Legal Dilemmas in the Digital Age

Connor D. Maag
University of Southern California

In the modern era of cyberspace and technology, advancements pose new threats to legal order. A 2010 census revealed that 2 billion people—over one quarter of the planet's population—use the Internet, communicating and sharing information all over the world. [1] This virtual reality is growing at an incredible rate, yet the laws that govern it are relatively immature and struggle to keep up. In an age of information, one reasonable question to ask is whether Internet censorship and personal freedom can coexist under international law. In contrast to several other nations—even those sharing similar Western philosophy—the United States tends to support the freedoms of speech and press, even when they could pose a threat to national security. Today, this ideal has reached a height of conflict in the new era of technology. Government censorship, copyright infringement and classified document hijacking are now major points of contention over international approaches to cyberspace policy. This article will discuss a number of issues regarding cyberspace and the regulation of this recent and relatively unexplored sector of law, while simultaneously proposing and analyzing solutions to such problems.

A description of cyberspace will lay the foundation to further understand problems in international law regarding the Internet. A range of opinions on Internet censorship will then be discussed to discern under what conditions it may be permissible to censor the Internet. The Pentagon Papers [2] are a case example that provides background in the American struggle to balance national security with freedom of press. Its contemporary counterpart WikiLeaks will then provide insight into modern cyberspace dilemmas. Finally, a discussion of copyright infringement within international law regarding the individual will highlight a holistic understanding of present cyberspace issues.

While the freedom of the press is often regarded as necessary and important, every government simultaneously has an obligation to protect its citizens. Whether it is China's censorship of Google, the WikiLeaks' disclosure of classified documents, or Canada's attempt to tame copyright infringement, nations constantly face the decision to either withhold information for reasons of national security or uphold the rights to free press. [3] This article will explore current debates in the international community about where the line should be drawn regarding national security.

This article argues that it is crucial for international law to promote free speech while maintaining the status of the Internet as a fair, responsible tool for society. At the same time, it is a tool the possesses great potential for abuse

It is crucial for international law to promote free speech while maintaining the status of the Internet as a fair, responsible tool for society

by copyright infringers and whistleblowers. The Internet knows no state boundaries, yet it has the ability to affect every state in every corner of the world. The reason why cyberspace requires a new definition of community is because of the broad-ranging connections that it fosters — evidenced by the 2 billion users each day. [4] In the new era of technology, an international cyberspace body would prove beneficial as a rule-setting and coordinating mechanism to maintain order and create unity under international law.

A central question of cyberspace law is determining who has sovereignty and jurisdiction in a virtual world. The territoriality principle and the effects principle offer two guides on a state's ability to deal with international cyberspace. Under the territoriality principle, a state holds the right to control any and all information entering its borders, and can then choose how to make that information available within its territory. Furthermore, any restriction of a nation's jurisdiction within its territory is forbidden. [5] This principle argues that cyberspace is not an overarching pseudo-state that transcends territory, but rather a communication line that becomes the territory of a nation anywhere within its boundaries.

The territoriality principle has been adopted by China, as seen in its strong regulatory efforts to prevent "detrimental information" from entering its territory by means of the Internet. [6] In 2006, web search engine giant Google expanded offices to mainland China, where it encountered state demands for censorship of online discussion on issues such as Tibetan independence and the Tiananmen Square protests of 1989. [7] It became clear that Baidu, a major market competitor, was given preference over Google under the same domestic laws, and a highly publicized debate over Chinese and American views on Internet freedom ensued. While China reserves the right to censor the Internet within its own borders, there was not even a standard censorship policy amongst different search engines, which Google viewed as an undeniable threat to free press. Google then threatened to stop censoring its search results and demanded transparency from China, and the Chinese media accused Google of imposing Western values on their culture. [8]

Defending China in this situation, it seems only logical that a nation reserves the right to control the Internet within its own territory. However, given the nebulous nature of cyberspace, UNESCO (the United Nations Educational, Scientific and Cultural Organization) takes a different stance. In 2006 UNESCO did not firmly support the freedoms of Internet expression when "[Internet] services are

They [The New York Times] argued that the Nixon administration sought to censor a national, public newspaper and deprive the world of the true and possibly unfavorable details of U.S. involvement in the Vietnam War

used […] to divulge information of a sensitive nature." This stance changed in the more recent UN Budapest Conference on Cyberspace held October 4-5, 2012, when Director for Freedom of Expression and Media Development, Guy Berger, lectured on the current UN position on Internet censorship. He explained that:

"The freedom of speech should not be compromised by measures taken in the name of cybersecurity—whether these measures are against cyberfraud or cyberwarfare. Security online is not a separate world from the world of rights, and particularly it has major bearing as regards to the right to freedom of expression." [9]

China, which is currently a member of the United Nations, clearly takes a rather different stance. Justifying their effort to ensure domestic social stability does not coincide with these positions asserted at the recent UNESCO summit. Berger went further to argue that the freedom of press in modern times is the result of such a hard-fought battle, and that it would be a great injustice to regress by censoring or limiting the Internet. [10] However, even the most liberal of nations, like the United States, do not always agree that the approach to censorship should be unconditional.

In the late 1960s, the American government faced a similar choice to either censor public press—in this case censor *The New York Times*—or potentially endanger national security by allowing the media's release of The Pentagon Papers. The Pentagon Papers referred to an official military-sponsored report on the entire history of American involvement in the Vietnam War. The records contained secret information about the U.S. military, and it was argued that their disclosure to the public (and in turn U.S. enemies) would pose a serious threat to national security. [11] When the Nixon administration found that the documents had been leaked to *The New York Times* and were to be published, the U.S. Court of Appeals for the Second Circuit placed a temporary restraining order on the newspaper to prevent the information from being released. [12] In response, *The New York Times* sued the U.S. government for attempting to restrict its first amendment right to freedom of the press. In a case heard before the Supreme Court, they argued that the Nixon administration sought to censor a national, public newspaper and deprive the world of the true and possibly unfavorable details of U.S. involvement in the Vietnam War.

Supreme Court Justice Black gave the majority opinion that the right to free speech and free press is absolute and should under no

circumstances be violated for stated reasons of national security. In contrast, Justice Stewart gave a dissenting opinion that the dangers of modern (nuclear) warfare should give the government discretion in national security matters. [13] The Court ultimately decided that the Nixon administration did not meet its "heavy burden in order to justify the restraint [on free speech]." [14] The government would have to provide a compelling justification for any potential censorship, and national security in this situation was not a strong enough argument.

Eventually, *The New York Times* did publish sections of the Pentagon Papers [15], but the opinions of Justice Black and Justice Stewart reflect the current debate in international cyberspace law: should governments or Internet service providers censor and regulate content for the sake of national security—do they have any legitimate right to censor cyberspace?

Today, the Internet is our equivalent to the newspaper as a communication medium with national reach. The difference today, however, is that a government's ability to block publication is severely limited when information and digital media can be spread around the world in seconds, with one click of a mouse. [16] This is precisely what happened in the WikiLeaks case.

WikiLeaks is a self-proclaimed whistleblower website, begun in 2006, that obtains and publishes classified government information on the Internet. Founded by an Australian and based in Sweden, the site claims that its purpose is to expose corrupt regimes primarily in Asia, the Middle East, and Africa in order to promote a more open and democratic world. [17] On the one hand, the site upholds and promotes the importance of free press by exposing corruption worldwide. However, the disclosure of military intelligence can be dangerous and frustrating for national governments, especially during armed conflict. The United States has utilized the effects principle in its legal response to WikiLeaks, because it claims the actions of the Swedish website pose a threat to American security.

Dubbed the "Afghan War Diaries," WikiLeaks published hundreds of thousands of classified reports on the United States' military activities in Afghanistan in 2010. [18] The most controversial aspect of the documents' publication was that the armed conflict was still occurring, and the reports may have offered valuable information to U.S. enemies on everything from base camp locations to troops' daily routines. Private First Class Bradley Manning (now standing trial for the release of classified documents to WikiLeaks) allegedly provided vast amounts of additional classified military information to the site, which was subsequently published. [19] Ironically, *The New York Times* collaborated with the Obama administration to determine which information might threaten national security before they published excerpts of the reports as well. [20] It is not surprising that the U.S. is angered over the situation, as the document leaks could prove a danger to national security, American diplomacy, and the status of conflicts in Afghanistan. Moreover, it should also be noted that once documents are leaked onto the Internet, there is no retracting the information. [21]

The Obama administration's vigorous response to the WikiLeaks case has attracted its fair share of supporters, including Senator Diane Feinstein of California who argued that

Julian Assange, the founder of Wikileaks

Attempting to re-classify already disclosed documents is essentially futile, as the initial action cannot be reversed

The World Intellectual Property Headquarters in Geneva, Switzerland

WikiLeaks founder Julian Assange is just an "agitator" of armed conflict, who contributes to violence more than to fixing the world's problems. On the other hand, advocates for absolute free speech like Justice Black in The Pentagon Papers case would probably argue that WikiLeaks is just another, more extreme exercise of the right to publish even classified information for public knowledge.

In congruence with UNESCO and the rulings in the United States to uphold free speech over national security, why should all information on the Internet not be free and allowed? Do all people reserve the right to knowledge and can they be trusted to responsibly use their right to free press? In order to better understand the effects of cyber freedom and the problems related to free press, the next section of this article examines the issue of copyrights under international law.

In addition to the debate over national security and free speech, the other prevailing topic of legal debate in cyberspace is between copyright protections and free speech. Current law struggles to address how to properly govern online activity, which infringes on copyright protections while simultaneously upholding individual rights to free speech and free press. [22] The Internet is permanent; once copyrighted or classified information is disclosed, it is usually irreversible and can spread rapidly across cyberspace. [23] The problem is that once a document is released, there is no telling when and where it has been copied or who has seen it—the copyright is effectively rendered useless. For a copyright owner, the ability to exclusively possess and distribute digital material for commercial profit is arguably the reason for a copyright in the first place. [24] One scholar, Alejandro Zentner from the University of Texas at Dallas, shows in a 2006 study that sales of copyrighted material have decreased dramatically, and Internet users have become 30% less likely to legally obtain music since the emergence of Napster in 1999. [25] This drastic increase of copyright violations over the Internet is of great importance to the issue of property rights and shows an imperative need to address cyber theft.

When people have the right to publish what they please, they may also distribute information and digital media that they do not own. People have the right to secure their own creative property and ideas through copyrights, but the current infrastructure of the Internet and file-sharing websites make effective copyright protection difficult. Countries must create a way to balance this dilemma between personal property and illegal publishing online.

One of the first attempts to do so was

the implementation of the Berne Convention of 1886, a multilateral treaty among 166 nations, which specifies international copyright protection for literary and artistic works. [26] This convention has since given birth to the World Intellectual Property Organization (WIPO), a United Nations agency dedicated to the protection of intellectual property through copyrights as well as trademarks and patents. [27] Although these conventions boast a large consensus on cyber copyright, cyber theft still remains prevalent, and it is often credited to a method called file-sharing. [28] Within the United States, the Napster case set an important early precedent, as it introduced the file-sharing programs so prevalent today. [29]

Napster is often credited as the pioneer of file-sharing websites for illegal music downloads and cyber theft, and left a legacy in cyberspace copyrights that will not soon be forgotten. The site does not actually send copyrighted files to other users, but rather connects the files of all users who are simultaneously logged on the site and allows users to download them. [30] This scenario, harmless by definition, most often results in users sharing copyrighted materials such as music, software and films. In fact, when the site was operating in 2001, one survey showed that 87% of shared files on Napster were copyrighted music. [31] Unsurprisingly, Napster was sued by major record companies, but the legacy of the story lies in the Supreme Court's ruling that a website cannot be held liable for contributory negligence merely because the system allows for misuse—for example, Napster's potential for copyright violations. [32] The Napster case also set precedent that a search engine (defined as anything from Napster to Youtube to Google) must be put on notice for specific instances of copyright infringement before they can be held liable for users' conduct. [33] In the instance of Napster, the court held that the company should be responsible for policing the wrongdoings on its own site to the best of its ability, but was allotted up to three days to remove copyrighted material if notified by a complainant. [34] The transmitting entity (in this case a file-sharing search engine) was not held immediately responsible for Internet violations on its own site. The bottom line is that file-sharing websites that partake in copyright infringement are not held fully liable for users' misuse of their service; they are given notice and time to fix copyright violations on their sites, which does not put the fault on the site that simply connects the infringing web users together.

In Canada, the Society of Composers, Authors and Music Publishers of Canada sued the Canadian Association of Internet Providers in 2004 during a similar situation. Unlike the Napster case, however, the plaintiff did not sue for connecting users who make illegal downloads on a specific website, but rather providing the Internet service that offenders were using. This case, known as SOCAN, addressed the location of Internet Service Providers—called ISPs—in another attempt to find a party liable for Internet copyright violations.

In SOCAN, the Canadian Internet Service Provider was accused by a group of copyright holders who argued that providing the Internet service under which illegal sharing of copyrighted material took place constituted negligence. [35] The Canadian Supreme Court held that an Internet intermediary (an ISP) was not liable so long as it was acting as a content transmitter and not a content provider; as long as the ISP does not provide the illegal content, it is not liable for unknowingly transmitting illegal content from one user to another. [36] So long as there is fair use and good intention, the ISP is not at fault. [37] Under the territoriality principle followed by countries such as China, a country possesses authority for all affairs within its territory—both for the intentional censorship and for the actions of ISPs (the claim to territoriality goes both ways, whether positive or negative).

Regardless, the Canadian Supreme Court did not choose to adopt the doctrine of territoriality and still concluded that an ISP was

DISPUTES ARE ON THE RISE AROUND THE WORLD, BUT AS OF YET THERE IS NO CONCRETE, UNIFIED SYSTEM FOR INTERNATIONAL LAW-MAKING AND LAW ENFORCEMENT

not responsible simply because it was located in the country where the violations took place. [38] The court did not go as far as to assert that the content providers or downloaders on either side of the ISP were at fault, but a lack of comment by the Court suggests that the content provider is the main violator.

The surge of cases similar to SOCAN is now pressuring ISPs to filter content or regulate the information that they offer out of fear of litigation, even though there is no formal requirement in international law for them to do so. [39] Although a few, such as WikiLeaks, publically dissent from this phenomenon by continuing to publish protected information, the fear of litigation for actions online may provoke indirect censorship and deprivation of knowledge. Article 19 of the UN Universal Declaration of Human Rights states that all people have the right to "receive and impart information and ideas through any media and regardless of frontiers." [40] Yet, the fear of litigation for online behavior may encourage censorship and prove inimical to free speech.

The analysis thus far shows that there are three steps in any cyberspace transaction: one user initiates the transaction by posting material, an ISP or file-sharing site transmits the information, and the end user downloads the material. [41] As discussed previously, the Napster case set an early precedent in the United States that a transmitting site is not liable for copyright infringement. Similarly, the SOCAN case set a precedent in Canada that the ISP is not at fault either. While international law has yet to offer a clear guidelines on the matter, the discussed case examples demonstrate the approaches adopted by forward-thinking and influential nations in the realm of cyberspace that the transmitting institution (whether an individual, a nation or a corporation) should not be held liable for cyber theft as long as that institution promotes fair use in its services and does not seek to intentionally commit copyright infringement.

If file sharing sites and ISPs are consistently not held liable for the copyrights that are violated on their watch, then it could be argued that WikiLeaks and *The New York Times* in The Pentagon Papers case should not be legally liable under U.S. law for the information they transmitted either. WikiLeaks essentially acts as an ISP of political information and claims good faith in attempting to expose political corruption. The site does not create the information that it posts, just as Napster does not create illegal music files. It only transmits the information into the public sphere where at least the information is available. The UN might view this as simple practice of human

rights, as defined in Article 19. But while certain nations such as the U.S. and Canada support the human rights to free speech over the argument for national security, the amorphous nature of cyberspace still requires a system to adjudicate potential dilemmas which may arise between other nations, as well as protect individuals and intellectual property rights. The parties of the 166 nations at the Berne Convention suggest that this desire to protect IPP is fairly universal, even among developing nations.

A solution to these issues would be a governing cyberspace body. Institutions such as the European Union and the World Trade Organization are examples of a gradual international shift for nations to cede power to larger, specified governing institutions in certain situations. [42] An international body to govern cyberspace could help to standardize regulations, boost implementation, and aid international cooperation to address cyber crime. There is unequivocally one common, overarching theme in the cyberspace cases discussed thus far: disputes are on the rise around the world, but as of yet there is no concrete, unified system for international law-making and law enforcement.

Without actively protecting from wrongdoings—which could be as minor as a copyright violation or as major as cyber warfare—states may open themselves to harm just as if they had chosen not to protect the physical borders of their nations. In the same year that Napster emerged, the 1999 Harvard Law Review asserts that, "Internet regulations are necessary to protect state sovereignty" for this very reason. [43] In order to maintain the legitimate freedom of press and freedom of expression in the international sphere, a system must be put in place to ensure that cyberspace remains free.

Treaties such as the UN Universal Declaration for Human Rights and the Berne Convention put forward by the United Nations, WIPO and UNESCO offer a strong framework upon which a more formal governing body can be constructed. One proposed solution is to organize national state Internet servers that all answer to a collective, regulated international server overlooked by an international tribunal. One power of such a tribunal proposed by UNESCO would be to unify Internet domain names and restrict usage of the sites found guilty of cyber crime. [44] Perhaps even super-injunctions to prevent leaks of confidential material would prove useful. [45] This way, violators would be more likely to be held accountable for leaking classified information. Essentially, the Internet needs to be unified in order to create a structure that allows for order in cyberspace law.

Arguments against an international governing body for cyberspace generally take the position that the Internet is a unique system that should be left to govern itself, because it is too vast and intangible to ever effectively control. The fallacy of this argument is that the Internet provides too much opportunity for abuse. Governments unjustifiably censor information contrary to the desire of the United Nations; file-sharing sites infringe upon copyrights and intellectual property laws; and the current system discourages the freedom of speech. However, practical obstacles to the construction of an international governing body remain. There are apparent differences between the Internet censorship policies of many nations at present. This is an especially pertinent issue because cyberspace has no boundaries and has recently proven to interact between the physical boundaries of differing nations. Despite these challenges, the combination of rapidly developing cyberspace and increasing globalization has brought new urgency to addressing concerns about intellectual property and freedom of speech within an international legal framework. [46]