There is no rulebook for the Internet. No laws. No guide telling us what we can and cannot do. There is only code. Code, the basis of the Internet, dictates what occurs on the Internet (Lessig, 1999). While this allows one person to send an email with a virus attached to millions of people, it also allows an Internet Service Provider to scan for that virus and alert their clients about the virus. That is the beauty of this paradigm. The code can be changed and modified, as needed, by the industry to fit the desires of the consumer (Lessig, 1999). This is the optimal situation to secure the Internet’s future. With the Internet in the hands of industry—those of both corporations and inter-industry organizations—and not governmental (and super-governmental) organizations, it can best continue to move forward to resolve problems such as inappropriate content, Spam, security, and TCP/IP problems.

Code is a word used by Lessig to describe computers and what they allow us to do and not do. While specifically it may only refer to software, Lessig uses it to refer to hardware as well. As used here, it will refer to just that, the hardware and software used to limit and enable access to the World Wide Web and other facets of the Internet. Knowing this, “In cyberspace we must understand how code regulates—how the software and the hardware that make cyberspace what it is regulate cyberspace as it is…Code is never found; it is only ever made, and only ever made by us” (Lessig 1999).
Because the architecture makes the rules, by extension the people who create the architecture create the rules. Companies like Microsoft and America Online, organizations like Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF): these are the groups who make the rules. ICANN has near exclusive control over the domain registration (Watch). While ICANN has come under fire recently for lack of accountability, and potential risks, there is no substantial evidence to suggest that ICANN will misuse their power (Watch). IETF is a body that works to standardize the Internet through a series of resolutions and recommendations. The IETF also provides a “a forum for the exchange of information within the Internet community between vendors, users, researchers, agency contractors, and network managers” (IETF). Microsoft, being the industry juggernaut it is, has the power to set industry standards with no outside input. With the dominating market share, Microsoft figures to be a factor in any technological advance. For various reasons, these groups make the rules. Keeping control in these groups will lead to the greatest success of the Internet. The collective knowledge and experience between the people in IETF, ICANN, Microsoft and others is astounding. To surrender control to a group that, in comparison to these, has little or no hands-on experience, would be erroneous.

Most Internet users gain access via some internet service provider, or ISP. Depending on the ISP chosen, the Internet can look very different to three different people—while the content of the Internet does not change. If one user is using a high-speed connection or a LAN, there may be no filtering of material to the user. He sees the entire Internet and can access every corner of it. A second user may, for instance, use an ISP such as AOL that allows multiple accounts. Each one of these accounts can be
filtered independently. So while one account may be limitless, another may have restrictions placed on various websites or features. Finally, a third Internet user may always connect with a filter because his ISP, PAX for example, restricts all inappropriate websites (PaxWay.com 2004). With options like these, users can choose which one is the best for them. This makes sense as different people in different situations will want and need different levels of protection and restriction.

Spam has become an issue for most all e-mail users. This is a problem the government cannot tackle at the moment. With spammers going offshore (and oftentimes across the ocean) and out of the range of US jurisdiction, Congress is left with no means to resolve this problem. Lessig refers to this problem in his story of a town called ‘Boral’ (Lessig 1999). The town of Boral tries to outlaw online gambling but is unable to because the hosts of the gambling websites just move overseas and are unreachable by the Boral prosecutors. While the government cannot, these companies can. Software, such as “Spam Assassin” offered by many ISPs, has become a popular way to limit spam. Spam Assassin can mark and remove spam mail based on a series of criteria. This method has very high success rates (SpamAssassin 2005). Hotmail, G-Mail and other webmail services have offered similar solutions to limit spam. This kind of approach is a very viable solution—in part because it is the only way—and will allow for more interference free Internet use.

Security issues on the Internet are becoming less and less problematic. With protections, such as Secure Socket Layer, transfer of data can be totally encrypted from the user to the host. This allows submission of sensitive information, i.e: credit cards, without fear of it being stolen. VeriSign, an industry leader in security, regulates SSL
certificates. VeriSign serves as an authority to verify identities of Internet businesses. Customers feel at ease purchasing from a website that displays the VeriSign seal of approval because they know that their information is secure. They know that the website has taken proper measures to ensure that theft will not occur (VeriSign 2005). Since online auctions started, scam artists too started. It is very hard for local authorities to track down online con artists as information is unknown and it can take a while to get to the bottom of the case. However, options arose for both buyers and sellers. PayPal started as a means to pay people online. They offer a security policy in all auction purchases made through PayPal for both the seller and the buyer.

With more people using the Internet and more computers connected to the Internet, the old computer naming system, IPv4, is becoming too small. IPv4 was not made for its current use—it was designed for a closed military network where size and security were not given proper forethought (Pouffary 2000). Sometimes a user is communicating securely with a server and other times it is not. When he is, sometimes it is via SSL and other times via SHTTP. And simply, it does not allow enough addresses of computers through the end-to-end structure. That is why IPv6 is critical. It allows for many more IP addresses making networking issues less problematic. Secure connection is a prerequisite of the IPv6 system. IPv6 can also be more efficient in routing packets within local networks (Pouffary 2000).

All of this is not to say the government has no place on the Internet. After all, it was the government who invented the Internet. And it is not to say that the Internet has run perfectly and the industry has done a perfect job. However, government would not have done any better and likely would have been slower in creating solutions. AOL sees
a demand for increased filtering of content and spam filtering and it releases a new
version rapidly to meet the consumer’s demands. It receives immediate financial
compensation for making the changes before other ISPs. To have the government try to
fix this would have taken an act of Congress or at least a massive petitioning effort to the
agency charged with Internet oversight. And with a lack of oversight, it is possible for
companies disproportionately influence the process of change. But this is still a better
alternative to a slow government-lead system. While Microsoft can quiet smaller
companies opinions, it does so while pushing new ideas through faster. And any idea is
better than no idea.

As problems arise and people become agitated, solutions emanate from industries.
That is very evident in the problems facing the Internet. While solutions are sometimes
not immediately in sight and not immediately available, the industry has provided them in
a way that no other group could have: quickly and efficiently. The industry can modify
the code as it needs and make changes without the end user even noticing the changes
being made. This is the way that changes should be made to fix problems that will
inevitably arise in the future, as this is the way that solves problems most efficiently.
Works Cited


     http://www.ipv6.ru/events/ navbar/birmingham00/presentations/YanickPouffary/sl
     2005.
     http://www.verisign.com/products-services/security-services/secured-
Watch, I. "ICANN for beginners." February 3