Georgetown Journal of International Law
Summer, 2011

2011 Symposium on International Cyberlaw

Article

***1123** HOW (NOT) TO CENSOR: PROCEDURAL FIRST AMENDMENT VALUES AND INTERNET CENSORSHIP WORLDWIDE

Dawn C. Nunziato [FNa1]

Imagine if an, unknown person entered your home on a regular basis and removed books from your bookshelves. You would never be told which books were being taken away, and you would never be given a reason except that someone, somewhere, somehow, deemed them "extremist," "indecent," or simply "insulting," or felt that they might "incite" some form of hatred .... Couldn't happen in a democracy? Guess again. Under the guise of protecting citizens from "smut" and "offensiveness," Internet filtering programs routinely block access to thousands of World Wide Web search results, home pages, chat rooms, news groups, and other Internet options--in democratic countries as well as in authoritarian states .... No one can rely on the Internet anymore as a self-healing mechanism that can defeat censorship or blocking on its own. [FN1]

TABLE OF CONTENTS

***1124** I. INTRODUCTION

A growing number of countries censor speech on the Internet-- dictatorships and democracies alike. [FN2] Free speech advocates deplore this state of affairs and argue for achievement of a worldwide consensus in which all countries accord their

citizens nearly unrestricted Internet access. This Utopia of uncensored Internet access is, however, radically different from the current state of affairs and--given the trend toward more, not less, control over Internet access--is not likely to be achieved in the near future. Calls for the rest of the world to adopt the United States' First Amendment's version of broad free speech protections (like that recently made by Secretary of State Hillary Clinton) [FN3] are not likely to be heeded, especially since the United States is far from the mainstream of speech protections among democracies. [FN4] Furthermore, given the extent and technical success of efforts to censor Internet speech throughout the world, free speech Utopians can no longer rest ***1125** comfortably on the assurance issued by Internet pioneer John Gilmore two decades ago that "the Net interprets censorship as damage and routes around it." [FN5] Given that countries in recent years have successfully reined in the Internet and reimposed geographical controls and, with them, the prerogatives of the sovereign upon the formerly untamed, unregulable, and ageographic nature of the Internet, free speech Utopians can no longer rest assured that the "nature of the Internet" itself will combat and resist issues of censorship. For those of us committed to maximizing the potential for a free and open Internet, a different approach is therefore warranted.

Instead of arguing that the world should adopt the First Amendment's exceptionally broad substantive free speech protections or that an international consensus regarding free speech protections should be reached, in this Article I focus on the particular *procedures* by which countries censor and argue for the adoption of concrete and specific steps by which these countries should improve their implementation of Internet filtering systems [FN6] to better achieve their own substantive goals, as well as to achieve more speech-friendly results. While it is to be expected that different countries will adopt different substantive values regarding which Internet speech to restrict (for example, how to define and whether to restrict hate speech, Holocaust denial, pornography, etc.), [FN7] in restricting such categories of speech, I argue that countries should adhere to important procedural values and stringent procedural constraints (such as those embodied in First Amendment jurisprudence and the Due Process Clause). This strategy for enhancing free speech protections in nations throughout the world has the benefit of likely being palatable to other countries, because it does not require that they forego the prerogative of the sovereign to adopt and implement their own substantive free speech values. Rather, the approach I suggest assumes as its starting point the substantive free speech values adopted by each country, but recommends the adoption of meaningful procedures to safeguard whatever free speech values each country has adopted for its citizens.

***1126** In short, while I do not contend that countries the world over should implement *substantive* First Amendment values, I argue that other countries can and should implement *procedural* First Amendment and Due Process values. Adoption of such procedural First Amendment values would require sharply constraining the "prior restraints" on speech that are embodied in nationwide filtering systems, and implementing meaningful procedural safeguards on any prior restraints imposed, including operating filtering systems in an open and transparent manner that accords affected Internet users notice and an opportunity to respond to--and appeal--speech-restrictive actions.

II. OVERVIEW OF GLOBAL INTERNET CENSORSHIP

It is an unfortunate truth that today, many countries censor Internet content-- dictatorships and democracies alike--and the number of countries doing so is growing every year. This set of censorial regimes includes the obvious-- repressive regimes like China, North Korea, and others on Reporters Without Borders 10 worst enemies of press freedom list [FN8]--but also those countries we might least expect, including liberal democracies like the U.K., other western democracies, Asian democracies like South Korea, as well as Canada and Australia. According to the Open Net Initiative, more than three dozen states around the world now impose state-mandated technical filtering of speech on the Internet. [FN9]

Western European democracies, which we might expect to have liberal Internet free speech regimes, in fact have imposed a variety of types of restrictions on Internet speech and restrict categories of speech that are protected elsewhere in the world. Under the Council of Europe's cybercrime treaty, [FN10] hate speech is prohibited, as is Holocaust denial. Because such content is illegal, ISPs in countries adopting the treaty must take down such content if it is hosted domestically or block such content if it is hosted overseas. The United Kingdom has led the way in restricting access content deemed harmful, through the Project Cleanfeed program implemented not by the state per se but by a ***1127** nominally private entity, British Telecom, which I discuss in greater detail below. Norway, Sweden, Denmark, Italy, Germany, and Finland have followed the U.K's lead and have restricted Internet access to categories of speech that they deem harmful. Other countries have imple-

mented Internet filers to restrict certain categories of political speech or speech that is critical of their governments. Switzerland has blocked political sites that are critical of the Swiss government, while Turkey has required its ISPs to block websites, including YouTube, that host content insulting to Turkey's founder Mustafa Kemal Ataturk or to "Turkishness" generally. [FN11] South Korea, while shedding decades of authoritarian rule and adopting a democratic constitution in 1987, nonetheless actively imposes restrictions on political speech on the Internet, mandating that its ISPs block websites that contain pro-North Korea content or that promote the reunification of North and South Korea. South Korea also severely restricts political and election-related speech and has blocked access to or removed hundreds of thousands of election-related websites. [FN12]

Following the lead of the U.K. and Canada, Australia is poised to initiate one of the most restrictive regimes for Internet speech to date among democratic countries and plans to implement a nationwide mandatory Internet filtering system. The Australian Federal Government has announced that it will introduce "mandatory ISP-level filtering" of certain content deemed unprotected under its content classification scheme. Under this mandatory system, Australian ISPs will be required to block websites that contain harmful content proscribed by the state, including content that broadly deals with "matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults." [FN13]

In short, pervasive Internet censorship has extended well beyond the usual suspects--China, Saudi Arabia, North Korea, etc.--to established liberal democracies like the U.K., Canada, and Australia. Furthermore, many of these countries implement their nationwide filtering regimes ***1128** in a manner that is not open or transparent and that does not provide their citizens with notice or the opportunity to respond or to appeal adverse speech determinations. [FN14] Below I discuss certain First Amendment procedural values and constitutional values generally that I contend should be adopted by countries in implementing such Internet filtering regimes, even while they maintain their own substantive values regarding which categories of speech to protect and which to prohibit.

III. FIRST AMENDMENT PROCEDURAL VALUES

It is generally recognized that--aside from a few recent exceptions like its treatment of WikiLeaks websites [FN15]--the United States has adopted and implemented protections for free speech that are among the strongest of any country worldwide. [FN16] What is less well understood is that such protections not only have a substantive dimension-- defined in terms of the categories of speech that merit protection--like hate speech, group libel, virtual child pornography, and (non-obscene) pornography generally--but also procedural dimensions, which mandate the procedures and "sensitive tools" required for distinguishing categories of unprotected speech from protected speech and set forth procedures regarding how restrictions on unprotected speech should be implemented and scrutinized. First and foremost, the First Amendment's prior restraint doctrine greatly disfavors the imposition of prior restraints on, as compared to subsequent punishment of, harmful speech, and imposes strict procedural safeguards on any such prior restraints. These procedural safeguards impose meaningful constraints on the discretion of the censor in the first place and provide meaningful opportunities for affected individuals to rapidly appeal the censor's decision. Translated into the context of nationwide filtering or blocking of Internet speech, these safeguards would require, first, that any filtering be imposed subject to *clear and precise definitions of the speech to be regulated*; second, that the filtering scheme *operate in a transparent manner*, such that affected Internet users and content providers are ***1129** provided with information that the content was blocked and the reason for such blocking; and third, that the filtering scheme provide Internet users and content providers with the *opportunity to appeal any such blocking decisions*, to a *judicial body and in an expeditious manner*. [FN17]

Further, the First Amendment--like United States constitutional law generally--embodies the state action doctrine to determine what actions are properly chargeable to the state. The purpose of the state action doctrine is to flush out and prohibit attempts by the state to delegate its constitutional responsibilities to private entities in an effort to insulate such actions from judicial scrutiny or public oversight generally. In the First Amendment context, attempts by the state to transfer censorship functions to private entities acting at the behest of the state or in concert with the state will not insulate those actions from judicial scrutiny. Under the state action doctrine, courts in the United States will look past the nominally private form through which such speech restrictions are implemented and will attribute those actions to the state and subject them to appropriate

scrutiny.

Finally, under U.S. law--and under principles of international law generally-- courts have been careful to limit the "extra-territorial" reach of speech restrictions so as to protect the autonomy of each sovereign to effectuate its own prerogatives regarding what constitutes harmful speech, while not infringing on the prerogatives of other sovereigns to do the same. [FN18]

The procedures and values outlined above do not dictate what speech is to be restricted or what categories of speech are to be deemed harmful, and as such, are likely to be more acceptable to other countries. Rather, they impose meaningful, process-based safeguards on the implementation of restrictions of whatever categories of speech are deemed harmful by any particular government. These procedural values seek to minimize the impact on protected speech, however that category may be substantively defined. While it will likely be exceedingly difficult to convince the rest of the world to adopt the United States' substantive First Amendment principles regarding which categories of speech to protect, other countries may well be more receptive to calls to improve the functioning of their filtering regimes, while according deference to their determinations of which categories of speech to restrict on the Internet.

***1130** IV. INTERNATIONAL PROTECTIONS FOR FREEDOM OF EXPRESSION--IN REAL SPACE AND CYBERSPACE

To many Americans, the speech restrictions imposed by other countries--in general and with respect to Internet content in particular--appear to constitute a violation of fundamental human rights. Many free speech theorists maintain that access to information on the Internet should be unrestricted and that those of us who are committed to free speech should work to oppose the restrictions imposed by other regimes on Internet speech. Secretary of State Clinton recently expressed precisely these views in her speech in February at George Washington University, entitled "Internet Rights and Wrongs: Choices and Challenges in a Networked World." Secretary Clinton called for governments the world over to accept the First Amendment's fundamental premise of the uninhibited, robust, and wide-open marketplace of ideas in which freedom of expression on the Internet is guaranteed. While I believe that the world would be a better place if every nation adopted a version of our First Amendment, it is important to recognize that principles of international law allow each nation to determine, within broad limits, what types of speech are harmful and subject to restrictions for its citizens, in real space and in cyberspace. Although free speech is granted some protection by international treaties, this protection is subject to a host of limitations and exceptions [FN19]--far more than under the First Amendment [FN20]--and in any case, violations of such treaty obligations would not justify acts of intervention by the United States. Below I survey the international law protections for freedom of speech and the principles of self-determination and territorial sovereignty that apply to the protection of free speech, and conclude that such protections generally provide sufficient flexibility to accommodate the range of speech restrictions implemented by countries throughout the world, online and offline. As such, claims that another country is violating international free speech protections by imposing filters on speech deemed harmful within that country are likely to fall on deaf ears.

Several important treaties and documents of international law extend protection to freedom of expression as an international human right. These protections, however, allow for certain exceptions and limitations on this freedom that are arguably sufficient to accommodate a host of restrictions on this freedom. First and foremost, ***1131** Article 19 of the Universal Declaration of Human Rights (UDHR), adopted by the U.N. General Assembly in 1948, provides:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. [FN21]

Article 29 of the Declaration, however, makes clear that this right is not absolute, and that countries may place restrictions on this right "solely for the purpose of securing ... respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society." [FN22]

Although the Declaration is technically considered non-binding, many commentators consider it to be part of customary

international law, and therefore binding through general acceptance and state practice. As the Secretary General expressed the U.N.'s aspirations regarding the document, "[The Universal Declaration] is, as its title implies, truly universal in its application and applies to every member of the human family, everywhere, regardless of whether or not his Government accepts its principles or ratifies the Covenants ...." [FN23] The International Court of Justice has also implied that the Universal Declaration of Human Rights sets forth general principles of international law. [FN24]

The Human Rights Commission later adopted a binding covenant that would serve in addition to the UDHR and which would include a limited mechanism for hearing complaints from individuals whose rights were violated. The result was the International Covenant on Civil and Political Rights (ICCPR), [FN25] which has been adopted by 167 parties, ***1132** and which is considered a binding international law treaty. The ICCPR provides in Article 19 that:

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. [FN26]

However, like the right provided in the UDHR, the ICCPR rights are specifically made subject to the limitations set forth in Articles 19 and 20. Article 19 provides that:

> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. *It may therefore be subject to certain restrictions*, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
> (b) For the protection of national security' or of public order (ordre public), or of public health or morals. [FN27]

The ICCPR provides further, in Article 20, that any propaganda for war or advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, or violence, is prohibited by law. [FN28]

Further support for freedom of expression comes from the European Convention for the Protection of Human Rights, which has been signed by 47 nations, is considered binding, and is enforced by the European Court of Human Rights (ECHR). This Convention, however, like the Universal Declaration and the ICCPR, allows signatories to carve out exceptions and limitations to the protections granted to speech. Generally considered to be part of the national laws of the Member States of the Council of Europe, the European Convention provides in Article 10:

> ***1133** Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers ....
>
> The exercise of these freedoms, since it carries with it duties and responsibilities, *may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary*. [FN29]

In addition to these documents, there are a number of other regional agreements protecting freedom of expression. Article 11 of the Treaty of Lisbon, in force in all 27 European Union countries, provides:

> Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to re-

ceive and impart information and ideas without interference by public authority and regardless of frontiers ...

and that

The freedom and pluralism of the media shall be respected. [FN30]

In addition, within the Inter-American system, there are two human rights documents. The first is the American Declaration of the Rights and Duties of Man, which is nonbinding, but to which the United States is a party. Article 4 of this document provides:

> ***1134** Every person has the right to freedom of investigation, of opinion, and of the expression and dissemination of ideas, by any medium whatsoever. [FN31]

The second document that references the Universal Declaration of Human Rights is the American Convention on Human Rights, which is binding on its signatories and is subject to enforcement by both the Inter-American Commission and Inter-American Court of Human Rights. Article 13 of this document provides:

> Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice.
>
> 1. The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure:
>
> a. respect for the rights or reputations of others; or
> b. the protection of national security, public order, or public health or morals.
>
> 2. The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.
>
> 3. Notwithstanding the provisions of paragraph 2 above, public entertainments may be subject by law to prior censorship for the sole purpose of regulating access to them for the moral protection of childhood and adolescence.
>
> 4. Any propaganda for war and any advocacy of national, racial, or religious hatred that constitute incitements to lawless violence or to any other similar action against any person or group of persons on any grounds including those of race, color, ***1135** religion, language, or national origin shall be considered as offenses punishable by law. [FN32]

Although freedom of speech is protected by these international treaties, the treaties themselves limit the breadth of this protection and allow for countries to carve out exceptions to this protection, where necessary for "public order," "public morals," "territorial integrity," or other broadly worded exceptions. Furthermore, under the currently prevailing understanding of international law, the protection of free speech is an internal matter, one over which the state has exclusive control, and which is subject to the norm of non-interference in internal affairs. [FN33] As one commentator explains, "under the current understanding of the international law of free speech ..., the old fundamental tenet of the law of nations, state sovereignty, remains alive: the state has exclusive control over its territory and people." [FN34] Although some free speech advocates have argued that political intervention is warranted in cases where countries have violated their citizens' free speech rights, [FN35] there seems to be little political support for such intervention. [FN36] The U.N. General Assembly supports intervention only in cases of genocide. Given the international law norm of noninterference in internal matters of protection of freedom of speech, and given the extremist nature of the First Amendment's substantive values, it is unlikely that the United States' substantive

free speech values will come to be adopted by other countries of the world, at least in the near future. For those of us committed to maximizing free speech throughout the world, it is more likely that we can convince other countries to adopt and implement the First Amendment's procedural values, to enable them to more narrowly and precisely tailor their speech restrictions to target the speech harms they have identified, and ***1136** to accord their citizens meaningful procedural rights within whatever substantive free speech regime has been adopted within that country.

V. FIRST AMENDMENT PROCEDURAL VALUES, CONSTITUTIONAL VALUES, AND GLOBAL INTERNET CENSORSHIP

The free speech issues raised by Internet censorship worldwide are enormously complex and varied. Because United States substantive free speech protections differ in many ways from free speech protections provided in other countries, it is not likely that other countries will soon adopt our substantive free speech norms as their own. However, several non-substantive First Amendment values and constitutional doctrines generally may be instructive and persuasive to other countries. First, the state action doctrine is a doctrine of constitutional law applicable to the First Amendment's guarantees, which provides that the state cannot evade its responsibilities for protecting its citizens' rights by delegating these responsibilities to private entities. Second, under First Amendment jurisprudence, the prior restraint doctrine imposes meaningful procedural constraints on any restrictions of speech implemented prior to a judicial determination of the speech's illegality. Third, principles of constitutional law--and indeed of international law--impose limits on the extraterritorial reach of each sovereign's implementation of its own laws--and, for our purposes, on the extraterritorial reach of each nation's restrictions on Internet speech. Below I identify some representative problems presented by Internet censorship around the world and suggest how procedural First Amendment and constitutional values would apply to these issues.

A. *"Private" ISP Filtering and the State Action Doctrine*

Several countries around the world--including the U.K. and Canada--have developed systems to filter content suspected of being illegal under their free speech regimes. Yet, instead of imposing this filtering system directly as a government mandate (with whatever checks attend to such governmental action), they have implemented these mandates in such a way as to require their country's ISPs to "voluntarily" or "privately" impose these filters. In so doing, these countries presumably have attempted to evade their responsibilities for ensuring the protection of their citizens' free speech rights, by delegating censorship responsibilities to private actors.

The United Kingdom, for example, in 2004 adopted and implemented through its ISPs one of the most comprehensive systems of Internet filtering to date--the Cleanfeed system, initially implemented ***1137** by the U.K's largest ISP, British Telecom. This filtering system, which has been described as "the first mass censorship of the web attempted in a Western democracy," [FN37] is a mandatory online content filtering system implemented in the U.K. Although Cleanfeed began as an effort to block access to child pornography-related content, as discussed in the next section, its mission and mandate has now expanded to encompass the monitoring and blocking of sites connected with racism, the incitement of hatred, and obscene adult content. [FN38] The Cleanfeed filtering system operates by blocking U.K. citizens' access to websites placed on a blacklist by the Internet Watch Foundation (IWF). The IWF is a private organization run by former police officers established in 1996 by the U.K. Internet industry to enable members of the public to report potentially criminal online content. Once a member of the public provides a report of suggested illegal content to the IWF, the IWF assesses these reports "according to UK law," as "reinforced by reciprocal police training." [FN39] Once an ISP is informed by the IWF that it is hosting potentially illegal online content, the ISP is required to expeditiously remove or disable access to the content.

The Cleanfeed system as implemented by U.K. ISPs is problematic from a free speech perspective for a variety of reasons that I discuss below. But first and foremost, this system is problematic because it is conceptualized as a private, voluntary implementation of a filtering system that is essentially outside the law--not one implemented by the government, and therefore not one that is publicly accountable. Even though the U.K. government "asked" all ISPs operating in the U.K. to implement the Cleanfeed system and comply with the IWF blacklist--and over 95% of ISPs have indeed complied--and even though the government has threatened to officially *mandate* compliance if full ***1138** compliance by ISPs is not achieved, [FN40] the U.K. government maintains that Cleanfeed is a voluntary, privately-implemented system that does not involve

government action and is of a voluntary nature. [FN41] This position is untenable, as I discuss below. But because such an implementation enables the state to evade public and judicial scrutiny for its speech-restrictive actions, it is an attractive model for other governments and one that has turned into a model for several other countries.

In 2006, Canada's largest ISPs launched Project Cleanfeed Canada, modeled after the U.K. Cleanfeed project, in conjunction with Cybertip.ca, Canada's child sexual exploitation upline. As in the U.K., analysts from Cybertip.ca make determinations as to which content is potentially illegal and place suspected URLs on the Cleanfeed distribution list. Canadian ISPs participate in this system and block URLs that have been placed on the Cleanfeed distribution list. As in the U.K., Canadian ISPs' participation is termed "voluntarily" and therefore not directly attributable to the state. [FN42]

Finland also appears to be following a similar model, although with greater direct involvement from the state. Finnish law authorizes its National Bureau of Investigation (NBI) to maintain a secret blacklist of websites that are suspected of hosting child pornographic images. In discussing this model, the Finnish Ministry of Transport and Communication stated that if the Finnish ISPs did not submit to this "voluntary" system of censorship, the government would make the censorship mandatory. [FN43]

Because, as a technical matter, the government in such cases is not technically mandating such speech restrictions and because such restrictions are "voluntarily" undertaken by private ISPs at the behest of the government in cooperation with "private" organizations like the IWF, these speech restrictive actions are technically outside the scope of applicable national laws protecting citizens' free speech rights, like the U.K's Human Rights Act. [FN44] As Professor Lilian Edwards explains in her ***1139** article "From Child Porn to China, in One Cleanfeed" [FN45] regarding the U.K. Cleanfeed system of nationwide censorship:

> [T]his censorship needs no laws to be passed, no court to rule, with the publicity that entails. It only needs the collaboration, forced or otherwise, of ISPs. ISPs are not public bodies; their acts are not subject to judicial review.

Because this type of private self-regulation technically occurs outside the reach of the law, it is increasingly attractive to governments worldwide, and likely to industry as well. However, it is insufficiently protective of free speech because it allows the government to evade its responsibility to protect and uphold its citizens' free speech rights.

In circumstances in which the state seeks to delegate such responsibilities to private actors, the state action doctrine--which is an important principle of both international law and United States constitutional law--should be invoked for the principle that censorship under such pervasive nominally private systems at the behest of the national government is properly chargeable to the state. The state action doctrine has been established by various international instruments, including a 2001 United Nations General Assembly Resolution, which provides that:

> The conduct of a person or group of persons shall be considered an act of State under international law if the person or group of persons is in fact exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority. [FN46]

The state action doctrine under international law has been interpreted in ways similar to that of the United States' domestic state action ***1140** doctrine, under which actions taken by nominally private actors, when performing functions that have traditionally or exclusively been performed by the state, are subject to the mandates of the Constitution, including the First Amendment. Under United States constitutional law the state action doctrine, first recognized in the First Amendment context in *Marsh v. Alabama*, [FN47] provides that when nominally private actors perform functions that have traditionally or exclusively been performed by the state, their actions are subject to the mandates of the Constitution, including the First Amendment. The state action doctrine rejects the proposition that powerful private entities are immune from constitutional scrutiny because of their nominally private status. Under the state action doctrine, U.S. courts will generally place constitutional obligations upon actors other than the government in the following circumstances: (1) where the actor is a government corporation; (2) where the actor performs "public functions" or functions that have been traditionally or exclusively performed by the government; or (3) *where the state has authorized, facilitated, encouraged, or otherwise become entangled or*

entwined with private unconstitutional conduct. [FN48] In these circumstances, courts refuse to allow the state to evade its constitutional obligations to protect freedom of expression (or other constitutional rights) by delegating such public functions to private entities or by encouraging such private entities to engage in acts that would violate citizens' constitutional rights. As the Court explained in *Lebron v. National Railroad Passenger Corp.*, [FN49] "[i]t surely cannot be that the government is able to evade the most solemn obligations imposed in the Constitution" by delegating such functions to a "private" entity. [FN50] The state action doctrine is thus designed to "flush out a state's attempt to evade its responsibilities by delegating them to private entities." [FN51]

The foundational state action decision in the First Amendment context is the 1946 case of *Marsh v. Alabama*, [FN52] in which the Supreme Court began to re-examine formalistic distinctions between public and private regulations of speech and scrutinized the restrictions on expression imposed by an entity wielding extensive power over individuals' ***1141** expression. In *Marsh*, the Supreme Court treated a private entity that essentially owned and ran a town and exercised the power to regulate the free flow of information within the town as the equivalent of the state for First Amendment purposes. The *Marsh* Court refused to allow the private status of the owner of the town--Gulf Shipbuilding--to insulate its speech restrictions from First Amendment scrutiny. Instead, it adopted an affirmative conception of the First Amendment [FN53] to ensure that the "channels of communication remain free" and available so as to enable individuals to become informed and to "act as good citizens" within our system of democratic self-government, even against restrictions of speech imposed by "private" actors.

The Court also recognized that the state was indirectly involved and implicated in empowering the private entity to restrict expression. The state had empowered Gulf Shipbuilding to exercise broad control over individuals' expression, and in so doing, became substantially involved and intertwined with the exercise of power that the private actor enjoyed. As the Supreme Court characterized the situation, this was an instance in which "the State [was] permitting a corporation to govern a community of citizens so as to restrict their fundamental liberties." [FN54] The Court recognized that a system in which the State conferred upon a powerful private entity the power to restrict expression was tantamount to one in which the State itself was restricting such expression.

The Supreme Court has further invoked the state action doctrine and imposed constitutional obligations in circumstances where the state has authorized, facilitated, or encouraged private entities to engage in conduct that violates citizens' constitutional rights (or that would constitute such a violation if engaged in by the government itself).

Consistent with this interpretation of the state action doctrine, because the governments in the U.K., Canada, Finland, among others, are expressly authorizing their nations' ISPs to filter the Internet access of their citizens and are themselves facilitating such systems, these actions should not be insulated from scrutiny under applicable free speech protections and should be deemed chargeable to the state, with the requisite scrutiny and procedural protections that attend to such government action.

***1142** B. *Procedural Safeguards for Free Speech under the Law of Prior Restraints*

Nationwide mandatory filtering systems--whether imposed by ISPs "voluntarily," as in the U.K., or mandated by the government, as in restrictive regimes like China or less restrictive regimes like those contemplated in Australia--impose "prior restraints" or restraints on speech prior to a judicial determination of the speech's illegality. Instead of imposing punishment on such speech after it has been published and adjudicated illegal by a court, these systems regulate the speech at issue before a court has made the determination that such speech is illegal. In the United States, such prior restraints on speech are presumptively unconstitutional and are subject to exacting constitutional scrutiny. [FN55] In order to be upheld, several procedural safeguards and checks must be in place in any such system of prior restraints, including *transparency* and *appealability* of the initial decision to restrict the speech; [FN56] *limits on the substantive discretion of the (nonjudicial) decisionmaker* charged with the determination whether to restrict the speech in the first place; [FN57] and *prompt judicial review in an adversary proceeding* before any final decision to censor is implemented. [FN58]

As a threshold matter, to be constitutional, any system of prior restraint requires transparency and openness in its operation, so that those affected by the censorship decision are provided with meaningful notice of the decision to censor and a meaningful opportunity to challenge that decision. Because prompt judicial review is essential to any constitutional prior re-

straint, affected users must be given the information necessary to initiate judicial review of the adverse decision. Such information, at a minimum, includes the fact that the content they seek to make available, or seek to access, has been censored. As applied to a filtering system, this transparency mandate would at the very least require that content providers and end users be made aware that such filtering has taken place so that they can have the opportunity to challenge any such filtering decision. To understand what is at stake in such a system, and how lack of transparency and openness implicates the rights of Internet users, consider the operation of a filtering scheme translated to the real space context.

***1143** Imagine a vast real space forum for authors and readers in which millions of authors bring their books to be made available for billions of potentially interested readers. The authors place their books on the bookshelves of the forum and then depart. Billions of readers also come to the forum to search for books of potential interest to them. Unbeknownst to either the authors or the readers, before the content of any book is made available to the readers--or at some point after the distribution of the books' contents-- the books are scrutinized by unseen and unknown censors to determine whether the content is "permissible," according to some criteria that are unstated and undiscoverable. If these censors determine that a book or some of its content is impermissible, it is placed on a blacklist and removed from circulation. When the readers enter the forum to select books of potential interest to them, they do not know which books have been placed on the blacklist, nor do the authors of the banned books ever learn whether (and why) their book has been banned. This scenario replicates in real space what occurs in cyberspace under certain filtering schemes when websites are placed on blacklists and the country's Internet users are prohibited from accessing such content.

Before turning to the procedural protections for speech provided by the First Amendment's prior restraint doctrine in the context of such scenarios, it is important to consider two preliminary points. First, regardless of whether the restraint is imposed *ex ante*--prior to any circulation of the content--or whether the restraint is imposed *midstream*--after initial circulation but prior to a judicial determination of the content's illegality--such a system embodies a constitutionally suspect prior restraint under U.S. First Amendment jurisprudence. Second, even if the prior restraint is imposed for the purpose of blocking the most disfavored category of speech that is accorded the least protection--viz., child pornography--the procedural safeguards provided by the First Amendment's prior restraint doctrine are nonetheless necessary.

1. Ex Ante and Midstream "Prior" Restraints

In terms of the real space censoring scenario outlined above, whether the restrictions imposed by the licensing scheme occur ex ante--before any reader has an opportunity to access the books' contents--or whether the restrictions occur at some point after the initial circulation of the books' contents, both types of restrictions would constitute presumptively unconstitutional prior restraints--restraints on circulation imposed *prior to a judicial determination* of the illegality of the content of the speech.

***1144** *Ex ante* prior restraints include those imposed by censorship boards responsible for screening films before they are made available to the public, [FN59] parade permits that require a licensor's decision before a protest or demonstration can occur, [FN60] and filtering schemes that are imposed ex ante, such as filters imposed by government bodies for specific words or phrases deemed harmful. [FN61] *Midstream* prior restraints include those restraints on speech that are imposed after initial circulation but before a judicial determination that the speech is illegal has been made. [FN62] Because midstream prior restraints are imposed absent the procedural safeguards that attend a judicial determination, they are as constitutionally suspect as ex ante prior restraints. Midstream prior restraints include filtering systems that involve evolving blacklists of websites that are maintained in response to tips or complaints from web users. These constitute prior restraints even though the restrictions are imposed after the content has been disseminated [FN63] (and even though the restrictions are imposed via a private, "voluntary" mechanism, as discussed above).

The Supreme Court considered an example of midstream prior restraints in the case of *Bantam Books v. Sullivan*. [FN64] In *Bantam Books*, the Rhode Island Commission to Encourage Morality in Youth was charged with investigating and recommending prosecution of booksellers for the distribution of printed works that were obscene or indecent. The ***1145** Commission reviewed books and magazines after they were already in circulation, and took it upon itself to notify distributors in cases in which a book or magazine had been distributed that the Commission deemed objectionable. The notices sent by the

Commission reminded distributors of the Commission's duty to recommend to the Attorney General prosecution of purveyors of obscenity, stating that the distributor's "[c]ooperative action will eliminate the necessity of our recommending prosecution to the Attorney General's department." [FN65] Upon receipt of such notices, the distributors routinely took action to stop further circulation of the identified works.

In reviewing the constitutionality of the Rhode Island scheme, the Supreme Court held that, even though the restrictions on publication were imposed midstream--after initial circulation and distribution (and even though such restrictions on publication were not mandated by the state), the Commission's actions nonetheless effectuated an unconstitutional prior restraint. The Court explained that "the separation of legitimate from illegitimate speech calls for ... sensitive tools" and reiterated its "insistence that regulations of obscenity scrupulously embody the most rigorous procedural safeguards." [FN66] The Court observed that, under the Rhode Island scheme, "the publisher or distributor is not even entitled to notice and hearing before his publications are listed by the Commission as objectionable" and that there was "no provision whatever for judicial superintendence before notices issue or even for judicial review of the Commission's determinations of objectionableness." Accordingly, the Court concluded that, in the context of this midstream prior restraint, the "procedures of the Commission are radically deficient" [FN67] and unconstitutional.

2. Prior Restraints Imposed to Restrict Child Pornography are Subject to the Most Stringent Procedural Safeguards

Among the most universally deplored and prohibited content--on the Internet and elsewhere--is the category of child pornography. There is nearly universal agreement that the possession, distribution, and/or creation of child pornography or child sexual abuse images is illegal and outside the protection accorded by freedom of expression. Yet, as the Supreme Court has observed, even where the state has excellent motives, "the separation of legitimate from illegitimate speech ***1146** calls for ... sensitive tools" [FN68] and this mandate applies as well to the separation of illegal child pornography from legal speech. Accordingly, in First Amendment jurisprudence, even efforts to advance the laudable goal of reducing child sexual abuse by restricting the dissemination of child pornography must be scrutinized using the same "sensitive tools" as are applicable to other efforts to restrict harmful or illegal speech. Indeed, the government's efforts to filter child pornography on the Internet have been subject to the same heavy presumption of unconstitutionality and the same requirements of procedural safeguards as prior restraints imposed to restrict other categories of unlawful content. In *Center for Democracy and Technology v. Pappert*, for example, the Commonwealth of Pennsylvania sought to combat online child pornography by enacting the Internet Child Pornography Act, which required ISPs serving Pennsylvanians to block access to certain websites allegedly associated with child pornography. [FN69] The Act permitted the Pennsylvania Attorney General or Pennsylvania district attorneys to seek an ex parte court order requiring an ISP to remove or disable access to items accessible through the ISP's service, upon a showing of probable cause that the item constitutes child pornography. The Act did not require an actual, final determination that the material to be removed actually constituted child pornography before it was placed on the blacklist. In consultation with the affected ISPs, the Attorney General's office decided to implement the Act by proceeding without even securing ex parte court orders and instead by providing "Informal Notices of Child Pornography" to ISPs of websites that were reported by an agent or a citizen and that the Office of the Attorney General had identified as suspected child pornography. The Informal Notice directed the ISP to remove or disable Pennsylvania citizens' access to the suspected material within five days of receipt of Notice. [FN70]

The statute was challenged as an unconstitutional prior restraint in violation of the First Amendment. In defense of the statute, the Attorney General explained that only material that its office had probable cause to believe constituted child pornography was requested to be removed. Notwithstanding this safeguard, the court found that the probable cause showing did not save the statute--nor did the fact that the attorney general only issued "Informal Notices" not court ***1147** orders, and that the process was therefore "voluntary" not coercive [FN71]--and that the system contemplated by the Act constituted an unconstitutional prior restraint.

3. Categories of Prohibited Speech Should Be Clearly Defined and Delineated

Another central requirement for any system of prior restraint is that the censor's discretion be meaningfully constrained by clearly defined and precise guidelines. While countries in response to their different historical challenges may reasonably

differ about what constitutes illegal content--hate speech, Holocaust denial, pornography, etc. [FN72]--it is important that the definitions of illegal speech--and especially illegal speech subject to prior restraint--be carefully and precisely defined so as to constrain the initial decision maker's or licensor's discretion. In its First Amendment jurisprudence, the U.S. Supreme Court has strictly scrutinized the discretion of licensors in systems of prior restraint and has rejected as unconstitutional any licensing scheme that reposits unbounded discretion in a licensing authority to determine whether or not speech is protected. For example, in *Shuttlesworth v. Birmingham*, [FN73] the Court evaluated the constitutionality of a parade permitting system that vested the City Commission with the broad discretion to deny parade permits in cases where "in [the Commission's] judgment the public welfare, peace, safety, health, decency, good order, morals or convenience require that [the parade permit] be refused." [FN74] In ruling on a challenge to the statute, the Court held that, because the permitting scheme constituted a prior restraint on expression that conferred "virtually unbridled and absolute power" on the Commission, it failed to comport with the requirement that any law subjecting the exercise of First Amendment freedoms to the prior restraint of a license must embody "narrow, objective, and definite standards to guide the licensing authority." [FN75]

Requiring that the criteria by which the censoring authority makes ***1148** the decision to censor be set forth with precision helps to cabin administrative discretion and also helps to limit "mission creep" within the censoring body. [FN76] Without a precise and detailed specification of the criteria for censorship, the censor can exercise unbridled discretion to restrict speech.

Not surprisingly, countries that filter Internet content the most extensively also have the broadest and vaguest definitions of content subject to censorship. China, for example, imposes mandatory filters on content that falls within any one or more of the following broad categories:

- violating the basic principles as they are confirmed in the Constitution;
- endangering state security, divulging state secrets, subverting the national regime, or jeopardizing the integrity of national unity;
- harming national honor or interests;
- inciting hatred against peoples, racism against peoples, or disrupting the solidarity of peoples;
- disrupting national policies on religion, propagating evil cults and feudal superstitions;
- spreading rumors, disturbing social order, or disrupting social stability;
- spreading obscenity, pornography, gambling, violence, terror, or abetting the commission of a crime;
- insulting or defaming third parties, infringing on legal rights and interests of third parties;
- other content prohibited by law and administrative regulations;
- inciting illegal assemblies, associations, marches, demonstrations, or gatherings that disturb social order; and
- conducting activities in the name of an illegal civil organization. [FN77]

Allowing the government to impose prior restraints on content that "disrupt[s] the solidarity of peoples," [FN78] "jeopardiz[es] the integrity of national unity," [FN79] or "harm[s] national honor or interests" [FN80] is precisely ***1149** the sort of standard-less discretion that fails to impose any meaningful constraints whatsoever on a decision maker.

The United Kingdom's nationwide filtering system suffers from similar flaws. Although the Internet Watch Foundation, which is responsible for adding URLs to the blacklist in the U.K., purports to specify and adhere to detailed criteria for determining whether to add a URL to the blacklist, these criteria are not actually made available to the public. Its website [FN81] provides the following information:

What are the criteria for a URL to be added to the list?

> The URLs are assessed according to UK law, specifically the Protection of Children Act 1978. and in accordance with the UK Sentencing Guidelines Council. All URLs added to the list depict indecent images of children, advertisements for or links to such content. This content is likely to be an offence to download, distribute, or possess in the UK .... The policy by which a decision is made to include a URL on the list can be seen here: http://www.iwf.org.uk/corporate/page.49.626.htm.

However, the policy page referenced above provides a broken link. [FN82] Accordingly, no information is provided about the policy by which a decision is made to include a URL on the IWF blacklist. In other places on its website the IWF indicates that "[a]ll reported URLs are assessed according to UK law, with each image being categorised in line with criteria set out by the UK Sentencing Guidelines Council," with a link indicated for the U.K. Sentencing Guidelines Council. [FN83] However, the link provided at this location is also broken [FN84] and no criteria are indicated. Further, the Internet Watch Foundation seems to be susceptible to the problem of mission creep. Although its initial mission was solely to reduce the availability of images of child sexual abuse, the target of its censorship has now been widened somehow beyond child ***1150** pornography to encompass adult content that is "criminally obscene," as well as hate speech and "incitement to racial hatred content." [FN85]

In order to constrain the discretion of the censor charged with making determinations whether to block Internet content, pursuant to the requirements that the First Amendment imposes on prior restraints, it is important for the decision maker to be guided by clear, precise, definite standards of what constitutes illegal content subject to censorship in the first instance.

4. Openness and Transparency within Filtering Systems

Bantam Books, as well as other cases invalidating systems of prior restraints, teach that in order for any system of prior restraint to be constitutional, the affected parties must at a minimum be made aware of such a decision to censor so that they can effectively challenge it. [FN86] One of the most fundamental requirements imposed on any prior restraint is the requirement that it be subject to judicial review before any final restraint is imposed. This, in turn, presupposes that affected parties have *notice* of any such censorship and a *meaningful opportunity to challenge* the initial decision to censor in a judicial forum. If an affected individual is not made aware that speech is censored, the constitutional requirement that the censorship decision be subject to prompt judicial review will be rendered meaningless.

Filtering systems in which the affected parties are not made aware that content has been filtered fail this threshold requirement. Surprisingly, on this score of openness/transparency versus secrecy/opaqueness in the operation of filtering systems, some of the most repressive and authoritarian countries fare better than liberal democracies. Saudi Arabia, for example, while implementing a very restrictive system of government-mandated Internet filtering consistent with its overall restrictive religious society, nonetheless operates its filtering system in a transparent and open manner, and appears to provide Saudi users with meaningful notice that their Internet access is being ***1151** restricted in general, as well with notice of specific acts of blocking in particular, as I discuss below. [FN87] Although Saudi Arabia's Internet restrictions are hostile to free speech on a number of metrics, [FN88] these restrictions operate in a transparent and open manner, providing citizens with clear notice of what Internet speech is being restricted and why.

In Saudi Arabia, all Internet traffic passes through a few government-controlled waypoints. The state-run Saudi telecommunications company controls all telecommunications services, while the Internet Services Unit (ISU), a department at the King Abdulaziz City for Science and Technology, is responsible for overseeing all Internet services in Saudi Arabia. [FN89] The ISU maintains a centrally-administered filtering system through which it blocks content "of an offensive or harmful nature to the society" and "which violate the tenets of the Islamic religion or societal norms," including "pornographic web pages," as well as pages related to "drugs, bombs, alcohol, gambling and pages insulting the Islamic religion or the Saudi laws and regulations." [FN90] While the restrictions imposed on free speech are substantial, the Saudi government is very clear about the mechanism by which it effectuates this filtering. It explains that "KACST [King Abdulaziz City for Science & Technology] maintains a central log and specialized proxy equipment, which processes all page requests from within the country and compares them to a black list of banned sites. If the requested page is included in the black list then it is dropped." [FN91] Regarding its justifications for filtering, the government explains on its official filtering webpage that:

> ***1152** God Almighty directed humanity in the Noble Qur'an in the words of His prophet Joseph: He said, My Lord, prison is more beloved to me than that to which they entice me, and were you not to divert their plot away from me I will be drawn towards them and be of the ignorant. So his Lord answered him and diverted their plot away from

him, truly, He is the All-Hearer, the All-Knower." Yusuf (12):33-34. [FN92]

In effect, the Saudi government employs a nationwide, transparent filtering scheme, known as SmartFilter, to "divert" its citizens away from content that is deemed sinful and in violation of Islamic religious or societal norms. When a Saudi Internet user seeks to access a website that is on the blacklist, SmartFilter displays a blockpage to users which informs the users, in both English and in Arabic, that "access to the requested URL is not allowed." [FN93] The United Arab Emirates, Oman, Bahrain, Sudan, Iran, Singapore, Thailand, and Yemen also implement their nationwide filtering systems in a transparent manner similar to that employed by Saudi Arabia, displaying blockpages when users seek to access websites that are on the country's blacklist. [FN94]

Saudi Arabia, in addition to providing clear information to the Internet user that the sought website is blocked, also provides users with a means to appeal the blocking decision, by submitting an unblocking request to the relevant authorities, "by using the special forms set up for such requests on the ISU web page." [FN95]

In short, in Saudi Arabia, while the extent of filtering is substantial, consistent with the Saudi government's overall attempts to promote Islamic beliefs and the government's general intolerance toward dissent of all kinds, such filtering is conducted by the government in an open and transparent manner. Users seeking to access sites on the country's blacklist are presented with a blockpage, which provides affected users with specific notice that the website they are seeking to access has been blocked, informs them of the general justification for ***1153** such blocking, and provides Internet users with an opportunity to challenge the blocking determination.

Similarly, in Finland, users seeking to access content that has been blocked by the nationwide mandatory filtering system receive the following message, specifically notifying the Internet user seeking access--if not the content provider [FN96]--that the website they are seeking to access has been blocked:

> POLICE.
> ENTRY DENIED. Your browser has tried to access a site for which the access has been prevented due to the act on preventive measures on distribution of child pornography. The police maintains and updates a list of these child pornography sites. It is punishable to possess or distribute images on these sites. For the police these images are evidence of sexual crimes against children. Any messages on the issue can be sent [to] the National Bureau of Investigation, email address krp-nettiesto@krp.poliisi.fi From this link you can read the criminal code related to the child pornography. [FN97]

In contrast, many other countries are far more opaque and secretive in their implementation of all aspects of their filtering systems. These systems operate in such a manner that their Internet users are not made aware that the website they are requesting or seeking to make available has been blocked, nor even that the country is implementing a nationwide Internet filtering system. According to the OpenNet Initiative, many countries--including Bahrain, China, Ethiopia, Libya, Morocco, Pakistan, Tunisia, Uzbekistan, and Vietnam--operate their nationwide filtering systems in a manner that either reflects efforts to conceal the fact that filtering is occurring or that fail to indicate filtering when it occurs. [FN98] Accordingly, "transparency and accountability are the exception in Internet filtering decisions, not the norm." [FN99]

The example of the United Kingdom is particularly disturbing on ***1154** this score. Although the United Kingdom generally has meaningful guarantees of freedom of expression, the nation's ISPs, as discussed above, have for the past seven years been implementing a nationwide Internet filtering program that operates in a secret, nontransparent manner. As described above, the vast majority of British ISPs implement the Cleanfeed system to block access to websites that have been deemed potentially illegal by the Internet Watch Foundation, an unaccountable private organization that maintains a list of URLs that are suspected of hosting illegal content that falls into one of the (expanding) categories of child sexual abuse, promoting racial hatred, or hosting criminally obscene adult content. [FN100] Apparently, the vast majority of U.K. Internet users are unaware that their Internet search results are being filtered in this manner. [FN101] Furthermore, the ISPs' implementation of Cleanfeed does not inform Internet users when the sites they have requested are filtered or blocked. Instead, when a U.K. user attempts to access a website that the IWF has placed on the blacklist, the user receives a generic "404"/"file not found" Internet error message, which conveys no information to the Internet user that the website has been placed on the blacklist. [FN102] In the words of commentator Lilian Edwards, the U.K. Cleanfeed system "could be the most perfectly invisible cen-

sorship mechanism ever invented." [FN103]

The lack of transparency with which the Cleanfeed system operates has led to other complications as well. In December 2008, the IWF apparently determined that the cover of the German rock band The Scorpions album Virgin Killer was illegal child sexual abuse. The image on the album cover, which depicts a naked ten year old girl with her genitalia obscured, had been made available on Wikimedia sites, in conjunction with an article about the album. Once the IWF added the Wikimedia and Wikipedia pages hosting the album cover to its blacklist, not only were millions of U.K. users prohibited from accessing the Wikimedia and Wikipedia web pages for this album, but also thousands of U.K. citizens were prohibited from editing (unrelated) articles on Wikimedia or Wikipedia. [FN104]

The U.K.'s model of silent, opaque filtering has been influential in ***1155** other European countries and has also been adopted in Canada. In 2006, Canada's largest ISPs launched Project Cleanfeed Canada, which is modeled explicitly on the U.K. Cleanfeed project, in conjunction with Cybertip.ca, a Canadian police organization. As in the U.K., analysts from Cybertip.ca make determinations as to content that is potentially illegal and place suspected URLs on the Cleanfeed distribution list. Canadian ISPs then block URLs that have been placed on the Cleanfeed distribution list. [FN105] And, as in the U.K., Internet users are not informed that the content they are searching for has been filtered. Rather, Internet users receive a standard Internet error message that the website they are seeking is unavailable. [FN106]

Consistent with general procedural due process norms and with the procedural safeguards embodied in First Amendment jurisprudence in particular, countries implementing nationwide filtering systems to restrict their citizens' access to content that they deem harmful--like the U.K. and Canada--should at the very least operate these systems in an open and transparent manner. These systems should operate in a manner such that (1) Internet users are made aware of the operation of such filtering systems generally, and (2) the censored content provider, and the Internet user whose access to such content was filtered, are specifically informed of instances in which the filters operate to block access to a particular website. Only then can affected content providers and users have the meaningful notice necessary to challenge the decision to censor.

5. Filtering Schemes Should Provide for Appealability of Filtering Determinations

Although First Amendment law contemplates that a system of prior restraint can initially restrict speech at the discretion of an administrative decision maker, the doctrine of prior restraints requires that the licensor's initial decision to censor be *subject to prompt judicial review* in an *adversary proceeding*. Although a decision to censor is constitutionally ***1156** permissible in the first instance, the effect of such a decision may only last for a very brief time--"the shortest fixed period compatible with [the forthcoming] sound judicial resolution." [FN107] United States courts have repeatedly emphasized the importance of the availability of *expeditious judicial review* of censorship determinations in the prior restraint context. [FN108] As the Supreme Court explained, "because only a judicial determination in an [inter partes or] adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final [prior] restraint." [FN109] In order for a filtering system to effectuate a constitutional prior restraint, such a system needs to provide for the opportunity to appeal and to secure the expeditious judicial review of an initial censorship decision. [FN110]

In summary, the *Pappert* court made clear that filtering of Internet content that the Attorney General's office had probable cause to believe involved child pornography constituted a prior restraint that was unconstitutional unless such a system allowed for prompt judicial review in an adversary proceeding of the initial decision to censor such content--even if that initial decision was made based on the Attorney General's determination that there was probable cause to believe the material was illegal child pornography or if the decision was based on an ex parte judicial determination to the same effect. Under *Pappert* and other prior restraint cases, for a filtering system to be constitutional, the initial decision to censor must be subject to appeal and prompt judicial review in an adversary proceeding.

Under many of the filtering systems implemented in other countries, provisions do exist for appeal of the censorship decision. However, the provisions for appeal do not provide for *judicial* determination and instead merely provide for a second

look by the administrative body that made the censorship determination in the first place. In the U.K., for example, the IWF website indicates that "any party with a legitimate association with the [blacklisted] content ... who believes they are being prevented from accessing legal content may appeal [broken ***1157** link] against the accuracy of an assessment. [FN111] The appeal procedure provided by the IWF, however, does not contemplate judicial review. (Further, as discussed above, it is unclear how a party would learn that the content she was seeking, or seeking to make available, was subject to the IWF's blacklist, since the Cleanfeed system merely provides Internet users with a generic 404/File not found error message when a requested website is on the IWF blacklist.) Rather, the appeal involves a second look by the IWF itself, and following that, a review by the relevant police agency, whose assessment is final. [FN112] Similarly, the Canadian Cybertip filtering system allows for an affected content provider to appeal the initial censorship decision, but that appeals process also does not contemplate judicial review. Rather, the Canadian appeals process provides for a second look by Cybertip Canada personnel, and then ultimately to a review by National Child Exploitation Coordination Centre--a branch of the Canadian Police Centre for Missing and Exploited Children [FN113]--whose decision is final. [FN114]

In summary, nationwide filtering systems impose prior restraints on speech, which under the First Amendment are unconstitutional unless they embody certain procedural safeguards and checks on the discretion of the decision makers responsible for filtering such speech. The First Amendment's procedural values would require that such prior restraints implemented by filtering systems be imposed subject to *clear and precise definitions of the speech to be regulated*; implemented *in a transparent manner*, such that affected Internet users and content providers are provided with information that the content was blocked and the reason for such blocking; and such that the filtering system provide Internet users and content providers with the *opportunity to appeal any such blocking decisions*, to a *judicial body and in an expeditious manner*.

C. *Limiting Extraterritorial Effects of Each Country's Filtering Scheme*

Finally, countries should configure their nationwide filtering schemes to limit their extraterritorial reach so as not to interfere with the political independence and sovereignty of other states. Although each ***1158** country is entitled to determine what speech is protected and what speech is unprotected within its territory, such determinations should not be implemented in ways that spill over to restrict speech within other nations, which may themselves have adopted different regimes for protecting speech. By implementing filtering schemes that operate to restrict only the Internet access of citizens within that country, a country appropriately limits the extraterritorial reach of. its Internet speech restrictions. For example, many European countries restrict hate speech and expression denying the Holocaust, while the United States does not. Accordingly, European countries desiring to block Internet hate speech or expression denying the Holocaust should do so in a way that does not restrict the availability of such speech by and to U.S. citizens. Fortunately, with recent advances in filtering technology, such geographical precision in filtering is increasingly feasible, such that speech that is prohibited in one country can be effectively blocked for citizens of that country but not for others. [FN115] Countries should take care to implement such precise filtering even for categories of speech where there is widespread agreement as to its illegality, like child pornography, because, even though there is widespread agreement as to restricting this general category of speech, countries differ as to the scope and definition of this category of speech, as I discuss below.

One instance of a country's failure to effectively limit the extraterritorial effects of its restrictions on Internet speech occurred in the case involving the dispute between France and Yahoo! The case came about because Internet search engine Yahoo! hosted an auction site in which it allowed its subscribers to auction off Nazi memorabilia. Under the French criminal law, it is illegal to "exhibit" in France public uniforms, insignias and emblems that "recall those used" by (1) an organization declared illegal in application of Article 9 of the Nuremberg Statute, such as the Nazi party, or by (2) a person found guilty of crimes against humanity. [FN116] Two French groups devoted to combating racism and anti-semitism sued Yahoo! in France, claiming that Yahoo!' s hosting ***1159** auctions of Nazi memorabilia violated French criminal law. [FN117] In its defense, Yahoo! claimed that, while it was willing to abide by French law within France, and while it removed Nazi memorabilia from the French country-specific version of its site available at Yahoo.fr, it did not have the technological means to restrict *only* French users from accessing its auction site available at its internationally available site Yahoo.com. [FN118] Furthermore, Yahoo! argued, such Nazi-related content was protected under the First Amendment, and therefore Yahoo! enjoyed the right to make such content available to U.S. citizens via its servers for Yahoo.com, which were hosted in the United States. Finally and most importantly, Yahoo! asserted that France did not have jurisdiction over Yahoo!, a United States

company whose servers were based in the United States.

The French court disagreed with Yahoo!, and held that Yahoo! was in violation of French criminal law for hosting an auction of content that was illegal within France. It rejected Yahoo!'s argument that there was no feasible way for Yahoo! to restrict access to such content only within France, and ordered Yahoo! to take all appropriate measures to deter and prevent access to auctions of Nazi memorabilia on its site by French residents within three months of the court's order or face a fine of 100,000 francs per day. While Yahoo! fought this order--for the next six years--in United States courts, [FN119] along the way Yahoo! decided to cease hosting auctions of Nazi memorabilia within Yahoo.com. Accordingly, the practical effect of the French court's actions was to impose France's speech restrictions beyond its borders, on a U.S. company, where the speech subject to restriction was protected by the First Amendment.

Instead of imposing the obligation on Yahoo! to restrict French citizens' access to Internet speech that was illegal in France--which ultimately resulted in Yahoo!'s removing such speech completely from its internationally accessible website--the more speech-friendly result would have been for France itself to impose nationwide filters on such speech to restrict its own citizens' access-- and only its own citizens' access--to such speech. To limit the extraterritorial effects of any one country's speech restrictions, each country choosing to restrict such speech should implement systems that filter the prohibited Internet speech at its *destination*, in lieu of seeking to secure removal of the speech at its *source*.

***1160** In summary, if countries choose to restrict Internet speech, they should implement nationwide restrictions so as to limit the extraterritorial reach and effect of such restrictions. Nationwide filtering of Internet speech achieves this goal of limiting the extraterritorial effects of each nation's speech restrictions, while respecting the prerogatives of other nations to restrict Internet speech--or not--within their borders.

VI. CONCLUSION

The broad substantive protections for speech provided under the First Amendment are unlikely to be adopted by the world's nations in the near future. Indeed, countries are increasingly filtering Internet speech and restricting a host of categories of content that they deem harmful on the Internet. Although it is less likely that other countries will soon adopt the First Amendment's broad substantive protections for speech, it is more likely that other countries could come to adopt the First Amendment's *procedural* protections for speech and implement the First Amendment's "sensitive tools" for distinguishing between protected speech and unprotected speech--however they define the latter category. The First Amendment's prior restraint doctrine as applied to nationwide filtering systems would require that several procedural safeguards and checks be in place in any such system, including *transparency* and *appealability* of the initial decision to restrict the speech; *limits on the substantive discretion of the filterer* charged with making the initial determination whether to restrict the speech; and *prompt judicial review in an adversary proceeding* before any final decision to censor is implemented. Further, the state action doctrine, as applied to systems of nationwide Internet filtering, would prohibit countries from attempting to evade their responsibility to protect their citizens' free speech rights by shifting censorship obligations to their nation's ISPs. Attempts by the state to transfer censorship functions to private entities acting at the behest of or in concert with the state should not insulate those actions from judicial scrutiny. Applying the state action doctrine, courts should look past the form through which such speech restrictions are implemented and attribute those actions to the state and subject them to appropriate review and scrutiny. Finally, countries choosing to restrict Internet speech should do so in a way that limits the extraterritorial reach and effect of their speech restrictions and respects the prerogatives of other nations to restrict Internet speech--or not--within their borders.

[FNa1]. Professor of Law, The George Washington University Law School. I am grateful to the participants of the workshop on Free Speech: Old Principles, New Circumstances, at the University of Oxford, St. Antony's College, for their insights on the ideas presented in this Article, as well as to the conveners of and participants in The Georgetown Journal of International Law Symposium on International Cyberlaw, and the editors of the Georgetown Journal of International Law. I am also grateful for the guidance of Professor Arturo Carrillo and the excellent research assistance provided by Bridget Rochester and Jared Rudolph.

[FN1]. Miklos Harazti, *Foreword* to ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE, at xv, xv (Ronald Deiber, et. al. eds., 2010).

[FN2]. *See, e.g.*, Jonathan Zittrain & John Palfrey, *Introduction* to ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 1, 2 (John G. Palfrey et al. eds., 2008) (explaining that more than three dozen states around the world now impose state-mandated technical Internet filtering and setting forth its systematic global study of all known state-mandated Internet filtering practices).

[FN3]. *See* Hillary R. Clinton, U.S. Sec'y of State, Internet Rights and Wrongs: Choices and Challenges in a Networked World, Remarks at The George Washington University (Feb. 15, 2011), http:// www.state.gov/secretary/rm/2011/02/156619.htm.

[FN4]. *See, e.g.*, RONALD J. KROTOSZYNSKI, JR., THE FIRST AMENDMENT IN CROSS-CULTURAL PERSPECTIVE: A COMPARATIVE LEGAL ANALYSIS OF THE FREEDOM OF SPEECHH (1st ed. 2009); Robert A. Sedler, *An Essay on Freedom of Speech: The United States Versus the Rest of the World*, 2006 MICH. ST. L. REV. 377 (2006); Stephanie Farrior, *Molding the Matrix: The Theoretical and Historical Foundations of International Law and Practice Concerning Hate Speech*, 14 BERKELEY J. INT'L L. 1 (1996).

[FN5]. Philip Elmer-Dewitt et. al., *First Nation in Cyberspace*, TIME INT'L (Dec. 6, 1993), http:// www.time.com/time/magazine/article/0,9171,979768,00.html.

[FN6]. For a general discussion of how nation-by-nation Internet filtering is implemented, see Steven J. Murdoch & Ross Anderson, *Tools and Technologies of Internet Filtering, in* ACCESS DENIED, *supra* note 2, at 57.

[FN7]. *See, e.g.*, Sedler, *supra* note 4, at 5 (explaining that nations other than the United States, with different histories and experiences, would "understandably be less protective of freedom of speech than we are ...").

[FN8]. *See* Selah Hennessey, *Reporters Without Borders Names World's Worst Media "Predators,"* VOANEWS.COM (May 5, 2010), http:// www.voanews.com/english/news/special-reports/human-rights/Reporters-Without-Borders-Names-Worlds-Worst-Media-Predators-92682084.html.

[FN9]. *See, e.g.*, Zittrain & Palfrey, *supra* note 2, at 2 (explaining that more than three dozen states around the world now impose state-mandated technical Internet filtering and setting forth its systematic global study of all known state-mandated Internet filtering practices).

[FN10]. *See* OPENNET INITIATIVE, Europe Overview, *in* ACCESS CONTROLLED, *supra* note 1, at 279, 286.

[FN11]. *See id.* at 284-85.

[FN12]. *See* OPENNET INITIATIVE, South Korea Overview, *in* ACCESS CONTROLLED, *supra* note 1, at 503, 510; NAT'L ELECTION COMM'N, REPUBLIC OF KOR., THE OVERVIEW OF CYBER CRACKDOWN SERVICE RELATED TO THE 18TH NATIONAL ELECTION (2010); Shin Hae-in, *Korea: Controversy Mounts Over Ban on Internet Election Messages*, KOREA HERALD, June 25, 2007.

[FN13]. *See National Classification Code 2005* (Cth) (Austl.) (describing Restricted Classifications of publications under Australian law), *available at* http://www.comlaw.gov.au/Details/F2005L01284.

[FN14]. *See infra* Parts V.B.3, V.B.4, V.B.5.

[FN15]. *See, e.g.*, Nicola Laver, *Revealing the Truth*, 64 INT'L B. NEWS. no. 6, at 14, *available at* http://www.ibanet.org/Article/Detail.aspx? ArticleUid=cea217a9-682c-4f6a-9465-5445603259d7; Navi Pillay, U.N. High Comm'r for Human Rights, Remarks Concerning Reports of Pressure Being Exerted on Private Companies to Halt Financial or Internet Services for WikiLeaks (Dec. 9, 2010), http://www.unmultimedia.org/tv/unifeed/d/16541.html (suggesting that United States entities' actions, taken together, were violative of the First Amendment).

[FN16]. *See, e.g.*, Sedler, *supra* note 4.

[FN17]. *See infra* Part V.B.

[FN18]. *See infra* Part V.C.

[FN19]. *See infra* text accompanying notes 22-32.

[FN20]. *See, e.g.*, KROTOSZYNSKI, *supra* note 4.

[FN21]. Universal Declaration of Human Rights, G.A. Res. 217 (III)A, U.N. Doc. ARES/217(III), art. 19 (Dec. 10, 1948) (hereinafter Universal Declaration).

[FN22]. *Id.* art. 29.

[FN23]. U.N. Secretary General, *United Nations Action in the Field of Human Rights*, ¶ 67, U.N. Doc. ST/HR/2/Rev.2 (1983); *See also* Louis B. Sohn, *The Universal Declaration of Human Rights*, 8 J. INT'L COMMISSION JURISTS 17, 26 (1967) (explaining that the Declaration "has achieved the character of the world law superior to all other international instruments and to domestic law.").

[FN24]. *See* Richard B. Lillich, *The Growing Importance of Customary International Human Rights Law*, 25 GA. J. INT'L & COMP. L. 1, 1-7 (1995); *cf. Filartiga v. Pena-Irala*, 630 F.2d 876 (2d Cir. 1980) (finding U.D.H.R. binding in U.S, at least in part).

[FN25]. International Covenant on Civil and Political Rights, Dec. 16, 1966, S. TREATY DOC. NO. 95-20, 999 U.N.T.S. 171.

[FN26]. *Id.* art. 19.

[FN27]. *Id.*

[FN28]. *Id.* art. 20.

[FN29]. European Convention for the Protection of Human Rights and Fundamental Freedoms, E.T.S. No. 005, 213 U.N.T.S. 222, *opened for signature* Nov. 11, 1950 (entered into force Sept. 3, 1953), *amended by* Protocol 11, E.T.S. No. 155, *opened for signature* May 11, 1994.

[FN30]. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Communities, Dec. 13, 2007, 2007 O.J. (C 306) 1.

[FN31]. American Declaration of the Rights and Duties of Man, O.A.S. Res. XXX, May 2, 1948, *reprinted in* Basic Documents Pertaining to Human Rights in the Inter-American System, OEA/Ser.L.V./II.82, doc. 6, rev. 1, at 17 (1992).

[FN32]. Organization of American States, American Convention on Human Rights, Nov. 22, 1969, O.A.S.T.S. No. 36, 1144 U.N.T.S. 123.

[FN33]. *See, e.g.*, William Magnuson, *The Responsibility to Protect and the Decline of Sovereignty: Free Speech Protections under International Law*, 43 VAND. J. TRANSNAT'L L. 255, 259 (2010) (stating that under the current understanding of the international law of free speech, the state has exclusive control over its territory and its people, while arguing that the responsibility to protect should apply to the right of freedom of speech).

[FN34]. *Id.* at 290.

[FN35]. *See, e.g., id.* at 312 (claiming that "the arguments justifying an international obligation to intervene in the case of genocide are just as valid, if not more, when applied to an obligation to intervene in the case of widespread violations of free expression.").

[FN36]. *See id.* at 259.

[FN37]. Martin Bright, *BT Puts Block on Child Pom Sites*, OBSERVER (U.K.), June 6, 2004, http://www.guardian.co.uk/technology/2004/jun/06/childrensservices.childprotection.

[FN38]. As set forth on the IWF web site, its mandate is "to minimize the availability" of potentially criminal internet content, specifically:

- Images of child sexual abuse hosted anywhere in the world.
- Criminally obscene adult content hosted in the UK.
- Non-photographic child sexual abuse images hosted in the UK.

About the IWF, INTERNET WATCH FOUND., http://www.iwf.org.uk/about-iwf (last visited June 7, 2011).

[FN39]. *See IWF Facilitation of the Blocking Initiative*, INTERNET WATCH FOUND., http://www.iwf.org.uk/services/blocking (last visited June 11, 2011).

[FN40]. *See* NIKOLAOS KOUMARTZIS, BT'S CLEANFEED AND ONLINE CENSORSHIP IN THE UK: IMPROVEMENTS FOR A MORE SECURE AND ETHICALLY CORRECT SYSTEM 24 (2009).

[FN41]. *Id.*

[FN42]. *See* OPENNET INITIATIVE, United States and Canada Overview, *in* ACCESS CONTROLLED, *supra* note 1, at 369, 375.

[FN43]. *See* Kai Puolamäki, *Finnish Internet Censorship*, ELECTRONIC FRONTIER FIN. (Feb. 18, 2008), http://www.effi.org/blog/kai-2008-02-18.html#how-the-censorship-works.

[FN44]. Like the First Amendment of the United States Constitution, the U.K.'s Human Rights Act of 1998 technically applies only to state action. In the United Kingdom, the Human Rights Act of 1998 was enacted to incorporate the European Convention on Human Rights into domestic law. Under Section 6(1) of the Act, the obligation to act consistently with the European Convention on Human Rights is limited to "public authorities," and so technically excludes private corporations and entities, as does the First Amendment. Further, in the Human Rights Act of 1998, most of the individual rights are specified, as in the United States, to be held against the state, which suggests that Act's obligations were intended to be binding

only against state actors. *See generally* Stephen Gardbaum, *The "Horizontal Effect" of Constitutional Rights*, 102 MICH. L. REV. 387 (2003).

[FN45]. Lilian Edwards, *From Child Pom to China, in One Cleanfeed*, 3 SCRIPTED 174 (2006), *available at* http://www.law.ed.ac.uk/ahrc/script-ed/vol3-3/editorial.asp.

[FN46]. GA. Res 56/83, art. 9, U.N. Doc. A/RES/56/83 (Dec. 12, 2001).

[FN47]. Marsh v. Alabama, 326 U.S. 501 (1946).

[FN48]. *See* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW 514-17 (3d ed. 2006).

[FN49]. 513 U.S. 374 (1995).

[FN50]. *Id.* at 396 (holding that Amtrak, a government-created and government-controlled corporation, was a state actor for First Amendment purposes, but declining to determine whether its speech restrictions were constitutional).

[FN51]. Nat'l A-1 Adver. v. Network Solutions, Inc., 121 F.Supp. 2d 156 (D.N.H. 2000).

[FN52]. *Marsh*, 326 U.S. at 501.

[FN53]. For a detailed discussion of the affirmative conception of the First Amendment, as well as its application to Internet speech restrictions, see generally DAWN C. NUNZIATO, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN THE INTERNET AGE (2009).

[FN54]. *Marsh*, 326 U.S. at 509.

[FN55]. *See, e.g.*, Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963) (explaining that "[a]ny system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity."); Near v. Minnesota, 283 U.S. 697, 713 (1931) (explaining that "the chief purpose [of the First Amendment is to] prevent previous restraints upon publication.").

[FN56]. See *infra* Parts V.B.4, V.B.5.

[FN57]. See *infra* Part V.B.3.

[FN58]. See *infra* Part V.B.5.

[FN59]. *See, e.g.*, Freedman v. Maryland, 380 U.S. 51 (1965).

[FN60]. *See* Shuttlesworth v. City of Birmingham, 394 U.S. 147 (1969).

[FN61]. *See* Mainstream Loudoun v. Bd. of Trs. of the Loudoun Cnty. Library, 24 F. Supp. 2d 552 (E.D. Va. 1998) (holding that public library's imposition of filtering software effectuated an unconstitutional prior restraint (1) because it failed to embody substantial safeguards necessary to render the prior restraint constitutional prior restraint; (2) because the library had abdicated the decision-making authority regarding which Internet content to block to a private software filtering company; and (3) because the filtering software did not base its blocking decisions on legally acceptable definitions of constitutionally unprotected speech).

[FN62]. 372 U.S. 58, 58 (1963); *infra* text accompanying notes 64-67.

[FN63]. *See, e.g.*, Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d. 606, 655 (E.D. Pa. 2004) (explaining that, although blocking/filtering systems that allowed for websites to be blocked after they were initially made available to the public were not "prior restraints in the traditional sense [because] they do not prevent speech from reaching the marketplace [in the first place] but remove material already available on the Internet from circulation," such systems are nonetheless "administrative prior restraints as that term has been interpreted by the Supreme Court."); Fort-Wayne Books v. Indiana, 489 U.S. 46 (1989) (seizure of books prior to trial based on finding of probable cause of books' obscenity effected an unconstitutional prior restraint); A Quantity of Books v. Kansas, 378 U.S. 205 (1964) (same); Marcus v. Search Warrant, 367 U.S. 717 (1961) (same).

[FN64]. *Bantam Books,* 372 U.S. at 58.

[FN65]. *Id.* at 62 n.5.

[FN66]. *Id.* at 66.

[FN67]. *Id.* at 70.

[FN68]. *Id.* at 66.

[FN69]. Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d. 606, 610 (E.D. Pa. 2004).

[FN70]. *Id.* at 622.

[FN71]. On this point, the court explained that the informal and technically noncoercive nature of the attorney general's removal requests did not insulate them from constitutional scrutiny. The court explained that removal requests issued by law enforcement officials were not interpreted by the recipient ISPs as being voluntary, even if technically they did not have the force of law. *See id.* at 611.

[FN72]. *See, e.g.,* Sedler, *supra* note 4.

[FN73]. 349 U.S. 147 (1969).

[FN74]. *Id.* at 149-50.

[FN75]. *Id.* at 150-51.

[FN76]. *See, e.g.*, Robert Faris & Nart Villeneuve, *Measuring Global Internet Filtering, in* ACCESS DENIED, *supra* note 2, at 5, 25 (explaining that, because "[f]iltering decisions are .... often made by selecting categories for blocking within software applications, which may also contain categorization errors resulting in unintended blocking, [t]he temptation and potential for mission creep is obvious.").

[FN77]. OPENNET INITIATIVE, China Overview, *in* ACCESS CONTROLLED, *supra* note 1, at 449, 478.

[FN78]. *Id.*

[FN79]. *Id.*

[FN80]. *Id.*

[FN81]. *FAQs Regarding the IWF's Facilitation of the Blocking Initiative*, INTERNET WATCH FOUND., http://www.iwf.org.uk/services/blocking/blocking-faqs (last visited June 7, 2011).

[FN82]. *See* Broken Link to Blocking Criteria Policy Page, INTERNET WATCH FOUND., http://www.iwf.org.uk/services/hodine/sentencing-guidelines (last visited June 7, 2011). The author has made many attempts to check this link, from February through April 2011 and has found this link to be broken on each occasion. Indeed, the-waybackmachine.com, a website that crawls the internet and archives webpages, never shows this link being active despite over 4,400 archived pages for iwf.org.uk/ going back at least 10 years.

[FN83]. *See IWF URL List Policy and Procedures,* INTERNET WATCH FOUND., http://www.iwf.org.uk/services/blocking/iwf-url-list-policy-and-procedures (last visited June 7, 2011).

[FN84]. *See* INTERNET WATCH FOUND., *supra* note 82 and accompanying text.

[FN85]. *See Remit, Vision and Mission*, INTERNET WATCH FOUND., http:// www.iwf.org.uk/about-iwf/remit-vision-and-mission (last visited June 7, 2011); *IWF Reporting Page*, INTERNET WATCH FOUND., https://www.iwf.org.uk/report (last visited June 7, 2011) (specifying "We are the UK Hotline for reporting criminal online content and work with the Internet industry, police and international partners to get it removed" and indicating that an Internet user can report online content that falls within the following categories: (1) child sexual abuse images; (2) nonphotographic child sexual abuse images; (3) criminally obscene adult content; (4) incitement to racial hatred content).

[FN86]. *See infra* Part V.B.I.

[FN87]. See *infra* text accompanying notes 90-93.

[FN88]. For example, a 2008 Saudi law on the use of technology provides substantial penalties (five years imprisonment and a fine) for the use of the Internet to distribute content such as pornography or other materials that violate public law, religious values, or the social standards of the kingdom. *See* OPENNET INITIATIVE, Suadi Arabia Overview, in ACCESS CONTROLLED, *supra* note 1, at 561, 565. Websites relating to alternative religions (such as those discussing conversion from Islam to Christianity), websites espousing critical views of Islam, websites relating to minority Shia groups, sites of global free speech advocates, websites relating to gay and lesbian issues, sex education and family planning, have all been blocked. *See id.* at 566-67. Also blocked were websites containing content relating to alcohol, drugs, and those featuring provocative attire. *See id.* at 567.

[FN89]. *Introduction to Content Filtering*, INTERNET SERVICES UNIT, KING ABDULAZIZ CITY FOR SCI. & TECH., http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm (last visited June 7, 2011).

[FN90]. *Id.*

[FN91]. *Id.*

[FN92]. *Id.*

[FN93]. *Id.* There do not seem to be any direct adverse consequences for attempting to access blacklisted websites. However, Internet cafés in Saudi Arabia, as of March 2009, were ordered to install hidden cameras and to provide the names and ad-

dresses of their customers, so presumably these measures chill attempts to access disapproved content. *See* OPENNET INITIATIVE, *supra* note 88, at 565.

[FN94]. *See* Faris & Villeneuve, *supra* note 76, at 15-16.

[FN95]. *Id.*

[FN96]. The Finnish nationwide filtering system does not appear to provide content providers with notice that their websites have been blocked. *See Finnish Internet Censorship*, ELECTRONIC FRONTIER FIN. (Feb. 18, 2008, 7:27 AM), http://www.effi.org/blog/kai-2008-02-18.html (When adding a website to the secret blocklist, "apparently the police [do] not try to contact ... the owner of the censored site.").

[FN97]. *See id.*

[FN98]. *See* Faris & Villeneuve, *supra* note 76, at 17.

[FN99]. *Id.* at 25.

[FN100]. *See* INTERNET WATCH FOUND., *supra* note 85.

[FN101]. KOUMARTZIS, *supra* note 40, at 104.

[FN102]. *Id.* at 34 ("In case a request is made for accessing a URL [on IWF's blacklist,] a '404' response with the message 'page unavailable' is returned to the user.").

[FN103]. Edwards, *supra* note 45, at 175.

[FN104]. *See, e.g., Wikipedia Child Images Censored*, BBC News (Dec. 8, 2008, 11:08 AM), *available at* http://news.bbc.co.uk/2/hi/7770456.stm.

[FN105]. *See* OPENNET INITIATIVE, *supra* note 42, at 375. Although the blocking of U.K. citizens from editing Wikimedia or Wikipedia files may have been an unintended consequence of the IWF's blacklisting of the Virgin Killer websites, it nonetheless demonstrates the problems attendant to implementing filtering in a nontransparent manner.

[FN106]. As the Cybertip website sets forth on its FAQ page: Q. Are people able to tell which addresses are filtered under this system? Should they be able to do so? A. No. They get a standard message indicating they are unable to access the Internet address. *See Cleanfeed Canada, Frequently Asked Questions*, CYBERTIP, http://www.cybertip.ca/app/en/cleanfeed (last visited June 11, 2011).

[FN107]. Freedman v. Maryland, 380 U.S. 51, 59 (1965).

[FN108]. *See* United States v. Thirty-Seven Photographs, 402 U.S. 363, 372-74 (1971); Interstate Circuit, Inc. v. City of Dallas, 390 U.S. 676, 679-80 (1968); Bantam Books v. Sullivan, 372 U.S. 58, 70-71 (1963); Kingsley Books, Inc. v. Brown, 354 U.S. 436, 440 (1957).

[FN109]. *See* United States v. Pryba, 502 F.2d 391, 405 (D.C. Cir. 1974).

[FN110]. *See e.g., Thirty-Seven Photographs*, 402 U.S. at 372-74 (holding that delays in judicial determination as long as

three months could not be sanctioned; accordingly, federal statute imposing prior restraint must be construed to require a judicial decision within sixty days).

[FN111]. *See* INTERNET WATCH FOUND., *supra* note 81 (under heading "Are site 'owners' notified that they have been added to this list?").

[FN112]. *Content Assessment Appeal Process*, INTERNET WATCH FOUND., http:// www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process (last visited June 7, 2011).

[FN113]. *See National Child Exploitation Coordination Centre*, ROYAL CAN. MOUNTED POLICE, http://www.rcmp-grc.gc.ca/ncecc-cncee/index-accueil-eng.htm (last visited May 22, 2011).

[FN114]. *Cleanfeed Canada Appeal Process*, CYBERTIP!CA http:// www.cybertip.ca/app/en/cleanfeed_pl#anchor_menu (last visited June 7, 2011).

[FN115]. *See, e.g.*, Faris & Villeneuve, *supra* note 76, at 12-13 (discussing how country-specific filtering is implemented by ISPs within a country and on the Internet backbone at the country's international gateway).

[FN116]. France's Code Penal [C. PéN.] art. R645-1 (Fr.) makes it illegal to "wear or exhibit" in public uniforms, insignias and emblems which "recall those used" by:

- an organisation declared illegal in application of Art. 9 of the Nuremberg Statute, or by

- a person found guilty of crimes against humanity as defined by Arts. L211-1 to L212-3 or by the Law No 64-1326 of 1964-12-26.

[FN117]. *See* Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme, 169 F. Supp. 2d 1181 (2001), *rev'd*, 433 F.3d 1199 (2006).

[FN118]. *Id.* at 1185.

[FN119]. *Id.*