Written Comments in the Case of *Yildirim v. Turkey*

July 2011

OPEN SOCIETY
JUSTICE INITIATIVE

IN THE EUROPEAN COURT OF HUMAN RIGHTS

Application no. 3111/10

Yildirim v. Turkey

WRITTEN COMMENTS OF THE OPEN SOCIETY JUSTICE INITIATIVE

Pursuant to leave granted on 11 May 2011 by the President of the Chamber, acting under Rule 44 § 3 of the Rules of Court, the Open Society Justice Initiative hereby submits its written comments on the legal principles that should govern the resolution of the Article 10 issues presented by this case.[1]

Introduction

1. This case involves a court injunction blocking access for all Turkish-based users to the Google Sites domain. This denied the applicant access to his personal website which was hosted by that domain, so that he could not operate it. The purpose of the injunction was to block access to a single, third-party webpage also hosted by Google Sites, unrelated to the applicant's site, which included content deemed offensive to the memory of Mustafa Kemal Ataturk. There is no indication of any attempt by the Turkish authorities to contact or serve notice on Google Inc., the US based owner and operator of Google Sites, prior to issuing the blocking order.

2. These written comments address the following issues:

   - *A. Prior Restraint.* The general principles of European prior restraint law and practice in relation to web-based content.
   - *B. Collateral Censorship*. The permissible scope of measures blocking access to online content, including measures that affect lawful content.
   - *C. Remedies and Safeguards.* The remedies and procedural safeguards that are, or ought to be, available to Internet users to prevent or challenge blocking measures.

3. For space reasons, discussion of comparative law and practice will focus primarily on the leading jurisdictions of France, Germany and the United Kingdom.

A. Blocking access to Internet content as prior restraint subject to "most careful scrutiny"

4. European law and practice demonstrate that orders and procedures blocking access to the internet should be treated as a method of "prior restraint", and as such should be subject to "the most careful scrutiny."

Council of Europe and European Union principles

5. The development of the Internet has had a profound effect on human communication, providing a platform that grants billions of people around the world access to an unprecedented amount and diversity of information and ideas, regardless of frontiers.[2] At the same time, the Internet has enabled and empowered ordinary people to disseminate information and share their own ideas with a potentially global audience. Within a few decades, users worldwide have developed a "significant reliance on the Internet as an essential tool for their everyday activities."[3]

6. This Court has acknowledged the Internet's potential to further Article 10 values, noting that "[i]n light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the

[1] The intervener would like to acknowledge the *pro bono* assistance of the international law firm Dechert LLP in researching comparative law and practice. The Justice Initiative is solely responsible for any inaccuracies.

[2] See *Reno v. ACLU*, 521 U.S. 844, at 853 ("The Web is …comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services. From the publishers' point of view, it constitutes a vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers, and buyers.")

[3] Council of Europe (Committee of Ministers) Recommendation (2008)6 on Measures to Promote Respect for Freedom of Expression and Information With Regard to Internet Filters.

dissemination of information generally. The maintenance of Internet archives is a critical aspect of this role".[4]

7. The Committee of Ministers of the Council of Europe has urged that "prior control of communications on the Internet, regardless of frontiers, should remain an exception" and that member states "should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers."[5] Removal or blocking of access to "clearly identifiable" Internet content is permissible only if "the competent national authorities" have taken "a provisional or final decision on its illegality," provided that all the safeguards of Article 10 § 2 of the Convention are respected.[6]

8. *Prior restraint.* Google Sites hosts a large amount of data and information, and is comparable to the online archives of major newspapers or traditional libraries.[7] The purpose of the injunction in this case was to make a single, anti-Ataturk site hosted by Google Sites unavailable to Turkish-based users. Measures of this nature blocking access to web content amount to prior restraint. Given the very nature of the Internet, content posted on a more or less stable website or other platform is in a state of constant publication, as it reaches and is accessed by web users in an ongoing fashion. Blocking access to such content for any amount of time is therefore analogous to traditional prior restraint insofar as it prevents new readers or information receivers from accessing the blocked content in the future. Such blocking orders are comparable to shutting down a periodical or confiscating the entire print run of a book shortly after its publication (when a few people may have read it, but not most of its potential readership).

9. The Court of Justice of the European Union (CJEU) is currently considering the validity of a potential Belgian court order that would provide for prior restraint of Internet communications by requiring a Belgian Internet service provider (ISP) to install software that is capable of permanently monitoring and blocking all traffic that might violate the intellectual property rights of a national association of artists.[8] The Advocate General concluded that as the order would include both illegal and perfectly legal communications, the measure amounted to an "interference" with the ISP's clients' freedom of expression, within the meaning of Article 10 § 1 of the Convention and the corresponding Article 11 § 1 of the EU Charter of Fundamental Rights.[9] In the Advocate General's opinion, such a conclusion was inevitable, irrespective of "the technical procedures by which the communication control is actually achieved, the breadth and depth of the control exercised, and the effectiveness and reliability" of any such controls.[10]

10. *Most careful scrutiny*. This Court has long held that the significant dangers inherent in prior restraint require the "most careful scrutiny" by the Court, not only where the press is affected, but also for books and other publications.[11] To be consistent with Article 10, prior restraint regimes must be subject to a "particularly strict" legal framework, ensuring both tight control over the scope of the bans and effective judicial review to prevent abuse.[12] In *RTBF v. Belgium*, the Court held that a flawed legal framework on prior restraint had exposed broadcasters to a potentially large number of

---

[4] *Times Newspapers Ltd v. the United Kingdom* (Nos. 1 and 2), Judgment of 10 March 2009, para. 27. See also *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, Judgment of 5 May 2011.
[5] Committee of Ministers Declaration on Freedom of Communication on the Internet, 28 May 2003, Principle 3.
[6] *Ibid.*
[7] Google Sites, a component of a software package known as Google Apps, is a popular tool for creating and maintaining personal, family or small business websites. As of September 2010, Google Apps claimed some 30 million users worldwide. See http://techcrunch.com/2010/09/20/google-apps-now-used-by-30-million-employees.
[8] Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs compositeurs et éditeurs* (undecided).
[9] Opinion of 14 April 2011, para. 85; at: http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-70/10.
[10] *Ibid.* The Advocate General concluded that the measure interfered also with the users' right to respect for the privacy of their communications and the right to protection of their personal data, as protected by the EU Charter.
[11] *Observer and Guardian v. UK*, Judgment of 26 November 1991, para. 60. See also *RTBF v. Belgium*, Judgment of 29 March 2011 (injunction against public broadcaster's program on patient complaints against a surgeon); and *Obukhova v. Russia*, Judgment of 8 January 2009 (interlocutory injunction barring journalist from reporting on accident involving a judge and related court case).
[12] See *Association Ekin v. France*, Judgment of 17 July 2001 (ban of foreign-origin/language publication).

complaints that could easily result in long-term injunctions preventing discussion of matters of legitimate public interest (at para.114).

11. The Court's jurisprudence has been particularly critical of the practice of banning the future publication of entire periodicals, which goes "beyond any notion of 'necessary' restraint in a democratic society and, instead, amount[s] to censorship."[13] The same would apply to long-term injunctions blocking access to websites, or bundles of websites, that post new information in a regular fashion. The new social media – such as influential blogs, discussion forums or even video feeds – have significantly broadened the traditional definition of journalism or newsworthy material, and are an important source of information, ideas and political involvement for large numbers of people.[14] Amateur videos posted, for example, on YouTube have become in recent years an important source of information about (crackdowns on) democratic protests underway in closed societies.

12. European Union law provides similar protections against arbitrary interferences with Internet communications. The EU Electronic Commerce Directive (2000) requires member states to guarantee "safe havens," or limitations of criminal or civil liability, for ISPs, hosting services and other service providers, provided (a) that they do not have "actual knowledge of illegal activity or information" and (b) once notified of such illegalities, they act "expeditiously" to remove or to disable access to the information, known as the "notice and takedown" procedure.[15] The Directive does not require blocking or regulate the procedural aspects of "notice and takedown", which is left to the discretion of member states. A recent draft EU Child Exploitation Directive provides, in its current form, that member states may block access to child pornographic material, provided that such measures are "set by transparent procedures and provide adequate safeguards, in particular to ensure that the restrictions are limited to what is necessary and proportionate, and that users are informed of the reason for the restriction."[16]

13. *Regardless of frontiers.* Consistent with the plain language of Article 10, the Court has upheld the right of individuals to engage in cross-border communications, including in the traditionally highly-regulated field of broadcasting.[17] This right is recognized by the 2003 Declaration of the Committee of Ministers of the Council of Europe, which states that "prior control of communications on the Internet, regardless of frontiers, should remain an exception" and that member states "should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers."[18] Such freedom is essential to Internet-based communications, over which no country can claim complete control or jurisdiction. Indeed, in some ways, the Internet has made the distinction between internal and cross-border communications almost irrelevant. For example, web users located both within and outside Turkey use a foreign-based platform, such as Google Sites or YouTube, to post Turkish-language content that is aimed primarily at a domestic Turkish audience.

Comparative National Standards

14. The laws and practices of France, Germany and the U.K. provide further support for the principle that such prior restraint must be subjected to careful scrutiny.

---

[13] *Urper and Others v. Turkey*, Judgment of 20 October 2009, para. 44 (court orders suspending publication of newspapers for up to a month under terrorism laws). Compare this with the similar approach of the U.S. Supreme Court in the seminal case of *Near v. Minnesota*, 283 U.S. 697 (1931) (striking down a local statute that authorized the shutdown of a defamatory publication, unless the publisher could prove that "the matter published [was] true and [was] published with good motives and for justifiable ends"). See also *New York Times Co. v. United States*, 403 U.S. 713 (1971), Brennan, J., concurring (U.S. Constitution "tolerates absolutely no prior judicial restraints of the press predicated upon surmise or conjecture that untoward consequences may result"); *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58 (1963) ("Any prior restraint on expression comes to this Court with a 'heavy presumption' against its constitutional validity.")

[14] See Clay Shirky, "The Political Power of Social Media," *Foreign Affairs*, Jan./Feb. 2011.

[15] Electronic Commerce Directive (2000/31/EC), sec. 14. The European Commission is in the process of reviewing the implementation of the Directive to date with a view to introducing possible amendments.

[16] Article 21. For more information and an explanatory recital of the provision, see http://www.edri.org/blocking_negotiations. The draft Directive is subject to adoption by the European Parliament.

[17] *Groppera Radio AG and Others v. Switzerland*, Judgment of 28 March 1990, para. 50. See also *Khurshid Mustafa and Tarzibachi v. Sweden*, Judgment of 16 December 2008.

[18] Committee of Ministers Declaration on Freedom of Communication on the Internet, 28 May 2003, Principle 3.

15. *France*. In recent years, the national legislature has adopted several statutory regimes authorizing courts to grant blocking or takedown injunctions in relation to intellectual property infringements, illegal online gambling activities, child pornography, and other content that is illegal under general criminal or civil laws.[19] These laws do not differentiate between domestically- and foreign-hosted content, as long as the content is accessible within France.

16. The most important judicial precedent in this field has been a 2009 judgment of the *Conseil Constitutionnel* on the constitutionality of a statute that authorized a new administrative authority to order ISPs to suspend Internet access for up to a year for individual Internet users found to have repeatedly infringed online copyright. The *Conseil* held that granting such intrusive powers to an administrative agency, however independent, violated the constitutional guarantee of "the free communication of ideas and opinions."[20] The same statute authorized courts to order "any measures necessary to prevent or put an end" to online copyright infringements. The *Conseil* noted that the statute required courts to conduct "a full hearing of all [affected] parties" prior to ordering such measures, and held that such injunctions would be constitutional, provided the ordinary courts adopted "solely those measures [that are] strictly necessary to preserve the rights involved" (at para.38).

17. *Germany*. The legal grounds for blocking access to online content are very limited in Germany, although there have been few rulings from the higher courts on the issue, leading to some legal uncertainty. Lower courts have held that currently available filtering and blocking mechanisms affect the right to privacy of telecommunications,[21] guaranteed by Article 10 of the German Basic Law.[22] A special constitutional law implementing Article 10, known as the G10 Act,[23] requires that all statutes seeking to restrict those rights must indicate so explicitly in order for any restrictive measures to be valid (the "citation requirement"). At the moment, no statute authorizing blocking measures appears to comply with the citation requirement, hence putting in doubt the validity of even the already limited precedents of the past decade regarding the blocking of certain categories of online content.[24]

18. The primary statutory rationale for preventing access to certain forms of criminal online content, including neo-Nazi propaganda, has been the protection of youth.[25] The body tasked with implementing the relevant provisions, the Commission for the Protection of Youth in the Media, may notify both domestic and foreign ISPs of racist or hate speech posted by their users, and request that such content be deleted.[26]

19. However, it is not clear if the Commission or other authorities can lawfully request the blocking of foreign-hosted content when that is the only option for preventing access (e.g. if the foreign host refuses to take down such content voluntarily). In a legal opinion on this question prepared at the request of the Commission, researchers of the widely respected Max Planck Institute concluded that

---

[19] See, respectively, Law No. 2009-1311 on the Penal Protection of Literary and Artistic Property Rights on the Internet (2009, known as the HADOPI II Act); Law No. 2010-476 on Opening to Competition and Regulating the Online Gambling Sector (2010); Law No. 2011-267 on Internal Security Matters (2011); and the Law on Confidence in the Digital Economy (2004, implementing the E-Commerce Directive).

[20] Decision No. 2009-580 of 10 June 2009, para. 16; an official English translation is available at: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf

[21] Hamburg High Court Judgment of 12 November 2008 (No. 308 O 548/08). Filtering technologies block user access to web content by screening out illegal content based on specified keywords or other identifiers. Unlike blocking measures, filtering does not target a specific website or location on the web, but all content that falls within the filtering parameters. However, the end result is essentially the same, with users being prevented from accessing certain online content.

[22] Article 10 provides, in the relevant part: "(1) The privacy of correspondence, posts and telecommunications shall be inviolable. (2) Restrictions may be ordered only pursuant to a law…."

[23] Statute concerning restrictions of the privacy of correspondence, posts and telecommunications, 26 June 2001.

[24] A bill under formulation that seeks to regulate online gambling activities reportedly includes a provision complying with the citation requirement. The current version of the bill was leaked by the German Piracy Party.

[25] The statutory basis for such measures is the InterState Agreement on Youth and the Media (JMStV), in conjunction with the InterState Media Services Agreement (MDStV).

[26] See, among others, the Commission's 2008 report on cyber-hate, at: http://www.jugendschutz.net/pdf/report_cyberhate_2008.pdf. Unlawful content in this context includes display of Nazi symbols, content geared against the constitutional order or understanding among nations, violations of human dignity, or abuse of children or animals in pornographic materials. See MDStV, sec. 12.

such blocking measures would affect, in addition to the privacy of communications, a series of other constitutional interests, such as freedom of information and the press, freedom of professional and economic activity, and property rights. In addition, they tend to have harmful side effects, including the blocking of lawful content and interfering with the basic infrastructure of the Internet, as well as the free dissemination of information. Finally, the authors found that the relevant youth protection laws do not meet the citation requirement of the G10 Act, and that, ultimately, blocking of foreign-hosted content under such laws would be unconstitutional.[27]

20. A German statute authorizing filtering of child pornographic material (known as the Access Complication Act) was adopted in February 2010. [28] However, shortly thereafter it was suspended and then repealed in April 2011 due to concerns that it would restrict access to lawful content and that the only effective way of preventing the dissemination of such criminal material was by taking it down from the source platforms, in collaboration with domestic and foreign service providers.

21. German courts have held that the statute implementing the E-Commerce Directive does not, in itself, provide a valid basis for ordering content blocking.[29] Similarly, it is now settled in German law that ISPs and other intermediaries are not criminally liable for third-party content and that, as a result, criminal laws per se cannot be used to force them to block access to such content.[30]

22. *United Kingdom*. Under section 12 of the 1998 Human Rights Act, prior restraint measures are not to be granted at the interim stage (e.g. of a libel case) unless the court is satisfied that the applicant is "likely to establish" at trial that publication should not be allowed which the courts have interpreted to mean "more likely than not."[31] Furthermore, a party seeking an injunction against the media must demonstrate convincingly that the measure is strictly necessary.[32]

23. Two special statutory regimes authorize judicial blocking of access to online content to prevent copyright infringements;[33] and authorize *removal* of "terrorism-related publications" at the request of the police.[34] However, these provisions are only enforceable against service providers based in the U.K. or another E.U. member state.[35] They do not, therefore, authorize blocking of foreign-hosted content, and appear not to be used to that effect, the preferred option being seeking the assistance of foreign law enforcement to take down offending sites altogether. We have not been able to locate any British court cases authorizing or validating blocking measures aimed at foreign providers.

24. The Internet Watch Foundation (IWF) was set up by British ISPs to prevent access to child pornograpy. It maintains a blacklist of offending sites worldwide and issues non-binding notices to providers when it believes the material would be "capable of sustaining a criminal prosecution" if it were to be put before a jury.[36]

25. Injunctions can be used to prevent publication of other unlawful online content, such as defamatory material posted on the website of a British newspaper. However, there has been little case law on these questions, and it is not clear that British courts would require domestic ISPs to block access to foreign-hosted material that violates domestic laws—and if so, under what circumstances. It has been

[27] U. Sieber and M. Nolde, *Internet Blocking Orders: National Law Enforcement in a Global Cyberspace?* (Sperrverfügungen im Internet. Nationale Rechtsdurchsetzung im globalen Cyberspace?), Duncker & Humblot, Berlin (2008).
[28] In German, Zugangserschwerungsgesetz (known as ZugErschwG).
[29] See, inter alia, the Bundesgerichtshof (BGH) Judgment of 27 March 2007, VI ZR 101/06 (involving a Rolex Watches attempt to block eBay sales of fake watches).
[30] See e.g. Munich District Court I Judgment of 17 November 1999 (the CompuServe case).
[31] *Cream Holdings v. Banerjee*, [2005] 1 A.C. 253 (House of Lords).
[32] *Venables v. News Group Newspapers* [2001] Fam. 430, paras 44 and 85.
[33] The Digital Economy Act 2010, secs 17-18 grant powers to the Secretary of State to make regulations for the issuance of judicial blocking injunctions, although no regulations have been issued to date.
[34] Terrorism Act 2006, sec. 3, authorizes law enforcement authorities to request the removal of criminal content that constitutes either "encouraging acts of terrorism" or "disseminating terrorist publications."
[35] The Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007, sec. 4.
[36] See IWF Code of Practice, at http://www.iwf.org.uk/members/funding-council/code-of-practice.

argued, for example, that there is "no established legal procedure" for ordering ISPs to block potential leaks of UK classified information, or indeed any publications that violate criminal laws generally.[37]

* * *

26. European law provides that internet blocking orders must be strictly necessary and capable of protecting a compelling social interest. The need for such an injunction must be convincingly established, and adopted as a measure of last resort. However, the refusal of foreign access providers to take down any objectionable content cannot be a sufficient basis, in itself, for granting blocking injunctions. In European practice, blocking orders against political expression protected by Article 10 are practically unheard of.

B. Overbroad blocking orders leading to "collateral censorship"

27. Blocking orders that indiscriminately prevent access to an entire group of websites, amount to "collateral censorship" which should be avoided as unnecessary and disproportionate, especially where it is technically possible to target only the offending website.

Council of Europe and European Union Principles

28. One central question raised by the current case is the extent to which procedures that result in the blocking of a significant amount of lawful content – that may or may not be related to the publisher of the unlawful content – are compatible with Article 10. This Court has held that forms of speculative or punitive prior restraint, such as the suspension of a periodical based solely on prior violations of content-based laws, go "beyond any notion of 'necessary' restraint in a democratic society and, instead, amount[s] to censorship."[38] This rationale must apply even more forcefully to the collateral suppression of websites that have not been found to be unlawful. There is nothing in the jurisprudence of this Court to suggest that such sweeping censorship could be considered necessary and proportionate, and to hold otherwise would amount to a significant reduction in the protection provided by Article 10. Justification for such broad measures would require an especially pressing social interest in the suppression of the material, akin to a national emergency, that clearly outweighs the interests of the affected legitimate speakers, and such action could remain necessary and proportionate only for a short period of time.

29. In addition, such invasive procedures must have a clear basis in law to avoid being considered arbitrary. In the *Scarlet* case currently before the CJEU, the Belgian courts had been asked to order domestic ISPs to introduce a very broad filtering system, that would block communications "with respect to all its customers, *in abstracto* and as a preventive measure, at the cost of the ISP and without time limit" (at para. 26). The request was made on the basis of a 1994 statutory provision authorizing Belgian courts to grant "cease and desist orders against intermediaries whose services are used by a third party to infringe a copyright or related right" (at para.14). The Advocate General concluded that the legislation was not sufficient to provide the foundation for such an invasive blocking system, which affected significant Charter interests including freedom of expression. As a result, the measure would run afoul of the "prescribed by law" requirements developed by this Court with reference to Article 10 § 2 and related provisions of the Convention; the blocking system would, in fact, "border on the arbitrary" (at para. 105).

Comparative National Standards

32. No instances of large-scale blocking of Internet content, akin to that of the current case, have ever been ordered or implemented in France, Germany or the U.K., by either judicial or administrative authorities.

33. *France*. In *Licra and UEJF v. Yahoo! Inc.*, two anti-racism groups requested an injunction to prevent Yahoo from allowing French-based users to purchase, through its US-based auction site, Nazi memorabilia and other items that are criminal in France. A French court of appeal accepted jurisdiction and ordered Yahoo to take "all necessary measures" to deter and prevent access to such

[37] See Prof. Lilian Edwards, *Wikileaks, DDOS and UK criminal law: the key issues*, 22 December 2010; at: http://uk.practicallaw.com/1-504-3391?q=wikileaks.
[38] *Urper* case, note 13 above (our translation).

auctions by French-based users, as well as pay a fine.[39] However, the French courts did not order French ISPs to block access to any part of Yahoo sites.[40]

34. In 2008, the Court of Cassation confirmed the blocking of *Aaargh.com.mx*, an openly anti-Semitic and Holocaust-denying website.[41] This is apparently only the second injunction of its kind to date, i.e., that is not related to illegal gambling, child pornography or copyright violations. The block did not affect any other websites. The ruling appears to be consistent with the case law of this Court, which has held, under Article 17 of the Convention, that denial of the Holocaust is not entitled to Article 10 protection.[42]

35. *Germany*. In 2002, administrative authorities of North Rhine-Westphalia ordered ISPs operating in that state to block access to foreign-based sites containing racist or neo-Nazi content. Some of these blocking orders were upheld by lower courts, in controversial rulings that relied primarily on the youth protection provisions described above.[43] These cases did not reach the top federal courts and, as noted, are of uncertain precedential value due to more recent rulings regarding the implications of constitutional Article 10 and the G10 Act on the privacy of communications.[44]

36. The statutes permitting blocking for the protection of children place a number of restrictions on such injunctions to prevent collateral censorship. Blocking can only be ordered when direct actions against the offending content provider are not likely to be effective; and provided the blocking measures are "technically possible and reasonable."[45] Reasonableness must be decided on a case by case basis by weighing the different interests involved, including the constitutional rights of privacy and free expression. A legal opinion prepared by the Bundestag Scientific Services questioned whether current blocking measures could be considered "necessary" in most cases, given how easily they can normally be circumvented.[46] Similar doubts have been expressed by the courts: in one civil case, the Hamburg High Court denied a blocking request and noted that it took the court itself only minutes to find detailed instructions online on how to circumvent blocking measures.[47]

37. *United Kingdom*. As noted above, the only system of significant foreign-content filtering/blocking that is currently operational in the U.K. relates to child pornography and is run voluntarily by the ISPs and the non-governmental Internet Watch Foundation. The blocking technologies used for this purpose, known as Cleanfeed and WebMinder, are generally capable of blocking access to specific unlawful content within a blacklisted site, limiting or eliminating any collateral blocking. The system does not authorize or cause the blocking of entire web platforms or large domains.[48]

---

[39] Judgment of 20 November 2000 (Superior Court of Paris); an English version is available at: http://www.coe.int/t/dghl/monitoring/trafficking/docs/activities/EGSNT2002-9rev_en.asp#P3897_346108.

[40] Yahoo did not appeal the French judgment, and later removed Nazi items globally from its auction sites and introduced other safeguards. Further attempts to criminally prosecute Yahoo and its chairman in France over racist and anti-Semitic content hosted on its US servers were dismissed by French courts.

[41] Decision No. 07-12244 of 19 June 2008. For a summary of a similar 2005 case, see: http://merlin.obs.coe.int/iris/2005/7/article19.en.html.

[42] See *Lehideux and Isorni v. France*, Judgement of 23 September 1998 (Grand Chamber); and *Garaudy v. France*, Decision of 7 July 2003 (Admissibility).

[43] See, inter alia, Judgment of the Dusseldorf Administrative Court of 10 May 2005 (No. 27 K 5968/02) (preventing access to two US-based websites with radical right-wing content, including material that glorified or played down the Holocaust). For a case dismissing a blocking order in a similar case, see Judgment of the Minden Administrative Court of 31 October 2002 (No. 11 L 1110/02).

[44] In fact, it was recently revealed that, in August 2010, the Dusseldorf Regional Government ordered two ISPs to block access to two online gambling sites. The enforcement of the orders was immediately suspended while the case is pending before the Cologne Administrative Court. The ISPs are challenging, inter alia, the compatibility of the blocking orders with Art. 10 of the Basic Law.

[45] See InterState Agreement on Youth and the Media, sec. 20 §§ 3 and 4; and the InterState Agreeement on Broadcasting, sec. 59 § 4.

[46] G. Pursch and V. Bar, *Opinion on Blocking Orders Against Internet Providers*, 27 January 2009; at http://www.netzpolitik.org/wp-upload/bundestag_filter-gutachten.pdf.

[47] See note 21 above.

[48] In December 2008, the IWF added to its blacklist a single Wikipedia page including the cover image of a music album. This measure interfered with the ability of UK-based users to edit Wikipedia pages generally. However, the blocking measure was lifted entirely within a matter of days, upon appeal by the Wikipedia Foundation and a public outcry. See http://en.wikipedia.org/wiki/Virgin_Killer.

38. The blocking system for copyright infringements under the Digital Economy Act 2010 is currently not operational, in the absence of relevant regulations by the Secretary of State. Under the Act, such regulations may be issued only if the Secretary is satisfied, inter alia, that online copyright violations are "having a serious adverse effect on businesses or consumers" and "making the [blocking] regulations is a proportionate way to address that effect." Were such regulations to be adopted, blocking injunctions could then be granted by a court against websites facilitating the infringement of "a substantial amount" of copyrighted material. Prior to granting an injunction, courts would be required to consider, among other factors, any "steps taken by the service provider … to prevent infringement of copyright", whether the injunction would have "a disproportionate effect on any person's legitimate interests", and "the importance of freedom of expression."[49] The evidentiary standards of Section 12 of the Human Rights Act would also apply.

39. *Turkey*. A 2007 statute authorizes courts and an administrative agency to issue blocking injunctions whenever there is "sufficient ground for suspicion" that online content may violate one of eight specific criminal offences, including insulting the memory of Mustafa Kemal Ataturk, the founder of the Turkish republic.[50] There are no further restrictions or qualifications of blocking measures, including any requirement that such measures should be proportionate or not unduly interfere with freedom of expression. "Sufficient ground for suspicion" is not defined. At the same time, Law 5651 does not explicitly authorize collateral blocking. In addition to Law 5651, Turkish courts increasingly invoke general criminal and civil laws to grant blocking injunctions in defamation, privacy, copyright and other cases, even though these laws make no express provision for blocking of Internet content.

40. In practice, courts and the designated administrative agency have issued thousands of blocking orders. There have been several cases, in addition to the current one, in which web domains or platforms with significant numbers of Turkish users (including YouTube, Geocities, DailyMotion, and Google services) have been blocked for entire months and years, causing considerable collateral censorship.[51] It appears that often the primary aim of these measures is to retaliate against foreign providers that refuse to take down content that is found objectionable by the Turkish authorities.[52] In some cases, content unrelated to Ataturk or any of the other offences listed in Law 5651 – such as videos ridiculing a former general, displays of a burning Turkish flag, or gay discussion forums – have led to extensive blocking of foreign-hosted content and platforms. In any event, it is highly questionable, in view of this Court's recent case law, whether it is permissible under Article 10 to criminally sanction criticism, or even ridiculing, of a former head of state (be it a founding father) who has been dead for more than 70 years.[53]

* * *

41. The lack of any instances of collateral blocking of large proportions, such as of entire web platforms, in European practice—let alone judicial practice—testifies to their truly exceptional nature. In addition, the fact that practically all blocking methods currently available are susceptible to circumvention by average users is relevant as to whether they can be considered "strictly necessary".

C. Remedies and Procedural Safeguards

42. Domestic laws should provide robust and prompt remedies against blocking orders in order to safeguard against unnecessary and disproportionate interferences with Article 10.

---

[49] See DEA, sec. 17 §§ 3-5.

[50] Law No. 5651 on the Regulation of Internet Publications and Suppression of Crimes Committed by Means of Such Publication (May 2007), art. 8. A 1951 statute makes it a crime to "defame or insult Ataturk's memory." See Law No. 5816 on Crimes Committed against Atatürk.

[51] Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship, January 2010, at http://www.osce.org/fom/41091.

[52] In one such case, YouTube agreed to take down globally six third-party video clips, and make unavailable to Turkish users another four clips, that a Turkish court had found to violate Law 5651. However, the Turkish authorities still refused to lift their complete ban on YouTube, insisting that YouTube should also take offline the remaining four videos so that no one in the world would be able to access them.

[53] See, in particular, *Otegi Mondragon v. Spain*, Judgment of 15 March 2011 (reigning monarch not immune, in his institutional capacity, from harsh political criticism); and *Editions Plon v. France*, Judgment of 18 May 2004 (maintaining injunction against a book more than nine months after a president's death was unjustified, despite a breach of doctor-patient confidentiality).

Council of Europe and European Union principles

43. It has been argued that court injunctions and administrative orders blocking access to Internet content constitute interferences with Article 10 rights amounting, in principle, to prior restraint. The right not to be subjected to arbitrary prior restraint – given the potentially irreparable damage caused by such measures – implies certain basic procedural protections, such as the right to prompt judicial review of the interim measures themselves.[54] More generally, Article 13 of the Convention guarantees the right to an effective domestic remedy to everyone with an "arguable claim" of a violation of Article 10.

44. The fair trial provisions of Article 6 may also apply to prior restraint proceedings. In the recent case of *RTBF v. Belgium*, this Court held that "there is now widespread consensus within the member States of the Council of Europe on the applicability of Article 6 safeguards to interim measures, including injunctions."[55] Noting that injunctions often remain in place for considerable periods of time, the Court was "not satisfied that the deficiencies of an interim procedure could be corrected within the main proceedings, given that any injury suffered in the interim could become irreversible."[56] Those safeguards include the applicants' right to be notified of any injunction proceedings, which must be conducted in adversarial fashion by an independent tribunal.[57] Such rights apply to "everyone" who is a party to the proceedings as defined in Article 6 § 1, including persons located or residing abroad and any affected third parties.[58]

45. In his *Scarlet* opinion, the Advocate General of the CJEU noted that the blocking system under consideration by the Belgian court would go into effect "without there being an explicit opportunity for those affected, i.e. Internet users, to oppose the blocking of a specific [copyright-infringing] file or to contest its merits." This contributed to the AG's finding that the system was not "prescribed by law."[59]

Comparative National Standards

46. *France*. The injunction procedures described above provide for pre-blocking notification of ISPs and content providers, and for expedited and adversarial judicial proceedings to determine whether blocking is warranted, except in the case of child pornography where judicial review is available after the fact. The French Constitutional Council held that copyright-related blocking injunctions would only be constitutional if granted pursuant to "a full hearing of all parties".[60]

47. *Germany*. Given the lack of an explicit statutory basis for blocking, the general fair hearing rules apply, including the duty of notification and rights of appeal. The online gambling bill, which would introduce a limited administrative blocking system, provides for prior notification and a right of recourse. Simple Internet users should, in principle, have standing to challenge blocking of foreign-hosted content that affects their constitutional rights but there have been no court rulings to date.

48. *United Kingdom*. Under the voluntary blocking scheme for child pornography, the IWF notifies ISPs, which must then act expeditiously to remove the content. Notification of the content providers and primary publishers is regulated by each ISP. Injunctions to prevent copyright infringement under the Digital Economy Act 2010 must satisfy extensive notification requirements and other procedural safeguards.

49. *Turkey*. There is no clear duty to notify the primary content providers or other affected sites, and they are almost never notified in practice. Injunctions are routinely issued on an *ex parte* basis, such that it

[54] Para. 10 above. See also *The Sunday Times v. UK (No. 2)* (1991), para. 51 ("news is a perishable commodity and to delay its publication, even for a short period, may well deprive it of all its value and interest").
[55] Para. 64 (our translation from the French original). See also *Micallef v. Malta*, Judgment of 15 October 2009.
[56] *Ibid*.
[57] See e.g. *Munes Dias v. Portugal*, Decision of 10 April 2003 (Admissibility); and *Tishkevich v. Russia*, Judgment of 4 December 2008 (finding that the right of notification is "fundamental").
[58] This applies even to third parties whose civil rights have been affected by administrative or executive action. See *Zander v. Sweden*, Judgment of 25 November 1993 (decision by public authorities to grant a waste-dumping license affected the applicants' right to use water from their wells for drinking).
[59] Para. 106.
[60] Note 20 above, para. 38. See also Constitutional Council Decision No. 2011-625 DC (holding that administrative blocking of child pornography was constitutional, given the availability of prompt judicial review and the compelling need to block access to such harmful content in speedy fashion).

is sometimes hard even to identify the court that issued the injunction. Injunctions tend to remain in place for a long time, due in part to the fact that affected sites are not properly notified, especially foreign sites, and there is hardly any effort to actually prosecute those posting illegal content.

Standing to challenge blocking orders

50. From a practical perspective, blocking injunctions such as those ordered in the current case affect the Article 10 rights of at least four categories of persons: (i) the author or primary publisher of the allegedly unlawful content, who may have also posted lawful content on the same web location; (ii) the foreign-based service provider (such as Google Sites) that hosts the allegedly unlawful third-party content and may suffer a complete blocking of access to its services in the relevant country;[61] (iii) other content providers, both within and outside the country, who have no connection to the unlawful content but may suffer "collateral blocking" of content they have posted on the same site or platform (such as the current applicant); and finally (iv) other Internet users within the country of jurisdiction who are prevented from accessing any of the blocked content.

51. It should be uncontroversial that, as immediate victims, persons in the first and second categories are entitled to the full protection of Article 6, coupled with the procedural safeguards against prior restraint inherent in Article 10. By the same token, persons in the third category should be, at the very least, entitled to challenge any blocking injunctions issued in proceedings to which they were not originally parties but which directly affect their right to impart information and ideas. The domestic courts in the current case granted the applicant standing in that respect.

52. It is submitted that persons in the fourth category ("simple users") are also adversely affected in the exercise of their right to receive, and potentially re-publish, the information and ideas to which access is blocked, and should be similarly entitled to challenge blocking injunctions.[62] Such a position is consistent with the plain language of Articles 10 and 13 of the Convention—granting "everyone" the right to receive information and ideas, and to an effective remedy for its protection—as well as the Court's evolving jurisprudence. Thus, in *Mustafa and Tarzibachi v. Sweden*, the Court upheld the Article 10 right of an immigrant family to install and use, against the objections of their landlord, a satellite TV dish that allowed them to receive information and maintain cultural links with their country of origin.[63]

53. The case for granting standing to simple users is particularly compelling when blocking orders affect a significant amount of online material that is authored by multiple users or hosted outside the country where the blocking order was made. It is not reasonable in such circumstances to expect the primary publishers of potentially unlawful content, or even major hosting services such as Google Sites, to fight every case in the courts, and under the laws, of some 200 jurisdictions. Users in the country of jurisdiction would thus be left to the mercy of overly diffuse interests and practical obstacles for foreign litigants, which can also be abused by national authorities, as appears to be the case in Turkey (see above). The real harm in today's Internet world is suffered by those being blocked out of the global conversation, whether as speakers or "mere" listeners, and they should have a right to ask to be let back into the agora. This is not an argument for *actio popularis*; it is the nature of the Internet, and of national blocking orders, that grants every user a legitimate action. The alternative would be a legal regime for the Internet which is fragmented by the potentially arbitrary claims of dozens of national jurisdictions.

6th July 2011

James A. Goldston
Darian Pavli
Open Society Justice Initiative

[61] The foreign host may or may not be criminally liable itself. Turkish Law 5651, like the E-Commerce Directive, appears to grant intermediaries immunity from criminal prosecution, at least until they are notified of the fact that they are hosting third-party criminal content and refuse to take it down.
[62] The position of the Turkish courts is that such persons have no standing to challenge blocking orders. See, for example, *Akdeniz v. Turkey*, App. No. 20877/10, which is being considered jointly with the current case.
[63] See note 17 above.