2012

Communications Disruption and Censorship under International Law: History Lessons

Jonathon Penney

Communications Disruption & Censorship under International Law: History Lessons

Jonathon W. Penney
Oxford Internet Institute, University of Oxford
Citizen Lab / Centre for Global Security Studies, University of Toronto

Abstract

With Internet censorship on the rise around the world, a variety of tools have proliferated to assist Internet users to circumvent such censorship. However, there are few studies examining the implications of censorship circumvention under international law, and its related politics. This paper aims to help fill some of that void, with an examination of case studies wherein global communications technologies have been disrupted or censored— telegram cable cutting and censorship, high frequency radio jamming, and direct broadcast satellite blocking— and how the world community responded to that disruption or censorship through international law and law making. In addition to illustrating some of the law and politics animating global communications censorship, I extrapolate lessons and insights for the challenges posed by Internet censorship today, such as the international legality of censorship circumvention, the nature of censorship justifications, and the potential liabilities for those engaged in censorship resistance under newly emerging doctrines of international law.

1. Why International Law?

A few previous studies have examined or noted the legal implications of Internet filtering [1], mapping [2], or censorship circumvention [3], yet none have examined, in depth, how circumvention of state-implemented Internet censorship fits within international law and its politics, perhaps because the use, distribution, or development of Internet censorship resistant systems or censorship circumvention tools— what I refer to as censorship resistance activities— are often seen as the work of private citizens, organizations, and other non-state actors, and not subjects of the international system.

Yet, those involved with censorship resistance activities should pay heed to international law— and developments in international rule-making—for several reasons. First, international law has evolved in important ways in recent decades, with new legal concerns and potential liabilities emerging for organizations, corporations, and other non-state actors involved in transnational activities like censorship resistance [4]. And many states, like the United States, have increasingly sponsored Internet censorship resistance activities, potentially raising other international legal issues like state responsibilities [5, 6].

Second, new international legal rules formulated by treaties and conventions, often negotiated in secret, can quickly shift global Internet regulatory norms, providing new forms or possibilities of censorship and surveillance. For example, many past and present national laws raising Internet censorship concerns were enacted to bring countries in line with their international legal obligations— like the Digital Millennium Copyright Act in the U.S. (implementing the Berne Convention) or lawful access laws in Canada (to meet obligations under the Council of Europe's Convention on Cybercrime). Similarly, the Anti-Counterfeiting Trade Agreement (ACTA), currently being negotiated, may oblige signatory states to pass broad anti-circumvention laws— which could outlaw censorship circumvention tools— similar to provisions proposed in the controversial U.S. bill, Stop Online Privacy Act (SOPA).

Third, the "legitimacy" of censorship resistance activities has been questioned or criticized [7, 8], so situating such activities within broader international legal rules or norms can provide meaningful "moral, rhetorical and at least arguable legal support" to justify censorship resistance and its various components like filter circumvention or anonymous access [9].

Those are just a few reasons why international law remains a relevant and worthy focus. Despite this relevance, few studies have systematically explored the international legal dimensions of Internet censorship resistance activities. This paper aims to help fill at least some of that void, with an examination of case studies wherein global communications technologies have been disrupted or censored— telegram suppression and cable cutting, high frequency radio jamming, and direct broadcast satellite blocking— and how the world community responded to that disruption or censorship through international law and law making.

In addition to illustrating some of the law and politics animating global communications disruption and censorship, I extrapolate from these case studies some

lessons and insights for the challenges Internet censorship today, such as the legality of censorship circumvention, the nature of censorship justifications, and the potential liabilities for those engaged in censorship resistance under emerging doctrines of international law.

1.1 A Legal Impasse?

When legal scholars assess the legality of state censorship regimes they often profess a stalemate under international law because any international rights to information or expression inevitably conflict with the sovereign right of states to police national territories, leaving state censors free to block content while citing their "legitimate" sovereign right to protect national security or preserve local morality against offending content [10, 11]. So international law, it is often assumed, has little to say about Internet censorship, and even lesser to offer in constraining or resisting it.

Yet, there is reason to believe this is an overly simplified account [12] and examining case studies involving global communication disruption or censorship, and its legal and political dimensions, could offer insight into this, and other relevant issues or concerns for those advocating for free and open Internet communications.

2. Global Communications Disruption and Censorship: Three Case Studies

Internet censorship is often compared to Cold War radio censorship [13], but the telegraph offers our first case study.

2.1 Telegraph Cable Cutting & Censorship

One of the earliest instances where transnational communications were disrupted by states involved the telegraph— submarine cable cutting and cable message suppression in the late 19th and early 20th Century.

The first transatlantic submarine cables, through which telegraph cables could be communicated, were laid by the 1850s, only a few years after the introduction of telegraph. Through efforts led mainly by Britain, an extensive web of submarine cables were subsequently laid between countries in Europe, Africa, and Asia, and by the 20th Century most of the world was linked, establishing one of the earliest global telecommunications networks. British companies, with the assistance of the Empire, owned and controlled the vast majority of this submarine cable network [14, 15].

The submarine telegraph cable network proved a powerful tool for commerce, diplomacy, and the free flow of information allowing rapid, safer, and more secure communications between governments, dissemination of information between populations, and more efficient coordination for world shipping and trade [16].

2.1.1 Two Network Vulnerabilities

Much like Internet censorship today, the submarine cable network's importance to global communications also made it a target for disruption by hostile states who, strategically, could isolate or weaken enemies by disrupting state and commercial communications. And while submarine cables were much more secure than land cables, they could be damaged, and with the right equipment, cut [17]. In fact, as early as 1885, Russia planned to cut British submarine cables during the Penjdeh crisis, which would disrupt transnational communications not only for Britain, but a number of countries not involved in the confrontation [18].

The submarine cable network was also vulnerable to censorship. Most of the global network was controlled by public and private companies from a handful of states— with Britain the most dominant, though Germany had also invested heavily. If either state decided to block or suppress telegraph communications, they would likely have the means to do so.

2.1.2 International Response

Given its obvious importance to global communications and commerce, the international community established formal measures to protect the telegraph communications system, including the 1875 International Telegraph Convention and the 1884 International Convention for the Protection of Submarine Cables. These measures codified previous treaties and customary international law, and proved effective in protecting the telegraph cable network, at least in times of peace.

Britain, for example, took steps to secretly establish an elaborate "censorship" system of telegram surveillance and blocking through its control over key cable way-stations around the world. But by the 1890s, British officials questioned the system's legality under the 1875 Telegraph Convention and annexed Service Regulations, which not only declared that "all persons" have a "right" to communicate by "international telegraph", but also provided that states could not block a telegram, even for national security reasons, without immediately notifying its sender [19]. These provisions, as well as those expressly allowing secret codes in telegraph communications— which became widely used— greatly impeded telegram surveillance and blocking [20].

The Submarine Cables Convention was similarly effective in deterring cable cutting with a range of prohi-

bitions and requirements, including requiring states to compensate owners for damage done to cables [21].

2.1.3 The Impact of War

Despite this success, these conventions' failure to properly address censorship and cable-cutting during war was a major oversight. As noted, the 1875 Telegraph Convention's Service Regulations originally provided that if a state blocked a telegram's transmission because it was contrary to law, public order, decency, or national security, it had to immediately notify the telegram sender. However, the Service Regulations were revised in 1908 to add an exception to this notice requirement— telegrams sent by other state governments could be blocked without notice, if giving notice would pose a "dangerous" national security threat; this was interpreted by states like Britain, to mean existential threats like war [22].

This "exception" led to pervasive cable censorship and espionage during World War I, with the state infrastructure created to conduct "war time" communications surveillance, cryptology, and censorship, often becoming, after the war, permanent "peace time" state surveillance or signal intelligence agencies like Britain's Government Code and Cypher School, established in 1919, which is today known as Government Communications Headquarters or GCHQ [23].

The Submarine Convention also neglected war times, and cable-cutting between hostile states became increasingly common in the early 20th Century. In fact, submarine cable-cutting was likely the first premeditated acts of the First World War, when Britain and France cut German submarine cables spanning the Atlantic and North Sea on August 9, 1914 [24].

2.1.4 Alternative Measures: Litigation

Without recourse under international treaty or convention, non-state actors (i.e. companies) turned to litigation in national and international judicial forums to seek redress for cables damaged during war. For example, in the 1923 *Case of the Cuba Submarine Telegraph Company (Claim No. 27)*, the British government (on behalf of British companies) famously brought a claim against the United States in a London-based international claims tribunal, seeking compensation under customary international law principles for cables cut during the Spanish-American War. Though on uncertain legal grounds, such high profile and costly litigation successfully pressured or shamed some countries into settling and paying damages [25].

Though the Telegraph Convention was later revised, no international agreement was ever settled to address telegraph communications at war; however, the idea that cable communications between neutral countries, even during war time, were "inviolable" and thus should remain free of disruption was largely established. Articulated by the Institute of International Law in 1878, this principle had near universal acceptance [26] and was largely codified in Article 54 of the Fourth Hague Convention of 1908. Telegraph communications became less important after the First World War, with the development of the wireless telegraph and radio communications [27].

2.2 High Frequency Radio Jamming

Freedom of information and radio jamming were major international issues after the Second World War. This prominence was due not only to U.S. influence— whose foreign policy was centered on First Amendment values— but also developments during the war itself. Both war propaganda and state censorship, enabled by radio transmission jamming, were pervasive during the war and viewed by the world community as a serious threat to peace and stability [28]. The development of high frequency shortwave radio technology before the war— which made the transnational propagation of radio broadcasts possible— led countries like Germany to deploy a war strategy of "broadcast defense" involving systematic jamming of foreign radio stations [29].

2.2.1 The Free Flow of Information Doctrine

The consensus solution in the years immediately after the war, was a policy promoted by the U.S. and its allies: the free flow of information doctrine. That is, the promotion of unrestricted global flow of information and ideas across state borders. The free flow doctrine, it was argued, could address state propaganda and censorship at the same time, undermining both with a diverse array of information sources [30].

The consensus on the free flow doctrine was reflected in the near complete absence of any radio jamming after the war, as well the wide range of international conventions, declarations, and agreements established at the time that codified the doctrine's principles, like the right to "seek, receive, and impart information" enshrined in article 19 of the United Nations' 1948 Universal Declaration of Human Rights (UDHR) and the UN's 1946 Declaration on Freedom of Information— which declared information freedom a "fundamental human right"— adopted unanimously in the General Assembly's first session [31, 32].

2.2.2 Cold War Information Politics

The early Post War consensus on the free flow doctrine weakened as U.S.-Soviet relations began to deteriorate, after the Soviet Union began jamming U.S. radio broadcasts directed at Russia in 1948. The Soviets, and their allies in the Eastern bloc, would continue to jam Western broadcasts like the BBC, Voice of America, Radio Free Europe, and Liberty Radio, for most of the Cold War. And freedom of information would become a flashpoint for international legal disputes between East and West, with the West promoting the free flow of information and the Soviets advocating the sovereign right of states to restrict it [33].

These struggles over information law and politics would take place across a vast range of international forums, including the International Telecommunications Union (ITU), UNESCO, and the UN General Assembly. And notwithstanding the West's success in having radio jamming prohibited and the free flow doctrine recognized in numerous international documents and forums— for example, every ITU resolution from 1947 onward condemned radio jamming— such measures did little to deter Soviet jamming activities, whom often cited national security justifications [34].

As with telegraph cable cutting, international law's failure to settle disputes over radio jamming and international broadcasting led some states and non-state actors to seek redress in alternative measures or forum, like the International Frequency Registration Board (IFRB), the ITU's enforcement arm, which established both a global radio jamming monitor, and a formal complaints process for states seeking redress.

2.2.3 IFRB Radio Jamming Monitoring

The IFRB was initially set up to resolves disputes concerning interference with international broadcasts, and to administrator and enforce the terms of the International Telecommunications Convention (ITC) and its annexed Radio Regulations. Due to the divisive nature of Cold War international politics, its strict enforcement capacity was seriously weakened [35].

However, one of the IFRB's more (mildly) successful Cold War projects— which may have been a great success if given time— was its global "radio interference" or radio jamming monitoring program [36]. Given the highly charged international disputes over radio jamming, few countries other than the Soviet Union went on the record to admit they were deploying jamming and but there was little information available about the location, scope, and spillover effects of jamming activities. The IFRB's monitoring program was the first and most technically sophisticated attempt to credibly map those details.

The IFRB's radio jamming monitoring was established in response to Western lobbying at the ITU's 1984 High Frequency World Administrative Radio Conference (HF-WARC). Radio broadcasts were being jammed around the world in 1984 at "record levels", with no real recourse for states or international broadcasters under treaty or convention. Perhaps seeking alternative means to fight the jamming activities, Western governments persuaded the HF-WARC to issue a resolution requesting the IFRB to monitor and report on radio jamming around the world [37].

The IFRB, working jointly with the U.S. National Telecommunications and Information Administration (NTIA), established a globally coordinated effort to monitor the location and extent of international radio broadcast jamming worldwide [38].

The IFRB issued reports in 1985, 1986, and 1987, setting out the location of 100 sources of radio jamming globally, with most located in Soviet or Eastern bloc country territory [39]. Those reports were tabled at the 1987 HF-WARC, formally confirming radio jamming activities being conducted by the Soviet Union, Bulgaria, Czechoslovakia, and Poland, as well as a number of smaller developing countries. The aim was to stir more international pressure on jamming countries to cease, or at least scale back, their activities [40].

Interestingly, by the time of the second session of the 1987 HF broadcast conferences, jamming had "diminished considerably". Though certain Western broadcasts like Voice of America remained jammed for various languages in the USSR, jamming activities in smaller Eastern bloc was significantly scaled back, with some, as in Poland, ceased completely [41].

As with other times when jamming activities received international attention, the Soviet government was undeterred; but smaller countries, like developing countries or those in the Eastern bloc, were much more responsive to monitoring. They may, as James Savage and Mark Zacher have suggested, have felt "constrained from jamming because of cost or the possible damage to their reputations..." [42].

Of course, there were many factors at play here; by the late 1980s, for example, the U.S. and Soviet Union were cooperating more closely, and behind the scenes American lobbying likely played some part in the downtrend in radio jamming activities. Still, IFRB monitoring and reporting, with its robust methodology and technical sophistication, constituted the "gold standard" in radio jamming tracking, with its high profile reports seen as both credible and objective; a Cold War precursor to contemporary efforts to map and track global Internet censorship.

2.2.4 IFRB / FCC Complaints Process

Another alternative channel used by countries on either sides East-West divide on Cold War radio jamming, was the IFRB complaints process. Though, as noted, the IFRB had little actual enforcement capability, its pronouncements to bring to bear some pressure on states acting in breach of the ITU Convention and Radio Regulations.

This was apparent in the radio jamming disputes between Cuba and the United States. In the 1960s, Cuba began jamming radio broadcasts originating in the southern U.S., and would do so, off and on, for most of the Cold War [43].

Though there was some concern that the disputes may lead to a military confrontation, but that did not materialize. Instead, both countries, among other actions, utilized international and national formal complaints processes [44]. Both, for example, lodged formal complaints against each other with the IFRB, which would investigate and issue compliance rulings in response to complaints that state governments, or non-state actors in state territories, were violating the ITC rules or regulations. Cuba also lodged complaints with the Federal Communications Commission (FCC) about clandestine unlicensed anti-Fidel Castro pirate radio broadcasts originating in parts of Florida [45].

Both countries achieved some success with these complaints. Though the IFRB was unable to enforce its findings, its investigations into Cuban radio jamming pushed the Cuban government to the negotiating table in various international forums [46] and, overall, Cuban jamming efforts were never more "than limited and half-hearted"[47]. And the FCC, in response to Cuban complaints, closed down anti-communist and anti-Castro pirate radio states in Florida in 1980 [48].

Much like the less powerful developing and Eastern bloc countries that the IFRB's monitoring program exposed, Cuba appeared more responsive to bad press and international exposure for its jamming activities, compared to world powers like the Soviet Union.

2.3 Direct Broadcast Satellite TV Jamming

The final case study of global communications disruption, to be briefly discussed, was international disputes over direct-to-receiver satellite broadcasting, or direct broadcast satellite (DBS), in the 1970s.

DBS developed in the late 1960s, and provided the capability to beam television signals directly to targeted populations across national borders. Not surprisingly, it stirred international controversy and, like other global communications conflicts during the Cold War, led to disputes about the legality of states blocking or jamming DBS signals [49].

Early on international lawyers and legal scholars questioned whether traditional "state sovereignty" justifications for communications jamming— based on theories of territorial control over airwaves or national security— could justify satellite jamming or blocking. Since satellites operated far beyond the airspace that international law recognized as subject to territorial control, the airwave theory was inapplicable. And the national security justification was also weak, given that satellite jamming often meant interfering with the capabilities of the satellite itself; preventing it from broadcasting at all [50]. These questions concerning the legality of regulating or jamming DBS, led to good faith international efforts to negotiate a treaty to cover DBS communications and transmissions [51, 52].

However, international law largely gave way to international politics. And unlike the East-West divide on radio jamming, things were more complicated for DBS. Television's cultural and political power far exceeded radio, and more states perceived DBS as a threat to national control over television broadcasting. World politics subsequently divided along three lines over DBS: the U.S. and some developed Western countries advocating the free flow of communications, the Soviet and its Eastern bloc allies pushing for full jamming powers, and a third group of countries, mainly developing nations, which supported more moderate regulatory powers over DBS transmissions [53].

This new regulatory coalition— between the "East" and "South"— was successful in promoting its agenda in various international forums, like the ITU, UNESCO, and the UN General Assembly. For example, it achieved some recognition for the concept of "prior consent", that is, DBS should not be transmitted into a state's territory without its prior consent in a General Assembly resolution in 1972, with 102 voting in support and only the United States voting against. This was later referred to as the "Jammers Charter". [54].

Though never formalized, the notion of prior consent only complicated relevant law and weakened the case for free flow of information principles.

3 Internet Censorship Resistance Today: Lessons and Implications

So, beyond an historical examination of global communications disruption or censorship, do these cases offer any insights, lessons, or implications for Internet censorship resistance today? I believe so.

3.1 The Legality of Internet Censorship Resistance under International Law

3.1.1 A Reasonable Legal Foundation

With the U.S. State Department embracing "Internet freedom" as a element of American foreign policy and countries like China and Iran ramping up the both cyber-security and Internet censorship capabilities in response, geo-politics once again permeate and complicate global communications policy, much as they did for the telegraph, radio, and satellite communications.

Within this broader geo-political context, critics have questioned the legitimacy of "Internet freedom" and related activities like Internet censorship resistance [55, 56]. These criticisms often have both a legal and political component, questioning the how state or non-state actors can justify censorship circumvention tools that supposedly undermine national laws that implement local policy preferences on security or cultural policy (and are presumably enforced by Internet filtering or censorship regimes).

Notwithstanding uncertainty as to the legality of different forms of communications censorship under international law, a reasonable and legitimate legal basis for Internet censorship circumvention, and related activities, can be easily articulated.

Internet censorship resistance activities help promote important and recognized international legal rights and principles, like freedom of information, freedom of expression, and right to "seek, receive, and impart information and ideas". All of these values have been recognized under international law in a broad range of treaties, conventions, international legal precedents, and declarations, many of which were discussed above— like the UN Declaration on Freedom of Information, and article 19 of the UN's 1966 International Covenant on Civil and Political Rights and 1948 Universal Declaration of Human Rights, the latter of which is today largely understood to represent customary international law. Meaning, it is binding on all states.

Moreover, a panoply of international telecommunications conventions, regulations, and resolutions have condemned communications disruption and censorship— across a variety of technologies like those herein discussed— throughout the twentieth century. And Internet censorship resistance activities, engaged in both by state and non-state actors, is also consistent with the principles of the free flow of information doctrine, a policy that had near unanimous international support in the Post War years, and though that consensus weakened, the free flow doctrine still retains influence and wide international support.

Though international disputes over the legality of global communications disruption and censorship left many questions unanswered, those efforts did lead to the important recognition and codification of international legal principles that provide a reasonable legal foundation for Internet censorship resistance today.

3.1.2 Censorship Justifications and their Limits

Critics, however, may counter that that Internet censorship circumvention— both state and non-state efforts like BBC World Service's effort to deliver online content to heavily censored regions [57]— undermines national and regional laws governing local culture, morality, and security, which are enforced by Internet filtering and censorship. And justifications based on public morality or security arise from the state sovereignty, a bedrock principle of international law.

True, state sovereignty is a fundamental international legal principle, but our case studies also offer insight as to how far the principle can be stretched to justify censorship.

To begin with, though the need the police local morality is often cited as a basis for Internet censorship or filtering— and modern international legal documents often include as a potential limit on free expression— it was historically limited in scope. For example, in the 1875 Telegraph Convention, no private telegram could be blocked for reasons of morality, decency, or even public order, without also notifying the sender (after 1908, only State sent telegrams could be blocked without notification if notice would be "dangerous" to national security). And with respect to satellite and radio communications, the most common "state sovereignty" theories offered to justify jamming activities were not based on public morality, but control over airspace or national security, with the latter being the most robust. Indeed, national security has long been the central and most powerful justifications for telecommunications censorship and surveillance regimes [58].

However, the national security justification has also been limited. For example, during international debates about DBS communications, scholars questioned whether theories of national security based on customary international legal principles could justify satellite jamming; this led to international efforts to negotiate a new treaty to cover satellite communications and its regulation. Moreover, before the Telegraph Convention's Service Regulations were revised in 1908, no private or State telegram could be blocked for national security without also immediately notifying its sender. Even under the 1908 Lisbon revisions, national security censorship was limited—only State telegrams (not private) telegrams could be legally blocked without notifi-

cation, and only if such notice would pose a "dangerous" threat to national security (e.g., the sending State and blocking State were at war).

In other words, these case studies suggest that certain justifications for Internet censorship and filtering, may not, historically, have been as broad as commonly described or understood today.

3.1.3 Resisting Cold War Analogies

Among certain political science and public policy circles, and certainly within the national security establishment, there is growing trend to describe and address the challenges of Internet cyber-security matters through the lens of the Cold War [59]. While there is certainly descriptive and analytical reasons in drawing on Cold War experiences to understand current developments like the "militarization" of cyberspace [60], these case studies also suggest that adopting Cold War strategies may do more harm than good to Internet censorship resistance. Historically, international legal protections for free and open global communications have always been more robust in times of peace. This was certainly the case with the Telegraph Conventions, which all provided relatively effective protection against telegram blocking and cable cutting among peaceful countries but were either inapplicable, or wholly inadequate, during times of war.

Similarly, radio communications were never more free and open and unencumbered by censorship and other jamming activities than they were during the peaceful years after the Second World War, before the Cold War was in full swing. State and national security officials eager to approach Internet and cyber-security issues with Cold War strategies have self-interested reasons for doing so—free and open Internet communications are easier to limit and control when at war.

3.2 Liabilities for Censorship Resistance under International Law?

An additional lesson from these case studies is the potential for national or international litigation over transnational communications disputes. In the past, states and non-state actors seek redress over communications related disputes or injuries through other means— like litigation— when there is insufficient or uncertain international enforcement or protection. Sometimes, as with British companies seeking redress for telegraph cable cutting, this involves national or international litigation. Sometimes, as with radio jamming, this can involve states filing formal complaints or claims with national or international bodies or tribunals.

3.2.2 Litigation in International Forums

Avoiding potential entanglement in international disputes and related litigation between states may be one good reason for organizations involved with Internet censorship resistance to shun official state sponsorship. As with the radio jamming wars between Cuba and the United States, officially sponsored U.S. radio broadcasts were specifically targeted by foreign jammers, and were the subject of complaints lodged in international forums.

Of course, shunning state sponsorship may also leave an organization vulnerable to legal complaints from foreign governments; the FCC shut down non-licensed pirate radio stations in Miami in response to complaints from the Cuban Government.

3.2.2 The Haystack Factor: The Alien Torts Statute and Potential Liabilities in U.S. Courts

The potential for litigation over Internet censorship circumvention, and related issues, is even more acute today, given recent trends in both international law and U.S. federal law. Indeed, beyond international disputes, censorship resistance activities may also attract liability in U.S. state courts. International law has evolved in recent decades, with new legal rights, responsibilities, and potential liabilities arising for non-state actors like corporations and organizations [61]. These changes, combined with other key changes in domestic U.S. law— the growth of legal claims for violations of international law brought under the Alien Tort Statute— create a new minefield of potential liabilities for U.S. companies and organizations engaged in transnational activities abroad [62].

The Alien Tort Statute (ATS)— a simple statute passed in 1789— was likely meant to allow foreign plaintiffs— such as merchants and ambassadors— the right to sue American citizens in U.S. courts for violations of international law causing injury to person or property [63]. Today, the ATS has been interpreted to allow a broader range of international claims, with increasing numbers of successful plaintiffs obtaining judgments and settlements, with awards ranging from $1.5 million to a jury award of $766 million compensatory and $1.2 billion punitive [64].

A central concern, is that U.S. companies and organizations may be found liable under the ATS for aiding and abetting human rights abuses, or other breaches of international law, committed or condoned by foreign governments [65]. And while these issues are far from settled, at least one U.S. Circuit Court of Appeal have suggested "reckless disregard" is sufficient intent for liability under such ATS claims [66].

But do those engaged in censorship resistance activities have anything to worry about concerning these legal changes? Internet censorship resistance activities are fraught with complicated international legal issues— including human rights— with serious risks and dangers. It is not difficult to envision a person suffering serious harms for being caught using a censorship resistant system or tool, when dealing with censorship regimes and security apparatus in countries like China or Iran. Indeed, the notion that a U.S. company may be held liable under the ATS for Internet-related actions, leading to human rights abuses is far from speculative, given that Yahoo Inc. settled just such an ATS legal action brought against it for intentionally or negligently assisting Chinese authorities in tracking down Chinese human rights activists and dissidents [67].

Yahoo Inc.'s decision to assist Chinese authorities can certainly be distinguished from those fighting Internet censorship. But if a legal claim were ever brought against an organization involved in developing or distributing censorship resistant tools, it would probably look like the Haystack controversy, wherein developers greatly exaggerated the capabilities of a program allegedly designed to allow citizens— in countries like Iran and China— to safely circumvent Internet censorship and surveillance [68]. In such a case, it would not be a stretch to claim Haystack developers exhibited "reckless disregard"— and indirectly aided state authorities— if an Iranian citizen were arrested or otherwise harmed for using the flawed Haystack tool.

Of course, there are other complex issues in such cases, and ATS case law continues to evolve— the circuit courts are split on certain issues, with two high profile corporate liability ATS cases currently before the U.S. Supreme Court [69]. Still, these are legal concerns that cannot be ignored by those involved in censorship resistance activities.

3.3 Influencing the Middle

A final lesson to be taken from our case studies is the value for researchers, developers, and activists to work on influencing the "middle". That is, rather than focusing on high profile (and commonly cited) countries like China and Iran that are committed to broad and sophisticated Internet censorship, focus instead on the broader middle— the range of countries that engage in some level of Internet filtering or censorship but whom may be more responsive to bad press or international exposure, because they are more concerned about their reputation and the economic costs of censorship.

During the Cold War, the Soviet Union was unrelenting both in its resolve and technical capacity to jam Western radio broadcasts, and no amount of international exposure or condemnation deterred it from that path. But, as noted in our study, less developed countries like Cuba and poorer countries within the Eastern bloc were more easily swayed by international exposure through IFRB monitoring and complaints process, like due to a range of factors like the costs involved in radio jamming, sensitivity to international reputation, or simply wishing to avoid stepping into the middle of an ongoing dispute between superpowers— the United States and the Soviet Union.

In ways, the IFRB radio jamming monitoring program implemented in the 1980s, was an earlier version of the Internet censorship mapping and tracking being conducted by important projects like the OpenNet Initiative and Herdict. The success of the IFRB— even if the program was short lived— provides additional insights into their great value and potential influence.

References

[1] OpenNet Initiative. 2004. A Starting Point: Legal Implications of Internet Filtering. September 2004, http://opennet.net/docs/Legal_Implications.pdf. Accessed April 21, 2012

[2] J. Wright, Tulio de Souza, and I. Brown. 2011. Fine Grained Censorship Mapping: Information Sources, Legality, and Ethics. In *First USENIX Workshop on Free and Open Communications on the Internet(FOCI).* August, 8 2011. http://static.usenix.org/events/foci11/tech/final_files/Wright.pdf.

[3] Derek Bambauer. 2009. Cybersieves. In *Duke Law Journal*, 59:3, 441-443.

[4] See Roger P. Alford. 2012. Apportioning Responsibility Among Joint Tortfeasors for International Law Violations. In *Pepperdine Law Review*, 38:2, 223-224 (discussion changes in modern international law).

[5] R. Dingledine. 2011. Presentation: Tor and Circumvention, Lessons learned. http://2011.indocrypt.org/slides/dingledine.pdf (stating the Tor Project receives funding from U.S. Department of Defense and State Department).

[6] Psiphon Inc. 2012. About Psiphon Inc. http://psiphon.ca/?page_id=94 (indicating Psiphon

initially received funding from the European Union).

[7] Evgeny Morozov. 2011. Freedom.gov. In *Foreign Policy* (online). http://www.foreignpolicy.com/articles/2011/01/02/freedomgov?page=full (noting that Internet freedom is viewed in some quarters as "another Trojan horse for American imperialism").

[8] Tricia Wang. 2011. The Great Internet Freedom Bluff of Digital Imperialism. In *Cultural Bytes* (online). http://culturalbyt.es/post/1141832150/internetfreedom

[9] Michael Froomkin. 2011. Lessons Learned Too Well. In *Miami Law Research Paper Series*, 35. http://ssrn.com/abstract=1930017.

[10] Concerning this point and censorship more generally, see: Rochelle B. Price. 1984. Jamming and the Law of International Communications. In *Michigan Yearbook of International Legal Studies*,5, 391-392.

[11] With respect to Internet censorship, see for example, Katherine Tsai. 2011. How to Create International Law: The Case of Internet Freedom in China. In *Duke Journal of Comparative and International Law*, 21, 402-403, 402fn (questioning whether international law has an answer to China's sovereign claim to censor Internet content).

[12] John Palfrey. 2007. Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet. In *Global Information Technology Report*, World Economic Forum, 2006-2007, 71.

[13] Eszter Hargittai. 2000. Radio's Lessons for the Internet. In *Communications of the ACM*, 43:1.

[14] United Nations Environment Program (UNEP) and International Cable Protection Committee (ICPC). 2009. Submarine Cables and the Oceans: Connecting the World. UNEP, 13.

[15] A. Pearce Higgins. 1922. Submarine Cables and International Law. In *Brit. Y.B. Int'l L.*, 2, 28-30.

[16] UNEP et al, at 13, 26.

[17] P.M. Kennedy. 1971. Imperial Cable Communications and Strategy, 1870-1914. In *The English Historical Review*, 86:341, 728.

[18] Kennedy, at 732.

[19] Jill Hills. 2006. What's New? War, Censorship, and Global Transmission. In *International Communication Gazette*, 68, 197-198.

[20] Hills, at 197.

[21] Higgins, at 35.

[22] Hills, at 197-200.

[23] Hills, at 197, 199-201.

[24] See generally, Robin Mansell and Marc Raboy. 2011. *The Handbook of Global Media and Communications Policy*. London: Wiley & Sons, ch. 2.

[25] Higgins, at 30.

[26] R.G.R. Goffin. 1899. Submarine Cables in Times of War. In *Law Quarterly Review*, 15, 145.

[27] Mansell et al, at ch. 2.

[28] Jonathon W. Penney. 2011. Internet Access Rights: A Brief History and Intellectual Origins. In *William Mitchell Law Review*, 38:1, 21-23.

[29] James G. Savage and Mark W. Zacher. 1987. Free Flow versus Prior Consent: The Jurisdictional Battle Over International Communications. In *International Journal* 42, 344, 347.

[30] Penney, at 22-23.

[31] Penney, at 23-24.

[32] Savage et al, at 348.

[33] Savage et al, at 347-348.

[34] Savage et al, at 343-344, 348, 362-363.

[35] Madelaine Eppenstein and Elizabeth J. Aisenberg. 1979. Radio Propaganda in the Contexts of International Regulation and the Free Flow of Information as a Human Right. In *Brooklyn Journal of International Law*, 5, 158-159.

[36] Savage et al, at 362.

[37] Mary W. Sowers and Gregory R. Hand. 1990. Monitoring of Harmful Interference to the HF Broadcasting Service: Summary of Monitoring Programs Held Between 1984 and 1989. In *National Telecommunications and Information Administration Technical Report 90-262*, 2.

[38] Sowers et al, at 2-3.

[39] Sowers et al, at 2-3.

[40] Savage et al, at 362.

[41] Sowers et al, at 2-3.

[42] Savage et al, at 362.

[43] Savage et al, at 350.

[44] Omar J. Arcia. 1996. War Over the Airwaves: A Comparative Analysis of U.S. and Cuban Views on International Law and Policy Governing Transnational Broadcasts. In *Transnational Law & Policy*, 5:2, 203-205.

[45] Arcia, at 202.

[46] Arcia, at 204.

[47] Savage et al, at 350.

[48] Arcia, at 202.

[49] Savage et al, at 357.

[50] Samuel D. Estep and Amalya L Kearse. 1962. Space Communications and the Law: Adequate International Control After 1963? In *Michigan Law Review*, 60, 877-879.

[51] Estep et al, at 877-879.

[52] See generally Juliana Maio. 1978. Direct Broadcast by Satellite: A Domestic and International Legal Controversy. In *Comm/Ent L.S.*, 1.

[53] Savage et al, at 357-359.

[54] Savage et al, at 359.

[55] See Morozov, *supra* (noting that Internet freedom is viewed in some quarters as "another Trojan horse for American imperialism").

[56] See Wang. 2011. The Great Internet Freedom Bluff of Digital Imperialism. In *Cultural Bytes* (online), http://culturalbyt.es/post/1141832150/internetfreedom

[57] Karl Kathuria. 2011. Report: Casting a Wider Net— Lessons Learned in Delivering BBC Content on the Censored Internet. Canada Centre for Global Security Studies and the Citizen Lab, Munk School of Global Affairs, University of Toronto, http://www.munkschool.utoronto.ca/downloads/casting.pdf.

[58] See generally, Hills, *supra*.

[59] David Ignatius. 2010. Cold War Feeling on Cybersecurity. In *Real Clear Politics (Online)*, http://www.realclearpolitics.com/articles/2010/08/26/cold_war_feeling_on_cybersecurity_106900.html.

[60] Ron Deibert. 2010. Militarization of Cyberspace. In *MIT's Technology Review*, http://www.technologyreview.com/computing/25570/.

[61] See Roger P. Alford. 2012. Apportioning Responsibility Among Joint Tortfeasors for International Law Violations. In *Pepperdine Law Review*, 38:2, 223-224.

[62] Alford, at 235.

[63] Gary C. Hufbauer and Nicholas K. Mitrokostas. 2004. International Implications of the Alien Torts Statute. In *Journal of International Economic Law*, 7:2, 246.

[64] Alford, at 235-236.

[65] Alford, at 235.

[66] Neil Conley. 2007. The Chinese Communist Party's New Comrade: Yahoo's Collaboration with the Chinese Government in Jailing a Chinese Journalist and Yahoo's Possible Liability. In *Penn State Law Review*, 111:1, 205.

[67] Catherine Rampell. 2007. Yahoo Settles With Chinese Families. In *Washington Post (Online)*, http://www.washingtonpost.com/wp-dyn/content/article/2007/11/13/AR2007111300885.html?hpid=topnews

[68] Evgeny Morozov. 2010. More on Internet intellectuals and the Haystack affair. In *Foreign Policy Magazine (Online Blog)*, http://neteffect.foreignpolicy.com/posts/2010/09/14/more_on_internet_intellectuals_and_the_haystack_affair

[69] Lyle Denniston. 2012. Argument Preview: Human Rights Abuses and the Law. In *Scotusblog*, http://www.scotusblog.com/?p=139654 (previewing arguments in the SCOTUS appeal *Kiobel et al v. Royal Dutch Petroleum (10-1491)*).