Rollins College
Rollins Scholarship Online

Honors Program Theses

Spring 2019

Treatment and Evolution of Digital Rights: A Comparative Analysis of China, Russia, the United States, and Germany

Karina Barbesino
kbarbesino@rollins.edu

Follow this and additional works at: https://scholarship.rollins.edu/honors

Part of the American Politics Commons, Asian Studies Commons, Chinese Studies Commons, Comparative Politics Commons, Eastern European Studies Commons, International Relations Commons, Other International and Area Studies Commons, Public Policy Commons, Science and Technology Policy Commons, and the Science and Technology Studies Commons

Recommended Citation
Barbesino, Karina, "Treatment and Evolution of Digital Rights: A Comparative Analysis of China, Russia, the United States, and Germany" (2019). *Honors Program Theses*. 97.
https://scholarship.rollins.edu/honors/97

This Open Access is brought to you for free and open access by Rollins Scholarship Online. It has been accepted for inclusion in Honors Program Theses by an authorized administrator of Rollins Scholarship Online. For more information, please contact rwalton@rollins.edu.

TREATMENT AND EVOLUTION OF DIGITAL RIGHTS:

A COMPARATIVE ANALYSIS OF CHINA, RUSSIA, THE UNITED STATES, AND GERMANY

Karina Barbesino

A Senior Honors Project Submitted in Partial Fulfillment of
Requirements of the Honors Degree Program

May 2019

Faculty Sponsor: Dr. Joan D. Davison

Rollins College

Winter Park, Florida

Contents

Section 1: Introduction……...…….3

Section 2: Evolution of the Conceptions of Human and Digital Rights……..….6

Section 3: China……...……..16

Section 4: Russia……...…….22

Section 5: United States……...……..27

Section 6: Germany……...…….33

Section 7:Comparative Analysis and the Consideration of Regime Type……...…….39

Section 8: Conclusion……...…….51

Section 9: Bibliography…….56

Introduction

Thirty years ago, in the same year that witnessed pro-democracy protests in Tiananmen Square and the fall of the Berlin Wall, the first email that marked the birth of the internet was easily overshadowed. In 1989, approximately 500,000 users were connected through MCI Mail and CompuServe email servers. Later in that same year, Tim Berners-Lee and his team at CERN invented the World Wide Web, but it was not open to public use until 1991 (Waring, 2018). As of January 2019, the total number of internet users across the world reached 4.39 billion, more than half of the world's total population (Kemp, 2019).[1] The impact the internet and other digital technologies have on the lives of those who have access to them cannot be overstated; nearly every facet of the daily lives of individuals, corporations, and governments are affected.

One such area of society that has been empowered by the internet is human rights. The internet and digital technologies allow for the recognition, advocation, and protection of human rights. People around the world have access to faster and exponentially more information than ever before. The possibilities for education, politics, healthcare, work and equality have greatly expanded. The internet provides new opportunities for the progression of humanity, but not without a cost.

Last year in Shanghai, Dong Yaoqiong livestreamed herself throwing black paint on a poster of Chinese President Xi Jinping in an act of protest against him and the Chinese Community Party. Within hours police were at her door and she has not been heard from since (Ma, 2018). In 2017, the German police orchestrated a coordinated raid in all but two of its states. The homes of 36 individuals accused of posting alleged hateful and extremist content on social media were raided (Shimer, 2017). Maria Motuznaya, 23-years old, was placed on Russia's official list of extremists and terrorists after memes she posted on her social media account when she was 20 years old resurfaced. She faced up to six years in prison as a result (Robinson, 2018). While reporting on and livestreaming a demonstration by immigration activists in Memphis, Tennessee, journalist Manuel Duran was arrested and placed in Immigration & Custom Enforcement (ICE) custody. After having all criminal charges dropped in court, Duran was immediately detained by ICE (U.S. Press Freedom Tracker, 2018).

The transformative power of the internet to both empower and infringe on human rights has not been lost on states. As a relatively new domain, the policies in cyberspace remain in their trial periods. Each state is implementing, redacting, and implementing again policies affecting their citizens' rights in order to strike a balance between national security and collective and individual rights. Several influential leaders in cyberspace have emerged for different reasons: the United States, Russia, China, and the European Union. Although the European Union can be considered a state actor, rather than a political system, because of the trait of shared sovereignty, this thesis will use Germany as a case study for reasons of consistency, equal level analysis, and

[1] However, despite claims in 2013 by Google Executive Chairman Eric Schmidt that everybody in the world would be connected to the internet by 2020 (Gross, 2013), a substantial portion of the global population remains unconnected. In 2016, 90 percent of the population that does not have access to the internet are in developing countries, highlighting the issue of disproportionate modernization across regions.

due to the arguably hegemonic role of Germany in the European Union (Paterson, 2011; Kornelius 2010, Schönberger, 2012).[2]

Each state places various degrees of emphasis on human rights affected by the internet. On one end of the spectrum, Germany aims to protect its citizens' data and privacy, while on the opposite end China enforces stringent censorship. The United States and Russia fall somewhere in between. Regarding the nature of this research, and the often-secretive nature of states' domestic cyber policies, an acknowledgement must first be made in the difficulty to accurately quantify the numbers and statistics of internet users and victims of internet crackdowns. An honest effort will be made to cite primary sources from each state but will often be qualified by state-biased think tanks and military reports.

The goal of this thesis is to provide a comparative analysis of the state of digital rights in four states across the human rights spectrum: China, Russia, the United States, and Germany. In order to do so, a review of literature regarding internet access as a human right will be conducted, as well as an overview of the evolution of digital rights. Next, a brief overview of the major domestic cyber policies and international stance of each of the four cases will be presented. Once a clear understanding of the digital rights situation for each state is established, a comparative analysis will be undertaken. In order to aid in the process of this analysis and provide insight for further research, this thesis offers several hypotheses on the relationships between government transparency and invasiveness in individual sovereignty and political stability and likelihood of government interference in citizens' digital rights. These are:

H_1: As a state's transparency decreases it is more likely to be invasive of its citizens' digital rights.

H_2: As a state's transparency increases it is more likely to protect its citizens' digital rights.

H_3: States with low levels of political stability are more likely to interfere in their citizens' digital rights through policies that are claimed necessary to protect national security.

H_4: States with high levels of political stability are more likely to implement policies to protect their citizens' digital rights.

Rather than simply providing an overarching analysis of the stance individual governments have on their respective citizens' digital rights situation, these hypotheses and their results aim to search for a deeper correlation. As a relatively new field, the analysis of the treatment of digital rights and the progression of policies affecting these rights in various situations in the current world order are critical to understand how and when the current international policy gap concerning human rights affected by the internet and digital collections will be resolved.

This thesis will be looking at domestic policies relating to cyberspace and the internet mostly between 1995 and 2019, unless policies prior to the internet are worth noting. This

[2] This is a debatable claim (Kundnani 2012). For the purpose of this thesis, Germany will be understood as the representative of its own policies as well as EU policies because the issue of cybersecurity is comparable to economic and trade issues. Therefore, according to the EU charter jurisdiction, the issue of cybersecurity falls on the union level.

timeframe was deliberately chosen in order to provide consistency between the four case studies. Despite the internet being publicly accessible since 1991, its accessibility in the four case studies varies. For example, it was not until 1994 that China became officially recognized as a country accessible to the internet (CERNIC, 2001). As is often the case with policy analysis, by the time this thesis will be finished it would be of no surprise if new laws and policies are implemented in each case study; however, in order to avoid ceaseless additions this thesis will only analyze policies prior to March, 2019.

The data concerning digital rights violations for this thesis will come from Freedom House's annual Freedom on the Net reports for each state. In these reports an overall internet freedom score is given to each country out of 100, where 100 is the worst and 0 is the best. This score is a cumulation of three subsections: obstacles to access, limits on content, and violation of users' rights. The last of these subsections, violation of users' rights, is of particular interest and will be used heavily during the comparative analysis section. This score is out of 40, where 40 represents the highest volume of users' rights violations, and 0 represents no user rights violations. To supplement the sections relating to human rights, Transparency International and Human Rights Watch will also be cited. The World Bank's global governance indicators will be used to determine a state's transparency and political stability levels. The former will be measured by the control of corruption governance score and the latter by the political stability and absence of violence/terrorism score. Both of these scores fall between -2.5 to 2.5, the lower end of this range being the worst while the upper range is the best. Finally, wherever possible an honest effort to use primary policies in their original languages will be made for the Germany and China sections. Where this is not possible, academic journals and news articles for these languages will also be sought.

I. SHOULD A RIGHT TO THE INTERNET EXIST?

> *"Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States."*
> *(La Rue, 2011)*

In June of 2011, amidst the chaos of the Arab Spring, the United Nations special rapporteur, Frank La Rue, published a report declaring that the internet and human rights are unquestionably intertwined. Previous declarations, charters, and conventions already acknowledged this connection, going so far as to affirm that access to the internet is a human right,[3] but this was the first definitive assertion by the United Nations. Numerous articles quickly took this report to mean that the United Nations considers access to the internet to be a human right (Howell and West, 2016). However, critics soon emerged and contested this interpretation of the report and instead used the above quote to justify, among other arguments, that the internet is an enabler of rights, but not a right by itself.

Three main arguments emerged in the question of whether the internet constitutes a human right. One camp argues that it is undoubtedly a right and thus states should be obligated to provide access to it. Another argument is made that because the internet ensures the safeguarding of natural rights it is a legal right. Lastly, there are those who say the internet is not a human right and saying otherwise will lead to the devaluation of other rights. Yet, despite these different interpretations there tends to be a general agreement on the role of the internet on protecting and facilitating other human rights.

Within the last two decades an increasing number of charters, conventions, and reports have argued that the use of the internet allows individuals to exercise various fundamental human rights protected by the UDHR, ECHR, ICCPR, and ICESCR, including: the right to information protected by Articles 19, 20, and 26 UDHR, the right to control access to information protected by Article 12 UDHR, the right to privacy protected by Article 17 ICCPR and Article 8(2) ECHR, freedom of expression protected by Article 19 UDHR, and freedom to assemble protected by Article 20 UDHR (Mathiesen, 2014; Watt, 2017). The progression of the recognition of the internet in protecting these established rights can be seen in Table 2.1 and Table 2.2 where an increase in the rights associated with the internet has increased over the years.

A. The Internet is a Human Right

Academics and practitioners classify human rights as negative or positive rights (Callaway and Harrelson-Stephens, 2007**)**. Negative rights refer to rights that must be protected from outside intrusion and include rights such as freedom of expression and freedom from torture. In the context of internet access this means states would be prohibited from interfering in or blocking citizens' ability to connect. Positive rights refer to human rights that a state must

[3] Namely courts and parliaments in both France and Estonia affirmed that internet access is a human right (Cerf, 2012).

provide for its citizens and is often attributed to rights such as the right to education and the right to legal recourse. In the case of internet access, this would mean governments must ensure that all citizens have equal access which requires a government to provide adequate infrastructure and resources to make internet connectivity possible. As Penney (2011) noted, the "Special Rapporteur examined Internet access rights in both senses, not only talking about people's freedom to access Internet content, but also state obligations to provide access to the physical infrastructure necessary for Internet connectivity" (Penney, 2011:15). Accordingly, despite not explicitly stating that the right to the internet is a human right, it can be assumed through this context and a close reading of UDHR Article 19, restated here for convenience:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers (G.A. Res. 217A).

The controversy begins when, in his 2011 report, La Rue explained that Article 19 "was drafted with foresight to include and to accommodate future technological developments through which individuals can exercise their right to freedom of expression" (La Rue, 2011). The term that justifies this interpretation is "media." Despite being drafted over half a century prior, La Rue underscores that the UDHR and subsequent conventions were purposefully written in such language so as to later incorporate more advanced means of communication. Indeed, Land (2013) concludes that through the drafting process of the ICCPR and UDHR, media has been confirmed to mean both the channel and the form of expression.

Semantics are important in determining the legitimacy of the right to the internet. It is valid to say that initial human rights conventions have not aged well in the digital age. For example, General Comment No. 16 issued in 1966 on privacy lacks explicit mention of pressing issues, including:

> banning untargeted, mass surveillance, bulk metadata collection and retention; intelligence services/law enforcement access to communication data held by third-party providers and internet companies including in a 'cloud'; the relationship between private companies and governments; biometric data gathering (through, for example, finger-printing, facial recognition software) and transborder access to non-publicly available data, circumventing the requirements of the Mutual Legal Assistance Treaties. (Watt, 2017:788)

Yet, it would have been impossible to explicitly account for and anticipate all of these issues prior to their inception. As such, it is to the discretion of UN policymakers and states in accordance with these conventions to carefully interpret and integrate modern issues with fundamental rights.

Article 19 of the UDHR is often used to spearhead the recognition of the internet as a human right but it is not alone. Under Article 27 of the UDHR, individuals have a right to enjoy their culture, religion, language and share in scientific advancements and its benefits (G.A. Res. 217A). This latter portion furthermore takes into account the foresight the original writers of the UDHR possessed. Loss of access to information technologies, specifically the internet, would be detrimental to the world's most marginalized people where access to the internet directly translated to "health, education, employment, the arts, [and] gender equality" (Edwards, 2012). Technological progress and the fulfillment of fundamental rights, particularly freedom of

association and expression, are inseparable. The timing of the UN special report, published during the internet-enabled Arab Springs, further undermines the connection between access to internet, as both a "media" described in Article 19 and a "scientific advancement" stated in Article 27, and human rights.

Simply put: times change. Modernization and globalization aided to usher in the Information Age through the internet. Cultures, systems of governance and technologies are all subject to change, the latter just happened to transform incredibly fast. In order to not be left behind, interpretations of human rights must also change to ensure the adequate protection of human rights.

B. The Internet is a Legal Right

The internet has empowered and transformed the way in which individuals communicate and share information. Indeed, as Powell, Byrne and Dailey (2010:163) emphasize, the internet "has become a 'basic requirement' for social inclusion and economic participation," both of which are fundamental rights protected by the UDHR. Furthermore, it is widely recognized that the absence of access to the internet disadvantages and excludes individuals from a modern lifestyle and equal social opportunity, thus is arguably a human rights violation (Hammond, 1997; O'Hara and Stevens, 2006; Tully, 2014).

However, despite a general acknowledgement of the importance of the internet in upholding human rights, even La Rue admits that "there is no right to the internet 'as such'" (Land, 2013:400). Upon closer inspection, while the UN report did bring just focus on the importance of the internet in connection to human rights and calls for states to work towards universal access to the internet, it did not explicitly state the internet is a human right. Similarly, the UN Human Rights Council Resolution on Internet and Human Rights passed in 2012 includes the "promotion, protection, and enjoyment of human rights on the Internet," but does not mention the internet as a human right (York, 2012).

After coming to this conclusion, Tomalty (2017) suggests clearly distinguishing human rights between "legal human rights," such as those articulated in the UDHR, ICCPR, and ICESCR and natural rights, as in "the moral rights taken to be held by all humans simply by virtue of being human." Tomalty (2017:6) clarifies that the latter must be grounded in morally relevant attributes of humanity in which the most dominate attribute is arguably that natural rights are "grounded in fundamental interests shared by all, or at least the majority, of humans." This implies that natural rights are more basic and inherent to humanity, regardless of society or era, and exemplified in the right to not be tortured and freedom from slavery. By this logic, access to the internet, as a commercial product of humans, is not a natural right because having access cannot be held universally by all humans simply in virtue of being human.

That is not to say that a legal right for the internet does not exist. Legal rights are social constructs that can emerge over time, in light of technological and societal advancements. In its most basic form, legal rights are a social construct are decided by people, not discovered (Tomalty, 2017). Legal rights must be created in order to protect natural rights, therefore the natural rights articulated in human rights conventions are both natural and legal, but not all legal rights are natural. For example, UDHR Article 15 protects an individual's right to a nationality. Nationality is a social construct that encompasses a more fundamental human right, namely freedom of movement which is arguably a natural right. Although both are now legal and human rights due to their presence in legal human rights documents, only UDHR Article 13 freedom of

movement, is a natural right. The implication of this differentiation would be domestic implementation. If a state acknowledges a legal right to internet access without international treaties recognizing it as a human right, this implies a state could be exempt from having to provide internet access for all people within the country. Instead, much like the legal right to vote, ability to exercise this right is contingent upon citizenship, age, and other factors.

As previously discussed above, access to and use of the internet involves several natural rights including freedom of expression, association, information, and education. Although it is possible to exercise these rights through other means, the scope of the internet and its presence in increasingly more aspects of society necessitates its access to ensure equal opportunities. Given the apparent enduring nature of the internet in society, it is important to recognize that the internet is a legal right and should be protected as such.

C. The Internet is not a Human Right

The UN Special Report used the protests in the Middle East and North Africa as proof of the transformative power of the internet to be used as a conductor for human rights such as freedoms of expression, information, and association. Yet, mention of the internet as a human right was starkly absent, as it should be. Vinton Cerf (2012), a co-creator of the networking technology that made the internet possible, noted this absence in his op-ed piece in *The New York Times* and concluded this was due to the understanding that "the Internet was valuable as a means to an end, not an end in itself." Human rights are characterized by their necessity to maintain human dignity. It is possible to live without the internet and equating access to it to rights that afford shelter, food, and water to individuals is wrong. In fact, access to the internet is so intrinsically bound to already existing human rights that formalizing its recognition as a separate right is unnecessary and could arguably dilute and threaten other rights (Tully, 2014; Land, 2013).

The internet is undoubtedly an important means to exercise existing human rights and therefore aids in progressing the human condition. However, access to the internet is simply an enabler of rights, it must not pretend it is a right by itself. The speed in which technology is changing makes predicting technological developments and how these developments will impact civil and human rights impractical at best and impossible at worst. The international community should be aware of this and remain cautious about "immortalizing any particular kind of technology in international law" (Land, 2013:400).

While the internet is often praised for its ability to disseminate mass amounts of information, this same attribute contributes to the violation of other rights. As Tully (2014:184) aptly suggests, "it is equally apparent that Internet access and use can threaten the enjoyment of human rights for certain groups and the potential to affront human dignity." The Committee on the Rights of the Child has oft been concerned with increasing access to the internet internationally:

> Estonia has been requested to assess sexual exploitation and child trafficking on the Internet. Pornographic and other harmful material was accessible to children via the Internet in Monaco, Croatia, Greece, Costa Rica, Norway, Micronesia and Japan. Germany was commended for attempting to protect children from this information. Children were exposed to racist and violent images and games through the Internet in Luxembourg and Austria. Indeed, children were sexually abused following contact

> established on websites in Sweden and Slovenia. Internet chat rooms frequented by children had been arbitrarily closed in South Korea. (Tully, 2014:183)

Additionally, the use of the internet to facilitate and expand human trafficking networks and the prostitution of women has violated the rights advocated for by the Committee on Elimination of Discrimination against Women, Denmark is one such case of many (United Nations, 1997). Recognizing access to the internet as a human right indirectly violates well-established basic human rights of children and women.

Philip Alston (1984:614) cautioned that "a proliferation of new rights would be much more likely to contribute to a serious devaluation of the human rights currency than to enrich significantly the overall coverage provided by existing rights." Declaring access to the internet to be a human right gives way to a valid fear of a domino effect of calls for further rights in other technologies, the culmination of which might "dilute the protections for freedom of expression in general" (Land, 2013:400). Each state has a hierarchy of human rights that they place importance on. These hierarchies have led to disagreements on ideological values and the refusal to accept legal obligation, the combination of which resulted in the division of the UDHR into the ICCPR and ICESCR (Tolley, 1987). The addition of more rights would add unnecessary complexity and lead to further disagreements between states about each right's moral and legal worth. This would not only call into question the scope of states that would accept the legal obligation of providing and protecting internet access, it would also once more call into question the validity of more fundamental rights. Furthermore, the fact that countries, even democracies, claim that the internet takes a back seat to national security implies that access to it cannot be an inalienable human right (Goel, 2019).

II. EVOLUTION OF DIGITAL RIGHTS

For the purpose of this thesis the term "digital rights" will refer to the practices that are protected and realized by the use of digital technologies, particularly the internet. Which human rights this definition encompasses has changed over time and is subject to further changes in the future as technology progresses. Anticipating the threats to fundamental human rights prior to the publicization of the internet, the Council of Europe passed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981. This was the first international convention to address the "increasing flow across frontiers of personal data undergoing automatic processing" (Council of Europe, 2001). As shown in Tables 2.1 and 2.2, the main concern of this convention was to safeguard the right to privacy, a theme that remained consistent throughout the years in various digital rights conventions and charters.

The 2001 Convention on Cybercrime is the first international treaty that aims to address crime in cyberspace by harmonizing the national laws of involved countries and improving investigative techniques (ETS No. 185, 2001). Article 15 of this convention specifically states that the implementation and application of powers and procedures addressed in the convention are pursuant to the obligations outlined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms and the ICCPR. Unlike the 1981 convention, there is an article within the Convention of Cybercrime that protects a right outlined in the ICESCR, namely the rights of children.

Table 2.1 *ICCPR Articles*	**1981** Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	**2001** Budapest Convention on Cybercrime	**2002** People's Communication Charter	**2006** APC Internet Rights Charter (revised)	**2011** Charter of Human Rights and Principles for the Internet
Right to Legal Recourse (Article 2)	—	Article 15	Article 7	Theme 7.2	Article 18
Gender Equality (Article 3)	—	Article 15	—	Theme 1.5	Article 2(c)
Right to Equality Before the Law (Article 14)	—	Article 15	Article 15	—	—
Privacy (Article 17)	Article 12(2), Article 11	Article 15	Article 13	Theme 5	Article 8
Freedom of Thought, Conscience and Religion (Article 18)	—	Article 15	—	—	Article 6
Freedom of Opinion and Expression (Article 19)	—	Article 15	Article 2	Theme 2, 3	Article 5
Prohibition of Propaganda (Article 20)	—	Article 15	Article 14	—	Article 5(e)
Right to Peaceful Assembly (Article 21)	—	Article 15	—	Theme 2.3	Article 5(a),6
Freedom of Association (Article 22)	—	Article 15	—	—	Article 6
Rights for Children (Article 24)	—	Article 15	Article 11	—	Article 12
Right to Participate in the Conduct of Public Affairs (Article 25)	—	Article 15	Article 10	—	Article 15
Rights for Minorities (Article 27)	—	Article 15	Article 8, 9	Theme 1.9	Article 2(b)

Table 2.2 *ICESCR Articles*	**1981** Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	**2001** Budapest Convention on Cybercrime	**2002** People's Communication Charter	**2006** APC Internet Rights Charter (revised)	**2011** Charter of Human Rights and Principles for the Internet
Gender Rights (Article 3)	—	—	—	Theme 1.5	Article 2(c)
Right to Work (Article 6)	—	—	—	—	Article 14
Just Work Conditions (Article 7)	—	—	—	Theme 1.7	—
Social Security (Article 9)	—	—	—	—	Article 4, 17
Rights for Children (Article 10)	—	Article 9	Article 11	—	Article 12
Right to Education (Article 13/14)	—	—	Article 5	—	Article 10
Take Part in Cultural Life and Benefit from Scientific Progress (Article 15)	—	—	Article 9	Theme 4.3	Article 11

The Convention on Cybercrime, also known as the Budapest Convention, has been ratified by forty-nine parties, including the United States and Germany. Both of which also ratified the ICCPR (see Table 2.3). China, which is not a signatory of the ICCPR, is also not a signatory of this convention. Russia, however, has ratified the ICCPR but their primary objection to the Budapest Convention has less to do with the human rights pursuant to the ICCPR and more to do with the allowance for "unilateral trans-border access of data by law enforcement agencies of one country without notifying the authorities in another county, thus…violating state sovereignty" (Barmin et al., 2011:74).

The remaining three categories listed in Tables 2.1 and 2.2 are charters aimed to expand the scope of digital rights and bring awareness to policy-makers on the domestic and international levels. Each charter specifically states that access to the internet/cyberspace is a human right. Indeed, this movement has led Estonia, Finland, and Costa Rica to recognize internet access as a human right (Tully, 2014). Furthermore, a 2012 Global Internet User Survey found that eighty-six percent of internet users agreed or strongly agreed that the internet should

be considered a basic human right (Internet Society, 2012). Yet, despite progress at the individual and national levels, international organizations and treaties have yet to definitively make this leap.

Table 2.3 *Signatory Statuses*

State	ICCPR	ICESCR	Right to the Internet
China	Signed	Ratified	Not Recognized
Russia	Ratified	Ratified	Not Recognized
United Sates	Ratified	Signed	Not Recognized
Germany	Ratified	Ratified	Not Recognized

Source: (Neumayer, 2007)

As demonstrated in Tables 2.1 and 2.2, in the earlier years of digital rights there was an emphasis on the relationship between the internet and the rights afforded by the ICCPR. However, starting in the twenty-first century as the demand for digital rights grew charters and conventions began to expand which rights are deemed related to cyberspace and the internet. In the case of the rights outlined in the ICCPR, the right to privacy has consistently remained a key component of digital rights. Similarly, minority rights (Article 27), freedom of expression (Article 19), and right to legal recourse (Article 2) are also repeatedly emphasized. Additionally, with each new charter increasingly more rights under both the ICCPR and the ICESCR are specifically named to warrant additional protections.

Similarly, the rights afforded by the ICESCR have been increasingly incorporated in digital rights charters and conventions over time. Although not initially seen as related to digital rights, the last decade has seen the expansion of the scope of human rights considered to be digital rights. Most notably, the right to take part in cultural life and benefit from scientific progress (Article 15) and the rights of children (Article 10) are repeatedly recognized by digital rights charters.

As noted above, the division of digital rights along ICCPR and ICESCR lines may help to provide insight in their acceptance or rejection by states and subsequently international organizations. The incorporation of more ICESCR rights may aid in the acceptance of future cyber conventions by states which ratified the ICESCR. A government's view on digital rights may influence its domestic cyber policies and willingness to ratify international treaties. Yet, as seen in the case of Russia in the Budapest Convention, this is not absolute. Regardless, the expansion of digital rights showcases the growing influence of technology on almost every facet of society.

III. HUMAN RIGHTS IN THE CONTEXT OF CYBER FREEDOM AND SECURITY

The level of importance placed on human rights on the international and national levels is directly related to the dominant ideologies of the world order and specific state contexts in which it exists. The current world order was forged from the aftermath of the Cold War which saw the United States as the unequivocal world hegemon. The American preponderance of power ensured that the liberal international organizations created during that time, and to some extent continue to be, a reflection of American liberal values. During this time, liberalism was the

dominant theory in international relations because it happened to be the ideology of the most powerful state at the time (Sterling-Folker, 2015). This sentiment carried on throughout the 1990s which saw a drastic increase in the number of international organizations and preponderance of liberal values, including the importance of human rights.[4] This can also be seen by the expansion of digital rights as norms, consistent with constructivist theories. Thus, the acceptance of digital rights as a norm is contingent upon the attitudes towards liberal values in a world order. If the norm is not sufficiently spread and accepted before a shift in the world order then that may hamper its legitimacy and strength, a situation that is now unfolding in China, Russia, and even democracies like India (Goel, 2019).

Although the post-Cold War world was best described as a liberal one, some theorists argue that liberal theory was hard-pressed to accurately explain it (Gleditsch, 2008). This critique also extends to the seeming degeneration of the liberal order today. The importance placed on liberal ideological values that advocated for the protection of individual sovereignty in order to benefit society are diminishing in a global society where emerging actors are not liberal or even democratic. The golden years of global governance are gone, replaced now with fragmented international organizations and gridlock on decisions of transnational issues, cybersecurity being one of them (Stephen, 2017). The emerging non-liberal, non-democratic powers—China being the most notable, but Russia should not be overlooked—do not subscribe to the liberal ideological characteristics of global governance, even if they do benefit from the existence of these institutions (Zhang, 2016). Yet, this does not mean the end of global governance necessarily. As explained by Stephen (2017), global governance may still occur but without the dissemination of liberal values.

Whether global governance without the promise of the protection of liberal values like human rights will result in rules and institutions that can effectively tackle the complex transnational issues of cybersecurity and human rights is unclear. In order to solve the global challenge of cybersecurity a "hardheaded assessment of which players really matter in getting to an acceptable answer and a process of bargaining to get them aligned" is required (Barma, Ratner and Weber, 2012:66). Yet, the range of perspectives on this issue at the national level between powerful states are diverse and often rooted in a state's hierarchy of human rights. Therefore, to expect a consensus to be drawn in a world order where emerging actors do not champion traditional liberal norms is ill-timed.[5] However, as Deudney and Ikenberry (2018) suggest, liberal democracies are remarkably robust and have faced and recovered from worse. They would advocate that if a return to the fundamentals of liberal democracy is accomplished, then institutional innovations may emerge to adapt and respond to global challenges.

Despite previous interstate demonstrations of cyber capabilities, many nations did not view cybersecurity as a top priority national security until 2001. Days following the September 11th attacks the Federal Bureau of Investigation warned of further possible attacks, including cyber terrorism (Spencer, 2002). The issue of cybersecurity then took on a different hue and debates ensued on the capabilities of cyberwarfare; would it equate to mass destruction,

[4] Whether these institutions and the order of this time were truly liberal is debated (Barma, Ratner and Weber, 2012).

[5] In 1998, fearing that information weapons would be on the same scale as weapons of mass destruction, Russia promoted a proposal to the UN to restrict what states can do with cyber weapons but was curtailed by the United States (Barmin et al., 2011). Even in the golden years of global governance and liberal values progress was not made on tackling cybersecurity which seems to suggest that Barma, Ratner, and Weber (2012) were right in their analysis.

trademarked by direct physical damage on infrastructure resulting in civilian casualties, or mass disruption, defined as the ability to change, delay, delete or redirect data in order to cause economic, social or political disorder. The last decade has witnessed sufficient proof for the case of mass disruption in the forms of the 2007 Estonian cyberattacks that resulted in the sporadic take down of banking systems, government communication, and media outlets and more recently the 2016 Russian hacking of the Democratic National Committee and other democratic organizations (McGuinness, 2017; Diamond, 2016). However, although no cyberattack to date has resulted in the loss of life, political theorists like Deudney and Ikenberry (2018) are confident in the mass destruction capabilities of cyberwarfare—a claim that can be supported by the 2010 Stuxnet computer worm which is known as the first cyberattack to cause physical damage across international borders (Lindsay, 2013). Considering the current rapid pace of cyberspace potential, the next decade will be crucial in setting international norms. Although it is unlikely that a return to liberal fundamentals will reach the same level of international priority, deliberation, and collaboration as it did in the second half of the twentieth century within this timeframe, it is possible that the fear of the potential of cyberwarfare will bring all states to the negotiating table.

On the national level, the fear generated by the possibility of a cheaper and more accessible weapon of mass destruction could help to justify some states' domestic cyber policies. Yet, this excuse could be used in order to justify limits on human rights related to the internet when in actuality a state's domestic cyber policies are implemented to maintain political stability. This theme will be explored in later sections. Regardless, according to Keohane (2002), a government's first task is to protect their people, thus policies that prioritize national security over individual sovereignty are acceptable. Furthermore, an argument can be made that modernized states are the most vulnerable to cyberattacks due to a reliance on technology to sustain fundamental systems like infrastructure and power grids which provides both economic and social stability to a state. For these reasons, it is not surprising that some emerging states, and even the United States, sometimes subscribe to domestic policies that place national security over citizens' derogable human rights. However, this alone does not explain the approach of some modern regional powers. For example, Germany and other western European countries have implemented domestic policies that serve to protect digital rights. The hypotheses provided in the former section of this thesis will attempt to explain this divergence, that is the existence and protection of these practices as rights relates to levels of transparency and political stability in a state.

China

I. DOMESTIC CYBER POLICIES

"As in the real world, freedom and order are both necessary in cyberspace: Freedom is what order is meant for, and order is the guarantee for freedom. We should respect internet users' rights to exchange ideas and express their minds and we should also build good order in cyberspace in accordance with [the] law as it will help protect the legitimate rights and interests of all internet users" (Phillips, 2015).

-President Xi Jinping at the Opening Ceremony of the Second World Internet Conference, 2015.

China registered to become the 71st country on the global computer network and received CN as the "highest level domain name" in 1994, however it was not until January of 1995 that the 64K special lines were put into operation that internet access services began to be offered to the public (Shahbaz, 2018; Cnnic.com.cn, 2012). China experienced unprecedented expansion of internet use after realizing "the significance of computer information in its economic development and encouraged fast development of Internet in commercial use to embrace the new information era" (Liang and Lu, 2010:104-105). An indication of this tremendous expansion is the increase of internet users over the years. The Chinese Internet Network Information Center (CNNIC) reported approximately two million users in 1998, more than 100 million in 2005, and surpassed 298 million by the end of 2008, exceeding the number of internet users in the United States (Liang and Lu, 2010). As of December 2017, the total number of internet users in China reached 771.98 million (Statista, 2017).

With such a massive internet user base, the effect of cyber policies is especially imperative to widespread human rights violations or protections. In the case of China, internet development accompanied "the government's tight control and regulation over Internet infrastructure, its commercial and social use, and its potential political ramifications" (Liang and Lu, 2010:104). Article 35 of the Chinese Constitution gives citizens of the People's Republic of China freedoms of speech, press, assembly, association, procession, and demonstration (CHINA, 1983). Yet, media regulations undermine these rights by allowing authorities to crack down on news stories that "expose state secrets and endanger the country" (Xu and Albert, 2017). Indeed, the protection of national sovereignty is regularly used as an argument to censor information deemed harmful to Chinese political or economic interests and surveil and punish both citizens within and outside the country, as well as foreign journalists, activists, and NGOs inside of mainland China. In fact, China is regularly reported as the worst abuser of internet freedom according to Freedom House (Shahbaz, 2018).

Various laws/regulations (see Table 3.1) outline under what conditions different online activities and information are deemed illegal. The culmination of these conditions, as stated in Article 19 of the Provisions on the Administration of Internet New Information Services (Congressional-Executive Commission on China, 2005), are the following:

(1) violating the basic principles as they are confirmed in the Constitution;
(2) jeopardizing the security of the nation, divulging state secrets, subverting of the national regime or jeopardizing the integrity of the nation's unity;
(3) harming the honor of the interests of the nation;

(4) inciting hatred against peoples, racism against peoples, or disrupting the solidarity of peoples;
(5) disrupting national policies on religion, propagating evil cults and feudal superstitions;
(6) spreading rumors, disturbing social order, or disrupting social stability;
(7) spreading obscenity, pornography, gambling, violence, terror, or abetting the commission of a crime;
(8) insulting or defaming third parties, infringing on the legal rights and interests of third parties;
(9) inciting illegal assemblies, associations, marches, demonstrations, or gatherings that disturb social order;
(10) conducting activities in the name of an illegal civil organization; and
(11) any other content prohibited by law or rules.

These conditions either directly relate to or are the foundation that results in policies that both violate and protect multiple digital rights. On one hand, these conditions seem to ensure the protection of various rights like minority rights (4) and the rights of children (7). Regarding the former, this condition seems to imply that citizens may not directly inflame racism or hatred against peoples. However, this does not hold true for state-sponsored racist policies like the detainment of over an estimated one million Uighurs in Xinjiang province. Furthermore, an argument can be made that this condition does not have the fifty-five recognized minority groups in mind, but rather is equally applicable against minorities in order to protect the Han majority. Alternatively, the majority of these conditions allow for the violation of freedom of expression (2, 6), freedom of privacy (2,3) which affects the right to information, freedom of religion (5), freedom of association (9), freedom of assembly (9), and the right to political participation (1,6,10). Policies use these conditions as guidelines which legalizes varying degrees of state surveillance and censorship.

However, prior to these conditions a national project was already underway to protect the state from the feared democratic influence of the internet. In 1998, the Golden Shield Project, now more commonly known as the Great Firewall of China, was launched by the Ministry of Public Security. What has been referred to as the world's largest firewall is a combined censorship and surveillance project that utilizes firewalls, internet registration, keyword filtering, bandwidth throttling, and government controls on website access in order to establish a cyber boundary around the Chinese internet (Qiu, 2000; Xu and Albert, 2017; Whiting, 2008). The main function of this ongoing project is to censor and control information on the internet on both the domestic and global level (Dowell, 2006). Despite previously being relatively easy to circumvent through the use of virtual private networks (VPN), Freedom House reported in their 2018 Freedom on the Net report that "the [Chinese] government took new measures to restrict the use of circumvention tools to bypass blocking and filtering; Apple complied by removing hundreds of virtual private network services from its online app store" (Freedom House, 2018a). Even foreign companies operating within mainland China are conceding to recent pressure to stop aiding in the circumvention of domestic cyber policies that restrict digital rights.

The level of online censorship and surveillance, although consistently among the strictest worldwide, has fluctuated over the years. This is in part due to the often vague nature of the legislature which allows for quick changes in policies and different interpretations. Internet users and business owners are particularly vulnerable to this legislative breadth and vigor which holds

them in "constant fear and therefore strengthens their self-censorship" (Liang and Lu, 2010:109). A possible cause for what Council of Foreign Affairs Senior Fellow Elizabeth C. Economy calls a state of "schizophrenia" in regard to Chinese media policy could be the realization that China needs to allow citizens to enjoy some freedom of press, but fears the repercussions which may lead to a demand for more rights (Xu and Albert, 2017). The most recent show of the fluctuation of online control has occurred since President Xi Jinping came into power. Under the now permanent rule of President Xi, "censorship of all forms of media has tightened" (Xu and Albert, 2017). This is best exemplified by two new major domestic policies that went into effect in 2017: the Cybersecurity Law and the National Intelligence Law (see Table 3.1). The former drastically strengthens online censorship and is the "latest step in China's long-term campaign for jurisdictional control over content on the internet" (Wagner, 2017). Although this idea of internet sovereignty, defined as the principle that states should have complete control over the internet within their domain, formally dates back to the 2010 government white papers and long-running projects like the Golden Shield project, it is now being reinvigorated and fortified. Since this law came into effect, censorship activity increased by over 40 percent between 2016 and 2017 (Patrick and Feng, 2018). WeChat, a Chinese multi-purpose application with over one billion active users, has seen an increase in arrests since the Cybersecurity Law came into effect (Jao, 2018). In fact, individuals within mainland China have been arrested for the content of their private messages in WeChat (Dou, 2017). The latter of these laws, although characterized as defensive, is seen by others as an offensive obligation to participate in surveillance, and thus consequently increases censorship. This is done through Article 7 which states that "any organization or citizen shall support, assist, and cooperate with state intelligence work according to law" (Girard, 2019). An average of nearly one new directive every two days has followed in the wake of these two laws in order to further "fine-tune" the dos and do nots of online activity (Shahbaz, 2018).

With new directives and regulations comes the potential for further effects on human rights. A current nationwide project called the Social Credit System (SCS) is a result of increasing surveillance. Described by author Luo Peixin (2018:3) in *Social Credit Law: Principles, Rules and Cases*, the SCS is "a management system that takes big data as its basis, is supported by technological capacities, and is back by law; it is an important modern method to forward the country's governance systems and management capabilities." Construction plans for the SCS were first announced in 2014 and is planned to launch a full roll out in 2020 (Hatton, 2015). This system accounts for citizens' on and offline behaviors and rates their trustworthiness which then determines what opportunities, or lack thereof, a citizen has in life. For example, those with bad ratings may be banned from air and rail travel and those with good ratings may benefit from waived deposits at hotels and expedited security access (Shahbaz, 2018). In addition to violations of privacy and expression, the SCS has also been accused of violating the right to movement, thus expanding the scope of human rights affected by internet policies.

Table 3.1 *China Major Laws and Regulations*

Law/Regulation	Date Promulgated	Purpose
Criminal Law of the People's Republic of China	March 1997	Outlines what constitutes a crime by category of endangerment of national security, endangerment of public security, and disruption of the socialist market economy. Later amendments criminalize cybercrimes.
Measures on the Administration of Security Protection of the International Networking of Computer Information Networks	December 1997	Strengthens the security protection of the international networking of information networks and maintains public order and social stability by outlining what online activities are banned by use of international networking.
Measures on the Administration of Internet Information Services	September 2000	Regulates Internet information services activities by requiring internet information services to obtain a patent through the government to provide services.
Regulations on Telecommunications of the People's Republic of China	September 2000	Regulates the order of the telecommunications market and extends prior regulations to include voice, text, data, images and any other information using wire or wireless systems.
Provisions on the Administration of Electronic Bulletin Services via the Internet	November 2000	Regulates the content, retention period, and genre of electronic bulletin services.
Decision of the National People's Congress Standing Committee on Safeguarding Internet Security	December 2000	Defines how the internet should be used in order to promote a healthy development of China's interests.
Provisions on the Administration of Foreign-Invested Telecommunications Enterprises	December 2001	Requires partially foreign-invested and foreign enterprises to follow national laws/regulations to conduct business in China.
Provisions on the Administration of Internet News Information Services	September 2005	Regulates Internet news information services in a way to safeguard national security and the public interest. No foreign-invested or wholly foreign news venture can establish an Internet news information service.
Cybersecurity Law	June 2017	Centralizes internet policy and obliges internet companies operating in China to censor users' content, restricts online anonymity, and localizes personal data in China.
National Intelligence Law	July 2017	Obliges individuals, organizations, and institutions to assist Public Security and State Security officials by spying and reporting on each other. Gives the Chinese government access to any data on social media.

Sources: (Amnesty International 2018; Girard, 2018; Shahbaz, 2018; [NPC Standing Committee, 2000; Freedom House, 2018a)

II. INTERNATIONAL STANCE

Freedom and order, while seemingly at odds in realist and liberal theoretical frameworks in international relations, have a symbiotic relationship in the eyes of the Chinese government on both the national and international level. As Zhang discusses, despite advocating for realist trademarks like order and state sovereignty, China does not reject the international organizations that have developed from a liberal order due to its current hierarchical ranking in these institutions. Now that the liberal order is declining, China affirms the importance of order in general to tame chaos that would presumably ensue otherwise, yet the type of order is not yet clear. Considering the antagonist stance China has taken towards digital rights domestically despite condemnation from international organizations and NGOs, China may aim to avoid liberal solidarism. Instead, China pushes for a liberal pluralist order which still maintains international organizations but upholds the importance of national sovereignty against what it perceives to be the current priority for rights and democracy. In order to facilitate this, China must first normalize their own approach to digital rights so that a future order could not condemn rights that are not recognized.

When confronted by other states, particularly the United States, and international organizations about its human rights record, China often counters by exposing the tainted human rights records of other nations. This can be seen since 1998 when the Chinese government began issuing a publication entitled *Human rights record of the United States* in response to U.S. pointed criticisms of Chinese policies (Zhang, 2016). By doing so China is both standing firm in its own treatment of digital rights but also delegitimizing the United States' arguments based on U.S. hypocrisy.

In addition to fighting back against condemnation, China is also taking the initiative to promote its own digital rights agenda, including internet sovereignty. According to the 2018 Freedom on the Net report, the Chinese government hosted two to three week "training camps" for media officials from multiple countries to teach about its own censorship and surveillance systems (Shahbaz, 2018). President Xi publicly laid out a national plan to transform China into a "cyber superpower" and presented China's domestic cyber policies as "a new option for other countries and nations that want to speed up their development while preserving their independence" (Shahbaz, 2018). Staying true to this promise Chinese firms already provided "high-tech tools of surveillance to governments that lack respect for human rights" (Shahbaz, 2018). This has proven to be a mutually beneficial project in the case of Zimbabwe where China is receiving biometric data of millions of Zimbabweans without their consent in order to train artificial intelligence programs to recognize darker skin tones.

China's Belt and Road Initiative, also known as One Belt One Road, has attracted international attention as a massive global infrastructure project but the "Information Silk Road" (National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce of the People's Republic of China, 2015). that comes with it is not as well-known. This project has been described by Council of Foreign Affairs scholars Stewart M. Patrick and Ashley Feng (2018) as China's attempt "to export its policy of authoritarian cyber controls, giving countries the right to regulate and censor their own internet." In order to accomplish this goal the Chinese government is laying transcontinental and cross-border optical cables, effectively undermining previous global internet and telecommunications infrastructures. As a

result, global data is more vulnerable to the surveilling and censoring of Chinese intelligence agencies (Shahbaz, 2018).

These international actions seem consistent with Chinese domestic policies in their treatment of digital rights. China's international cyber stance can be perceived as an attempt to construct and disseminate a norm that calls for the subservient status of digital rights and more generally human rights to global and domestic order. By making this a global norm, China would no longer be subject to oft criticism from regulatory bodies and the international community.

Russia

I. DOMESTIC CYBER POLICIES

"Propaganda of drugs and violence, human trafficking and child pornography—that's the reality of today's Internet" (Ognyanova, 2015).

-Article written by Jury Luzhkov, mayor of Moscow in 2004.

Russia has a long, complicated history with information. In the days of the Soviet Union, information and the media were so tightly controlled to the point that the ownership and use of photocopiers was regulated by the state (CEU School of Public Policy, 2017). This long-term use of state control of information may contribute to the current attitude of Russian citizens toward internet censorship; 60 percent of Russians believe that the banning of certain website and materials is necessary, according to a 2016 poll conducted by the Levada Center, a Russian independent, non-governmental polling firm (Taylor, 2016). Indeed, according to Nathalie Maréchal (2017) in her article *Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy*, many Russians think the internet is dangerous and threatening.

This fear is then often fanned by the Russian government and political class to portray the internet as "unreliable, biased, and dangerous" to Russia's 98.8 million internet users (Ognyanova, 2015; Maréchal, 2017; Statista, 2019). The 1990s witnessed a brief relief in restrictions of freedom of press before the government was seized by a new oligarch class which in turn justified President Vladimir Putin's "liberation" of media from oligarchs to state control when he assumed office in 1999 (Maréchal, 2017). Since then, the internet has been under tight state control. However, unlike China, Russia has rarely relied on obstacles to access, such as infrastructural barriers and application level blocking, but instead on censorship, fear, and intimidation (Maréchal, 2017). Katherine Ognyanova (2015) recognizes one mechanism that allows the Russian state to control the media, which is increasingly dependent on the internet, as the selective application of unrelated laws including: "building codes, tax laws, criminal laws, and intellectual property laws" (Maréchal, 2017:31).

According to the 2018 Freedom on the Net report, various articles in the Russian criminal code establish penalties for nine specific activities:

> "general defamation (Article 128.1 of the criminal code), defamation against a judge or prosecutor (Article 298.1), insulting the authorities (Article 319), calls for terrorism (Article 205.1), insulting religious feelings (Article 148), calls for extremism (Article 280), calls for separatism (Article 280.1), and incitement of hatred (Article 282)…spreading false information on the activities of the Soviet Union in World War II (Article 354.1)" (Freedom House, 2018c).

Furthermore, the Russian administrative code establishes penalties for two additional activities: "displaying Nazi symbols or symbols of organizations deemed extremist" (Article 20.3 of the administrative code) and "the dissemination of extremist materials" (Article 20.29 of the administrative code) (Freedom House, 2018c). According to these laws, the digital rights most directly at risk are freedoms of expression (of which, freedom of speech is granted by the Russian constitution), religion, and political participation, which then more indirectly puts the

rights to privacy, assembly, fair trial, and association at risk. This has resulted in Russia's consistently poor ranking and scores in international indices for freedom of expression: Reporters without Borders ranks Russia 148/180, 1 being the best and 180 being the worst, in the 2018 World Press Freedom Index (Reporters Without Borders, 2018). In Freedom House's 2017 Freedom of the Press report Russia ranked 83/100, where 1 is the best and 100 the worst (Freedom House, 2017). This then translates to Russia's current 67/100 score in Freedom House's 2018 Freedom on the Net report.

Within further laws and regulations, the justification of extremist content online is most frequently used to validate censorship, imprisonment, and death. For example, the Russian website Russiangate was blocked by Roskomnadzor (a Russian media regulator) for purported "extremist content" a few hours after Russiangate published a report about an investigation of real estate holdings for Alexander Bortnikov, the FSB (internal intelligence service) chief (Schreck, 2018). In another case, Dmitry Popkov, the editor-in-chief of an independent local newspaper called *Ton-M* in Siberia that often reports on abuses of power and corruption, was murdered. Russian authorities deny responsibility (CPJ, 2017). The Bloggers Law, explained in Table 4.1, is one recent example of a Russian law that legalizes and facilitates the violation of digital rights. Russian actions can be accomplished by the purposefully vague nature defined in laws which can be interpreted to include content that other countries would consider harmless (Maréchal, 2017). Freedom House identifies removal-worthy content, according to Russia, to including "LGBTI (lesbian, gay, bisexual, transgender, and intersex) expression, information on the conflict in Ukraine, and material related to the political opposition," the last of which seems to apply to the aforementioned two examples (Freedom House, 2018c).

Website black-listing is a common tool of the Russian government for censorship. The number of affected websites has steadily increased over the years—between 2012 and 2013 federal legal amendments gave Roskomnadzor and other agencies authority to make decisions regarding what content warrants a website to be blocked. Roskomnadzor maintains a list of blocked websites which authorities claim contain child abuse imagery, drug-related content, information about suicide, copyright infringements, information about juvenile victims of crime, and calls for public actions or rallies (Maréchal, 2017; Freedom House, 2018c). Similar to Chinese censorship, Russia also portrays taking the high-ground of protecting the rights of children to justify reassertion of state control over internet content. Unlike China, the protection of gender equality rights is not a main argument for censorship. In fact, images of Anna Zhavnerovich, a Moscow woman who was severely injured due to domestic violence, were disseminated online and some internet users celebrated the violence against women (James and Jones, 2017).[6] This type of censorship is upheld by internet service providers (ISP) who must refer to Roskomnadzor's blacklist and who are encouraged to overestimate the reach of blocking orders in order to avoid the consequences of heavy fines and loss of state licenses for reason of under-censoring (Maréchal, 2017). In addition, ISPs have no legal specification on how to restrict access resulting in accidental blockings. Consequently, 97 percent of accidental blockings were caused by ISPs blocking according to IP addresses instead of domain name or website URLs (Freedom House, 2018c).

[6] Though it is important to note that this could also be interpreted as a push in the right direction for gender equality in Russia because of Zhavnerovich's decision to come forward and shame her ex-boyfriend despite online harassment.

Table 4.1 *Russia Major Laws and Regulations*

Law/Regulation	Date Promulgated	Purpose/Relevance
Foreign Agents Law	July 2012	Registered NGOs that receive some foreign funding and engage in activities deemed political are subject to audits and are marked as a foreign agent in official statements. Smears organizations that are critical of the Russian government.
Law on Information, Information Technology and Information Security *(amendments)*	February 2014	Allows blocking of websites that instigate riots, extremist or terrorist actions without a trial. Extends the overreach of the original law which fought child pornography. Newest amendment requires foreign internet services to store user data in Russia.
Bloggers Law	August 2014	All online outlets including blogs and personal pages with social networking site with more than 3,000 daily readers must register with Roskomnadzor (mass media regulator).
Law on Mass Media (amendments)	January 2016	Prohibits foreign nationals and organizations from owning more than a twenty-percent stake in any Russian media outlet.
Law on News Aggregators	January 2017	Requires internet search engines with more than one million daily users to check truthfulness of information deemed publicly important before dissemination. News deemed false must be removed from websites or face financial penalties which leads to self-censorship in private companies and the free flow of online information.
Yarovaya Law (package of amendments)	July 2018	Obliges online services to provide encryption keys to the internet, requires telecommunications providers to hold records for six months and provide any information that is federally requested, introduces prison terms of up to seven years for calling for or justifying terrorism online. Limits citizens' privacy and ability to express political dissent.

Sources: (Freedom House, 2018c; Maréchal, 2017; Nocetti, 2015; Article 19, 2017; Freedom House, 2017)

Not all Russian citizens remain complicit in digital authoritarianism, particularly after a steady worsening of their internet freedoms over the course of the last six years (Freedom House, 2018c). Russian internet penetration has increased in recent years, meanwhile an increasing number of citizens are growing restless and fighting back against censorship and surveillance, particularly following the government's move to block the telecommunication app Telegram for refusing to provide encryption keys to the FSB in April, 2017 (Freedom House, 2018c). Thousands took to the streets and a "Digital Resistance" formed to support digital rights, particularly the right to the internet (Aleksejeva, 2018). Concurrently, stricter laws were passed

to restrict online anonymity, specifically by blocking VPNs and requiring other telecommunication apps to link users to their personal information according to a 2018 amendment to the Law on Information, Information Technology and Information Security (see Table 4.1).

Russia's System of Operational-Investigatory Measures (SORM), a surveillance technology used to provide intelligence agencies with telecommunications content, was also expanded in April 2015 to incorporate deep packet inspection (DPI) technology. This update provides greater access and searching capabilities of online communications, such as social media platforms, to intelligence agents (Freedom House, 2018c). The information that is collected and stored for long-term use includes recordings and locations (Soldatov and Borogan, 2013). Although the European Court for Human Rights deemed SORM in violation of the European Convention on Human Rights in the 2015 court case *Zakharov v. Russia*, SORM added more classified regulations that continue to affect all ISPs in Russia (Zakharov v. Russia, [2015]).

Rumors of an internet "kill switch" have emerged following Russian cyber exercises that revealed vulnerabilities in "RuNet's security infrastructure preparedness against potential external aggression" (Nocetti, 2015:5). This kill switch would allow the Russian government to shut down the internet in Russia and could be used at the government's discretion. This implies that should large-scale civil protests break out, the Russian authorities would be able to undermine them by blocking access to the internet. These types of internet shutdowns have already been used by the governments of Egypt, Uganda, and Iran, in an effort to control information regarding politically sensitive events (DeNardis, 2014). Besides violations of political participation rights, an internet shutdown has far-reaching consequences on the freedoms of expression, movement, and work (AccessNow, 2019). Despite a UN Security Council meeting where Russia reassured members that no such kill switch exists in Russia, its existence is not unheard of in other countries. Additionally, the strengthening of Russia's state internet control does not rule out the possibility of such a project becoming reality in the future (Nocetti, 2015).

II. INTERNATIONAL STANCE

In 2014, President Vladimir Putin said the internet was a project of the CIA and is "still developing as such" (Kelley, 2014). Given the deep mistrust Putin has of the United States and its foreign policies, or arguably his desire to foment anti-U.S. sentiment within Russia, this is not an entirely unexpected accusation. Moreover, the United States' computer network beat out the Soviet Union's OGAS due to political infighting and became the internet that we all know today (Baraniuk, 2016). Naturally, this gave U.S. companies the advantage by allowing them to control large portions of the internet (Zimmer, 2017). This undoubtedly feeds into the paranoia of the former KGB spy who is now aiming to make Runet, the Russian internet, independent (Matsakis, 2019).

Russia's apparent goal of a fully autonomous internet took its first step with the newest amendment to the Law on Information, Information Technology and Information Technology which plans to create a Russian collection of national intranets separate from the current globally-interconnected World Wide Web (Kelley, 2014). Much like the Chinese Information

Silk Road, Russia's ambition poses a threat to current global infrastructure which in turn could affect the implementation of digital rights.

How these rights would be affected may be inferred based on Russia's involvement in the Shanghai Cooperation Organization (SCO). This organization was founded in 2001 and is comprised of Russia, China, Uzbekistan, Kyrgyzstan, Kazakhstan, Pakistan, India, and Tajikistan and currently has four observing states: Afghanistan, Belarus, Iran, and Mongolia (Albert, 2015; Michel, 2017). It is the Russian government's relationship with China within the SCO that is most telling of Russia's international stance towards digital rights; their combined effort is being used within this framework to aid member states in becoming better at "networked authoritarianism" (Maréchal, 2017). This is then compounded with the SCO advocation of restricting the flow of information that falls into three categories: terrorism, extremism, and separatism. As described above, extremism is often a blanket reason applied to any form of opposition online and thus results in policies that infringe on digital rights. Furthermore, the SCO advocates for the "preventing [of] other nations from using their core technologies to destabilise [sic] economic, social and political stability and security" (Kizekova, 2012:2). All these appear to be indicators that the Russian stance towards global digital rights mirrors its own domestic stance—one of censorship and surveillance. The implication mirrors those discussed in the China section: the construction and dissemination of a norm that called for the avoidance of criticism and devaluation of digital rights.

Under the leadership of Putin, Russia's global and domestic stances on digital rights remain consistent. An original rival to U.S. internet supremacy, Russia will no doubt continue to undermine and advocate for the deterioration global internet infrastructures and digital rights in order to assert its own digital sovereignty. Interference in the United States' 2016 presidential election exemplifies Russia's ability to not only shake global confidence in the internet and cyberspace—a feeling still shared by many Russian citizens—but also serves as a justification for the implementation of "networked authoritarianism" by a state to protect its citizens from such interferences.

United States

I. DOMESTIC CYBER POLICIES

"The final freedom, one that was probably inherent in what both President and Mrs. Roosevelt thought about and wrote about all those years ago, is… the freedom to connect – the idea that governments should not prevent people from connecting to the internet, to websites, or to each other. The freedom to connect is like the freedom of assembly, only in cyberspace."

-Secretary of State Hillary Clinton's statement on internet freedom on January 21st, 2010.

The right to freedoms of speech and press are protected by the First Amendment to the Constitution. In 1997, the landmark *Reno v. American Civil Liberties Union* Supreme Court case unanimously reaffirmed that the First Amendment extends to protect online speech (*Reno v. ACLU*, [1997]). This decision rendered the 1996 Communications Decency Act, the first notable attempt to regulate the dissemination of online pornographic material, unconstitutional and set the precedent for future debates on online censorship (US Legal, 2019). As such, lower courts have over the years repeatedly struck down attempts to regulate online content. Consequently, Freedom House has consistently rated the United States as free in their yearly Freedom on the Net reports which commenced in 2011. Yet, the United States' internet freedom score has increased from 13 to 22 from 2011 to 2018, indicating an overall worsening trend in internet freedom.

There is no singular federal regulatory body for the internet in the United States, nor is internet infrastructure state-owned. Private telecommunication companies such as Verizon, AT&T, Sprint, and T-Mobile[7] own and maintain infrastructure, allowing for multiple connection points. Not only does this make the possibility of internet shutdowns highly unlikely, it serves as a protective layer for citizens against spontaneous government censorship of political and social content. However, laws governing other aspects of civil life have increasingly been extended to the internet including: copyright violations, child pornography, content deemed "harmful" to minors, gambling, and financial crimes (Freedom House, 2011). Of these listed, child pornography and "harmful content" for minors have garnered the most legislative attention, in turn stirring debate over how far freedom of speech applies. The three most influential laws regarding this subject are the 1996 Communications Decency Act, 1998 Child Protection Act, and 2001 Children's Internet Protection Act (see Table 5.1). Of the three, the first two were struck down for being unconstitutional for violating the freedom of speech provisions of the First Amendment. However, the latter was upheld in 2003 due to its limited scope of implementation, namely only in public libraries.

[7] A T-Mobile and Sprint merger is in the works, however it is just as unlikely as likely to actually occur. (Cheng, 2019).

Table 5.1 *United States Major Laws and Regulations*

Law/Regulation	Date Promulgated	Purpose/Relevance
Executive Order 12333	December 1981	Laid the foundation for how the NSA and other federal agencies may conduct surveillance of the population within the United States. Authorizes the collection of Americans' metadata and communication content when collected "incidentally." Used as justification for PRISM and the MYSTIC program which was used to document all outgoing and incoming calls from target countries.
Patriot Act	October 2001	Broadens the use of wiretapping devices from telephone numbers to internet and e-mail origins, without prior warrant requirement so long as the information to be obtained is likely relevant to the investigation against international terrorism. Broadens the definition of terrorism to include domestic terrorism.
Children's Internet Protection Act	December 2001	Requires libraries and some schools to install content filtering software on their computers in order to block access to certain content, including: pornography and bomb-making recipes. The software unintentionally blocks various other kinds of speech, including: comedy, personal care, short poems, and health sites.
Homeland Security Act	November 2002	Establishes the Department of Homeland Security. Gives authority to the secretary of Homeland Security to direct and control investigations the require information to investigate and prevent terrorism.
Intelligence Reform and Terrorism Prevention Act	December 2004	Established the Office of the Director of National Intelligence to oversee the intelligence community. Section 6001 amends the definition of agent of a foreign power in the FISA to add a "lone wolf" provision referring to a foreign national who engages in international terrorism. Thus, easing the process to apply for a court order.
Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendment Act	July 2008	Gives the NSA the ability to collect users' communications data along with its content from U.S. tech companies and through physical infrastructure. Allows for the direct authorization of mass surveillance of foreign nationals and the indirect mass surveillance of U.S. citizen communications.
USA FREEDOM Act	June 2015	An extension of the expiring provisions of the Patriot Act without significant changes to mass surveillance practices. However, limits what can be done with U.S. citizens' information in court and federal proceedings when the NSA does not follow existing procedures. Also limits bulk collection of Americans' phone records under Section 215.
Cybersecurity Information Sharing Act	December 2015	Protects U.S. companies from being sued for violating user privacy when disclosing information to federal agencies. Requires the Department of Homeland Security to tell private companies' information about threats. Criticized for not clearly defining when the use of data can be used for cybersecurity or law enforcement purposes.
Clarifying Lawful Overseas Use of Data Act (CLOUD)	March 2018	Updates the 1986 Stored Communications Act by clarifying how to govern transnational data transfer. Expands the scope of law enforcement access to user data by legitimizing law enforcement requests sent to U.S. companies regardless if the data is stored within or outside the country.

Allow States and Victims to Fight Online Sex Trafficking Act	April 2018	Cracks down on websites that promote prostitution and sex trafficking which has led to the preemptive censoring of legitimate content by companies in order to avoid penalties.

Sources: (Gellman and Soltani, 2014; Homeland Security Act of 2002; Bazan, 2004; Butler, 2015; Keane and Swire, 2018; Freedom House, 2018d)

The United States' relatively lax stance on censorship, while beneficial to some digital freedoms like those of assembly, association, speech, and press, facilitates the near violation of others, specifically gender equality and minority rights. Without stringent regulations, the issue of websites promoting prostitution or sex trafficking, where the majority of victims are female, has emerged. Although this may not be strictly considered a violation of their rights, the disparate impact on women is important to note. Moreover, a study conducted by Amnesty International found that 33 percent of female internet users between the ages of 18 and 55 experienced online abuse or harassment at least once (Amnesty International, 2017). The Pew Research Center found that a quarter of African-Americans have been targeted and harassed online due to their race or ethnicity. Similarly, 10 percent of Latinx individuals also faced racial-targeted harassment compared to only 3 percent of white Americans (Duggan, 2017). While acts of harassment may not constitute a violation of minority rights, the incitement of racial tensions online may lead to escalated racial tensions offline.

The Allow States and Victims to Fight Online Sex Trafficking Act (see Table 5.1) was signed into law in 2018 with a primary purpose of prosecuting such websites. However, once again, critiques emerged to argue that companies will preemptively censor legitimate content to avoid penalties, thus undermining freedoms of press and speech (Freedom House, 2018d).

An even greater concern in recent years to digital rights in the United States is net neutrality, referring to the regulation of internet infrastructure so that network service providers must treat internet traffic equally. Because internet infrastructure is owned mainly by private telecommunication companies in the United States, if net neutrality is foregone, then an emergence of a pay-to-play business model is expected to emerge. This would mean ISPs would be able to control the speed in which certain websites operate, thus providing preference to those who are able to pay more.

This concern was then legitimized when the Federal Communications Commission (FCC), the leading quasi-regulatory internet body in the United States, voted in December 2017 to overturn provisions related to net neutrality in the 2015 Open Internet Order (Freedom House, 2018d). This move received harsh criticisms from open internet advocates and think tanks who claim that without net neutrality protections internet users and access to information will be adversely affected. In response, states like California are enacting their own net neutrality laws despite threats of federal lawsuits (Kelly, 2018).

Perhaps the most infamous of United States' domestic cyber policies, revealed by the 2013 Snowden leaks, is the prevalence of cyber intelligence gathering on its own citizens. Authorized by the Patriot Act in 2001 and further expanded upon by Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, surveillance of both U.S. and

non-U.S. citizens became commonplace (see Table 5.1). Two types of surveillance emerged: upstream and downstream. The former refers to the collecting of communications as they travel through infrastructure and the latter, infamously exemplified by PRISM, refers to the collection of communications from multinational technology companies like Google, Facebook, and Yahoo, often times through force (Electronic Frontier Foundation, 2019). The Snowden Revelations incited international uproar due to their scope; any U.S. and non-U.S. citizen within or outside of the country who is believed to have communications to or from any foreigner with foreign intelligence information, regardless of how vaguely interpreted, is potentially subject to surveillance. Critics like the Electronic Frontier Foundation, an international non-profit digital rights advocacy group, were quick to point out that not only do these practices undermine users' right to privacy, they also undermine fundamental legal rights, including the Fourth Amendment which protects citizens from unreasonable searches and seizures.

Following these revelations public outcry led to subsequent policies to marginally curtail mass surveillance. One of such policies is the 2015 USA FREEDOM Act which extended provisions of the Patriot Act under the condition to limit the bulk collection of Americans' phone records (Shahbaz, 2018). Despite this attempt, long-term distrust of government surveillance coupled with earlier explanations of online harassment has led internet users to practice self-censorship. Reminders of mass surveillance especially effect users' willingness to express minority public opinions online, according the 2018 United States Freedom on the Net Report (Freedom House, 2018d).

The history of censorship in the United States presents three models to different censorship scenarios and their effects on digital rights. First, prior to 2013 when citizens of the United States were unaware of mass governmental surveillance, general freedoms of speech, press, and assembly were at their peak. Albeit this is at the expense of gender, child, and minority rights which then diminished these groups' freedom of expression due to self-censorship. Second, after the public became aware of mass surveillance, a decline in freedom of expression and assembly was witnessed as described in the previous paragraph. Third, in the same vein, mass surveillance itself violates the digital rights to privacy, expression, and association by limiting anonymity, but in turn protects marginalized groups because of self-censorship and regulation of disinformation and hate speech. For that reason, surveillance and a completely open internet are double-edged swords. The former is not intrinsically repressive, nor is the latter wholly egalitarian in the case of the United States.

II. INTERNATIONAL STANCE

At the turn of the century, U.S. President Bill Clinton embraced the proliferation of the internet as a tool in which "liberty will be spread by cell phone and cable modern" (Griffiths, 2018). The United States took the lead in the West, emphasizing the importance of the internet and digital rights in advancing democracy and liberal values. Indeed, the internet's ability to allow users access to vast amounts of information is often cited as a defining factor for the democratization of states (Bimber, 2003; Freyburg et al., 2011; Schimmelfennig 2014). This idea

stems from the notion that by providing a variety of sources of information and thus differing opinions, citizens will be more willing to participate in the policy-making process (Weare, 2002). Scholars like Benkler (2006) and Jenkins (2006) argued that the internet would increase exposure to more diverse perspectives outside of mainstream thought, including a greater diversity of political information independent of state control. This diversity of information would then help citizens make better decisions, therefore simultaneously benefiting both democracies and liberating individuals in oppressive countries (Mutz and Martin, 2001; Diamond 2010).

For this reason, the United States has been a strong international advocate for an open internet, free from censorship and surveillance under repressive regimes. Following an internet shutdown in Egypt during political unrest, U.S. President Barack Obama declared that the U.S. "stand[s] for universal value, including the rights of the Egyptian people to freedom of assembly, freedom of speech, and the freedom to access information" (Tully, 2014:179). Similarly, Secretary of State Hillary Clinton acknowledged the importance of digital rights, even the controversial right to the internet, in the opening quote of this section.

The efforts by the United States to champion internet access have encountered several setbacks. The 2013 Snowden revelations revealed the United States' hypocritical stance on privacy and surveillance. Despite publicly denouncing digital authoritarianism and encouraging foreign nationals to utilize digital media to exercise their digital rights, the United States differentiates the rights of non-U.S. and U.S. citizens as such: "US persons may only be targeted if there is a judicial warrant from the Foreign Intelligence Surveillance Court (FISC), whereas non-US persons can be targeted without FISC-approved individual warrant" (Watt, 2017:775). This division clearly undermines the universality of digital rights, thus threatening their recognition as a human right. Surely the international community sees the irony of the Obama administration's explicit recognition of global privacy rights in Presidential Policy Directive No.28 and the continuous reinstatement of mass surveillance practices through various policies with differing names (Margulies, 2013).

The position the United States touts regarding digital rights does not align with its own domestic policies, let alone its international stance. Prior to 2013, the advocacy by the United States for an open internet had legitimacy, as did its criticisms of Russia and China for restricting their citizens' online rights. However, a post-Snowden United States continues to face a serious backlash and effectively breed distrust even among its allies (Spiegel Online, 2013). Furthermore, the lack of action by the United States concerning Chinese mass internment and censorship of its Uighur population in Xinjiang and the spread of malicious disinformation to breed hostility against the Rohingya in Burma highlights how the United States is mostly a figurehead for the free internet movement, rather than a proponent to its normalization (Fuchs et al., 2018; CBSN Originals, 2018).

This is not to say that the United States is not an important influence for the protection of digital rights. Despite an overall worsening trend in internet freedom and digital rights, the United States remains a remarkably strong case for freedoms of speech, assembly, and political participation. In a time of rising digital authoritarianism, the United States serves as a model for

how the internet can be used to further diversity in political discourse with minimal legal or technical restriction on publication or access (Freedom House, 2011). Moreover, even what has become known as the "greatest privacy meltdown of our time," (referring to the Snowden revelations) had only a small impact on internet users' online behaviors (Preibusch, 2015:48). In short, the United States is not the perfect advocate for its own purported values but its global influence and state-level progress to rectify the hypocrisy have made it an important actor.[8] Additionally, the United States' emphasis on freedom of speech allows for NGOs within its civil society to be proponents for internet freedom.

[8] However, this may be changing under the Trump administration. Reports emerged this year that a proposal is in the works to use social media to identify people who are falsely claiming Social Security disability benefits. Such a proposal allows for further surveillance of the American pubic and disproportionately affects those with disabilities (Pear, 2019).

Germany

I. DOMESTIC CYBER POLICIES

"The freedom of expression also protects repugnant and ugly remarks. But, freedom of expression is not a pass to commit crimes. Those who share criminal content online must be held accountable to justice. Calls for murder, hate speech, or Holocaust denial are not expressions of freedom of expression but are instead attacks on the freedom of expression of others."

-Minister of Justice and Consumer Protection Heiko Maas on January 3rd, 2018.

The use of propaganda to incite hatred against minorities was prevalent prior to and during the second world war in Germany. Therefore, post-WWII legislation was intended to criminalize such activity. With the introduction of the internet Germany was quick to extend its Criminal Code to encompass online content, particularly through Section 130 which addresses incitement of hatred:

(1) Whosoever, in a manner capable of disturbing the public peace
   1. Incites hatred against a national, racial, religious group or a group defined by their ethnic origins, against segments of the population or individuals because of their belonging to one of the aforementioned groups or segments of the population or calls for violent or arbitrary measures against them; or
   2. Assaults the human dignity of others by insulting, maliciously maligning an aforementioned group, segments of the population or individuals because of their belonging to one of the aforementioned groups or segments of the populations, or defaming segments of the populations,

shall be liable to imprisonment from three months to five years. (Appell, 2019)

Much like the United States and other democracies, Germany must battle between how to tackle online hate speech in conjunction with upholding freedoms of expression and media and the right to privacy, all of which are protected by Germany's Basic Law Articles 5 and 10, respectively. Harsher boundaries around online speech and activities are seen as more legitimate to many Germans compared to civilians of other countries because of their country's history (Freedom House, 2018b). German penal law routinely allows for censorship in the cases of hate speech, dissemination of child pornography, glorification of violence, and Holocaust denial.

Of these categories, laws protecting against child pornography have been the hardest to uphold. The Access Impediment Act was passed in June of 2009 and was intended to block websites containing child pornography. Before implementation took into effect, a new governmental party coalition formed and criticized the act on civil rights grounds. Consequently, when the law was promulgated it was altered to only use the take-down provision rather than blocking websites due to heavy backlash from internet freedom activists who said the law was the beginning of internet censorship and a violation of expression (European Digital Rights, 2011). In April 2011, governing bodies decided to repeal the law altogether. However, the introduction of a new law, the Network Enforcement Act (also called NetzDG, see Table 6.1), at the start of 2018 has brought this issue up once again for public debate.

Table 6.1 *Germany Major Laws and Regulations*

Law/Regulation	Date Promulgated	Purpose/Relevance
Act for Limiting the Secrecy of Letters, the Post, and Telecommunications	2001	Allows secret services to intercept, monitor, and record private communications, and it differentiates between the protected professions. Allows for the surveillance of counselors and journalists in certain situations
Freedom of Information Legislation	2006	Establishes information held by public authorities should be open and available, however has exceptions and every request requires fees
Act on Strengthening Press Freedom	June 2012	Improves protections for journalists and their sources, strengthens related sections in the Criminal Code and Code of Criminal Procedure
Asylum Law (amendments)	2017	Allows for the copying and analyzing of arriving refugees' electronic devices' in order to determine where the person came from and where they spent their time if he or she does not provide identity documents.
Source Telecommunications and Online Surveillance Law	June 2017	Allows law enforcement and the state to install malware known as State Trojans on electronic devices for surveillance purposes and perform online searches to investigate criminal offenses. Amends the German Criminal Code.
German Privacy Act (BDSG-new)	July 2017	Governs the exposure of personal data and protects individuals' personal rights when personal information is being processed. Does not apply where GDPR applies.
Law for More Effective and More Practical Criminal Proceedings	August 2017	Includes an extensive list of criminal offenses that could allow for the deployment of spyware on suspects' electronic devices for the purpose of copying and monitoring written and spoken text.
Social Network Enforcement Law	October 2017	Pushes to curb the dissemination of hate speech, terrorist propaganda, and fake news on social media, establishes fines against social networking companies in the event that they do not remove flagged criminal content from their platforms
Network Enforcement Act (NetzDG)	January 2018	Obliges social media platforms with more than 2 million registered users in the country to delete offensive illegal content within 24 hours and or else face hefty fines. These platforms are given one week to review content that is deemed more legally ambiguous.

Sources: (Freedom House, 2018b; Freedom House, 2013; European Digital Rights, 2011; Appell, 2018; OpenNet Initiative, 2010; Deloitte, 2019)

NetzDG was the result of Minister of Justice and Consumer Protection Heiko Maas' push to mitigate the increasing amount of hate speech online as a result of the influence of social media in recent elections, the polarization of political opinions, and the rise of civil unrest (Appell, 2018). Under this law, internet platforms must ensure that their websites only contain legal content, thus shifting the responsibility away from internet users. Social media companies in particular are compelled to remove hate speech. For this reason, NetzDG draws criticism from

both sides of the political spectrum in Germany, including the far-left Left Party and the far-right Alternative for Germany. Human Rights Watch also argues that this law violates Germany's obligation to respect free speech because (1) the burden of censorship falls on companies under conditions that then encourages censoring of potentially lawful speech as a precaution and, (2) NetzDG fails to provide judicial oversight (Appell, 2018). Despite criticisms against the implementation of this law, which Chancellor Angela Merkel has said is subject to alteration, the intention seems to strike a balance between freedom of expression and hate speech which violates others' freedom of expression (Cooper, 2018). Yet, by doing so even Maas points out that digital rights are subservient to the law, opening the door for further policies to legally limit rights and bring into question the inalienability of digital rights.

This sentiment also holds true when it comes to users' privacy. According to Germany's Criminal Procedure Code Section 100a, "telecommunication of an individual may be monitored and recorded if:

1. Specific facts substantiate the suspicion that somebody was the perpetrator or participant in a serious crime as listed in paragraph 2 or, in cases where the attempt is liable to persecution, has attempted to commit such crime, or has prepared such crime by means of a criminal offense
2. The alleged crime would weigh heavily even taken individually
3. Investigating the act or determining the suspected person's location by other means would be significantly impeded or futile without surveillance" (OpenNet Initiative, 2010).

This provision gives a legal basis to require German ISPs and online service providers to retain some types of data for up to six months, even without initial suspicion of illegal activity. This has been the case in the southern state of Bavaria where a bill was introduced in the beginning of 2018 that has been called the hardest policing law since 1945 (Bröckling , 2018). Under this law, concrete evidence of a specific crime is unnecessary for police to preventatively access any information technology system (Freedom House, 2018b). Similarly, amendments made in 2017 to the German Asylum Law (see Table 6.1) allows for the copying and analyzing of refugees' electronic devices in order to determine their place of origin in cases where documentation cannot be provided (Freedom House, 2018b). Moreover, new legislation like the Law for More Effective and More Practical Criminal Proceedings shown in Table 6.1 allow law enforcement agencies to install malware on suspects' electronic devices in order to aid in criminal investigations. One such malware is the "Bundestrojaner", or federal Trojan horse, which has been legally in use since August 2017 (Prantl, 2018). This software clandestinely records data in order to extract needed information and has been justified by German authorities as a measure against terrorism and right-wing extremism.

Germany's position within the European Union greatly influences domestic policies. In April 2017, Germany's federal parliament, the Bundestag, incorporated in its own domestic law the European Union rules on net neutrality (Freedom House, 2018b). Prior to this, Germany defined basic requirements for a non-discriminatory data transfer system, however no requirements were established (Freedom House, 2013). As discussed in the previous section, net

neutrality ensures equal opportunity to view, interact with, and share information online for internet users and is essential for the full enjoyment of the right to information.

In May 2018, the General Data Protection Regulation (GDPR), which has been called the most important change in data privacy regulation in 20 years, went into effect (European Commission, 2019). This law contains 70 opening clauses in order to allow European Union member states to legally enact and modify the GDPR to fit their domestic environment. In order to conform to the requirements of the GDPR, Germany replaced its previous privacy act, the BDSG, with the BDSG-new (see Table 6.1) in the same month (Deloitte, 2019). Under this new law and regulation, any company, regardless of where it is located, that processes the personal information of individuals residing in the European Union must respect that individual's rights or else face hefty fines (European Commission, 2019). These rights include: breach notification, right to access, data portability, privacy by design, access to a data protection officer, and the right to be forgotten (European Commission, 2019).

Among its goals of obtaining more meaningful consent, increasing data collection transparency, and giving users the ability to manage their data directly, the GDPR also legally reinforced a new digital right in Germany: the right to be forgotten (European Commission, 2019; Freedom House, 2018b). This right "reflects the claim of an individual to have certain data deleted so that third persons can no longer trace them" (Weber, 2011:121). Furthermore, this right allows internet users to withdraw their consent to data processing at any time. The right to be forgotten differs from the right to privacy because rather than dealing with information that is not publicly known, it is used to remove information that is publicly known at any certain time and blocks third parties from accessing the information when it is gone (Weber, 2011). Much like the right to the internet, the right to be forgotten has been criticized for degrading the concept of human rights (Mayes, 2011). Furthermore, the right to be forgotten is seemingly at odds with freedoms of expression and press and the right to privacy. The GDPR has rules providing exceptions to the right to be forgotten in cases where the exercising of freedom of expression and information are necessary, however these exceptions are not well defined (Human Rights Watch, 2018b). Such a right may also be used as a justification for censorship or as a legal way to rewrite history in the hands of the wrong government. This right has also been criticized for enabling people in positions of power to abuse it in order to remove harmful articles that discuss their previous criminal convictions (Human Rights Watch, 2018b). Yet, advocates claim that it is the only way to resolve perpetual online stigmas from scenarios such as long-standing minor infraction records, false accusations, and revenge porn (Arthur, 2014).

This right was first established in a May 2014 EU Court of Justice decision in the case of *Google Spain v. AEPD and Mario Costeja.* The GDPR also ensures the protection of this right, however debate surrounding its legitimacy is still occurring in Germany, particularly after the June 2018 European Court of Human Rights case of *M.L and W.W. v. Germany*. This case decided that there was no violation of Article 8 (right to respect private life) in the case of two German half-brothers who murdered a popular actor and were seeking to prohibit a media company from keeping a transcript of a past interview on its internet portal (*Google Spain v. AEPD and Mario Costeja,* [2014]). In this case, the scenario resulted in the freedom of press to

outweigh the right to be forgotten. However, the right to be forgotten has been successfully utilized against Google where approximately 670,835 requests to delete search results in the European Union have been assessed. The scope of these requests would affect over 2 million URLs, nearly 112,000 of which coming from Germany (Google, 2018).

Apart from the controversy that surrounds the right to be forgotten, the GDPR gives users back partial control over their data and holds large social media companies accountable. In general, media and internet freedom are well-respected within Germany where substantial safeguards are in place to protect essential digital rights. Perhaps the best example of the ability to exercise these rights is the lively debate surrounding them in Germany. For this reason, of the four case studies Germany has the best score for Freedom House Freedom on the Net score of 19 out of 100 in 2018.

II. INTERNATIONAL STANCE

As the unofficial leader of the European Union, regulations like the GDPR generally require the support of Germany. Therefore, for the purpose of this analysis, the impact of the GDPR on international relations will be a proxy for Germany's international stance. As previously discussed above, the GDPR applies to all companies that process the personal information of individuals located within the European Union, regardless of the location of the company. Furthermore, those outside of the European Union whose data is being collected or processes by companies within the European Union are also affected (Read, 2018). Given the global nature of the internet, this has far reaching implications and virtually every company or organization with at least one client or employee located within the EU must follow the regulation. Consequently, the GDPR forces non-EU and EU-member states to confront regulatory differences and raises questions about internet, user, and territorial sovereignties. Regulatory differences are especially pronounced between the United States and the European Union where a well-established transcontinental data transfer system has been in place for decades (Kobrin, 2004). The GDPR places users' and internet sovereignties above territorial sovereignty. Indeed, there are concerns that the facilitation of the expansion of internet sovereignty by the GDPR already violates Israeli sovereignty (Or-Hof, 2018). Unlike China's or Russia's view of internet sovereignty, which falls within territorial sovereignty, the European Union sees internet sovereignty as transnational because it falls within user sovereignty.

The NetzDG law also has international influence. Article 19, a British human rights organization that advocates for freedom of expression, argued that the NetzDG "severely undermine[s] freedom of expression in Germany, and is already setting a dangerous example to other countries" (Global Network Initiative, 2017). Despite Freedom House's score as one of the most free countries on the net, the NetzDG is setting a precedent for less free countries on how to force social media companies to act as censors. In Singapore, the government cited the NetzDG law as a positive example while it attempts to crack down on fake news through overly broad criminal laws (Ministry of Communications and Information and Ministry of Law, 2018). Additionally, Russia cited provisions in NetzDG when proposing its own laws to censor Russian citizens (Human Rights Watch, 2018a). Human Rights Watch also warns that the implications of the NetzDG law had a domino effect in the aforementioned countries as well as the Philippines,

Venezuela, Kenya, and the United Kingdom (Human Rights Watch, 2018a). Therefore, despite being an advocate for digital rights domestically and attempting to strike a balance between censorship of freedoms of expression, Germany is currently serving as an indirect advocate for systematic censorship internationally.

Comparative Analysis and the Consideration of Regime Type

I. TRANSPARENCY

Transparency and human rights have an arguably overlapping relationship. This governmental trait is a required prerequisite for both good governance and the protection of human rights. Human rights and good governance have a mutually reinforcing relationship, and both set the boundaries in which governments must work. Transparency allows individuals to hold governments accountable when they work outside those lines; therefore, without it the status of human rights and good governance are hard to clearly decipher.

Patrick Birkinshaw (2006) recognizes that a specific attribute of transparency, namely the freedom of information which extends from access to government information, deserves special protections and argues that this particular attribute ought to be treated as an internationally recognized human right. For the purpose of this thesis, the direct overlapping of transparency and human rights will be delinked as the specific attribute Birkinshaw mentions falls within the domain of digital rights.[9] As such, transparency will simply refer to openness of governmental operations to ensure that the government is working in the best interest of its people, not select groups.

Indeed, the internet is fundamentally a transparent endeavor. It facilitates the limitless transborder exchange of photo, texts, videos, sounds, documents, and more. This data and information can then be sorted, stored, and queried by anyone with access to the internet. This of course is in an ideal world; the reality is the internet is controlled by states and where an internet user is located can greatly affect access to information.[10] It would then logically follow that the transparency, that is openness of the governmental system to the general public, of a state may affect the treatment of digital rights.

This section will first examine the transparency of each case study and their treatment of digital rights. Although the concepts of control of corruption is not a perfect measure of transparency because it does not wholly encompass the concept transparency, this indicator will be used as a proxy variable for transparency because it does address transparency, accountability, and corruption in the public sector. This indicator includes both oversight and civil society access and acknowledges the relationship between accountability and transparency by way of corruption levels. When initially using this indicator, the percentile rank was used but, in an effort to provide greater accuracy, was opted out in favor for the governance score.[11] The standard error which measures the precision of the estimate of each indicator for both the transparency and political stability sections were evaluated. Each score was found to be at or

[9] It is also for this reason that the voice and accountability global governance indicator was not used to measure transparency. This indicator measures the perceptions of the extent in which a country's citizens are able to participate in their government by exercising various rights, thus overlapping with digital rights. Moreover, the voice and accountability indicator was analyzed and the results seemed to indicate collinearity between the measures.

[10] Various types of software exist to circumvent a state's internet sovereignty, VPNs come first to mind. However, these can also be affected, criminalized, or controlled by states. While in China the author experienced this when during the 19th National Congress of the Communist Party of China many VPNs temporarily stopped working.

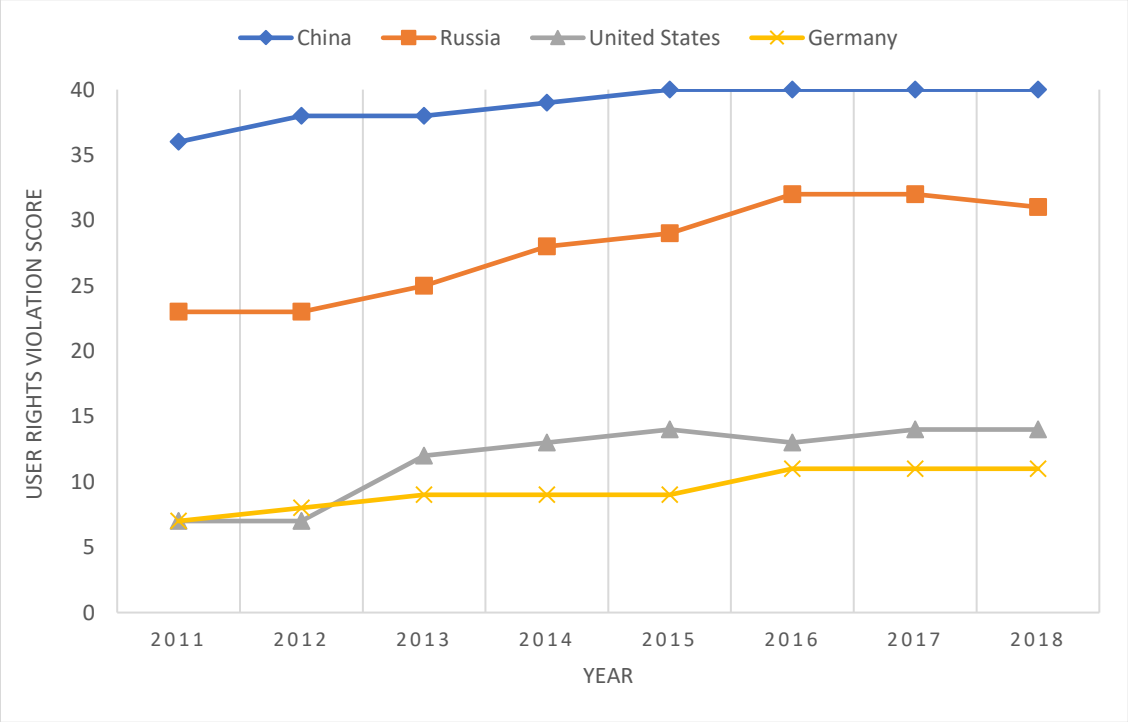
[11] However, both measures of control of corruption demonstrated largely the same findings.

below 0.24, indicating a sufficiently precise score.[12] The analysis of the control of corruption indicator and Freedom House violation of users' rights scores and internet freedom scores will be used to assess the following hypotheses: H_1 as a state's transparency decreases it is more likely to be invasive of its citizens' digital rights and, H_2 as a state's transparency increases it is more likely to protect its citizens' digital rights. Transparency will be measured by the World Bank's control of corruption global governance indicator. This indicator accounts for the extent to which public power is exercised for private gain, as well as the level in which the state is influenced by elites and private interests.

A. China

China, the consistently worst abuser of internet users' digital rights according to Freedom House (see Figure 7.1), superficially seems to appear to have a correlation between transparency and internet freedom score, albeit not an expected one. The control of corruption governance score (transparency) improved every year for a total improvement of +0.26 between 2011 and 2016 (see Figure 7.2).

Figure 7.1 *Freedom House User Rights Violation Scores 2011-2018*

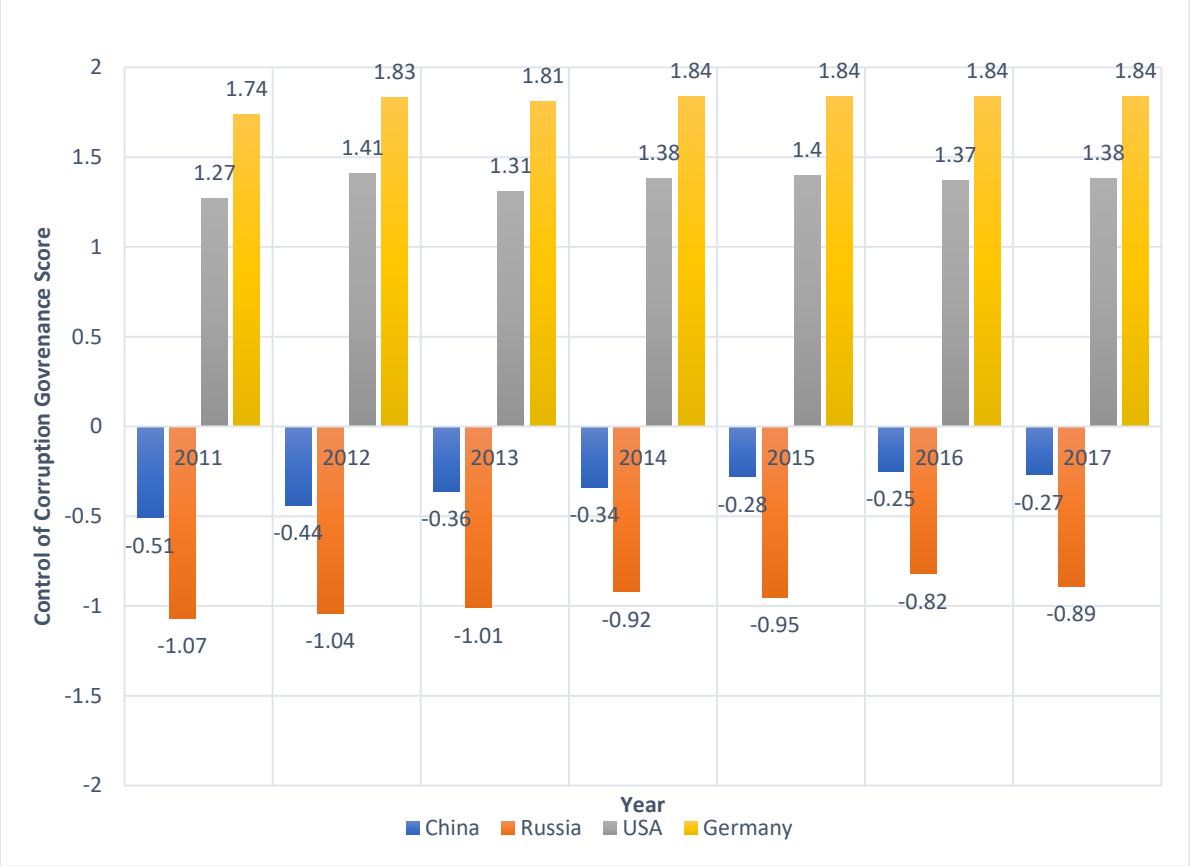


Source: Data from Freedom House Freedom on the Net Reports for China, Russia, United States, and Germany from 2011-2018

[12] The control of corruption standard error was more precise than political stability with a highest score of 0.16.

This improvement could be attributed to President Xi's campaign against corruption which began following the 18th National Congress of the CCP in 2012. In the same year, corruption within the CCP was "spiraling out of control" which was exasperated when top CCP politician Bo Xilai was under investigation after his wife was convicted of murdering a foreigner (Schmitz, 2017). This event may have catalyzed Xi's crusade against corruption which has thus far led to the investigation and punishment of hundreds of thousands of government officials (Schmitz, 2017). Concurrently, Figure 7.1 shows that China's Freedom House scores for violation of users' rights has also risen consistently, indicating a worsening of users' rights. Indeed, China reached the scale's highest score of 40 in 2015 and remained there since.

Figure 7.2 *World Bank Control of Corruption Global Governance Indicator 2011-2017*



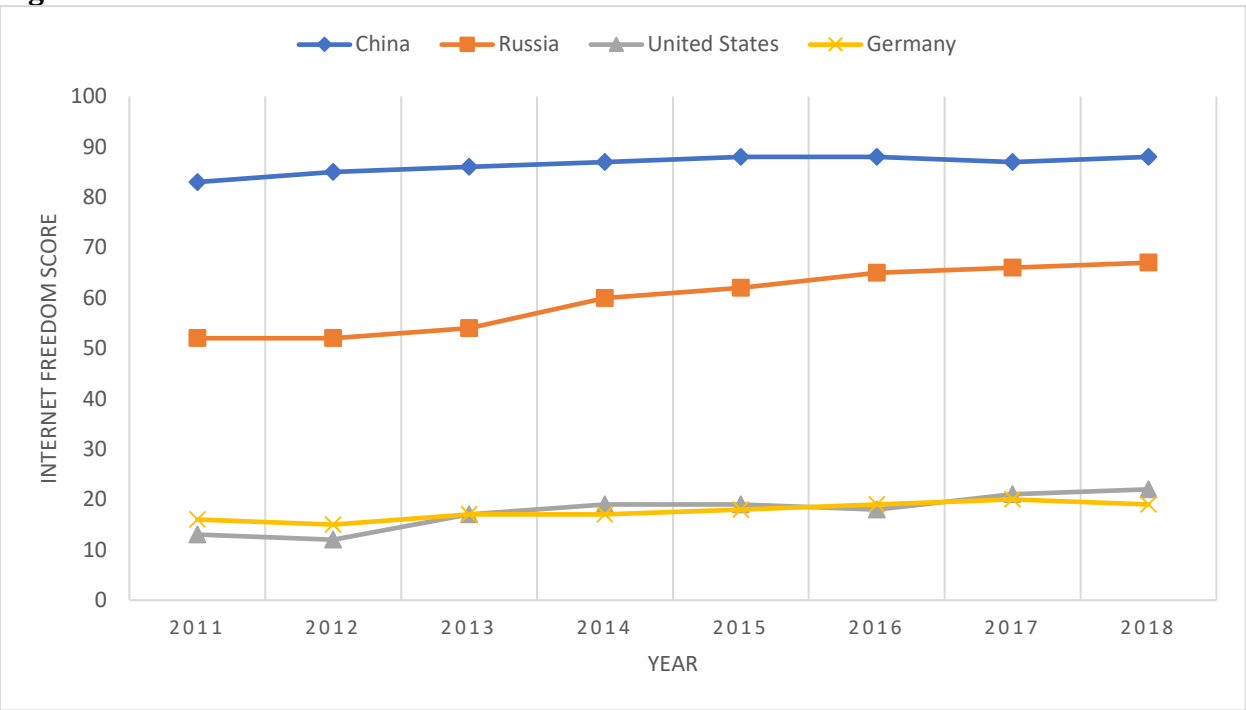
Source: Data from World Bank's Control of Corruption Indicator[13]

Looking at Figure 7.3, China's overall freedom score has also been worsening since 2011, with the exception of a 1-point dip in 2017. Upon closer inspection, this dip was due to a slight improvement in obstacles to access the internet. This subsection remained constant in 2018 but the overall internet freedom score returned to 2016 levels due to a worsening of limits on content. Therefore, this slight "improvement" is not related to digital rights but a slight improvement of infrastructure and internet penetration rates. Interestingly, this dip in 2017 is also mirrored in Figure 7.2 by a -0.02 worsening of transparency. A possible explanation could

[13] Governance scores begin in 2011 to mirror the onset of Freedom House's Freedom on the Net reports in order to provide more accurate analysis. No scores were provided for 2018.

be the CCP's opaqueness in dealing with anti-corruption and bribery. In 2017, the Central Commission for Discipline Inspection (CCDI) was authorized to conduct random checks on the "Leading Cadres' Personal Matters Report Form," a 16-page background check form (Zheng, 2019). Ironically, the CCP's attempts to increase transparency by weeding out corruption has led to less transparency in its proceedings.

Figure 7.3 *Freedom House Internet Freedom Scores 2011-2018*



Source: Data from Freedom House Freedom on the Net Reports for China, Russia, United States, and Germany from 2011-2018

A. Russia

As easily the least transparent state out of the four case studies, Russia has no clear relationship between transparency and digital rights abuse. Between 2011 and 2014, Russia's control of corruption governance score improved slightly by +0.15 but worsened slightly by -0.03 points in 2015 (see Figure 7.2). According to Transparency International, this initial improvement could be attributed to President Medvedev's anti-corruption campaign, particularly anti-bribery legislation and the Law on Amendments to the Criminal Code and the Code of Administrative Offenses of the Russian Federation to Improve State Anti-Corruption Management (Kremlin, 2011). However, corruption under President Putin has been inconsistent, albeit relatively consistently bad, with a marginal improvement in 2016 of +0.13 but a return to almost 2014 levels in 2017. Despite being corrupt himself, President Putin pushes to improve the state anti-corruption system (Cooke, 2014; Kremlin, 2016). While Russia's transparency teetered over the last decade, its internet freedom score and violation of users' rights score remained consistent. Figures 7.1 and 7.3 show a worsening of internet freedom and users' rights between 2011 and 2017, but with an exception of a 1-point improvement in 2018. In 2015, Russia's internet freedom score crossed over from partially free to not free and has remained so.

B. United States

The United States is a robust democracy, as such the control of corruption scores are significantly better than the previous two case studies. This is due to extensive laws, acts, and statutes put into place, on the state and federal level, that date back to the founding of the United States. Such legislation continues to be expanded upon, including the introduction of the American Ant-Corruption Act of 2011.

Yet, corruption does exist within the United States which explains the fluctuation of its control of corruption scores in Figure 7.2. Despite high levels of corruption control and a relatively large increase of +0.14 in 2012 compared to 2011, Figure 7.2 shows a drop of -0.1 the following year. Indeed, in 2013 60 percent of Americans felt this drop and expressed concern, albeit falsely, that corruption increased since 2011 (Bidwell, 2013). Although public opinion on corruption is not always accurate, Transparency International did conclude that the United States has fallen six places in its 2018 Corruption Perceptions Index since 2017, confirming a general downward trend since 2015 (Detrick, 2019). During this time, a general upward trend can be seen in Figures 7.1 and 7.3, indicating a worsening of internet freedom and users' rights violations. However, given the inconsistent nature of the transparency scores it is not accurate to correlate the transparency trends starting from 2016 to the trends in Figures 7.1 and 7.3.

C. Germany

Germany has the highest rankings every year out of the four case studies according to the World Bank's control of corruption global governance indicator. This ranking has remained consistently at 1.84 since 2014 and experienced only minimal fluctuation in the two years prior to that. A 2013 Freedom House report attributed Germany's institutional setup as the reasoning for its ability to ensure integrity and avoid corruption in state bodies (Freedom House, 2013). Figures 7.1 and 7.3 show mild inconsistency between Germany's internet freedom scores and users' rights violation scores. Figure 7.1 shows that Germany is steadily increasing its violations to its users' violations over the last 8 years, increasing from a score of 7 to a score of 11. Meanwhile Figure 7.3 shows that between 2011 and 2017 Germany's internet freedom worsened, except in 2012 when it improved by 1 point due to a 1-point improvement on limits on content. Unlike the United States, Germany's internet freedom score is not mostly influenced by its violations on users' rights. Instead, limits on content and obstacles to access is more varied over the years and influence the overall internet freedom score more. Regardless, neither the general upward trend seen in Figure 7.3 nor the clear upward trend seen in Figure 7.1 appears to correlate with the generally stagnant transparency trend seen in Figure 7.2.

D. Key Findings

This thesis hypothesized both that a correlation exists between a state's transparency and treatment of digital rights. Two hypotheses were specifically stated; H_1 as a state's transparency decreases it is more likely to be invasive of its citizens' digital rights and, H_2 as a state's transparency increases it is more likely to protect its citizens' digital rights. The data presented in Figures 7.1, 7.2, and 7.3 not only refute these hypotheses, but suggest that a strong correlation appears to not exist. If such a correlation existed, then China, as the worst violator of digital rights, would be the least transparent state. Yet, Russia is significantly less transparent but is marginally more respective of digital rights. However, a possible explanation for this discrepancy is that Russia is an exception to the rule. The analyses of the other three states seem

to suggest general patterns, especially when considering that the indices chosen are not perfect measures.

China's transparency scores and Freedom House scores might superficially suggest that there may exist a correlation, however this may be a coincidence of the data.[14] Similarly, despite a clear upward trend in Germany's violation of users' rights, no general upward or downward trend is witnessed in the same years for transparency. Russia's and the United States' teetering transparency scores run concurrently with the general upwards trends of internet freedom and violation of users' rights scores.

Generally speaking, states with greater transparency tend to have less violations of users' rights and, consequently, better internet freedom scores. However, a correlation between transparency and treatment of digital rights is not clearly demonstrated. Instead, the data represented in these figures concerning transparency and treatment of digital rights appear to be dependent variables of another factor, perhaps regime types. It is perhaps no coincidence that the two states with positive transparency scores and lower scores for violation of users' rights are both liberal democracies. Nor is it perhaps a coincidence that the states with negative transparency scores and higher violation of users' rights scores are both authoritarian regimes. Given the authoritarian nature of China, it is surprising that there is an upward trend in transparency, however this can be attributed to President's Xi anti-corruption campaign. It is in the best interest of authoritarian governments to violate digital rights because of media's ability to bring attention to and shame corrupt individuals and political scandals, which may result in political unrest.

Moreover, although the data collected in this thesis does not appear to demonstrate a clear correlation, one may still exist. The inability of the data to confirm these hypotheses may be due to the secretive nature in which states implement internet and cyber policies. United Nations High Commissioner for Human Rights, Navi Pillay, warned of a "disturbing lack of transparency about governmental surveillance policies and practices" (Pally, 2014). This lack of transparency makes determining a state's overall treatment of digital rights impossible to determine. Consequently, the scores by Freedom House in Figures 7.1 and 7.3, while helpful, do not show the whole picture. For example, prior to the Snowden revelations in 2013 the United States' internet freedom and users' rights violations scores were declining despite ongoing surveillance. Only after the revelations were exposed did these scores change. Perhaps a correlation may still exist if all the data were present. In transparent states it may seem like there are more violations of digital rights because information regarding policies is more open to the public. This could help explain how in China as transparency increased, so did knowledge of users' rights violation.

II. POLITICAL STABILITY

The level of political stability in each case study will also be measured by a World Bank global governance indicator, in this case more directly by the political stability and absence of

[14] When the voice and accountability indicator was being considered a similar analysis to the one presented above was conducted. This indicator produced results that seemed to affirm H_1 and H_2 but, as mentioned in an earlier footnote, this is a probably a result of collinearity.

violence/terrorism indicator. This indicator measures the likelihood of political instability along with politically motivated violence, including terrorism, protests, riots, and war. This indicator, along with the Freedom House data, will be utilized to analyze the following hypotheses: H_3 states with low levels of political stability are more likely to interfere in their citizens' digital rights through policies that are claimed necessary to protect national security, and H_4 states with high levels of political stability are more likely to implement policies to protect their citizens' digital rights.

These hypotheses work under the assumption that a relationship between political stability and treatment of human rights exists, thus implying a relationship between political stability and digital rights also exists. The former already has a substantial amount of literature backing it by various human rights scholars (see Henderson, 1991; Mitchell and McCormick, 1988; Poe and Tate, 1994). Although a relationship exists, Mitchell and McCormick (1988) would disagree that there is a direct relationship, but rather political stability is a factor within regime type. These scholars found that democracies and states affected by democracy development tend to have greater respect for human rights (Mitchell and McCormick, 1988). Political instability then relates to regime type by the presence or absence of regular and irregular government change in different types of regimes. Feng (1997) concluded that democracies tend to allow major and frequent regular government change and reduces the probability of irregular government change, thus allowing for a politically stable environment. By contrast, non-democracies do not allow for frequent major regular government change, instead the rule of one dominant party eventually evolves into irregular government change, otherwise known as political instability.

Although a state's government type does affect treatment of human rights and level of political stability separately, this section will look to see if a direct correlation between political stability and digital rights appears to exists. This will allow for a more nuanced analysis of the relationship between human rights and political stability by analyzing specific case studies over the last decade which has seen the decline of the old liberal order.

A. China

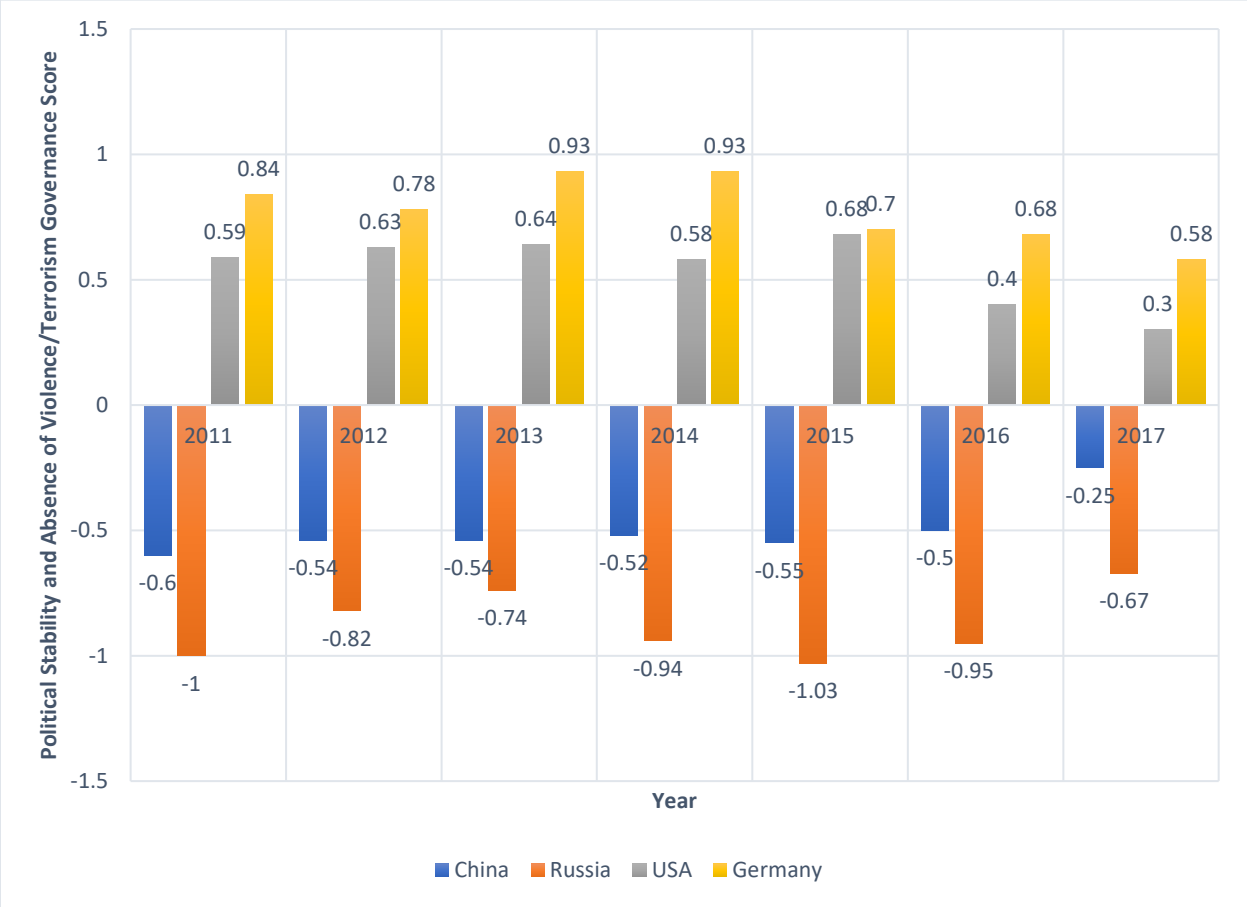
Despite two decades of collective leadership and smooth transitions of power, China's political stability and absence of terrorism ranking has remained in the lower quartile range since 2000. Additionally, China's political stability governance scores remained negative throughout the last decade (see Figure 7.4). The CCP's strategy of choosing successors, sometimes years prior to the expected ending of the current leader's term, allowed for strong continuity of CCP rule without the upset of elections (Palmer, 2018). However, this tradition that began with Deng Xiaoping in the 1980s was suddenly abolished when President Xi[15] ended term limits in 2018. This move may afford temporary and factitious political stability as many repressive dictatorships tend to do in their early years but coincides with a plethora of destabilizing internal factors (Von Rohr, 2014). The carceral archipelago[16] of the western provinces of Tibet and

[15] Often called Emperor Pooh, a nod to the censorship of Winnie the Pooh in China due to the supposed likeness he shares with the animated character.

[16] (Foucault, 1975) Coined from the book *Discipline and Punish* which talks about surveillance systems and technology in modern societies to practice social control in all areas of social life.

Xinjiang, rising separatist sentiment in Taiwan, militarization within the nine-dash line, and terrorist attacks all contribute to China's low levels of political stability (Tsirbas, 2016).

Figure 7.4 *World Bank Political Stability and Absence of Violence/Terrorism Global Governance Indicator 2011-2017*



Source: Data from World Bank Control of Corruption Global Governance Indicator

Figure 7.4 shows that Chinese stability reached a low point of -0.55 in 2015, effectively breaking what seemed to be an improvement from 2011 to 2014. This coincides with China's violation of users' rights scores reaching their highest levels. This seems to align with Hypothesis 3. Indeed, as already discussed in the China section, policies aimed at controlling internet users' digital rights are often justified by their necessity to maintain national security. In 2017, the World Bank saw a noticeable increase in Chinese stability of +0.25 from the previous year, almost reaching 2000 levels. This also coincides with a slight improvement in China's internet freedom score, seen in Figure 7.3. However, this same trend is not mirrored in Figure 7.1 and thus does not represent an improvement in protecting citizens' digital rights. Interestingly, in 2000 and 2017, years of relatively higher political stability, more major domestic cyber laws were passed to restrict citizens' digital rights than in less stable years (see Table 3.1). Perhaps these policies were implemented in order to prepare for instability that is expected to come. If so, the possibility of time lags in both transparency and political stability as they relate to digital rights must be considered.

B. Russia

The World Bank indicator in Figure 7.4 shows that Russian stability has varied more on a yearly basis than China. Figure 7.4 begins during the 2011 parliamentary ballot and 2012 presidential vote in Russia. During this election cycle Russian leaders were anxious about the internet's potential for political disruption, particularly following the use of social media as a catalyst for the events in the Arab Spring (Nocetti,2015). The implementation of the 2012 Foreign Agents Law (see Table 4.1) reflects these concerns about the internet's potential. Furthermore, Figure 7.4 shows a noticeable decline in political stability in 2014, most likely attributed to the beginning of the annexation of Crimea. The ongoing conflict with the West over Ukraine provided justification for a further repressive internet agenda which included the implementation of two major domestic cyber policies (see Table 4.1; Nocetty, 2015).

These events coincide with a marked increase in Russia's internet freedom and violations of users' rights scores in 2014, the former of which has since steadily continued to increase while the latter peaked in 2016 and 2017. Rural and urban protests since 2013 can also account for the worsening in political stability throughout these years and resulted in further crackdowns on digital rights. Figure 7.4 shows slight improvement in Russia's political stability in 2016 and more noticeably in 2017, possibly due to a marginal economic improvement that seemed to foreshadow an end to the recession was in sight (Holodny, 2017). Concurrently, Figure 7.1 shows a peak in Russia's violation of users' rights score in these two years, indirectly refuting Hypothesis 4 which predicted times of stability would see policies that protect digital rights. Hypothesis 3 seems to hold some truth in that Russia, as a less stable country, violates users' digital rights in order to protect national security, specifically naming extremism as justification.

C. United States

According to Feng (1997), it is expected that as a democracy the United States would be more politically stable than the non-democracies of China and Russia. This is confirmed in Figure 7.4 where even at its least stable in this given time period, the United States' political stability and absence of violence/terrorism governance score remains consistently positive. Even at its lowest point of 0.3 in 2016, the United States was far more stable than both China and Russia in the same year, which ironically was their most stable year.

Although not seen in Figure 7.4, according to the World Bank's political stability and absence of violence/terrorism ranking indicator, the United States was most stable in 2000.[17] Between 2002 and 2005, the United States experienced its most political instability most likely due to the 9/11 terrorist attacks and the beginning of the wars with Iraq and Afghanistan. Although Freedom House was not publishing reports during these years, Table 5.1 shows that three major domestic cyber policies were implemented during these years. These policies allow for the direct violation of digital rights and act as the foundation for future policies to further harm digital rights.

Figure 7.4 shows that between 2011 and 2015 the United States' stability remained relatively consistent, varying at most by 0.1. These scores coincide with the United States' violation of users' rights scores sharply increasing from 2011 to 2013, and then more slowly from 2013 to 2015 (see Figure 7.1). Once again, in years of relatively higher stability the United

[17] Data has been collected since in 1996.

States drafted laws, or extended older laws, that negatively impact digital rights. As already discussed in the transparency analysis, the upsurge seen in Figure 7.1 for the United States in 2013 is not the result of sudden increase in policies but rather the public only just becoming aware of such policies already existing.

A similar logic helps to explain the decrease in violations in users' rights score in 2016. The violation of users' rights 2016 score coincides with a drop in political stability in 2016, which is most likely due to the 2016 presidential elections. The simultaneous drop in political stability and slight drop in violation of users' rights could both be attributed to Russian offensive cyber operations on the 2016 presidential election (McKew, 2018). The fact that the 2016 drop in political stability did not return to 2015 levels in 2017 is then a result of growing political unrest and protests and is mirrored by the return to a slight increase of higher violation of users' rights scores. The data concerning the United States seems to align with both Hypotheses 3 and 4. Regarding Hypothesis 3, the relative political instability between 2001 and 2004 witnessed the implementation of domestic cyber policies that curtailed citizens' digital rights in order to protect national security from further terrorism. As a whole, Hypothesis 4 is supported by how the United States retains high levels of political stability and does have policies and laws in place to protect digital rights, starting from its constitution to state laws protecting privacy and net neutrality.

D. Germany

Once again, Feng would attribute Germany's stability to its democratic governance. Yet, over the years Germany's stability has teetered. Although not available in Figure 7.4, Germany's highest level of political stability since 2002 was in 2006 after Chancellor Merkel assumed office in 2005. During this time of high political stability, an important piece of legislation was passed to improve transparency (see Table 6.1). Between 2006 and 2012 the Germany's World Bank political stability governance score steadily declined, possibly as a result of Merkel's party lacking an outright majority and needing a political coalition to govern (World Bank, 2019). Before noticeably improving in 2013, Germany passed another legislation to defend journalists' freedom of information and by proxy digital rights. Despite an improvement in stability in 2013, Figure 7.1 shows that Germany's violation of users' rights score increased within the same year, possibly due to greater awareness of surveillance technologies in Germany.

Stability takes another hit in Germany following an influx of refugees starting in 2015. The refugee crisis in Germany enflamed social tensions and resulted in various laws and regulations (see Table 6.1) to curb online hate speech, fake news, and harmful content (Freedom House, 2018b). This is reflected in the increase in Germany's violation of users' rights scores beginning in 2016. Political instability remained an issue in 2017, particularly due to the proliferation of disinformation leading up to the federal elections in September (Freedom House, 2018b). The emergence of the Alternative for Germany (AfD) and the slow collapse of the Social Democrats (SPD) have also contributed to the disruption of Germany's political stability in the last two years. The lack of an outright majority to form a government by one political party undoubtedly contributes to Germany's recent political stability scores (Conley, 2018).

Despite this, Germany's violation of users' rights score in 2018 did not increase. In fact, new legislation from the European Union is helping to counter Germany's domestic cyber policies that may infringe on digital rights. Unlike the previous three cases studies, when Germany's political stability is relatively higher, it has not proactively implemented policies that

violate digital rights. Instead, it partially affirmed Hypothesis 4 and implemented policies, that originated at the regional level, to protect digital rights. Perhaps this is due to its involvement in the European Union and its more robust protection of human rights through additional human rights conventions. As a leader in the European Union, Germany must also act as a role model, therefore it must be more careful, or secretive, about protecting digital rights particularly in times of stability. Germany does seem to confirm Hypothesis 3 because in times of lower political instability it enacted various policies that interfered in their citizens' digital rights in order to maintain public order.

E. Key Findings

By analyzing each case study's political stability and treatment of digital rights over the years it seems that there is some merit to their hypothesized relationship. For the ease of the reader, those hypotheses were: H_3 states with low levels of political stability are more likely to interfere in their citizens' digital rights through policies that are claimed necessary to protect national security, and H_4 states with high levels of political stability are more likely to implement policies to protect their citizens' digital rights.

Generally speaking, states with less political stability do tend to violate their citizens' digital rights more than more politically stable states, and always with the excuse that it is necessary to protect national security. However, national security can reference different concerns depending on the state. In the case of China and the United States, protecting national security meant protecting against terrorism. For Germany and Russia, it meant protecting against extremist speech. For the former extremist speech means hate speech and for the latter it equates to speech that threatens Russian elites or the government. In the United States and Germany, where political stability levels are higher, when stability falters policies were implemented that harm digital rights, but not always. When Germany faced a steady decline of political stability from 2006 to 2012, instead of implementing policies that violate digital rights, some policies were implemented to guarantee more protection of them. Although this may have been seen as well at the state level in the United States, it was not witnessed nationally. This difference, as previously discussed, may be a result of the influence of the European Union which holds Germany more accountable. Conversely, the United States does not have an equally influential regional body that could affect its domestic policies. Additionally, the United States is a greater power than Germany and as such does not feel as obligated to abide by the rules and guidelines of international bodies. As states with relatively lower political stability given their regime type, the implementation of policies that harm digital rights in Russia and China confirm Hypothesis 3. Furthermore, in times of even lower political stability, China cracked down further on digital rights.

The affirmation of Hypothesis 4 is less clear. At the surface-level more politically stable states have more policies that protect digital rights. This can be seen in both the United States and Germany. Yet, this does not hold true when looking within each case study. For non-democratic states, this Hypothesis is refuted. Figures 7.1 and 7.4 show that despite a dramatic improvement in political stability in China in 2017, China's violation of users' rights score remains at the highest possible level, indicating no correlating improvement. Similarly, Russia's rise in political stability in 2017 is met with no improvement of the treatment of digital rights. This can be interpreted as the governments' attempts to reinforce their rule. Similarly, for the democratic case studies Hypothesis 4 is also debunked. Between 2011 and 2015, the United

States experienced high levels of political stability, yet during this time implemented secretly and overtly policies that infringe on digital rights. When experiencing high levels of political stability in Germany, however, regional policies like the GDPR were implemented, but not at the national level.

Conclusion

This thesis demonstrates that the view a country takes on digital rights can sometimes be predicted by its signatory statuses on the ICCPR and ICESCR. China, Russia, and Germany all ratified the ICESCR. Consequently, they all have particularly robust laws aiming to protect children's rights (Article 10 of ICESCR). As discussed in these states' individual sections, they all have cited the protection of children's rights, which are affected by dissemination of child pornography, as reasons for implementing online constraints. Interestingly, the United States, which has signed but not ratified the ICESCR, has often signed laws protecting against child pornography only to later nullify them on the grounds that they are unconstitutional.[18] The United States remains the laxest of the four case studies in regards to children's rights in relation to the internet. Often children's rights take a backseat to freedom of expression in the United States, which is a reflection of the United States' hierarchy of human rights where ICCPR rights come before those found in the ICESCR. As a state that signed and ratified both the ICCPR and ICESCR, a similar debate often occurs in Germany with mixed results.[19] Although Russia also ratified both human rights conventions, the same issue is not seen, at least not as noticeably, most likely due to the asymmetric power of the state over society which allows it to largely ignore public criticisms.

From the early conception of the internet, even prior to its commercialization globally in the 1990s, scholars and governments were already concerned with its impact on human rights. The right to privacy was among the earliest concerns to be addressed by laws and charters and remains a high concern. The scope of human rights that are affected by the use of the internet and digital technologies continues to expand, thus drawing concern about their protection from human rights organizations. Most recently, the implementation of the Social Credit System in China exemplifies the emergence of a new digital right: the freedom of movement. As an active trailblazer for oppression of digital rights, the further violation of this right can be expected by other states taking note from China. Although not yet publicly seen, the right to belong to a country may also be affected in the near future due to the increasing conflicts posed by differing stances on internet sovereignty lines as a result of the expansion of internet policies and infrastructures. A state's stance on internet sovereignty seems to follow its IR theoretical perspective on state sovereignty. China takes a constructivist realist approach where country borders determine both state and internet sovereignty, yet China's expansion of internet infrastructure and censorship training camps suggest an approach to disseminate their own norms. Russia views internet sovereignty and state sovereignty with a strict realist lens. In both cases, China and Russia advocate for complete control of their domestic policies and ignore international criticisms. The United States and Germany both adhere to neoliberal policies in regard to internet sovereignty, but perhaps Germany more so due to its involvement in the

[18] The Child Pornography Prevention Act of 1996 is one such example. The Supreme Court struck down this act in 2002 because it was found too broad and thus violated the First Amendment (Ashcroft v. Free Speech Coalition, 2002).

[19] The Access Impediment Act of 2006 was an attempt to contain the dissemination of pornography but was repealed due to violation of freedom of expression. Similar debates are occurring again with the enactment of the 2018 NetzDG law.

European Union. Germany, through proxy of the EU, is constructivist through its use of expanding its internet sovereignty in order to influence other states to accept its digital norms. Thus while China and Germany both hold stances with potential constructivist implications, they value very different norms. Diverging perspectives on internet sovereignty are likely to become an increasingly present issue and requires further research.

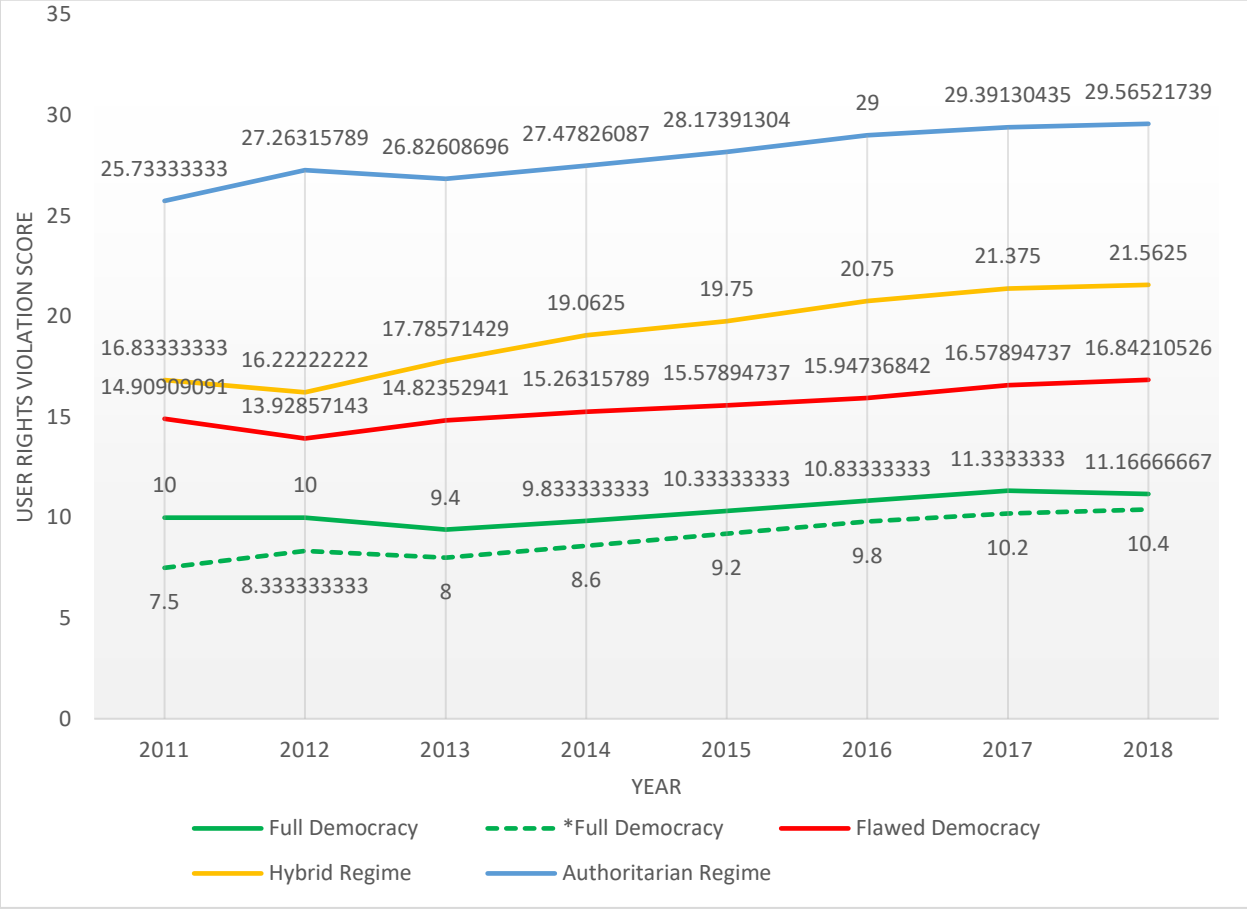
Aside from the already well-established rights, the development of policies and practices regarding the internet and other digital technologies has the potential to birth new rights. The first case of this comes from the European Union: the right to be forgotten. Such a right cannot be directly equated with pre-existing rights but falls closely within the concepts of right to privacy and freedom of expression. For reasons discussed above, it can be predicted that this right is more likely to take hold in states that have ratified the ICCPR. As technologies, particularly artificial intelligence, continue to advance further digital rights can be expected to emerge and will undoubtedly give rise to more ethical and legal concerns. Therefore, digital rights must be afforded particular attention in both states and international organizations. The case of the right to be forgotten is of particular interest because its timeline and success or failure will determine the feasibility of a regional body disseminating a digital norm. However, international organizations should not be complacent and wait. Instead, a proactive approach is needed to first create an international convention for digital rights. Within said convention, the question of whether internet access should be considered a human right must be formally addressed.

The types of policies enacted, and treatment of digital rights is largely affected by government type. The comparative analysis section of this essay posed and determined the validity of four hypotheses. The greatest insights to emerge from these hypotheses were; (1) a correlation between political stability and treatment of digital rights does exist, and (2) a correlation between transparency and treatment of digital rights is inconclusive, but an apparent correlation between government type and digital rights does exist. The latter insight prompted further analysis of all of the Freedom House Freedom of the Net reports between 2011 and 2018. The results of the analysis are shown in Figure 8.1. The trend lines suggest a clearly possible correlation between regime type and treatment of digital rights. The more democratic a state is, the less violations of users' rights are observed while the opposite is true the more authoritarian a state is. Figure 8.1 also shows a new insight; with the exception of full democracies, every regime type's treatment of digital rights has been worsening since 2013. The only reason full democracies do not demonstrate this trend is because of the United Kingdom's 2018 violation of users' rights score which acted as an outlier. For that reason, the dashed line represents the data of all full democracies excluding the United Kingdom. With this updated line, all regime types show a consistent worsening of the treatment of digital rights. This is a concerning trend that if not addressed through international conventions might continue.

Incorporating internet access into such a convention will likely cause factions among states split along government regimes types. Based on the information presented in this thesis, it could be predicted that full democracies and flawed democracies would be advocates of such a right. Conversely, hybrid and authoritarian regimes will be opposed. Perhaps decentralized or

fragmented legal approaches will be necessary to develop the initial treaties with the hope that digital rights norms subsequently will cascade.

Figure 8.1 *Average Violation of Users' Rights Scores According to Regime Type 2011-2018*



Source: Data collected from the Freedom on the Net Reports from 64 countries.[20] Each country was categorized into full democracy, flawed democracy, hybrid regime, and authoritarian regime based on the 2018 Democracy Index.[21]

**Full Democracies excluding the United Kingdom*

Moreover, the validation of the apparent correlation between regime type and digital rights has an impact on other avenues of research, including: the use of the internet for democratization, the dissemination of digital norms in various types of regimes, and the categorization of what digital rights are at risk based on regime type. By categorizing treatment of digital rights by regime type it may be possible to anticipate the evolution of a state's digital rights hierarchy. Based off the information provided in this thesis, emerging and established

[20] Not all countries had data reported for all years. This was taken into account when calculating averages for each year.

[21] Germany and 5 other countries are represented within the full democracy line. The United States and 18 other counties are represented within the flawed democracy line. Both Russia and China along with 21 other countries are represented within the authoritarian regime line. The hybrid regime line consists of 16 countries.

democracies tend to place freedom of expression and privacy over most other rights, except when in times of relative political instability. Democracies facing political instability will increase policies restricting online freedoms of expression in order to curb political disinformation and hate speech. Similarly, during times of instability due to acts of violence/terrorism, democracies are far more likely to enact surveillance policies that violate individuals' right to privacy.

Figure 8.1 shows that hybrid regimes' treatments of digital rights are currently worsening at the fastest rate. One possible explanation could be the success of authoritarian regimes to instill some form of political stability with higher levels of online constraints. A characteristic of hybrid regimes is instability (Menocal, Fritz, and Rakner, 2008). Therefore, these states may be more inclined to implement harsher internet policies after witnessing their success in authoritarian states. Current challenges to liberal democracies and democratization may dictate whether the digital rights norms related to democratic regimes or authoritarian regimes spread. Yet, the rise of digital authoritarianism[22] shows that some rights are equally at risk regardless of regime type. The most notable example is the right to privacy which is systematically undermined by the use of mass surveillance in both democracies and authoritarian regimes.

This research demonstrates the prevailing relationship between digital rights and regimes type. This relationship has important implications considering the reliance of the internet in the intensification and progress of globalization in the Global South. Despite no single prevalent regime type in the Global South, most of the states in this category recognize the necessity of globalization for economic growth and development. To the extent that globalization is linked to free movement of goods, capital, and ideas, there could perhaps be a preference to maximize digital rights to gain these benefits. As such, connecting to the internet may be a priority in the years to come.[23] During this transition to a globally connected world the types of policies to be implemented and subsequently the treatment of digital rights in these states may be predicted by the regime type. The future of digital rights as a norm could follow two trajectories when put in the context of the findings of this research. First, as the Global South goes online the dissemination of what digital rights norms will cascade depends on the regime types of the states in this category. The digital rights norms to prevail in this trajectory are dependent upon which type of regime has the most practitioners. Second, the acceptance of internet sovereignty over territorial sovereignty in cyberspace will give states that do not subscribe to the realist view of sovereignty an edge in disseminating their digital rights norms. This can be exemplified by the extension of digital rights norms by the European Union and Germany beyond their territory.

Yet, perhaps more important than the above-stated factors are the expected demographic and generational shift that may affect societal, and eventually states, attitudes toward digital rights. Younger generations and the generations to come depend upon the digital world and globalization, more so than older generations. As a result, younger cohorts might feel less of a

[22] Term coined in Freedom on the Net report 2018 (Shahbaz, 2018).
[23] Indeed, the African Union, with the support of the World Bank Group, aims to have every individual, business, and government in Africa connected to the internet by 2030 in order to lay the foundations for a digital economy (World Bank Group, 2019).

blind loyalty to their state, particularly due to a greater awareness of the practices of individual rights in other states. It could then logically follow that younger generations may support norms that treat digital rights, especially the right to internet access, as a derogable human right. While most globalized states are facing the issue of an aging population, parts of the Global South—namely Africa—have the highest percentage of youth populations (World Atlas, 2019). Therefore, as Africa becomes increasingly more connected and younger generations that grew up with the internet replace older generations around the world it could be the case that greater support for a movement toward a norm of digital rights might emerge. The beginnings of such a movement are already evident in the expansion of the scope of digital rights in charters and conventions. Therefore, although this research shows that regime type effects the treatment of digital rights and thus the conception of digital rights as human rights, technological and demographic change has the potential to alter the specific nature of global practices.

Bibliography

AccessNow. (2019). *What is an internet shutdown?*. KeepItOn. [online] Available at: https://www.accessnow.org/keepiton/ [Accessed 13 Apr. 2019].

Albert, E. (2015). *The Shanghai Cooperation Organization*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/backgrounder/shanghai-cooperation-organization [Accessed 9 Apr. 2019].

Aleksejeva, N. (2018). *#DigitalResistance: Protest Grows in Russia*. [online] Atlantic Council DFRLab. Available at: https://medium.com/dfrlab/digitalresistance-protest-grows-in-russia-b318b1304cc7 [Accessed 3 Apr. 2019].

Alston, P. (1984). Conjuring up New Human Rights: A Proposal for Quality Control. *The American Journal of International Law*, 78(3), pp.607-621.

Amnesty International. (2017). *Amnesty reveals alarming impact of online abuse against women.* Amnesty International USA. [online] Available at: https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/ [Accessed 3 Apr. 2019].

Amnesty International. (2018). *Amnesty International Report 2017/8 The State of the World's Human Rights.* [online] Available at: https://www.amnesty.org/download/Documents/POL1067002018ENGLISH.PDF [Accessed 9 Apr. 2019].

Appell, M. (2018). A New Responsibility for Internet Platforms: Germany's New Hate Speech Law. *American Institute for Contemporary German Studies.* [online] Available at: https://www.aicgs.org/2018/01/a-new-responsibility-for-internet-platforms-germanys-new-hate-speech-law/ [Accessed 13 Apr. 2019].

Arthur, C. (2014). What is Google deleting under the 'right to be forgotten' – and why. *The Guardian*. [online] Available at: https://www.theguardian.com/technology/2014/jul/04/what-is-google-deleting-under-the-right-to-be-forgotten-and-why [Accessed 9 Apr. 2019].

Article 19 (2017). *Digital Rights in Russia: An Analysis of the deterioration to Freedom of Expression Online*. [online] London: Free Word Centre, pp.6. Available at: https://www.article19.org/data/files/medialibrary/38696/case_studies_R02_A5_WEB.pdf [Accessed 13 Apr. 2019].

Association of Progressive Communications. (2006). *APC Internet Rights Charter*. [online] Available at: http://www.apc.org/en/ node/5677 [Accessed 13 Apr. 2019].

Baraniuk, C. (2016). Why the forgotten Soviet internet was doomed from the start. *BBC Future.* [online] Available at: http://www.bbc.com/future/story/20161026-why-the-forgotten-soviet-internet-was-doomed-from-the-start [Accessed 9 Apr. 2019].

Barmin, B., Jones, G., Moiseeva, S. and Winkelman, Z. (2011). International Arms Control and Law Enforcement in the Information Revolution: An Examination of Cyber Warfare and Information Security. *The Quarterly Journal*, pp.73-94.

Barma, N., Ratner, E. and Weber, S. (2013). The Mythical Liberal Order. *The National Interest*, pp.56-67.

Bazan, E. (2004). *Intelligence Reform and Terrorism Prevention Act of 2004: "Lone Wolf" Amendment to the Foreign Intelligence Surveillance Act*, CRS Report for Congress. [online] Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a448016.pdf [Accessed 13 Apr. 2019].

Bidwell, A. (2013). Majority of Americans Say Corruption Has Increased. *U.S.News & World Report.* [online] Available at: https://www.usnews.com/news/newsgram/articles/2013/07/10/majority-of-americans-say-corruption-has-increased [Accessed 4 Apr. 2019].

Birkinshaw, P. (2006). Freedom of information and openness: Fundamental human rights?. *Administrative Law Review*, 58(1), pp.177-218.

Bröckling, M. (2018). Ab Sommer in Bayern: Das härteste Polizeigesetz seit 1945 [Starting in summer in Bavaria: The harshest policing laws since 1945]. *Netzpolitik*. [online] Available at: https://netzpolitik.org/2018/ab-sommer-in-bayern-das-haerteste-polizeigesetz-seit-1945/ [Accessed 13 Apr. 2019].

Butler, J. (2015). Cybersecurity Information Sharing In the "Ominous" Budget Bill: A Setback for Privacy. [Blog] *Center for Democracy & Technology*. Available at: https://cdt.org/blog/cybersecurity-information-sharing-in-the-ominous-budget-bill-a-setback-for-privacy/ [Accessed 13 Apr. 2019].

Callaway, R. and Harrelson-Stephens, J. (2007). *Exploring International Human Rights: Essential Readings Critical Connections: Studies in Peace, Democracy, and Human Rights.* Lynne Rienner Publishers.

CBSN Originals. (2018). Weaponizing social media: The Rohingya crisis. *CBS News.* [online] Available at: https://www.cbsnews.com/news/rohingya-refugee-crisis-myanmar-weaponizing-social-media-main/ [Accessed 3 Apr. 2019].

Cerf, V. (2012). Internet Access Is Not a Human Right. *The New York Times*. [online] Available at: https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html?_r=1&ref=opinion [Accessed 2 Apr. 2019].

CERNIC. (2001). Evolution of Internet in China. *China Education and Research Network*. [online] Available at: https://www.webcitation.org/66O7ienSr?url=http://www.edu.cn/introduction_1378/20060323/t20060323_4285.shtml [Accessed 9 Apr. 2019].

CEU School of Public Policy. (2017). *Understanding Russia's Internet Policy*. [online] Available at: https://cmds.ceu.edu/article/2017-03-16/understanding-russias-internet-policy [Accessed 13 Apr. 2019].

Cheng, R. (2019). T-Mobile and Sprint merger: Here's everything you need to know. *CNET*. [online] Available at: https://www.cnet.com/news/t-mobile-and-sprint-are-merging-heres-everything-you-need-to-know/ [Accessed 13 Apr. 2019].

CHINA. (1983). 中华人民共和国宪法 [*The Constitution of the People's Republic of China]:(adopted on December 4, 1982 by the Fifth National People's Congress of the People's Republic of China at its fifth session.* [online] Available at: http://www.npc.gov.cn/npc/xinwen/2018-03/22/content_2052489.htm [Accessed 13 Apr. 2019].

Cnnic.com.cn. (2012). *The Internet Timeline of China 1986~2003*. [online] Available at: https://cnnic.com.cn/IDR/hlwfzdsj/201306/t20130628_40563.htm [Accessed 3 Apr. 2019].

Congressional-Executive Commission on China. (2005). *Provisions on the Administration of Internet News Information Services (Chinese Text and CECC Full Translation)*. [online] Available at: https://www.cecc.gov/resources/legal-provisions/provisions-on-the-administration-of-internet-news-information-services [Accessed 13 Apr. 2019].

Conley, H. (2018). The German Paradox: Strong Economy, Angry Politics, *Center for Strategic & International Studies*. [online] Available at: https://www.csis.org/analysis/german-paradox-strong-economy-angry-politics [Accessed 13 Apr. 2019].

Cooke, T. (2012). *Has Vladimir Putin Always Been Corrupt? And Does it Matter?*.[online] Wilson Center. Available at: https://www.wilsoncenter.org/event/has-vladimir-putin-always-been-corrupt-and-does-it-matter [Accessed 4 Apr. 2019].

Cooper, H. (2018). Angela Merkel signals potential changes to online hate speech law. *Politico*. [online] Available at: https://www.politico.eu/article/angela-merkel-signals-potential-changes-to-germany-online-hate-speech-law/ [Accessed 13 Apr. 2019].

Council of Europe. (2001). *Additional Protocol to the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows.* [online] Available at: https://www.refworld.org/docid/3dde11814.html [Accessed 10 Apr. 2019]

Clinton, H. (2010). Statement: Hillary Clinton on internet freedom. *Financial Times*. [online] Available at: https://www.ft.com/content/f0c3bf8c-06bd-11df-b426-00144feabdc0 [Accessed 13 Apr. 2019].

CPJ. (2017). Editor shot dead in Russia's Siberia. *Committee to Protect Journalists.* [online] Available at: https://cpj.org/2017/05/editor-shot-dead-in-russias-siberia.php [Accessed 13 Apr. 2019].

Deloitte. (2019). *The new German Privacy Act: An overview*. [online] Available at: https://www2.deloitte.com/dl/en/pages/legal/articles/neues-bundesdatenschutzgesetz.html [Accessed 13 Apr. 2019].

DeNardis, L. (2014). *The global war for internet governance.* New Haven, CT: Yale University Press.

Detrick, H. (2019). U.S. Is Perceived to Be More Corrupt Under Trump. *Fortune* [online] Available at: http://fortune.com/2019/01/29/us-corruption-transparency-international-2018/ [Accessed 4 Apr. 2019].
Deudney, D. and Ikenberry, J. (2018). Liberal World: The Resilient Order. *Foreign Affairs,* pp.16-24.

Diamond, J. (2016). Russian hacking and the 2016 election: What you need to know. *CNN*. [online] Available at: https://www-m.cnn.com/2016/12/12/politics/russian-hack-donald-trump-2016-election/index.html [Accessed 2 Apr. 2019].

Dou, E. (2017). Jailed for a Text: China's Censors Are Spying on Mobile Chat Groups. *The Wall Street Journal*. [online] Available at: https://www.wsj.com/articles/jailed-for-a-text-chinas-censors-are-spying-on-mobile-chat-groups-1512665007 [Accessed 3 Apr. 2019].

Dowell, W. (2006). The Internet, censorship, and China. *Georgia Journal of International Affairs,* pp.111-119.

Duggan, M. (2017). 1 in 4 black Americans have faced online harassment because of their race or ethnicity. *Pew Research Center Factank*. [online] Available at: https://www.pewresearch.org/fact-tank/2017/07/25/1-in-4-black-americans-have-faced-online-harassment-because-of-their-race-or-ethnicity/ [Accessed 13 Apr. 2019].

Edwards, S. (2012). *Is Internet Access A Human Right?*. [online] Amnesty International USA. Available at: https://www.amnestyusa.org/is-internet-access-a-human-right/ [Accessed 2 Apr. 2019].

Electronic Frontier Foundation. (2019). *Upstream vs. PRISM*. [online] Available at: https://www.eff.org/pages/upstream-prism [Accessed 13 Apr. 2019].

ETS No. 185 (2001). *Convention on Cybercrime*, Council of Europe [online] Available at: https://www.refworld.org/docid/47fdfb202.html [Accessed 10 April 2019]

European Commission. (2019). *2018 reform of EU data protection rules*. [online] Available at: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en [Accessed 13 Apr. 2019].

European Digital Rights. (2011). *German web blocking law repealed,* EDRi. [online] Available at: https://edri.org/edrigramnumber9-24german-internet-blocking-law-repealed/ [Accessed 13 Apr. 2019].

Foucault, M. (1975). *Discipline and Punish: The Birth of the Prison*. New York: Pantheon Books.

Freedom House. (2011). *Freedom on the Net 2011: United States Country Profile*, Freedom House [online] Available at: https://freedomhouse.org/report/freedom-net/2011/united-states [Accessed 13 Apr. 2019].

Freedom House. (2013). *Freedom on the Net 2013: Germany Country Profile*, Freedom House [online] Available at: https://freedomhouse.org/report/freedom-net/2013/germany [Accessed 13 Apr. 2019].

Freedom House. (2017). *Freedom of the Press 2017: Russia Country Report*, Freedom House. [online] Available at: https://freedomhouse.org/report/freedom-press/2017/russia [Accessed 9 Apr. 2019].

Freedom House. (2018a). *Freedom on the Net 2018: China Country Report*, Freedom House. [online] Available at: https://freedomhouse.org/report/freedom-net/2018/china [Accessed 9 Apr. 2019].

Freedom House. (2018b). *Freedom on the Net 2018: Germany Country Report*, Freedom House. [online] Available at: https://freedomhouse.org/report/freedom-net/2018/germany [Accessed 9 Apr. 2019].

Freedom House. (2018c). *Freedom on the Net 2018: Russia Country Report*, Freedom House. [online] Available at: https://freedomhouse.org/report/freedom-net/2018/russia [Accessed 9 Apr. 2019].

Freedom House. (2018d). *Freedom on the Net 2018: United States Country Report*, Freedom House. [online] Available at: https://freedomhouse.org/report/freedom-net/2018/united-states [Accessed 9 Apr. 2019].

Fuchs, M., Benaim, D. and Johnson, B. (2018). China is Violating Uighurs' Human Rights. The United States Must Act. *Foreign Policy.* [online] Available at: https://foreignpolicy.com/2018/11/28/china-is-violating-uighurs-human-rights-the-united-states-must-act/ [Accessed 3 Apr. 2019].

G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948)

Gellman, B. and Soltani, A. (2014). NSA surveillance program reaches 'into the past' to retrieve, replay phone calls. *The Washington Post.* [online] Available at https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html [Accessed 3 Apr. 2019].

Girard, B. (2019). The Real Danger of China's National Intelligence Law. *The Diplomat.* [online] Available at: https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/ [Accessed 3 Apr. 2019].

Gleditsch, N. (2008). The Liberal Moment Fifteen Years On. *International Studies Quarterly*, pp.691-712. (2012).

Global Network Initiative. (2017). *Proposed German Legislation Threatens Free Expression Around the World*. [online] Available at: https://globalnetworkinitiative.org/proposed-german-legislation-threatens-free-expression-around-the-world/ [Accessed 13 Apr. 2019].

Goel, V. (2019). India Proposes Chinese-Style Internet Censorship. *The New York Times*. [online] Available at: https://www.nytimes.com/2019/02/14/technology/india-internet-censorship.html [Accessed 2 Apr. 2019].

Google. (2018). *Search removals under European privacy*, Google Transparency Report [online] Available at: https://transparencyreport.google.com/eu-privacy/overview [Accessed 13 Apr. 2019].

Google Spain v. AEPD and Mario Costeja [2014]C-131/12 (CJEU).

Griffiths, J. (2018). China is exporting the Great Firewall as internet freedom declines around the world. *CNN World*. [online] Available at: https://www-m.cnn.com/2018/11/01/asia/internet-freedom-china-censorship-intl/index.html?r=https%3A%2F%2Fwww.google.com%2F [Accessed 9 Apr. 2019].

Gross, D. (2013). Google boss: Entire world will be online by 2020. *CNN Business.* [online] Available at: https://www.cnn.com/2013/04/15/tech/web/eric-schmidt-internet/index.html [Accessed 5 Apr. 2019].

Haass, R. (2017). *A World in Disarray: American Foreign Policy and the Crisis of the Old Order*. Penguin Books.

Hammond, A. (1997). The Telecommunications Act of 1996: Codifying the Digital Divide. *Federal Communications Law Journal,* 50(1), pp.180-208.

Hatton, C. (2015). China 'social credit': Beijing sets up huge system. *BBC News*. [online] Available at: https://www.bbc.com/news/world-asia-china-34592186 [Accessed 3 Apr. 2019].

Holodny, E. (2017). Russia is getting closer to pulling out of its recession. *Business Insider*. [online] Available at: https://www.businessinsider.com/russia-gdp-2016-2017-2 [Accessed 13 Apr. 2019].

Homeland Security Act of 2002.1.

Howell, C. and West, D. (2016). *The internet as a human right*. [Blog] Brookings. Available at: https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/ [Accessed 2 Apr. 2019].

Human Rights Watch. (2018a). *Germany: Flawed Social Media Law NetzDG is Wrong Response to Online Abuse*, Human Rights Watch. [online] Available at: https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law [Accessed 9 Apr. 2019].

Human Rights Watch. (2018b). *The EU General Data Protection Regulation Questions and Answers,* Human Rights Watch. [online] Available at: https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation [Accessed 9 Apr. 2019].

Internet Rights & Principles Coalition. (2014). *The Charter of Human Rights and Principles for the Internet.* [online] Available at: https://www.ohchr.org/documents/issues/opinion/communications/internetprinciplesandrightscoalition.pdf [Accessed 13 Apr. 2019].

Internet Society. (2012). *Global Internet User Survey Reveals Attitudes, Usage, and Behavior*. [online] Available at: https://www.internetsociety.org/news/press-releases/2012/global-internet-user-survey-reveals-attitudes-usage-and-behavior/ [Accessed 9 Apr. 2019].

James, Y. and Jones, S. (2017). When Russian Trolls Attack. *Wired*. [online] Available at: https://www.wired.com/2017/10/russian-trolls-attack/ [Accessed 3 Apr. 2019].

Jao, N. (2018). WeChat now has over 1 billion active monthly users worldwide. *Technode.* [online] Available at: https://technode.com/2018/03/05/wechat-1-billion-users [Accessed 3 Apr. 2019].

Keane, A. and Swire, P. (2018). The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems. [Blog] *Lawfare*. Available at: https://www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems [Accessed 13 Apr. 2019].

Kelley, M. (2014). Putin Just Called the Internet a 'CIA Project' – Here's Why. *Business Insider.* [online] Available at: https://www.businessinsider.com/putin-just-called-the-internet-a-cia-project-2014-4 [Accessed 9 Apr. 2019].

Kelly, H. (2018). California just passed its net neutrality law. The DOJ is already suing. *CNN*. [online] Available at: https://www.cnn.com/2018/10/01/tech/california-net-neutrality-law/index.html [Accessed 3 Apr. 2019].

Kemp, S. (2019). Digital 2019: Global Internet Use Accelerates. [Blog] *We Are Social.* Available at: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates [Accessed 5 Apr. 2019].

Keohane, R. (2002). The Globalization of Informal Violence, Theories of World Politics, and the "Liberalism of Fear." *Dialogue IO*, 1(1), pp.29-43.

Kizekova, A. (2012). The Shanghai cooperation organisation : challenges in cyberspace. (RSIS Commentaries, No. 033). RSIS Commentaries. Singapore: Nanyang Technological University.

Kobrin, S. (2004). Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global govenance. *Review of International Studies*, 30(1), pp.111-131.

Kornelius, S. (2010). Hegemon wider Willen. *Süddeutsche Zeitung.* [online] Available at: https://www.sueddeutsche.de/politik/euro-krise-hegemon-wider-willen-1.1028932 [Accessed 9 Apr. 2019].

Kremlin. (2011). *Amendments to bolster anti-corruption legislation.* [online] Available at: http://en.kremlin.ru/events/president/news/11147 [Accessed 4 Apr. 2019].

Kremlin. (2016). *Meeting of the Anti-Corruption Council.* [online] Available at: http://en.kremlin.ru/events/president/news/51207 [Accessed 4 Apr. 2019].

Kundnani, H. (2012). Germany: What Hegemon?. *European Council on Foreign Relations*. [online] Available at: https://www.ecfr.eu/article/commentary_germany_what_hegemon#ftn1 [Accessed 9 Apr. 2019].

Land, M. (2013). Toward an International Law of the Internet. *Harvard International Law Journal*, 54(2), pp.393-458.

La Rue, F. (2011). *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Addendum, Communications to and from Governments*. UN Human Rights Council.

Liang, B. and Lu, H. (2010). Internet Development, Censorship, and Cyber Crimes in China. *Journal off Contemporary Criminal Justice*, 26(1), pp.103-120.

Lindsay, J. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3), pp.365-404.

Ma, A. (2018). A Chinese woman who poured ink over a Xi Jinping poster has been missing for 2 weeks, and her father was reportedly detained. *Business Insider.* [online] Available at: https://www.businessinsider.com/dong-yaoqiong-pours-ink-on-xi-jinping-poster-whereabouts-unknown-2018-7 [Accessed 5 Apr. 2019].

Maas, H. (2018). DAS sagt der Justizminister [The Justice Minister says that]. *Bild.* [online] Available at: https://www.bild.de/politik/inland/heiko-maas/das-sagt-er-zur-kritik-an-seinem-gesetz-54367952.bild.html [Accessed 13 Apr. 2019].

Maréchal, N. (2017). Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. *Media and Communication*, 5(1), pp.29-41.

Margulies, P. (2013). Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy. *Indiana Journal of Global Legal Studies*, 24(2), pp.459-496.

Mathiesen, K. (2014). Human Rights for the Digital Age. *Journal of Mass Media Ethics*, 29(1), pp.2-18.

Matsakis, L. (2019). What Happens If Russia Cuts Itself Off from the Internet. *Wired*. [online] Available at: https://www.wired.com/story/russia-internet-disconnect-what-happens/ [Accessed 9 Apr. 2019].

Mayes, T. (2011). We have no right to be forgotten online. *The Guardian*. [online] Available at: https://www.theguardian.com/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet [Accessed 9 Apr. 2019].

McGuinness, D. (2017). How a cyber attack transformed Estonia. *BBC News.* [online] Available at: https://www.bbc.com/news/39655415 [Accessed 2 Apr. 2019].

McKew, M. (2018). Did Russia Affect the 2016 Election? It's Now Undeniable. *Wired.* [online] Available at: https://www.wired.com/story/did-russia-affect-the-2016-election-its-now-undeniable/ [Accessed 13 Apr. 2019].

Menocal, A., Fritz, V. and Rakner, L. (2008). Hybrid Regimes and the challenges of deepening and sustaining democracy in developing countries. *South African Journal of International Affairs*, 15(1), pp.29-40.

Michel, C. (2017). It's Official: India and Pakistan Join Shanghai Cooperation Organization. *The Diplomat*. [online] Available at: https://thediplomat.com/2017/06/its-official-india-and-pakistan-join-shanghai-cooperation-organization/ [Accessed 13 Apr. 2019].

Ministry of Communications and Information and Ministry of Law. (2018). *Deliberate Online Falsehoods: Challenges and Implications*.

National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce of the People's Republic of China (2015). *Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road*. Beijing: People's Republic of China.

Neumayer, E. (2007). Qualified Ratification: Explaining Reservations to International Human Rights Treaties. *The Journal of Legal Studies*, 36(2), pp.397-429.

Nocetti, Julien. (2015). Russia's 'dictatorship-of-the-law' approach to internet policy. *Journal on internet regulation*, 4(4), pp.1-19.

Nye, J. (2011). *The Future of Power*. New York: Perseus.

Ognyanova, K. (2015). In Putin's Russia, information has you: Media control and internet censorship. In M. M. Mervi, *Management and participation in the public sphere,* pp.62-75. Hershey, PA: IGI Global.

O'Hara, K. and Stevens, D. (2006). *Inequality.com: Politics, Power and the Digital Divide*. Oxford: Oneworld.

OpenNet Initiative. (2010). *ONI Germany Country Profile*, ONI. [online] Available at: https://opennet.net/research/profiles/germany [Accessed 13 Apr. 2019].

Or-Hof, D. (2018). Will the GDPR violate Israeli sovereignty?. [Blog] *The International Association of Privacy Professionals*. Available at: https://iapp.org/news/a/will-the-gdpr-violate-israeli-sovereignty/ [Accessed 13 Apr. 2019].

Pally, N. (2014). *Dangerous practice of digital mass surveillance must be subject to independent checks and balances*, OHCHR [online] Available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14875 [Accessed 13 Apr. 2019].

Palmer, J. (2018). China's Stability Myth Is Dead. *Foreign Policy*. [online] Available at: https://foreignpolicy.com/2018/02/26/chinas-stability-myth-is-dead/ [Accessed 13 Apr. 2019].

Paterson, W. (2011). The Reluctant Hegemon? Germany Moves Centre Stage in the European Union. *Journal of Common Market Studies,*49, pp.57-75.

Patrick, M. and Feng, A. (2018). *Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road.* [Blog] Council on Foreign Relations. Available at: https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road [Accessed 3 Apr. 2019].

Pccharter.net. (1999). *People's Communication Charter*. [online] Available at: http://www.pccharter.net/charteren.html [Accessed 13 Apr. 2019].

Pear, R. (2019). On Disability and on Facebook? Uncle Sam Wants to Watch What You Post. *The New York Times*. [online] Available at: https://www.nytimes.com/2019/03/10/us/politics/social-security-disability-trump-facebook.html [Accessed 9 Apr. 2019].

Penney, J. (2011). Internet Access Rights: A Brief History and Intellectual Origins. *William Mitchell Law Review*, 38(1), pp.10-42.

Peixin, L. (2018). *Social Credit Law: Principles, Rules and Cases*. Beijing: Peking University Press

Phillips, T. (2015). China's Xi Jinping says internet users must be free to speak their minds. *The Guardian.* [online] Available at: https://www.theguardian.com/world/2015/dec/16/china-xi-jinping-internet-users-freedom-speech-online [Accessed 2 Apr. 2019].

Powell, A., Bryne, A. and Dailey, D. (2010). The Essential Internet: Digital Exclusion in Low-Income American Communities. *Policy & Internet*, 2(2), pp.159-190.

Prantl, H. (2018). Die digitale Inquisition hat begonnen [The digital inquisition has begun]. *Süddeutsche Zeitung* [online] Available at: https://www.sueddeutsche.de/digital/staatstrojaner-die-digitale-inquisition-hat-begonnen-1.3843494 [Accessed 13 Apr. 2019].

Preibusch, S. (2015). 'Privacy Behaviors After Snowden', *Communications of the ACM*, 58(5), pp.48-55. doi: 10.1145/2663341.

Qiu, J. (2000). Virtual Censorship in China: Keeping the Gate Between the Cyberspaces. *International Journal of Communications Law and Privacy,* pp.1-24.

Read, M. (2018). The E.U.'s New Privacy Laws Might Actually Create a Better Internet. *New York Intelligencer*. [online] Available at: http://nymag.com/intelligencer/2018/05/can-gdpr-create-a-better-internet.html [Accessed 13 Apr. 2019].

Reno v. ACLU [1997] 521 US 844 (United States Supreme Court).

Reporters Without Border. (2018). *2018 World Press Freedom index.* [online] Available at: https://rsf.org/en/ranking/2018 [Accessed 13 Apr. 2019].

Robinson, O. (2018). The memes that might get you jailed in Russia. [Blog] *BBC News.* Available at: https://www.bbc.com/news/blogs-trending-45247879 [Accessed 9 Apr. 2019].

Schönberger, C. (2012). Hegemon wider Willen. Zur Stellung Deutschlands in der Europäischen Union. *Merkur.* [online] Available at: https://volltext.merkur-zeitschrift.de/preview/55360a9a546f88a5268d9c74/mr_2012_01_0001-0008_0001_01 [Accessed 9 Apr. 2019].

Schmitz, R. (2017). What Motivates Chinese President Xi Jinping's Anti-Corruption Drive? *NPR.* [online] Available at: https://www.npr.org/sections/parallels/2017/10/24/559004647/what-is-the-motivation-behind-chinese-president-xi-jinpings-anti-corruption-driv [Accessed 4 Apr. 2019].

Schreck, C. (2018). Russian Website Under Fire After Investigation of FSB Chief. *RedioFreeEurope RadioLiberty*. [online] Available at: https://www.rferl.org/a/russia-fsb-bortnikov-russiangate-real-estate/28998057.html [Accessed 13 Apr. 2019].

Segal, A. (2017). *An Update on U.S.-China Cybersecurity Relations*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/blog/update-us-china-cybersecurity-relations [Accessed 1 Apr. 2019].

Shahbaz, A. (2018). *Freedom on the Net Report 2018 The Rise of Digital Authoritarianism.* [online] Freedom House. Available at: https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism [Accessed 10 Apr. 2019].

Shimer, D. (2017). Germany Raids Homes of 36 People Accused of Hateful Postings Over Social Media. *The New York Times.* [online] Available at: https://www.nytimes.com/2017/06/20/world/europe/germany-36-accused-of-hateful-postings-over-social-media.html [Accessed 5 Apr. 2019].

Soldatov, A. and Borogan, I. (2013). Russia's Surveillance State. *World Policy Journal*, 30(3), pp.23-30.

Spencer, V. (2002). Cyber terrorism: mass destruction or mass disruption?. *Canadian Underwriter*. [online] pp.16-18. Available at: http://www.crime-research.org/library/mi2g.htm [Accessed 2 Apr. 2019].

Spiegel Online. (2013). German Trust in United States Plummets. *Spiegel.* [online] Available at: http://www.spiegel.de/international/germany/nsa-spying-fallout-majority-of-germans-mistrust-united-states-a-932492.html [Accessed 3 Apr. 2019].

Statista. (2017). *China: number of internet users in December 2017.* [online] Available at: https://www.statista.com/statistics/265140/number-of-internet-users-in-china/ [Accessed 9 Apr. 2019].

Statista. (2019). *Russia: number of internet users 2013-2019.* [online] Available at: https://www.statista.com/statistics/251818/number-of-internet-users-in-russia/ [Accessed 9 Apr. 2019].

Stephen, M. (2017). Emerging Powers and Emerging Trends in Global Governance. *Global Governance*, pp.483-502.

Sterling-Folker, J. (2014). All Hail to the Chief: Liberal IR Theory in the New World Order. *International Studies Perspectives*, 16(1), pp.40-49.

Taylor, A. (2016). 60 percent of Russians think internet censorship is necessary, poll finds. *The Washington Post*. [online] Available at: https://www.washingtonpost.com/news/worldviews/wp/2016/11/18/60-percent-of-russians-think-internet-censorship-is-necessary-poll-finds/?utm_term=.4f41b7d01317 [Accessed 3 Apr. 2019].

Tolley, H. (1987). *The UN Commission on Human Rights*. Boulder: Westview Press.

Tomalty, J. (2017). Is There a Human Right to Internet Access?. *Philosophy Now*, [online] (118), pp.6-8. Available at: https://philosophynow.org/issues/118/Is_There_A_Human_Right_To_Internet_Access [Accessed 2 Apr. 2019].

Tsirbas, M. (2016). What Does the Nine-Dash Line Actually Mean?. *The Diplomat*. [online] Available at: https://thediplomat.com/2016/06/what-does-the-nine-dash-line-actually-mean/ [Accessed 13 Apr. 2019].

Tully, S. (2014). A Human Right to Access the Internet? Problems and Prospects. *Human Rights Law Review*, pp.175-195.

United Nations (1997). *Report of the Committee on the Elimination of Discrimination against Women*. New York: UN General Assembly, pp.248-274.

U.S. Press Freedom Tracker. (2018). Journalist Manuel Duran, arrested while covering immigration protest, could be deported by ICE. *Press Freedom Tracker* [online] Available at: https://pressfreedomtracker.us/all-incidents/journalist-manuel-duran-arrested-while-covering-immigration-protest-could-be-deported-ice/ [Accessed 9 Apr. 2019].

US Legal (2019). *Federal Laws – Internet Law*. [online] US Legal Internet Law. Available at: https://internetlaw.uslegal.com/piracy-and-file-sharing/federal-laws/ [Accessed 13 Apr. 2019].

Von Rohr, M. (2014). Dictatorships and Chaos Go Hand in Hand. *Spiegel*. [online] Available at: http://www.spiegel.de/international/world/stable-dictatorships-are-not-the-lesser-evil-a-996278.html [Accessed 13 Apr. 2019].

Wagner, J. (2017). China's Cybersecurity Law: What You Need to Know. *The Diplomat*. [online] Available at: https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/ [Accessed 3 Apr. 2019].

Waring, O. (2018). When was the internet invented?. *Metro News*. [online] Available at: https://metro.co.uk/2018/03/22/when-was-the-internet-invented-7408002/ [Accessed 5 Apr. 2019].

Watt, E. (2017). The right to privacy and the future of mass surveillance. *The International Journal of Human Rights*, 21(7), pp.773-799.

Weber, R. (2011). The Right to Be Forgotten: More Than a Pandora's Box?. *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law*, 2(2), pp.120-129.

Whiting, M. (2008). *The Great Firewall of China a Critical Analysis*. Master. Department of Electrical & Computer Engineering Graduate School of Engineering and Management Air Force Institute of Technology.

Womack, B. (2016). Asymmetric Parity: US-China Relations in a Multinodal World. *International Affairs*, 92(6), pp.1463-1480.

World Atlas. (2019). *30 Countries With The Youngest Populations In The World*, World Atlas. [online] Available at: https://www.worldatlas.com/articles/the-youngest-populations-in-the-world.html [Accessed 13 Apr. 2019].

World Bank. (2019). *Germany: Political Stability Index*, The Global Economy. [online] Available at: https://www.theglobaleconomy.com/Germany/wb_political_stability/ [Accessed 13 Apr. 2019].

World Bank Group (2019). *All Africa Digital Economy Moonshot*. [video] Available at: http://live.worldbank.org/africa-digital-economy-moonshot [Accessed 13 Apr. 2019].

Xu, B. and Albert, A. (2017). *Media Censorship in China*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/backgrounder/media-censorship-china [Accessed 3 Apr. 2019].

York, J. (2012). *UN Human Rights Council Resolution on Internet and Human Rights a Step in the Right Direction*. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2012/07/un-human-rights-council-resolution-internet-and-human-rights-step-right-direction [Accessed 2 Apr. 2019].

Zakharov v. Russia [2015]47143/06 (ECHR).

Zhang, Y. (2016). China and Liberal Hierarchies in Global International Society: Power and Negotiation for Normative Change, *International Affairs*, pp.795-816.

Zheng, W. (2019). China's corruption watchdog probes officials' personal details. *South China Morning Post.* [online] Available at: https://www.scmp.com/news/china/politics/article/2188227/chinas-corruption-watchdog-probes-officials-personal-details [Accessed 4 Apr. 2019].

Zimmer, J. (2018). Google Owns 63,605 Miles and 8.5% of Submarine Cables Worldwide. *BroadBandNow*. [online] Available at: https://broadbandnow.com/report/google-content-providers-submarine-cable-ownership/ [Accessed 13 Apr. 2019].

1249 U.N.T.S. 13; 19 I.L.M. 33 (1980).

999 U.N.T.S. 171; S. Exec. Doc. E, 95-2 (1978); S. Treaty Doc. 95-20; 6 I.L.M. 368 (1967)

993 U.N.T.S. 3; S. Exec. Doc. D, 95-2 (1978); S. Treaty Doc. No. 95-19; 6 I.L.M. 360 (1967)

全国人大常委会 [NPC Standing Committee]. (2000). 全国人民代表大会常务委员会关于维护互联网安全的决定 [The Standing Committee of the National People's Congress Internet Security Safeguard Resolution]. [online] Available at: http://www.npc.gov.cn/wxzl/gongbao/2001-03/05/content_5131101.htm [Accessed 9 Apr. 2019].