International Ethernets: Sink or Swim?

Carrie Green
ccg3@duke.edu

Alberto Laverde
laverde@duke.edu

Melissa Lim
mjl10@duke.edu

John Wyrick
jtw9@duke.edu

December 14, 2002
1 The Problems of Internet Regulation

The average Internet user dislikes the idea of a law that regulates and restricts their online experience. However, the majority of laws do not hinder Internet freedoms; they either cannot be enforced or no enforcement is attempted. This has lulled the general public into a false sense of security, of feeling that the Internet is above the law and unable to be regulated. Worldwide, governments, committees, and other Internet regulating bodies are trying to change this by passing law after law as if there was no tomorrow. With the rapid rate of enactment of Internet laws, it is not uncommon for contradictory laws to emerge, as well as the issue of identifying meaningful laws. Additionally compounded by the complex and ever changing nature of the Internet, many laws are confusing and difficult to understand, not just their purpose, but their intent. Another issue is that as more legislation surfaces, more conflicts arise with pre-existing legislation, either by directly interfering with the policy or by having an affect beyond its intended scope. This is never-ending, the myriad of policy writers and legislators continue to draft new measures, adding to the chaos. The problem that the Internet faces: mass confusion and lack of coordination in the field of Internet Regulation. Below are the three cornerstones of this issue, separated for analysis: the lack of clarity in Internet law, the laws which conflict, and the uncoordinated efforts of different groups all trying to simultaneously legislate the Internet.
1.1 Lack of Clarity in Internet Law

Ignorance is not an excuse for breaking the law, but when the laws themselves are unclear there is a problem. The oft-referred-to legalese in any given law should clearly denote what constitutes an offense, who has the right to pursue it and in what court, and what measures may be taken as punishment. If these conditions are not met then proper enforcement becomes impossible. It defeats the purpose of having the law in the first place. For simplicity’s sake, this can be condensed into two ideas that must be addressed: the legal text itself being unclear, and the lack of clarity with regard to jurisdiction - who has the authority to deal with offences.

Consider when the regulation is at fault, in most cases due to loose and ill-considered or unintentionally vague wording. Errors in law enforcement will reflect the lack of clarity. If the text is interpreted too broadly, the law may encompass more than intended. Depending on how the problem factors into the legislation as a whole, it will either result in ineffective laws with sufficient loopholes granting criminals a legal excuse to escape punishment, or excessive laws which may be misused to wrongfully convict people or allow more action to be taken than was necessary. An example of this last case is the United Kingdom’s Regulation of Investigatory Powers Act (Matthew Broersma, UK Surveillance Laws May Be Illegal).

RIPA allows law enforcement agencies to access mobile phones and Internet data as part of their investigation. According to an article posted on C—Net, "The act, passed two years ago, may violate human rights laws because of a loophole under which law enforcement agencies may access data
that has been retained specifically for use in cases involving national security (Broersma).” This grants excessive powers to law enforcement performing routine criminal searches.

Closer to home, in a US District Judge named John Bates hearing a test case regarding the Digital Millennium Copyright Act (BBC News, Judge brands song swap laws ’unclear.’) declared the Act to be unclear. As related in a BBC News article, Judge Bates stated, “Congress ”could have made this statute clearer,” and ”This statute is not organized as being consistent with the argument for either side (BBC News).” If a judge feels that any law is unclear, then it invalidates the laws by introducing uncertainty in its application, which until resolved will render it ineffective. Leeway to either the defense or the prosecution from a vague law would result in an innocent individual being convicted or a criminal walking free. In either case, this is a condition to be avoided by resolving the ambiguity as swiftly as possible.

With regards to issues of jurisdiction, flawlessly and clearly enacted laws become ineffective when there are no means of enforcement. Enforcing a law entails the use of a judicial system or court to punish the offender as the law specifies. The problem with violations of Internet law and regulation is deciding what group has the right and power to apply the law in any given case. Given the global nature of the Internet, the victim and perpetrator could easily be on opposite sides of the world, with both countries claiming to have jurisdiction. A paper posted to the Cyberspace Law Institute by its co-directors better describe this problem:

Law enforcement is unusually problematic in the special environment of cyberspace; not only can it be difficult to locate an
anonymous or pseudonymous Internet user within any specific territorial jurisdiction, but the global nature of the Internet decreases the likelihood that the parties to online disputes will be subject to control by the same territorial law enforcement entities. (David Johnson & David Post, The New 'Civic Virtue' of the Internet)

The underlying problem is territory; it may different sovereign nations, states, or cities. How is a decision reached with regard to whom shall have the power to punish the crime? Even within the United States, offenders located across state borders makes decisions on jurisdiction difficult. Presented below are two opposing cases for consideration. First Pres-Kap, Inc. v. Sys. One, a company in Florida sued a user in New York. Which state has jurisdiction? Ultimately the state of Florida was denied jurisdiction, "because the New York user merely accessed the database electronically and had no contact with Florida (Albert Velarde, "Jurisdiction and the Internet).” So in this case because the act was done electronically, the victim’s state was denied jurisdiction. In the second, Software Inc. v. Reliability Research Inc results with the opposite outcome; the plaintiff in California charges the owner of a Nevada BBS to court for online libel. This time the victim’s state was granted jurisdiction (Velarde). While these individual cases were resolved, the contradiction between the two shows that a better method of resolving jurisdiction is needed.

So what happens when Internet cases are international? The answer is disappointing, and entirely unhelpful. A second article hosted on CLI relates a legal principle known as the Doctrine of Comity. In the Supreme Court’s interpretation, Comity states that, ”the recognition which one nation allows
within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protections of its law (David Johnson & David Post, Law And Borders–The Rise of Law in Cyberspace).” Translated out of legalese, Comity means a country may allow the laws of another country to apply for a specific case within their borders, if the host nation agrees. The key phrase, ”international duty and convenience,” turns the Doctrine of Comity into little more than one country asking favors of another. International law will apply in any Internet policy case where the people are from different countries, and this is assuming only crimes of citizen vs. citizen, or company vs. company. Should the conflict be between the nations themselves, could the case even be heard? Consider this C—Net article on enforcement, which opens with the following statement: "Former Yahoo CEO Tim Koogle could find himself cuffed if he sets foot on French soil. His alleged crime: Allowing the posting of Nazi collectibles on Yahoo’s U.S.-based site (Lisa Bowman, Law And Borders–The Rise of Law in Cyberspace).” The article explains that to post Nazi paraphernalia online is against France’s war crimes laws. Although the posting was done in the US, it can be seen in France. Comity really is no solution with respect to the Internet. While Tim Koogle remains on U.S. soil, France has no power to procure him for his perceived crime. Hence, for effective worldwide Internet policy, the question of how to resolve jurisdiction for individual Internet cases must be addressed.
1.2 Conflicting Internet Law and Regulation

Unclear laws are sufficiently disturbing onto themselves, and when laws interfere with each other confusion and ambiguity are exacerbated. The bulk of this dilemma is two fold. The first issue is in practice, policy may have a far wider range than intended. Secondly, policies may conflict and in many cases the conflicting policies may be equally valid. Consider legislation passed in Minnesota that requires Internet companies to follow a set of procedures before using the data they gather from their clients. On the surface this seems harmless enough. However, Minnesota is only one state. An Information-Week article on this subject notes that, “ISPs, Internet content providers, and online marketers say that if other states follow suit, the proliferation of potentially conflicting Internet privacy laws will hinder their operations nationally (John Rendleman, Minnesota Opt in on Privacy).” Imagine each of the fifty states having their own version of the legislation, and the resulting confusion that would follow for companies with national presence. Different branches would be held to different standards by their home states. Which would they follow? Could they follow any? Equally applicable policies are trouble.

An excellent example of a policy that warns of chaotic regulation is the now-infamous HR 5211. The bill is a proposal designed to give copyright holders the ability to take steps to prevent the spread of their work over public networks. However, the imprecise phrasing of the bill grants excessive leeway. A great conflict of this bill lies in its giving copyright holders immunity from virtually any other law for the purposes of ”protecting” their media. EFF
(Electronic Frontier Foundation) had this to say on the subject: "What the bill does is permit copyright owners to go and violate the law. This unprecedented power has never been granted even to law enforcement, much less to a single industry (Electronic Frontier Foundation, "The Berman P2P Bill: Vigilantism Unbound.")." This is outrageous! It may conflict with any other US criminal law or US code in existence. The international aspect is even more chilling, if other nations were to follow suit - the very idea of no one being above the law would be in jeopardy. HR 5211’s attempt at placing limits on the power was hampered by the vague criteria for the bill’s scope. The "enforcer" is not permitted to keep any file other than the copyrighted one from being available, except as "strictly necessary" - a term which translates into "if the enforcer wants to." As EFF is quick to point out, the bill will also affect users other than the legally identified violators: "ISPs, network administrators, and Internet users generally will also suffer under the Berman P2P Bill, as the Internet is flooded with an ever-changing hailstorm of legally encouraged "attacks." (Electronic Frontier Foundation)."

In short, HR5211 also will affect more individuals than the single reported target for an attack, potentially having a Denial Of Service (DOS) attack interfere with uninvolved parties who just happen to share the same ISP. This is an example of legislation that grants too much power and too broad a scope due to vagueness.

Another example is Panama. It enacted a policy that is too broad in its execution adversely affecting individuals outside its intended scope. Linux and Main reported on the decree issued by the Panamanian government, wherein all the ISPs (Internet Service Providers) in the country were in-
structed to swiftly block the ports used in sending data for Voice over IP. The intent was to eliminate competition for Panama’s cable & voice provider. They were purportedly losing money due to people using their Internet connection in place of standard phone lines for international calls (Linux and Main, Panama Begins Blocking IP Ports). This policy’s fault is that in attempting to safeguard a local phone company, Panama mandated port blocking by Panamanian ISPs. This has repercussions far beyond Panama’s borders. A client using Voice over IP in a country outside Panama - for example, say he’s in the U.S. - wants to connect with his friend in Argentina. If any of the data from their conversation happens to be routed through Panama, it will be blocked - and neither party is a Panamanian citizen on Panamanian soil. This policy results in a tussle between Panamanian interests and the international community. Neither party should be held responsible for legislation in a foreign country while they are residing elsewhere. This kind of policy must be prevented to avoid further tussles between nations.

1.3 Different Sources of Policy and Law

At the heart of this conflict is the lack of coordination present in Internet legislation. Nearly every national government that has Internet access has put restrictions and regulation on how that access may be used - and due to the international nature of the Internet, any policy they set for their own people may well have an international effect.

Russia is attempting to pass a bill to prevent the Internet from being used to oppose their government (Declan McCullagh, Russia Poised to Re-
strict Net Activities). The affect of this policy removes media from Russian servers that would have been accessible abroad. This has international impact, especially if the same server was also hosting valid material or content for others outside of Russia.

Similarly, China continues to build and maintain a complex firewall, restricting access for its citizens. Opposing this, the US is reportedly debating a Global Internet Freedom Act, aimed at negating government censorship worldwide (Michael Grebb, China’s Cyberwall Nearly Concrete). This is a tussle where two countries, Russia and China, have chosen to censor material, and the United States is drafting policy to counteract the censorship outside its borders.

These three examples demonstrate just how little communication there is between national governments in the field of Internet Regulation, as well as how much cooperation appears to be taking place. As events currently stand, any government with a desire to exert control over its citizens’ Internet rights is able to do so, but more often than not the regulation has an additional effect outside their borders.

Despite the nature of the Internet, which de-emphasizes the physically bounded world in favor of a boundary-free virtual world, national governments are preserving the concept of sovereignty as justification for their Internet regulation. This is responsible for the sheer difficulty in cooperation that makes joint regulation of the Internet so difficult. Since any law that is passed with the intent of being limited to the local must now, through the Internet, has the potential to cause international tussles requiring international intervention.
The disparate nations have differing positions on key issues such as censorship, and those positions influence the national perspective on regulation. The fact remains that since every nation is sovereign, reaching a compromise between the majority of them is a nearly impossible feat. So this idea of national power and sovereignty is both a defining factor in shaping the country’s Internet legislation, and simultaneously an element that perpetuates the lack of organization. Since every nation is equally distinct and sovereign, there is no international body overseeing the countries’ policymakers. There is also no overall plan to coordinate the regulation that is put into play or to resolve the conflicts that arise when countries disagree. Unless that changes, whether from one nation assuming power or a new entity altogether being created, the tide of disorganized regulation will not stop.

There are other regulating groups as well, aside from governments. Technically, any group that has the power to enforce policy has the power to regulate. Similar to national governments, these other groups have no binding relation to each other. As separate entities, no one may be termed the overseer of the others. For example, Internet Corporation for Assigned Numbers and Names’s (ICANN) original mission and goal was to create a body to handle DNS entries, overseeing that critical part of the Internet’s structure. The body was supposed to be open to the public so that opinions could be heard and acted upon. Yet in recent years ICANN has failed to present nearly as many opportunities for interaction as intended. The organization has grown in scope over the years, and some feel that ICANN is the de facto government of the Internet. But it is neither dynamic enough nor does it have enough support from the other governments of the world to effect real
2 Overview

2.1 Goal

Given the current state of affairs, then, it is apparent that a new standard needs to be created in order to make sense of the chaotic regulation that is regularly occurring on the Internet.

Initially, our goal was to create a standard of "Internet rights" for all people, where such ideals as universal access, freedom of speech, and other similar threads of thought would be upheld. Much like the Association for Progressive Communications (APC), we had hoped to create an international, universally enforced and supported bill of rights that would ensure that future regulation would not infringe on these basic Internet rights. Enforcement, we believed, would be brought about by an international body that mandated policies that superseded national sovereignty, and therefore would insure that such rights could be upheld equally and consistently.

Our ultimate goal still remains the same, but after analyzing previous efforts to establish standards on the Internet and international standards in general, we realized that our original conception would not work.

2.2 Precedents

There have been many previous attempts to lay international standards involving the Internet, with varying degrees of success. One of the more
effective organizations, the International Corporation for Assigned Names and Numbers (ICANN), is dedicated to "coordinat[ing] the assignment of... Internet domain names, IP address numbers, protocol parameter and port numbers, [and] coordinate the stable operation of the Internet’s root server system" ("ICANN Homepage"). In effect, they manage the smooth operation of the Internet because they provide unique global identifiers for websites everywhere. Undoubtedly they have indeed established guidelines for the international community to follow, mainly because the continued smooth operation of the Internet currently depends on their cooperation. Unfortunately, this causes the alienation of parts of the Internet community. Recently, the main reason for ICANN’s unpopularity is their decision to eliminate at-large committee elections (Kettmann, Steve. "ICANN Nixes At-Large Reps"), their lack of transparency, and their general lack of accountability if they choose not to take the advice of their committees (Klein, Cyber-Federalist Paper 14). Although not much has been said in defense of ICANN’s somewhat inscrutable administrative procedures, ICANN tries to explain their decision to eliminate the at-large committee elections as a move to give governments more of a say in the running of ICANN. Apparently, governments are now beginning to take an interest in their territory, and are recently starting to limit the power ICANN can wield. Andy Muller-Maguhn, a European at-large representative on the ICANN board comments, "...there is a major shift making the governments a much stronger part of ICANN and reducing at-large input to a quite unspecified role" (Kettman).

Perhaps even more troubling than the idea of ICANN running without accountability is the idea that ICANN’s mandate may be reduced to little
or no influence in the future, a possibility mentioned by Michael Geist, an Internet law expert at the University of Ottawa Law School:

ICANN is facing battles over its ability to run the domain-name system from a number of fronts, which all boil down to greater governmental involvement. I expect things to come to a head in North America at the ICANN meeting in Montreal in June 2003, when it seems likely that it will have its mandate severely curtailed if not eliminated (Kettman).

However, it still remains unclear how much power ICANN yields at this point because their records are not very transparent, and what information is made public tends to be buried in reams of overly bureaucratic paperwork—an impressive feat, considering it is all online.

Another influential organization, WIPO, has successfully set themselves up internationally as the arbiters of domain name disputes. Although officially declared as an intellectual property protection organization, WIPO initially targeted "cybersquatting" cases on the Internet in an attempt to reduce domain name abuse in general. Lately, however, WIPO’s arbiters have begun to expand beyond those parameters to protect existing copyright trademarks. By often working closely with ICANN (Macavinta, Courtney. "WIPO Domain Proposals Coming") and consistently ruling in favor of large businesses (Livingston, Brian. "Groups Cite Bias in Domain Name Arbitration"), WIPO is fast becoming the predominant domain name arbiter in the international community. However, much like ICANN, their dominance comes at a price. Both organizations have been accused of losing sight of their original intention: "Under the Uniform Dispute Resolution Policy adopted by ICANN’s board, trademark owners can only take away names that some-
one else is using 'in bad faith.' A sign of bad faith is registering a name 'primarily for the purpose of selling' it to a trademark holder’ (Livingston). Recent trends seem to suggest that WIPO is trying to expand its definition of "bad faith" beyond cybersquatting:

In the first half of 2000, WIPO awarded plaintiffs 84 percent of the names they sought. By contrast, another arbitrator, eResolution, awarded plaintiffs only 47 percent of the disputed names it ruled on.

Plaintiffs are allowed to choose which provider will decide their case, and the wind is shifting. In the first quarter of this year, WIPO received only 46 percent of the cases submitted. By the second quarter, WIPO was processing the majority: 54 percent (Livingston).

This expansion of arbitration boundaries has many on guard, costing WIPO trust from parts of the Internet community. WIPO argues that through this expansion, they are moving closer to their chartered intention: to foster intellectual property rights protection internationally and help in establishing a copyright standard ("About WIPO"). They have taken a large step towards that ideal, working with many nations to secure the WIPO Copyright Treaty at Geneva in 1996, which outlines the scope of copyright protection and lays down guidelines in dealing with more recent, controversial types of patents, such as computer programs or databases. It also attempts to address the general impact of current technology upon copyright protection today ("WIPO Copyright Treaty").

WIPO’s mission to harmonize copyright and patent protection has not been without friction, however, as many developing countries have raised objections to the recent WIPO Patent Agenda: "...several developing countries
said they were not prepared for harmonization of the international patent system based on a one-size-fits-all model that ignores the needs and interests of developing countries” (Oh, Cecelia. "Warning over Patent-harmonization Approach at WIPO"). Mainly the specific objections seem to call for more deliberation on the matter rather than accusing WIPO of overstepping its boundaries. Given more time, the Patent Agenda will likely go through with little problem. However, this does point out the widespread impact WIPO has over both nations and individuals, since domain name arbitration and intellectual property protection—although related—affect people on different levels of authority. One affects people on a policy level, the other affects them on a more personal basis. It is quite possible that WIPO is overextending itself and is trying to place too much under its jurisdiction. Although they seem quite capable of handling the tasks they have set themselves, it does call into question whether they should be handling this much power on this many levels of arbitration.

The International Telecommunications Union (ITU), although not as often mentioned in the news as ICANN or WIPO, has had a long and relatively successful career as an international organization dedicated to adapting new technology and establishing worldwide coherent standards on a regular basis. Established in 1865 (originally called the "International Telegraph Union"), its original intent was to "develop a framework agreement covering international interconnection...[decide] on common rules to standardize equipment to facilitate international interconnection, [adopt] uniform operating instructions which would apply to all countries, and [lay] down common international tariff and accounting rules” (ITU history). Today, the ITU continues
its mission on a broader scale, creating and maintaining telephone, radio, and space telecommunication standards internationally. They also have enjoyed the backing of the United Nations since the United Nations’s creation, becoming a UN agency in 1947 (“ITU Overview — a History”). Over the years they have shown themselves to be consistently effective at setting standards and advancing the minimum bar for telecommunication services around the world. They have successfully expanded the scope of telecommunications services slowly but surely to adapt to new technology at a surprising pace. Perhaps their only major problem currently is the fact that they only meet once every four years (“Constitution of the International Telecommunication Union.” Chapter I, Article 8-1), a pace too infrequent to keep up with the frenzied speed of today’s Internet technology development.

When talking about international standards and rights, one cannot forget about the United Nations itself. Over the last sixty years it has successfully established itself as the worldwide authority on human rights, and has set the minimum bar on human rights for all nations to follow. They were established in 1945 "when the Organization’s founding nations resolved that the horrors of The Second World War should never be allowed to recur” ("The United Nations and Human Rights"). One UN agency in particular, the UN Commission on Human Rights, is now considered the "main policy-making body dealing with human rights issues” ("The United Nations and Human Rights"). Depending on the General Assembly for the enforcement of their resolutions, the representatives of fifty-three member nations on the Human Rights Commission collectively agree upon and create human rights constitutions and investigates violations ("The United Nations and Human Rights").
Based upon their previous record, this commission has consistently raised the minimum standard of human rights, ensuring that while governments of each nation determine how to implement those rights, each nation is still held responsible for upholding them. It is to this model that our proposal aspires.

Surprisingly enough, the push for Internet rights, mainly spearheaded by the Association for Progressive Communications (APC) and the UN, has been in existence for at least a decade. Founded around 1990, the APC quickly declared its mission to spread Internet access beyond the hands of governmental agencies and provide a low-cost, simple method of connecting to the Internet. However, with the explosion of popularity that the Web generated, the APC was unable to compete with commercial providers: "Commercial providers were able to quickly undercut the prices of APC members, turning Internet access into a low cost, generic service" (Surman, Mark. APC Annual Report 2000, p. 47-8). Currently, the APC now focuses their efforts on spreading awareness and training on the use of the Internet, as well as continuing their push for universal Internet rights: "We in the APC believe in the Internet as a medium for the free expression of opinions; we work against censorship and the filtering of content, at the same time as we strive to facilitate a wider and strategic use of the Internet for social justice by providing information on technical possibilities and tools" (Hackenthal, Stefan. APC Annual Report 2000, p. 9). Their push seems to have waned in recent years, mainly due to accomplishing their central goal of securing widespread access to the Internet. These days, they are focused more on bringing Internet access to those who have not yet joined the information superhighway.
than in concretely securing Internet rights for those who can already connect to the Internet.

2.3 Feasibility

In light of these precedents, it seems clear that merely creating a full-blown Internet rights organization and giving it absolute power over nations is not a feasible plan. It takes time and effort for a new organization to build its identity and reputation before it can gain the trust needed from nations in order to implement their policies. Consider the United Nations, which was established in 1945 to uphold human rights and punish violators. Today the UN holds considerably more prestige and influence than it did at its conception, but violations continue to occur, and the UN still has a long way to go before it can say that it has reached its goal. Similarly, any new organization established to uphold Internet rights would have the same uphill battle to face, and progression would not be immediately apparent.

It may be more feasible if Internet rights were handled by a preexisting, established organization rather than starting a new organization or adding another random acronym to the list of international (but not necessarily effective) organizations already in place. The organization must have the sufficient reputation and influence to implement our proposed steps, but also have garnered enough support and collaboration with the nations of the world so that the resulting ”Internet bill of rights” will not simply be mandated in a dictatorial fashion.

ICANN has been able to decree their policies in the past mainly because
it is a non-profit organization that, to some degree, the Internet depends upon to function. Thus, this gives it considerably more leeway in its actions, although it is still unclear how much power ICANN actually wields independently. Currently, Internet rights are not essential for the Internet’s continued functionality, and so cannot be quickly established in the same way. Furthermore, ICANN is not equipped to oversee a rights-based system; their primary function does not have anything to do with rights enforcement. Although ICANN is independent and, therefore, may be considered "objective," their name does not carry as much prestige and recognition as the UN. Their notorious record for non-transparency would also handicap their ability to sustain a rights-based system without having their credibility questioned.

While it is true that WIPO runs a similar model to our proposal, the organization mainly focuses on intellectual property rights as opposed to access rights on the Internet. One may argue that since both are rights, it makes perfect sense to put access rights under their jurisdiction as well. However, intellectual property rights have a different purpose than access rights—while access rights mainly focus on keeping access to information as free as possible (depending on the country), intellectual property rights seek to restrict access (or, at the very least, replication) to a certain expression of an idea based off of the intentions of its creator. This leads to very different policies and methods of dealing with violations, which may put WIPO at a disadvantage in enforcing Internet rights. Human rights may be a closer analog to Internet access rights, and so perhaps the United Nations Human Rights Commission may be closer to the ideal our proposal seems to call for. While WIPO may be able to adapt to the demands needed to success-
fully manage an Internet rights organization, there are other closer-fitting organizations existing that may be better suited for the job.

The APC, the United Nations, and the ITU probably come closest to what our proposal wishes to accomplish. Their efforts to uphold Internet rights or institute consistent international Internet and telephone standards illustrate that they are already have been somewhat successful at implementing their ideas and collaborating with other nations. Any existing problems that either organization may have are easily remedied with more cooperation from the UN. Unfortunately, our proposal would likely not be compatible with the APC’s vision of total freedom in terms of Internet access, since our initial proposal implements the use of partial censoring mechanisms. Thus, it would be unlikely for this proposal to garner the APC’s support in this project. The ITU, if it met more often, would likely be able to handle the technical capacity of the proposal and set standards for the implementation of the tools provided for the nations. However, it may not be the best agency to handle the political aspect of Internet rights. The symbiotic relationship between the UN’s General Assembly and the Human Rights Commission would serve as a good model to base our political structure, but the actual political body of the Human Rights Commission is likely not technically savvy enough to handle the issues that will arise from Internet rights specifically, although their general policies in dealing with human rights and their violations is exactly the type of attitude that is needed to deal with Internet access rights. Thus, it would be best if ITU and the United Nations Human Rights Commission worked jointly to support this proposal. Ideally, there would be a technical group in charge of implementing the technical aspect, which would be under
the jurisdiction of the ITU, and a political group from the Human Rights Commission in charge, drafting the policy which would oversee how the tools would be used and investigate violations. The Internet rights council, then, would be composed of both these components together, so that they could meet, integrate knowledge, and come up with a coherent plan. The technical group would have to meet more often than the normal general body meeting of the ITU in order to keep up with technology, but hopefully the overall council would still maintain ITU’s previous record of efficiency and influence while incorporating the UN Human Rights Commission’s dedication to expanding and enforcing rights and freedoms.

Internet rights cannot be truly international unless they have support from a majority of nations, or at the very least, substantial support from many of the technologically advanced nations. Like the UN’s human rights committee, any organization that wishes to push for Internet rights cannot simply write a bill of rights and mandate it to be upheld. If governments do not have any input in the process of determining Internet rights, the resulting push to enforce those rights will neither be effective nor ethical. It is important to remember that international organizations such as the UN are usually composed of representatives of many nations; although they have the power to set down international laws, these laws cannot be and should not be upheld unless nations support them. As it is now, nations can only be ”controlled” through peer pressure from other nations. Trying instead to override national sovereignty would, in effect, extinguish any support or possible effort to create an Internet rights council.

Instead, a bill of Internet rights must come about through collaboration
with the nations of the world. Nations should be able to collectively debate and find a general consensus on the defined Internet rights to which people are entitled. We recognize that universally agreed upon Internet rights are difficult to determine, much less implement at this current period of time. Much discussion and debate must first occur before we can even begin to start listing concrete rights to uphold. We also realize that if we push for too much too soon, we risk losing all support for Internet rights. Thus we have modified our original conception of our proposal.

2.4 Proposed Method of Implementation

On the most abstract level, this Internet rights council will have to convince nations to gradually accept both the idea of Internet rights and the organization as a recognized body to oversee the enforcement and handling of violations of these rights. This will not be an easy task, but by using precedents such as the United Nations Human Rights Committee, APC, and ITU as a model, we know that this is likely the best method of garnering support and cooperation from the various nations.

As for our proposed bill of Internet rights, is currently based on a fundamental principle upon which we hope nations will base future Internet rights. While countries have obviously not met together to agree upon fundamental Internet rights, we anticipate a declaration of the following:

Nations have a right to define their own Internet policies. However, this does not mean that they have the right to affect or hinder access to information for people of other nations who have no such restriction.
Thus, our fundamental policy is as follows:

Anything can be broadcast or made available freely on the web. However, one’s own personal access to this information is limited by one’s own laws (state, national, or local) and policies.

In effect, instead of challenging national sovereignty, this implementation will instead work with and reinforce it in order to encourage countries to uphold Internet rights within their own borders. At the very least, this will keep Internet rights violation effects localized, so that one country’s regulation will not spread out to affect citizens in other nations. This will make it easier to deal with if or when problems do indeed arise. Thus, when problems arise they will be more easily dealt with and resolved. Adoption of this proposal will be more likely if our policy does not threaten their sovereignty and offers flexibility in implementation.

Another incentive for nations to cooperate is the technical benefits gained through our implementation. Judging from previous experience, legislation based solely upon policy would likely be ineffective or have unintended consequences. Thus our proposal also involves providing nations with tools to help enforce their own Internet laws within their borders and assists the Internet rights council if a nation fails to comply with the standards set in Internet bill of rights. However, our implementation will concentrate on the receiving end of an Internet connection, such as browser software, rather than the transmitting end, such as servers. By doing this, we do not have to try to shut down servers or force search engines to bypass certain sites. Instead, the nation in question can simply have levels of “clearance” for internet access. In essence, anything can be broadcast freely (as long as it is legal in its own
country), but only those with a sufficient access level can see it. Only those specifically "forbidden" to see it are actually blocked from those sites; anyone else is free to access the material at any time. This of course will require pooling together a myriad variety of technologies and, most importantly, a method of identifying a connection by country. After all, if one cannot determine from which country an information request is coming from, then one cannot determine their so-called "security clearance."

Naturally, technology alone cannot solve the problem. Left alone like this, such tools are more likely to be abused rather than used to encourage Internet rights. Thus, our proposal also calls for the formation of a council of informed representatives from member countries to handle access implementation policy. Of course, if this subcommittee is joined to ITU and the Human Rights Commission, the representatives would already be there, although more (or different ones) can be elected or appointed if need be. Once all the representatives are assembled, however, they will be able to discuss Internet rights among themselves, determine which are acceptable to implement, define what rights violations entail, and judge which restrictions cannot be put into place. Essentially, this representative body will be continually determining the minimum bar for Internet rights. Furthermore, it also provides a forum for governments to negotiate if an Internet rights violation does occur; the countries involved in the violation can try to resolve it between themselves first before calling in arbitration either by a third impartial country or the whole council in order to resolve the issue.

In essence, the purpose of the political component of our proposal, namely, an Internet rights council, is to foster communication between countries and
establish a grounded set of Internet rights parameters for the international community to uphold. The technical component is intended to allow flexibility for each nation to decide how they wish to implement Internet rights within those parameters. If nations wish to grant further Internet rights to their citizens above and beyond the initial minimum level, that is certainly to be encouraged. However, they should at the very least support the minimum; hopefully, like the UN, fellow nations’ peer pressure will aid in enforcement of these policies.

2.5 From the Implementation to the Ideal

At first glance, this implementation may seem somewhat counter-intuitive. After all, the technological aspect proposes to separate out countries on the Internet, while the policy aspect proposes to bring them together. They appear to be accomplishing different and possibly conflicting objectives. It also seems that to prevent the proliferation of current regulation, our proposal is advocating instating even more regulation on top of it. Is this really the path to Internet rights?

The answer to this question is twofold. First of all, the two components are not at odds with one another. On the contrary, both aspects actually depend on each other in order to work. Without the technological capacity to enforce what laws the Internet rights council enacts, the council would be little more than another international organization like those already in existence. It would become a redundancy in the hierarchical structure of the ITU and, by extension, the UN. In order to break this pattern and avoid the
mistakes of the past, this council must be able to provide the tools necessary for countries to enforce their own laws without affecting the citizens of other nations. Only after we have achieved this can we start thinking about raising the bar of Internet rights overall. Conversely, without the internationally represented council to oversee the implementation of the technology, as stated earlier there would be little chance of these tools being used to uphold Internet rights. Rather, they would likely be used to stifle them, since there would be no checks in place to make sure that this technology would not be abused. Certainly one could argue that someone somewhere would figure out how to break it, but even if they did, we still would not be any closer to establishing guidelines to protecting Internet rights unless we had a UN-like structure in place to systematically enforce it. The only other alternative in that scenario would be every person for themselves. The technologically savvy might be able to circumvent the restrictions, but most people would still be stuck behind the metaphorical (or, in some cases, literal) firewall.

As for the objection that this proposal will only heap more regulation on top of current regulation, one must look again at the purpose of the council to be established. The Internet rights council will provide governments with a framework to enforce their own laws more effectively within their own borders, which would leave them with no reason to continue with heavy-handed or haphazard regulation of their own. Indeed, in order to receive cooperation to implement the more efficient technology, the country in question would have to cease making or supporting such laws in the first place. Thus the inefficient and unpredictable regulation is weeded out, and more efficient and specific regulation takes its place. Furthermore, the real enduring purpose
of the Internet rights council is to ensure that each country’s Internet laws do not violate the minimum standard of Internet rights that all the member nations agreed upon. This is not just layering regulation on top of more laws, but rather an attempt to clarify and uphold a standard that is sorely missing on the Internet today.

It is time to stop thinking of this tussle as a war. It is not simply a case of “us vs. them” where there are people who wish to preserve rights and others who want to take them away. Policy is rarely ever that simple. By providing the tools and the framework to efficiently and specifically enforce regulation on the Internet, this proposal is providing a way for nations to work together to finally decide upon universal standards for Internet rights.

3 Policy

3.1 Proposal

The establishment and preservation of human rights on the Internet is an ever-pressing necessity; it is also an inevitable part of the Internet’s future. However, in order for the Internet rights to be established, two things must first be created: a governing body comprised of representatives from every nation with Internet accessibility and a policy for overseeing the control and enforcement of Internet laws and regulations. A governing body of national representatives as well as a policy designated to outline Internet regulation standards is vital for the creation and enforcement of human rights on the Internet throughout the world. Lawrence Lessig boldly said in his book Code
and Other Laws of Cyberspace the nature of Internet regulation, ”Regulation does not need to be perfect to be effective” (173). However, Internet regulation is necessary in order to preserve human rights on the Internet. This notion of human rights remains at the heart of our Internet regulation proposal. No Internet regulation policy on a worldwide scale will be perfect. However, our policy, which is based off of the successful aspects of previous Internet regulation attempts, will succeed in keeping the Internet a safe haven for the free exchange of ideas and information and safeguard basic human rights while working to raise the standard of human rights on the Internet for all countries.

3.2 The Establishment of the United Nations of the Internet

Before human rights on the Internet and even before any policy for Internet regulation can be developed a governing body must first be formed that is responsible for negotiating and defining human rights on the Internet and a policy for regulating and enforcing these rights. Representatives from every country with access to the Internet must unite to form a committee responsible for supervising Internet regulations and the enforcement of Internet laws. We shall call this committee the United Nations of the Internet, or UNI. The primary responsibilities of the UNI will be: defining Internet regulation policies, enforcing the Internet regulation policies, and providing a forum for joint conflict resolution. The foremost priority of the UNI is to establish basic human rights on the Internet. In order for this to happen,
then UNI must first define the policy that will be used for regulating the Internet. This policy should serve as a building block for all other activities conducted by the UNI. This includes not only a policy for monitoring and controlling Internet regulation by various countries, but also includes a policy for enforcing this policy. The second responsibility of the UNI is to supervise Internet developments and activities and enforce Internet access policies on a global scale. Finally, the UNI must also provide a forum for joint conflict resolution, not only between disputing countries but also between countries and their citizens when civil unrest due to Internet policies arises.

3.3 Human Rights and Internet Access

After a United Nations of the Internet committee has been created, the next step necessary for effectively promoting human rights on the Internet is the conception of a policy that governs the control and division of power over the Internet. This policy must specifically address three key issues regarding Internet regulation before any additional regulatory guidelines are engaged. The first issue is the right of the governing body of a country to establish laws and specific regulations of Internet use within their borders. The second issue is the right of an individual to access and use the Internet while abiding by the laws of the country. Finally, the last issue is the right of an individual to make information openly available on the Internet as long as it does not violate the regional laws.

Internet access policies created by the UNI will have to cover two different divisions of Internet standards in order for the promotion of human rights
on the Internet to be effective: the supervision of Internet regulation and
the enforcement of the policies established to protect and promote human
rights on the Internet. Even though the two divisions cover separate aspects
of Internet policies—one covers the rights to specific Internet uses while the
other defines a clear and agreeable set of guidelines that creates a system of
checks and balances upon the power or countries to regulate the Internet—both
are imperative for the promotion of basic human rights on the Internet. The
effectiveness of the regulation scheme is dependent on both solid policies and
the degree of cooperation by all countries participating in the United Nations
of the Internet. Without a policy for enforcement a policy for Internet access
would have no influence and without a policy for Internet access a policy for
enforcement would be void.

The first topic that our policy for Internet access and the supervision
of regulation on the Internet must address is the freedom of countries to
designate specific regulations on the Internet within their borders as long
as these regulations do not infringe upon the basic human rights. Each
country will have the right to direct activities on the Internet based on the
laws defined by the governing body of the country. While every country
has the power to make the Internet a freely open space for the exchange
of ideas and information or the ability to restricted the space of electronic
communication, it is essential that a country’s regulations do not extend
beyond its borders and that they do not infringe upon the basic human rights
of every Internet user. This guarantees two things. First, it guarantees that
individuals will not lose those their basic rights granted to everyone on the
Internet. Secondly, it guarantees that citizens of one country will not be
affected by neighboring or even distant counties’ regulation of the Internet. With this point in our policy for Internet asses and national regulation, we can avoid trying to reach the unattainable goal of agreement between every country for any one piece of legislation while simultaneously preserving each nation’s ability to determine what content is viewable within their borders.

The second topic that our proposed policy must address is the freedom for individuals to access the Internet and the degree to which this freedom may be restricted by governments. Governments may not legislate Internet restrictions of access if the legislation infringes upon the basic human rights of the Internet. Every individual, business, or organization will have the right to gain access to the Internet provided that they abide by the laws and policies of their respective regions. Therefore, the laws of the regions, whether they are the state, country, local, or national laws, must be publicly available for examination and review by any individual who uses the Internet. The Internet as an entity should be accessible to anyone and everyone who has the means to do so, but only as long as they obey all Internet laws that are applicable given their physical location. Therefore, our policy allows for flexible Internet regulation while still guaranteeing maximum accessibility for any given person in the world and maintaining a standard of human rights on the Internet.

Similarly, any individual or organization will have the right to broadcast information and ideas freely but, of course, regional laws apply to this right. For example, if a server is broadcasting propaganda that is banned in the country where the server is located, the government of that country has the right to demand the removal of the propaganda. On the other hand,
if the server is located in a county that allows the propaganda, no other countries reserve the right to demand the server to remove the material or shut down. The other countries may however, prohibit Internet users within their country from accessing the propaganda. Once these three necessary points have been established the UNI should then address any other issues they feel are necessary in order to create an adequate policy for control.

/subsectionEnforcement of Human Rights on the Internet

The next step the UNI must take is to formulate a policy for the enforcement of the controls, regulations, and most importantly, human rights on the Internet. It is critical that this policy be clearly defined and understood by every country so that it may serve as an appropriate system to supervise Internet rights. Thus, without an effective means of enforcement, human rights standards on the Internet and even regulation will never succeed and any policy for governing access to the Internet will be useless. Therefore, a policy for enforcement of Internet access must address three main sub-policies if the Internet is to become a regulated virtual environment that guarantees basic human rights to all users. The first would be a policy for joint conflict resolution, followed by a policy for the reprimanding countries that are violating human rights standards by over regulating or restricting access to the Internet, and finally a policy for the handling individual violators of national Internet laws and policies.

One of the benefits of having the UNI to supervise Internet regulation and a mutually agreed upon policy for enforcement human rights standards is that an environment for joint conflict resolution can be fostered that will allow for a speedy and efficient means for negotiations and resolution between
disputing countries. Through negotiations and conferences between disputing conferences, the UNI can append new policies or amendments to preexisting policies to both the enforcement and control policies. Such developments will serve to foster a free but non-abused cyber world. This will help bring an equal and higher standard of freedom on the Internet to all countries and individuals alike.

However, a policy for enforcing human rights standards and governing Internet regulation made by countries will not be complete until it outlines a method of action to supervise the enforcement of Internet regulations on individuals who are in violation of national Internet control and regulation policies. This policy should first give the governing bodies of countries the right to enforce their particular Internet regulation laws and policies, as long as these policies are just, by means they deem necessary. Since the Internet laws of one country shall not be applied to Internet users outside of the country’s borders, a country has the right to only enforce their Internet laws on individuals who are in violation of that country’s regulatory laws if they are within that country. This means that if an individual is broadcasting material that is in violation with the Internet laws of a country while located outside that country’s borders, the country has no jurisdiction to prosecute that individual. The country whose laws are being violated may, however, ban that material from being accessed by its residents and punish those who do access this material from within its borders.

After the policy for enforcing human rights standards on the Internet and governing regulations on individuals while still giving governments the power to make their own enforcement laws, the UNI must then stipulate
that governments make their laws clear and commonly know amongst all Internet users. This means that Internet users must be aware of the laws and regulations that are applicable to them while within the borders of a given country and that these users are also aware or the means the country will use to enforce their laws and regulations. In order to do this, the UNI will maintain a website that provides every country’s Internet laws and policy for enforcing these laws. Finally, the UNI must define a policy to handle governments that infringe upon human rights standards on the Internet or do not adequately enforce Internet regulations and laws amongst their users. If the power of the Internet is being abused in one country in such a way that is negatively impacting the use of the Internet elsewhere in the world and the governing body of that country does not act to prevent or stop this behavior, then the UNI should have the power to intervene and stop the abuse of the Internet. Without such an enforcement policy, the Internet can fall prey to a substantial amount of abuse as the regulatory policies and human rights standards on the Internet will serve no purpose and have no effect.

In order to effectively establish human rights on the Internet and give nations the right to regulate Internet access, the governing bodies of each country using the Internet must unite and form a collective group that, through the exchange of ideas and opinions, will lead to an overall positive development of the Internet and a standard of human rights. This group, which we have been referring to as the UNI, will become responsible for establishing human rights and national regulation of Internet access. Thus, the first step in instituting human rights on the Internet and supervising the control of Internet access is the formation of the UNI, and as such there is an immedi-
ate need for countries to submit representative to collectively form the UNI. Although it may be a bit optimistic to expect an agreement to be reached on every issue involving Internet access and human rights on the Internet, representatives in the UNI and participating countries should follow a simple, yet civil, code of conduct that is reflected in the United Nations. As long as this standard code of conduct is followed, the UNI will serve as a functional body of representatives that supervise over the regulation of the Internet.

3.4 The UNI and Our Policy

Naturally, any policy is only as good as far as it is accepted. Therefore, in order for the maintenance of human rights on the Internet to be successful, we need the majority of countries using the Internet to agree to our policy and submit representatives to the UNI. We can achieve this by getting the countries with Internet access to agree on the need for human rights on the Internet. Then, we get them to recognize our proposal as a potential for adequate and appropriate Internet regulation. Over time, these countries should become more involved with the UNI, and progressively the basis for human rights on the Internet will increase and countries will form an alliance with the UNI. Ideally, the creation of the UNI and the adoption of our policy will become the norm that the countries abide by in order to efficiently function on the Internet.

Because no organization currently exists that carries the full responsibilities that the UNI will carry, we must join with the United Nations and begin to gradually and progressively work towards a common goal. The UNI’s cen-
tral purpose is to promote human rights on the Internet. We envision the UNI to be a part of the United Nations that works closely with the human rights committee within the United Nations. By making the UNI part of the United Nations, it will gain credibility and recognition by countries active in the United Nations. Countries will also be able to depend on the United Nation’s reputation and consistent performance to keep the UNI from abusing its powers. The UNI will also provide a critical service to Internet users regardless of their physical location: it will host a web page containing all Internet laws and policies per country.

3.5 Internet Bill of Rights

Finally, we envision an Internet Bill of Rights that will be accepted by countries within the UNI. Currently human rights on the Internet contrast drastically depending on the social and cultural norms of various countries. Therefore, our Internet Bill of Rights will not initially become part of the UNI and Internet regulation, but our hope is that after the UNI has proved to be a successful form of Internet regulation and accepted by countries globally the standard of rights on the Internet will raise and our Internet Bill of Rights will be incorporated. Therefore, we have established an ideal Internet Bill of Rights that is closely modeled after the Internet Rights Charter of The Association for Progressive Communication. We believe that there are six basic human rights on the Internet:

1. The right to access the Internet and use it for communication.
2. The freedom of expression, opinion, and the exchange of information of the Internet and the protection against censorship against unpopular views, debate, or criticism.

3. The freedom to publish politically and culturally diverse content, the freedom to own and control software on the Internet, and the protection of user rights and fair standards.

4. The right to license and control Intellectual property.

5. The right to privacy and data protection and the freedom from surveillance on the Internet.

6. The right to set and implement technical standards on the Internet.

The long-term goal of the UNI is to establish these rights for all users of the Internet regardless of nationality.

4 The Technology

4.1 On Governance

Laws that attempt to regulate or influence behavior must affect the behavior through a constraining force that acts upon the behavior the law intends to impact. Failing to do so prevents laws from being successful regulators, and hence, worthwhile laws. The Internet world is no different (Lawrence Lessig, "Code and Other Laws of Cyberspace", page 6). Without constraints or a way to influence behavior on the Internet, Internet laws are meaningless.

On the Internet, governmental or institutional law has little impact onto itself. Code is the law of the Internet. Lawrence Lessig, in "Code and Other Laws of Cyberspace", states that the regulator on the Internet is code (Lessig, p. 6).
“This code presents the greatest threat to liberal or libertarian ideals, as well as the greatest promise. We can build, or architect, or code [the Internet] to protect values that we believe are fundamental, or we can build, or architect, or code [the Internet] to allow those values to disappear.”

Code unto itself does not have qualities of good or evil, it is a tool that designed to enforce requirements, or in this case, the laws or policies of the United Nations of the Internet. The laws and policies the code embodies have the clear intent of the regulating bodies, the United Nations of the Internet and the regional governments. They innumerate the rights and policies the citizenship afforded while on the Internet, and code is the tool of the laws and policies (Lessig, p. 93). Laws belong to the real space for citizens and code is the law of the virtual space for netizens.

To facilitate the United Nations of the Internet, code is the faithful recreation of real world laws to manage the traffic of 1s and 0s on the Internet. The symbiotic relationship of code and law, on the Internet, will together provide the United Nations of the Internet the proper tools with which to succeed. The laws explain in spoken word the freedoms. In turn they set the requirements for the code, which is the great regulator in the virtual world, explaining to the digits what may be seen and unseen to the real world. And together, they provide a regulable architecture.

4.2 The Regulable Architecture

As it is today the Internet is an open landscape that has proven difficult for governments to control (Lessig, p. 5). Yet to preserve the open and free nature, it must be maintained through governance and regulation. The
regulable architecture is “not just a legal text but a way of life—that structures and constrains social and legal power, to the end of protecting fundamental values” (Lessig, p. 5). Thus, the code that breathes life into the laws and policies on the Internet is born.

In the life of the Internet there have been a number of tools that regulate traffic on the Internet. Some tools attempt to restrict access and the freedoms of citizens, while others attempt to counteract the restrictive forces on the Internet. Three such tools hold the promise, given good policy from the United Nations of the Internet, to enforce the laws of each government, with the ability to grow the Internet rights for all mankind, as nations’ familiarity and comfort with the power and riches of the Internet matures.

4.2.1 Safeweb

The first technology is designed to circumvent attempts to limit a netizen’s rights (SafeWeb, ”TriangleBoy Whitepaper”, http://www.safeweb.com/tboy_whitepaper.html). Private, public, and government institutions, in their desire to control the Internet, have employed tactics such as monitoring, closed networks, or networks protected behind firewalls. SafeWeb offers a technology that circumvents censorship attempts by providing a proxy between a netizen and their target web site. This has proven so successful that institutions have expanded the sites they black list (make unavailable to their constituents) through their firewalls or other means, that SafeWeb servers have also made the black lists.

In the ever-escalating battle for circumventing restrictions, SafeWeb then evolved to include servant machines known as TrianglBoy Volunteers. These volunteers make it wildly challenging for institutions to prevent their netizens
from getting out to the SafeWeb network and again bypassing restrictions (TriangleBoy Whitepaper, http://www.safeweb.com/tboy_whitepaper.html). As of this writing, SafeWeb is no longer in broad use. It is currently only available to Voice of America with the intent to circumvent authoritarian regimes, such as China (Voice of America Works to Circumvent China’s Net Defenses, http://www.freedomforum.org/templates/document.asp?documentID=14785).

4.2.2 Platform for Internet Content Selection

PICS was born from the wish to censor based on type of content. The intent was to protect children and families from objectionable content published on the Internet. From the onset, the World Wide Web Consortium (W3C) and other agencies understood that the international nature of the Internet made regulation at the source difficult (Paul Resnick, ”PICS, Censorship, & Intellectual Freedom FAQ”, http://www.w3.org/PICS/PICS-FAQ-980126.html). The premise being that a server or content provider may is not obligated (due to lack of regulatbility) to heed requests for self-regulation by entities from foreign nations.

As a result, PICS was designed to shift control from a centralized model toward one where individuals, through their client software, would regulate their own access. The intended goal is to shift policy and control to the individual netizen rather than require that institutions regulate access for all (Resnick, http://www.w3.org/PICS/PICS-FAQ-980126.html).

This is achieved through the use of a labeling system which requires that all content be labeled using a standard vocabulary that appropriately identifies the type and nature of the content being requested by a client.
program. On the client, the netizen chooses the type of filtering or censorship they wish based on their personal preferences for the content they want to avoid. This was made possible through client software such as SafeSurf, CyberPatrol, and through implementation of label reading and filtering in common Internet web browsers.

However, this system has not been as successful as SafeWeb has been to empower the netizen on the Internet. PICS has only provided a standard by which labeling, content identification, and filtering would be possible. To that end there are six main components to a successful PICS implementation (Resnick, http://www.w3.org/PICS/PICS-FAQ-980126.html):

1. A clear labeling vocabulary and criteria for assigning labels
2. Assigning labels to content
3. Distributing the labels
4. Filtering software
5. Defining the filtering criteria
6. Installing and running the filtering criteria

However, the PICS architecture doesn’t provide any of the listed components. It only proposes how a system would work when these components are available.

4.2.3 The Domain Name System

The DNS is a universal Internet directory service that primarily provides translation of Internet domain names (netizen readable word-based addresses) to its IP address equivalent (computer readable). In simple overview,
the DNS architecture consists of translation tables, DNS servers, and protocols for retrieving and searching the tables from the DNS servers (Webopedia.com, http://www.webopedia.com/TERM/D/DNS.html).

The DNS has become a vital tool enabling Internet communication and traffic. Without it many netizens would have a difficult time enjoying the benefits the Internet has to offer. Through DNS netizens only need to recall domain names of sites they wish to visit or servers they would like to access. The address www.cs.duke.edu is much simpler and even more meaningful to a netizen than its IP equivalent of 152.3.140.5. The result is each netizen can quickly and easily identify and access virtual spaces on the Internet without being burdened with the computer meaningful IP addresses (DNS Resource Directory, http://www.dns.net/dnsrd).

The downside to the DNS service is that it is geo-politically challenged. The system does not provide association of a domain name or IP address to a geographic region on Earth. It is only cognizant of the Internet geography. It does this through master servers that contain all Internet address space information that propagate them through a hierarchy of DNS servers as translation requests are received, until a netizen’s machine is the ultimate recipient of the request it broadcast to its assigned DNS server. Geo-political information is not a part of the service. So when a request from a particular netizen is received, the service is unable to identify the location on Earth the request came from or where the target address being translated is physically located.
4.2.4 The Solution

Using available technologies as a basis for the regulable architecture will facilitate adoption and implementation. It eliminates the need to create a new set of systems from the ground up to layer over the Internet. With Internet usage growing at a rapid pace and with a current installed base of nearly 1 billion netizens (Global Reach, http://www.glreach.com/globstats/) it would be resource prohibitive to attempt to radically change the technology of the Internet to promote Internet rights.

Taking advantage of the basic services the three technologies discussed offer, a comprehensive system for maintaining and, through effective policy, growing netizens’ rights is possible. The resulting architecture would be a composite of the benefits of SafeWeb, PICS, and DNS while addressing their deficiencies. The composite would be known as SafePICS with eDNS. It will have a modular framework to fit the unique needs of the distinct nations and regions of the world. The philosophy being that one size does not fit all and through a scalable permissions framework, the desired level of robustness and resilience would be attainable by region. This also acknowledges the fact the nations of the world have different resource levels available and may not be able to dedicate much to maintaining a complex system.

To maintain effective technologies and ensure successful implementation of drafted policies and laws, the United Nations of the Internet will sponsor tUNI, technologies of the United Nations of the Internet. The group will be entrusted to implement the write laws of the Internet through code. It will also design and maintain the standards required to maintain the efficacy of
the necessary technologies. With this goal it will also evolve the technologies as the Internet evolves. SafePICS with eDNS. At the core of SafePICS with eDNS is region encoding. It is one key component to enabling the real world borders in the virtual world. Existing systems lack it and contribute to the difficulty of regulating the Internet (Lessig, pp. 9-13). The PICS module would be the base of the composite architecture and provides the simplest most cost effective implementation.

With the PICS module governments would be able to provide dynamic access to legal content by filtering out illegal content (see Figure 1). The basis of the system would not be much different than the current PICS standard. An enhancement would be the use of region encoding as an additional category in the vocabulary that is to be implemented with it. PICS is the simplest module available as its filtering component is already implemented in current browsers. The biggest improvements will be gained with PICS through policy decisions to ensure the main six components of PICS are correctly and universally implemented.

The next module that may be overlaid onto PICS is the SafeWeb component which makes up SafePICS. This piece will provide an additional measure of security by enforcing PICS through centralized servers. While PICS relies on client software providing the filtering and enforcing Internet rights, it requires that netizens obey the laws of their land and utilize the proper client software. While it may be a good solution for under-resourced developing nations, it may not be sufficient for larger nations with the desire to maintain better control over their netizens.

SafePICS centralizes control by requiring all traffic to be routed through a
SafeWeb server. This architectural component requires additional resources and must be scaled appropriately to meet the needs of a country. The technical requirements to meet usage demands are recommended by SafeWeb, Inc (SafeWeb, "Sales and Support", http://www.safeweb.com/sales_support.html). Traffic routing to SafeWeb servers would be promoted through laws and policies requiring ISPs within national borders to route all traffic through government sponsored SafeWeb servers within their borders. This, like PICS alone, better manages the international nature of the Internet raising virtual borders that are maintained by each participating nation.

SafeWeb integrates with PICS to create SafePICS through a three-tiered architecture where Internet content selection is mediated at the SafeWeb server level (see Figure 3). The SafeWeb server checks against a national rights PICS server to determine the legality of the content being requested by a netizen (see Figure 2). If the content is sanctioned, then the SafeWeb server will allow and serve the content to the client making the request. Likewise, if the content falls outside the legal parameters established by the homeland, the server will appropriately notify the requester and disallow access.

SafePICS grants nations and regions two additional benefits. The first is the use of the standard PICS clients. If netizens wish to use their regional PICS client enabled software, it allows them further filtering. This continues on the original intent PICS was designed for, personal censorship preferences. It may also be further expanded to any scope between the individual netizen and a national scope, allowing for sub-regional access controls at the client level, Region encoding within the client may be modified accordingly to meet
sub-regional needs.

The second benefit SafePICS offers a nation is the ability to manually override permissions to specific content. This particular feature is special that gives nations a tool to better handle compliance issues on their own. Through black listing or white listing of particular content a nation is able to address poorly labeled content and therefore allows or disallow content. It is also a method to regulate the content providers or offending nations into compliance with Policy for Enforcing Human Rights Standards and Governing Internet Regulation of the United Nations of the Internet. It provides a temporary measure until conflict resolution through the United Nations of the Internet yields a binding decision between the disputing parties.

The final component to the proposed SafePICS with eDNS architecture is the eDNS module. eDNS further enhances the overall SafePICS architecture by further enforcing regionalization. SafePICS manages regions through labels, however, it leaves much to the content provider and their home nation for successful enforcement. eDNS improves the robustness of region support by adding a region code component to the current DNS service. This one piece of functionality, as stated earlier, is a missing feature in DNS that gives the Internet its trans real world border, international, properties.

With a regional code associated with each domain name translation value in the DNS tables across the world, tracking the origin of content is enabled. This expands upon the white list and black list override option available in SafePICS by more easily granting it at national or regional levels. This gives the United Nations of the Internet an additional tool to enforce compliance to member nations. Beyond compliance enforcement, it also allows non-
authoritarian nations a way to allow their netizens full access to the Internet, while allowing sub-regions and netizens more control through SafePICS.

4.2.5 The Implementation

Universal implementation of SafePICS with eDNS will be contingent on the successful formation of the United Nations of the Internet and on the sponsorship of technologies of the United Nations of the Internet to help define universal conventions.

The weakest link of SafePICS with eDNS is the PICS module. To remedy this issue tUNI must work closely with the United Nations of the Internet committee to define common policies PICS will manage. This includes defining a clear universal labeling vocabulary and standardized criteria assigning labels, distributing the labels across label servers and client software developers, and assisting in defining filtering criteria for member nations. The other components to a successful worldwide implementation of PICS will be handled through assistive policy decisions and learned best practices from the United Nations of the Internet committee that are passed on to the member nations. These best practices and common policies will make possible the local implementation of PICS to successfully enforce rights within the receiving nation’s borders. Through effective enforcement of content labeling, and distributing, installing and running of the client software the system will work as promised for use by the United Nations of the Internet.

Use of SafePICS enhances an implemented PICS module and is contingent on the effective decision and policy making actions of the United Nations of the Internet. Implementation of SafePICS requires that the participating
nation apply the necessary resources fulfill usage demands by deploying sufficient SafeWeb servers. By deploying SafeWeb servers they will also need to regulate their ISPs to re-route all traffic through national SafeWeb servers with the PICS plug-in. Alternately, if a nation is able to afford a large implementation they could require that all ISP servers within their borders run SafeWeb and have hooks into the ISPs’ software that prevents traffic from by passing their national labeled SafeWeb servers.

Enhancing a SafePICS installation with eDNS gives a nation the greatest flexibility and ability to manage their Internet rights. The successful implementation of eDNS requires an upgrade to the current DNS architecture and all participating DNS servers so that location information may be associated with each domain name entry. tUNI will need to work closely with the United Nations of the Internet and ICANN’s DNS Root Server System Advisory Committee to enhance DNS with regionalization (ICANN, http://www.icann.org/committees/dns-root/).

Once eDNS is available, its use is dependent on the ability of a nation to deploy eDNS capable servers within their borders. Once local servers are available for resolution, a nation is able to manage the eDNS list of resolvable names by overriding entries. The eDNS service would have regional codes available so that incoming requests are identified by nation or region as well as the target address request. Since all IPs would be region identifiable the eDNS servers will be able to enforce requests from their own region and route requests from outside their region to the requester’s home servers.

Overall, the simplest, least complicated implementation of SafePICS with eDNS is one with only the PICS components enabled and relying on client
side filtering and server side labeling. With proper policies from the United Nations of the Internet and tUNI this will be an effective rights enforcement tool available to any nation. If additional features, robustness or rights management is required, the additional plug-ins of SafePICS and eDNS enhance the installation. These incur additional resource expenses to nations and the United Nations of the Internet (eDNS) yet they provide the necessary toolset the United Nations of the Internet to gain credibility and support for a successful governance of the Internet through laws and policies, with code as the regulator.

5 Conclusion

John F. Kennedy once said, ”Our privileges can be no greater than our obligations. The protection of our rights can endure no longer than the performance of our responsibilities.” (Kennedy’s speech May 18, 1963, quotes book, p. 305). Now, forty years later it has become more apparent than ever how we should apply Kennedy’s wisdom in the world of cyberspace. The Internet that we enjoy today will not be the Internet that we will experience tomorrow. Already, different organizations have emerged in the growing wave of attempts to control and regulate the Internet. We are at a crucial turning point in the age of the Internet and if we are not careful to protect what we have worked so hard for and what we so freely enjoy, then the Internet, as we know it today will only be a distant memory tomorrow. Regulation is inevitable, but human rights are necessary. We are simply trying to make human rights a standard and the regulation of the Internet fair and just for
users all over the world. If the responsibility of standardizing human rights and regulating the Internet falls into the wrong hands, the Internet will be doomed and human rights on the Internet will diminish. Therefore, the world must collectively join together to preserve the integrity of the Internet. Make no mistake, no system of rights and regulation on the Internet will be flawless, but we already know that much. Our purpose is not to foster flawless Internet regulation, but rather, to establish human rights on the Internet and work to progressively raise the standard of these human rights.
References


