered with if every publisher of information on the Internet could be identified against their will. With good reason there is no such requirement for "off-line" flyers, advertisements, notices etc. Also, Article 8 of the Convention and provisions of national constitutional law prohibit a blanket retention of information identifying who used an IP address at a certain time to access the Internet. Although a directive 2006/24/EC on the blanket retention of such data has been adopted by the EU, a general retention of data on all users in the absence of any suspicion of wrongdoing is a manifestly disproportionate interference with the right to privacy guaranteed under Article 8 of the Convention.[2] The EU directive on data retention is contested in multiple court cases[3] and can be

2 Breyer: Telecommunications Data Retention and Human Rights, European Law Journal, Vol. 11, No. 3, May 2005, pp. 365-375.

3 European Court of Justice, Action brought on 6 July 2006 - Ireland v Council (Case

expected to be annulled soon. It should also be noted that the Council of Europe has decided against imposing data retention requirements in its Convention on Cybercrime.

The Convention must therefore not be interpreted as requiring Finland to ensure the availability of communications data by ordering a general retention of communications data. Such a requirement would itself violate Articles 8 and 10 of the Convention. To the contrary, those articles need to be interpreted as putting strict limits on the legitimate processing of communications data identifying publishers and users of the Internet, hence banning blanket data retention practises. At least, Contracting States should not be denied the right to prohibit the personally identifiable logging of Internet publishers or users. Accepting the right of Contracting States to ban the recording of such data, Contracting States should also be given the right to block access to such data, as the resulting protection of privacy is the same in both cases.

3. The Convention should **not be interpreted as requiring Contracting States to authorize** their authorities to access the content or traces of telecommunications. The privacy of communications and the freedom of expression are rights of such importance and benefit in a democratic society that Contracting States cannot be obliged to allow for exemptions under the Convention in regard to telecommunications. Both articles 8 and 10 read that Contracting States *can* provide for exceptions, but do not say that they *must* do so.

At the time the Convention came into force, several Contracting States did not have any laws in place allowing for wiretaps or any other interferences with the privacy of communications (e.g. Germany). Those Contracting States can certainly not be said to have violated the Convention by maintaining without exception rights guaranteed in the Convention itself.

4. The reasonably effective **investigation of crime is possible without access** to communications data.

Admittedly, criminal acts committed via telecommunications networks can be difficult to investigate without access to communications data. However, these difficulties are not specific to the Internet. Identifying the author of an illegal on-line publication without communications data is difficult, but so is the identification of the author of an anonymous advertisement published in a

C-301/06); German Federal Constitutional Court, Action brought on 31 December 2007 (Case 1 BvR 256/08); Irish High Court, Action brought in 2006 – Digital Rights Ireland v Minister for Communications (Case 2006 No. 3785P); Hungarian Constitutional Court, Action brought by Hungarian Civil Liberties Union on 2 June 2008; Bulgarian Supreme Court, Action brought by Access to Information Programme on 19 March 2008.

newspaper or the author of a notice on a public notice board. Yet, in none of those cases is it impossible to identify the perpetrator. An advertisement or a notice may reveal some information on its author by its content (e.g. style of writing or spelling, printer used). Likewise, an anonymous on-line advertisement may reveal information it its style of writing and spelling or on the system used to submit the data. The victim may in both cases be able to provide information on the perpetrator (who knew of the information published, who had an interest in committing such an act?). A search of suspects carried out by the police may reveal the notepad the notice was written on or the computer an advertisement was posted on. Notes may be discovered, and witnesses may give clues. Investigating Internet crime without access to communications data is no more difficult than is investigating similar off-line crime.

The average success rate of criminal investigations is 55% in Germany, meaning that about one in two cases cannot be cleared up. It is therefore not specific to the Internet that it is often impossible to identify a perpetrator and prosecute a criminal act. While it is true that access to communications data would enable more perpetrators to be identified, the same is true for installing CCTV cameras in front of all public notice boards or banning the publishing of anonymous advertisements. It should however be left to the discretion of the Contracting States which measures they deem appropriate to facilitate the investigation of criminal acts.

Finding a violation of the Convention could at best be considered if it was completely impossible under the relevant law to prosecute violations of a certain nature. However, it was not completely impossible under Finnish law to prosecute calumny committed on the Internet. It has been explained above how this could be achieved without using communications data, just as it may be possible to identify the author of an anonymous notice on a physical notice board.

5. Besides, it needs to be kept in mind that even if access to communications data is provided to public authorities, the data is of limited use and investigations will still **often fail**. Communications data may lead to an Internet café, to a wireless public access point, to an anonymization service or a server located abroad, or to a computer used by several people. Communications data does not permit the identification of the perpetrator, as the connection could have been used by any family member, family friend, user of a public WLAN modem or illegitimate user of the account details.

The utility of communications data in criminal investigations should not be overestimated. Providing access to such data is but one of a multitude of possibilities of trying to facilitate the investigation of on-line crime. Japan did not

allow for any governmental access to telecommunications until the 1990s. It still had one of the lowest crime rates in the world.

6. Communications data is often misleading and leads to the **prosecution of innocent** citizens. The Contracting States should therefore not be required to give prosecutors access to it.

For example, in 2006, a 63 year old man from Nuremberg (Germany) was accused of downloading photos from the Internet without paying for them. It was later found that the act was committed by an unknown person using his wireless LAN Internet access network.[4] In 2007, the home of a German professor was searched for suspicion of distributing child pornography on the Internet. It was later found that his access provider had made a mistake in identifying him as the user of the relevant IP address.[5] A similar case had previously been reported in the US.[6] Sweden reported several cases of erroneous searches of homes where in fact the home owner's access code had been abused by criminals.[7]

These are but a few publicised errors that resulted from the use of communications data. A serious risk of such errors is inherent in using communications data as such data only identifies a device or an access point but never a person.

7. Even Contracting States that allow for access to communications data for prosecuting crime usually limit that access to serious crime (see for example Article 1 of directive 2006/24/EC) for reasons of **proportionality**. It is well within the margin of discretion enjoyed by Contracting States, if not a requirement of proportionality, to limit interferences with the secrecy of communications to serious crime. While it is true that these restrictions have substantial consequences for the investigation of non-serious crime committed on the Internet, it has been demonstrated that the identification of perpetrators without access to communications data is possible by other means. This possibility is sufficient under the Convention, especially for non-serious crime.

This is in line with the Convention on Cybercrime. Although Article 17 of that Convention provides for the disclosure of traffic data, Article 15 par. 1 reads:

---

4 http://www.presseportal.de/polizeipresse/p_story.htx?nr=920697.

5 http://www.lawblog.de/index.php/archives/2008/03/11/provider-liefert-falsche-daten-ans-bka/.

6 http://www.foxnews.com/wires/2006Oct25/0,4670,PeopleShaqBotchedRaid,00.html.

7 Stefan Kronqvist (Head of Information Technology Crime Squad in Sweden), Submission to the European Commission for the Public Hearing on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, http://web.archive.org/web/20060621103130/http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/PublicHearingPresentations/Kronqvist.html.

"*Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.*" German Parliament in 2007 adopted a provision restricting the access to communications data (*§ 100g Strafprozessordnung*), arguing that due to the graveness of the interference with the privacy of communications, the principle of proportionality may not allow for access to communications data even if it is the only means of identifying an offender.[8] The German Federal Constitutional Court has held the same.[9]

It is within the margin of discretion of Contracting States, if not a requirement of proportionality, not to qualify an act of calumny as a serious offence. An act of calumny does not, in itself, harm the life, health or freedom of a person. Accordingly, Finnish law provided for a maximum sentence of four months in prison.

8. Requiring Internet publications to be traceable would deviate from **general standards** in the "off-line world".

The world wide web can be compared to a public billboard. Everybody has the right to anonymously post an advertisement on a public billboard. The Internet can be compared to a Speaker's Corner in which anybody can speak up anonymously. Newspaper advertisements can be placed anonymously. Letters can be sent without identification of the sender. The Court should not require the Internet to be more traceable than the "off-line world".

9. Anonymous access to the Internet – including publishing services – is **indispensable** for many people:

- People in need (e.g. suffering from illnesses or other kinds of distress) may be willing to seek information or help and communicate with each other only in complete anonymity (e.g. Internet self-help forums for victims of sexual abuse).

- Whistle blowers are often prepared to alert the public to grave problems or

8 BT-Drs. 16/5846, 52.

9 I.e. case 1 BvR 330/96 of 12 March 2003, par. 75, http://www.bverfg.de/entscheidungen/-rs20030312_1bvr033096.html.

even criminal acts only in complete anonymity.

- Dissidents, bloggers, journalists and members of the opposition in authoritarian states (e.g. Burma, Tibet) who are pushing for democratic reform need anonymous services provided abroad to publish information and alert the public to the situation and developments in their countries. Without anonymity, they are threatened by arrest, detention and torture. Anonymous services protect the freedom and lives of those people. For example, the opposition in Burma could not communicate its messages to the outside world without means of anonymous publication on the Internet.

In the specific case before the Court, it may appear somewhat dissatisfying that the perpetrator was not identified. However, the whole picture needs to be kept in mind. The ability to use the Internet anonymously is in probably more than 99% of all cases used for legitimate and beneficial purposes and relatively rarely abused. The ability to use the Internet without fear of prosecution benefits society much more than traceability would profit potential victims.

The chilling effect of traceability has been recognised by the Courts[10] and is empirically proven. A survey conducted by German research institute Forsa in May 2008 found that with communications data retention in place, one in two Germans would refrain from contacting a marriage counsellor, a psychotherapist or a drug abuse counsellor by telephone, mobile phone or e-mail if they needed their help.[11] One in thirteen people (which extrapolates to 6.5 mio. Germans in total) said they had refrained from using telephone, mobile phone or e-mail at least once since legislation making telecommunications traceable came into force on 1 January 2008.[12]

In virtual as in real life, the freedom of – named or anonymous – expression must prevail as its benefits by far outweigh the number of abuses and the damage they can do.

10. The Convention should therefore **not be interpreted as requiring member states to allow for the traceability** of communications. We especially ask the Court not to require a level of traceability that is inexistent in "real life".

3.4 Preventing the publishing of illegal content

If an illegal publication has taken place, some Contracting States require

10 I.e. German Federal Constitutional Court, 1 BvR 256/08 of 11 March 2008, par. 148, http://www.bverfg.de/entscheidungen/rs20080311_1bvr025608.html.

11 http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf.

12 http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf.

hosting providers to take measures to prevent similar publications in the future. Principle 6 of the Council of Europe's Declaration on freedom of communication on the Internet refers to "*the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of the law.*"[13] Directive 2000/31/EC reads: "*Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.*" The German Federal Court of Justice (Bundesgerichtshof) has ruled that in case of a danger of a repetition of a violation in the future, hosting providers are obliged to take "reasonable" preventive measures.[14]

Such measures may include the removal of the account used by the perpetrator, the blocking of re-registrations using their e-mail address, the blocking of publications containing the name of the victim and such like. In the case at hand, it would have been possible for the provider of the dating service to block the publication of another link to the applicant's web page or of his phone number, as a filter automatically screening all advertisements for those strings could have been installed (although it would have been easy to circumvent by slightly changing the string, or by using another service).

According to the facts given by the Court, section 48 of the Finnish Personal Information Act provided that a hosting provider must verify the identity of senders or make sure that information published on its website by its users is legal. As it is impossible for an Internet hosting provider to examine the legality of all of its users' publications, service providers would be have been required under Finnish law to verify the identity of all users and thus block anonymous access to their services. Unlike the targeted measures discussed above, this requirement would impose a general, blanket identification of all users.

Banning all anonymous publications on a service clearly violates Article 10 of the Convention. Disproportionate or excessive measures such as a ban on all anonymous publications or a requirement for the hosting provider to review all content before publication must not be imposed under the Convention (see also Article 15 of directive 2000/31/EC and Principles 3 and 6 of the Council of Europe's Declaration on freedom of communication on the Internet[15]). Excessive

13 Adopted by the Committee of Ministers on 28 May 2003, https://wcd.coe.int/ViewDoc.jsp?id=37031.

14 I.a. judgement of 12 July 2007, I ZR 18/04 – eBay.

15 Adopted by the Committee of Ministers on 28 May 2003, https://wcd.coe.int/ViewDoc.jsp?id=37031.

measures disproportionally interfere with the freedom of expression of users wishing to anonymously make controversial content available to the public (e.g. "whistle blowers"). It is precisely such content which is often of the greatest value in a democratic society. Its publication and the availability of anonymous hosting services as a precondition to exercising our freedom of expression needs to be encouraged rather than stifled. The benefits of anonymous expression and its harmful effects have already been discussed in more detail above (3.3).

The Convention should therefore be interpreted as leaving it to the discretion of the Contracting States whether or not measures are imposed to prevent illegal publications. The case at hand does not concern the problem of preventive measures.

3.5 Financial compensation

Another way of providing redress to a victim is by financial compensation.

Such compensation can be paid for by the perpetrator if they can be identified. However, the problems involved with tracing Internet communications, including the legitimate legal limitations and restrictions on traceability, have been discussed in detail above (3.3).

Payment of compensation can also be imposed on the hosting provider concerned. Hosting providers can buy insurance against such liability. However, as explained above, imposing an obligation to compensate victims of illegal publications deters from the provision of easily available, anonymous, quick and free hosting which in turn decreases the availability of information of paramount importance to a democratic society. Principle 6 of the Council of Europe's Declaration on freedom of communication on the Internet states that hosting providers shall only be held liable for content published on their website "*if they do not act expeditiously to remove or disable access to information or services as soon as they become aware, as defined by national law, of their illegal nature*".[16]

Compensation can finally be paid for by the state or a publicly financed institution. Such institutions or funds exist in a number of Contracting States as it is a problem common to criminal acts that the perpetrator can often not be identified or does not have the means to compensate the victim. A publicly financed fund is indeed the best solution for ensuring compensation. It is the public that profits from the manifold benefits of its freedoms, and it is the public that should bear the cost of the occasional abuse of those freedoms.

However, it needs to be kept in mind that the publication of illegal content

16 Adopted by the Committee of Ministers on 28 May 2003, https://wcd.coe.int/ViewDoc.jsp?id=37031.

does not normally cause direct damage to a person. Even in the present case it is not clear whether the applicant suffered any damages. Also, the risk of incurring unrecoverable damages is inherent in life.

The Convention should therefore not be interpreted as requiring the compensation of victims of illegal publications. If the Court does not share this view, it should at least be left to the discretion of the Contracting States how they provide for a fair compensation of victims.

4 Summary

In summary, the Convention may be interpreted as obliging its signatories to provide victims of criminal acts with an effective remedy. However, a wide margin of discretion must be granted to the Contracting States as to which remedies they provide. Also, no duties may be imposed the fulfilment of which would itself violate human rights.

Freedom of expression on the Internet is protected under Article 10 of the Convention. The privacy of communications is protected under Article 8 of the Convention. Considering the importance of those freedoms and the fact that their benefits by far outweigh the damage caused by their abuse, the Convention requires the creation of effective mechanisms for having illegal content on the Internet removed, but does not require traceability of Internet publishers or users.

[...]