Unbordered Rights: The Geography of Cyberspace

https://www.e-ir.info/2019/12/05/unbordered-rights-the-geography-of-cyberspace/

P.J. BLOUNT, DEC 5 2019

This is an excerpt from *Reprogramming the World: Cyberspace and the Geography of Global Order*. Get your free copy here.

At the end of World War I, states gathered together to negotiate a structure for international governance intended to prevent conflicts like the one they had just experienced. The result of this negotiation was the Covenant of the League of Nations and an international organization that failed to live up to that promise.[1] While the League of Nations was primarily concerned with ensuring peace, there was an emerging theme in international governance endorsing the right of the self-determination of peoples. This was fueled in part by Point V of US President Woodrow Wilson's 14 Points, which called for an "adjustment of colonial claims" that weighed the "interests of the populations concerned" equally with the interests of colonial powers.[2] As the League of Nations was being formed, numerous activists courted Wilson and others in an attempt to move the role of human rights to the fore of the emerging international system.[3] Human rights, however, did not make the cut in the final covenant.

The call for self-determination would be ignored until 1945, when the world was again reeling from a world-scale conflict coupled with the horror of the Holocaust. The newly negotiated UN Charter established a new international organization, the United Nations, which would serve as the central international fora in which states could interact. The UN Charter also implemented a role for human rights in the system of international governance. While the prevention of conflict maintained priority,[4] Article 1(2) of the Charter says that states are to have "respect for the principle of equal rights and self-determination of peoples."[5] This was a sea change moment in the development of international law in that it made human rights part of the political geography of states. While the Charter has many gaps that keep the UN from directly enforcing those rights, it made human rights a valid inquiry for international governance. Article 1(2) was followed by a bevy of documents that supported this new international identity for the individual, such as the Universal Declaration of Human Rights, the Genocide Convention, the Covenant on Civil and Political Rights, and the Covenant on Economic and Social Rights. This expansion of political geography also included the slow development of international criminal law used to hold perpetrators of international crimes individually criminally liable for acts that violated international law.[6]

This post-WWII expansion was important, but it was soon evident that the primary place that the sovereign state holds in international governance made the state the primary entity through which rights flowed to the individual. Due to the jurisdictional "claw back provisions" in the Charter, the state was the primary provider and impediment to human rights.[7] This resulted in human rights documents, negotiated by states, defining human rights in general, non-specific terms giving states leeway in their interpretation of the content of those rights. So, for instance, while the US was actively endorsing UDHR, it was actively violating many of the rights of African Americans within its borders. This tendency of states to define rights to conform with their political geography can be seen very clearly in the universality of the acknowledgement of the freedom of speech compared to its very uneven application across the globe.[8] So, while the individual was given identity in the international legal geography, that identity is subservient to its national identity as the state remains the dominant source of rights.

Notwithstanding a few important regional human rights bodies, individuals have for the most part been unable to assert rights outside of the context of the political geography of the state in which they exist. The geography of Cyberspace is such, though, that it allows the individual to take part in a political geography that is not defined by

territorial borders. Cyberspace gives the individual identity in an alternate political geography and allows individuals to be the mediator of their own rights. This chapter will investigate how Cyberspace changes international political geography by examining how Cyberspace reallocates rights through the reallocation of identity. Legal structures give "primacy to entitlements" and "release the entitled person from moral precepts and other prescriptions in a carefully circumscribed manner."[9] Such legal structures are shown here to be diminishing in importance as the "spatio-temporal location" of individuals is no longer a controlling condition for gaining the "artificial status of bearers of individual rights."[10]

This chapter will first address how encryption technologies enable individuals to mediate their own speech and associational rights in the space of Cyberspace. This section will investigate how digitized networks diminish a state's ability to constrain individual action. Spatial changes though do not simply empower individuals against states, it often empowers states against individuals. The second section will examine the use of mass surveillance technologies by states as a way of mediating the rights of individuals in extraterritorially, which causes a fissure in the usual understanding of the political space of the state. The final section will use the phenomenon of hacktivism to show how this reallocation of rights rewrites international political space and gives it global complexity.

The Encrypted Self

Modern cryptography was born in Bletchley Park, England during WWII under the hand of Alan Turing.[11] The elite group that Turing led was tasked with cracking the encrypted messages sent through the German Enigma Machine. This complex electro-mechanical machine had over 150 trillion possible combinations with which to encrypt a message, and the German military reset the combination each day. This meant that though the Allies could intercept the encrypted messages each day, it was physically impossible to manually decrypt the messages by running all possible combinations. Turing was a mathematician whose work had already described a theoretical machine, which came to be known as a Turing machine, that was foundational to the development of the modern computer.[12] At Bletchley Park, Turing worked to build a physical machine that would quickly move through the possible combinations of the Enigma Machine in search of that day's combination. His work can be credited with changing the tide of the war for the Allies.

Cryptography today is a digital game. The Enigma Machine was based on the number of combinations for encrypting a text, and this number was a result of the physical settings that could be produced by its rotors and plug board. It was strong encryption until a machine was built that worked faster. An Enigma Machine would be no match for a smart phone, much less a military grade computer, due to the comparatively massive amounts of processing power on modern devices. This same processing power can be leveraged to create powerful encryption that is difficult for computers to break. To crack digital encryption users must either have a key or have a computer powerful enough to do the math in reverse. Many encryption techniques are premised on the inability of contemporary computers to do such math, and it is often stated that the fastest way to decrypt some digital messages is to wait until computer technology has advanced to the point that it can do the functions necessary to decrypt the message.

Encryption may seem esoteric to the individual user, but most people use some sort of encryption technology on the Internet daily. In fact, encryption technologies form the bedrock that commerce on the Internet relies on.[13] The ability to exchange data securely is paramount to the various trust systems implemented on the Internet. As an example, if an online business such as Amazon cannot ensure that a customer's credit card information will be secure then it is likely that that business will not have any customers at all. Encryption is foundational to trust on the Internet.

Encryption, though, is not just a commercial or military technology. Individuals have long used encryption to keep their messages or identities secret, and modern computing has opened up the ability of individual users to gain access to advanced encryption technologies. The example of PGP, found in Chapter 3, is indicative of this. PGP was classified by the US as a munition, and the US sought to stop the export of the technology to foreign countries. However, the nature of the Internet was such that the US was unable to stop the spread of the program across digital networks. The result being that individuals worldwide had access to military grade digital encryption. The effect of

this was to spread the freedom of expression embedded in the code (Chapter 4 above) rendering it "no local ordinance."[14]

Encryption technologies do two primary things. First, like the Enigma Machine they can encrypt the contents of a communication. Second, and unlike the Enigma they can hide the identity of the communicator by hiding the device's IP address thereby concealing the device's location.[15] As examples, PGP does the former, and the Tor web browser does the latter.[16] Encryption enables a spectrum of activities, but this section will examine two. The first of these activities is the much touted use of encryption by political dissidents in oppressive regimes.[17] The Internet itself offered the benefits of "cost, speed, and ease of use" to social movements and political dissidents.[18] Encryption enhances these benefits by allowing dissidents to organize and communicate in places where such rights are not guaranteed under the local law.[19]

As discussed in Chapter 4, Encryption technologies are closely tied to the anarcho-libertarian tradition in Cyberspace and specifically the Cypherpunks. This tradition frames cryptography as anti-authoritarian and pro-democratic. Encryption is a means with which to attack dominance and power of the state.[20] Specifically they attack the dominance of the state through a technical renegotiation of identity. Cypherpunks argue that power structures maintain control on power by controlling the information that is necessary to a deliberative democracy.[21] As an example, Julian Assange, the founder of WikiLeaks, wrote a file encryption program "designed for activists in repressive regimes" and named it "Rubber Hose."[22] The name is a reference to the physical violence that the state would need to inflict in order to gain access to the contents of the encrypted files. Political dissidents are obviously criminals within their own state, but encryption allows them to remove themselves from the political geography constructed within a given territory. Greenberg casts this freedom in terms of physical geography noting that cryptography can free the individual from "governments that don't hesitate to knock down doors and haul away political enemies."[23] The individual escapes being identified by escaping their own location and thus escaping the political identity imposed on them through state mechanisms.

The criminal nature of political expression in some states leads us to a second activity that is polarized from political dissent: cybercrime. While the uses of encryption by political dissidents is important, cybercrime activities make up a substantial amount of the encrypted bandwidth used.[24] This is crime of all sorts: extortion and fraud schemes, child pornography, identity theft, and terrorism.[25] Similar to dissidents, encryption allows criminals to step outside of their geographic strictures and escape the power of the state. However, only in the former instance can we say that the individual is expanding their rights to escape domestic political geography. Cybercriminals usually engage in activities that are criminal within both their and their victim's jurisdiction – meaning that they are only escaping their legal geography. Encryption protects both from the power of the state, but it allows dissidents to expand their political rights while it allows criminals to subvert their legal obligations. The extension of self beyond the state and its implications for political geography may best be seen in the role of encryption in terrorism.

After the Paris and San Bernardino attacks of 2015,[26] a public debate erupted over whether the government should have a back door to commercial encryption technologies in order to combat terrorism.[27] This debate was primed by revelations in the Snowden Leaks, which will be discussed in the context of state surveillance below. Here, though, the emphasis will be on how terrorist networks are able to extend themselves beyond their territorial confines to influence "world opinion."[28] Terrorists are seemingly both political actors and criminal actors. Indeed, it is uncontested that post 9/11 there are a number of terrorist organizations that now qualify as global political actors in an "'open source' anarchy."[29] Terrorist networks use the Internet for propaganda and recruiting as well as to communicate via encrypted networks. These technologies have allowed terrorist organizations to step beyond their territorial geography and subvert international geography through cybergeography.

In fact, it could be argued that terrorists have organized themselves around a decentralized logic similar to the Internet's, and Bergen and Hoffman argue that the terrorist networks have a very specific strategy of diversifying the threat that they pose.[30] This means that threat innovates along with technological innovation.[31] By decentralizing, these organizations are able to recruit operatives within the territorial geography of the target country and the digital connection to the recruit serves as a medium to wield power in that state. Cyberspace gives terrorists political identity and allows terrorist organizations to function as "quasi-states" that push subversive political ideology through

violence.[32] This is not to say that encryption causes terrorism nor to say that it changes the content of the political message of terrorism. Instead, the argument is that encryption changes the political geography that surrounds the terrorist. It facilitates the strategy of allowing potentially anyone to become a global political actor by taking up the terrorist cause.

Of course, terrorism is an extreme case and there are many documented legitimate uses of encryption technology to challenge political regimes.[33] The point here is not to choose a side in the debate over encryption. It is instead to show how it extends the political reach of the individual by "shift[ing] the balance of power from those with a monopoly on violence to those who comprehend mathematics and security design."[34] Encryption extends increased autonomy to the individual to assert rights denied within territorialized political geography.[35] As noted earlier, there is a current debate over whether the government should be able to require a back door into encryption programs. The U.S. government could certainly require this through legislation, but to some extent it would be a futile move.[36] This is because, as we see from PGP, anyone can code and release an encryption program, and as we see from the Liberator 3D-printed gun in Chapter 6, it is very easy to distribute code in contravention to U.S. law. The result is that states lose exclusive control over the communicative conditions of their own political geography.[37]

Encryption enables the individual to have a "choice" in the "medium through which citizens exercise their political autonomy," where before that choice was lacking.[38] Encryption allows the individual to gain access to a political geography and participate on terms that are different from those produced by compressed territorial, legal, and political geographies. If the Internet is indeed the "public space of the 21st century," then encryption technologies can be seen as marking the limits of its political geography.[39]

Taming the Masses

Adolph Eichmann, a former Nazi leader, was kidnapped by the State of Israel from his home in Argentina to whence he escaped at the end of World War II. He was then secreted out of the country and into the jurisdiction of Israel where he stood trial for his role in the Holocaust.[40] It was generally agreed that Israel violated the sovereignty of Argentina in this extraordinary event,[41] but the two later signed an agreement settling the matter. The violation occurred because in international law territorial jurisdiction reigns supreme, or in other words, international governance favors Argentina's border over Israel's interest in justice. This is why states use extradition treaties to govern the transfer of individuals within their territorial jurisdiction to other states that may have jurisdiction over a criminal act. In the usual scenario, Israel would be forced to concede to Argentina's dominance over its own territory and request that Argentina relinquish Eichmann.

Eichmann illustrates an important feature of the 1945 spatial settlement, which is that states are generally prohibited from mediating the rights of individuals extraterritorially. The right to self-determination is expressed internationally through "political independence" of the state.[42] States depended on territorial integrity to ensure that they maintained supreme authority within a given geography. In the wake of 9/11 however, states – or at least the US – have begun to conceive of themselves as having mutable borders that can be extended at will.[43] Cyberspace is an instrumental tool in their conception of themselves in this manner. States now routinely mediate the rights of individuals in other countries through digital surveillance and other cybertechnologies.[44]

Essentially, the same features that enable individuals to extend their rights through Cyberspace, also enable governments to use Cyberspace to surveil the individual. Despite the fact that encryption technologies are freely available, the bulk of Cyberspace communications happen on commercially encrypted networks. The networks collect vast quantities of data about individuals in a phenomenon known as "big data." As Lessig notes "[e]verything you do on the Net produces data" that "is in aggregate extremely valuable."[45] For instance, an ISP would have a record of IP addresses connected to by a user that would reveal interests, shopping habits, and professional and private associations. Beyond IP addresses bevies more information are held on computers, and as the US Supreme Court noted the "sum of an individual's private life can be reconstructed" from the data on a cell phone.[46] A government's ability to access this information reveals much more about an individual that traditional surveillance would.[47]

This type of data is collected for commercial purposes not for a single individual but for all users. As noted in Chapter 2, Cyberspace is a ubiquitous medium, meaning that if governments can tap into the commercial entities they can gather profiles of information on individuals worldwide.[48] It is this sort of activity that Edward Snowden revealed when he leaked a large trove of documents he collected as a National Security Agency (NSA) contractor.[49] These documents revealed a hidden legal and technical infrastructure implemented by the US and its allies in the wake of 9/11 to intercept communications. The documents gave an "unparalleled first-hand look at the details of how the surveillance system actually operates."[50] Central to the public discourse on the Snowden Documents were their legality under US law in respect to US citizens, which is an important and interesting legal debate. The inquiry here though will not be into the legality of the US actions, it will instead focus on how these actions reshaped international political geography. Specifically, it argues that the Snowden leaks reveal how the US reshaped the political geography of individuals it identified as "foreign."

PRISM serves as an excellent example of this US capability for mass global surveillance. First revealed in June of 2013, PRISM is secret a program that received direct feeds of data from a number of commercial companies such as Microsoft and Google that collectively "cover the vast majority of online email, search, video and communications networks."[51] This program required telecommunication companies to send all communications related to a "selector," such as an email address, to the NSA. PRISM constituted 91% of the "internet communications that the NSA acquired."[52] Similarly, the NSA engaged in "upstream collection" that relied on the "compelled assistance … of the providers that control the telecommunications backbone over which communications transit."[53] The Privacy and Civil Liberties Oversight Board (PCLOB) reports that "approximately 26.5 million Internet transactions a year" are collected through upstream collection.[54] Both of these push intelligence collection away from the locus an individual inhabits and into the Cyberspace an individual inhabits. Collected data is then retained in a database that can be queried by authorized NSA employees in order to find information on a target.[55]

The historical context of this surveillance system is important to understanding what it reveals about the changes in political geography. The overall surveillance program was authorized immediately after the 9/11 terrorist attacks via an executive order from George W. Bush.[56] The post 9/11 environment was such that "few foreign policy objectives have garnered as much support as the struggle against terrorism."[57] The Justice Department later determined that the President's Surveillance Program (PSP) needed a court approval, so it sought authorization from the classified Foreign Intelligence Surveillance Court (FISC).[58] The program itself went through several iterations as the government struggled to meet constitutional compliance behind closed doors, and it was eventually given statutory authority, albeit in vague terms, in §702 of the Foreign Intelligence Surveillance Act (FISA).[59] At the center of the adjustments was ensuring that the surveillance methods were properly within the bounds of the search and seizure restrictions in the US Constitution's 4th Amendment.[60] Under the FISA – the same legislation that created the FISC – the US government does not need a warrant to gather "foreign intelligence" from individuals that are not US persons and are reasonably believed to be "located outside of the United States."[61] In other words, the 4th amendment does not apply to non-US citizens outside the borders of the US. As a result, the NSA's surveillance was premised on the non-territorial-ness of the target. Snowden argues that the use of "foreign" is a "rhetorical shift [that] is a tacit acknowledgement by governments that they recognize they have crossed beyond the boundaries of justifiable activities."[62] Snowden also revealed that the foreign surveillance sometimes bled back through the borders of the US[63] "turn[ing] the U.S. into a foreign nation electromagnetically."[64] The uses revealed by Snowden show that "[t]echnology is agnostic of nationality," and the US only required a "reasonable belief" that the individual was outside of US territory to fulfill the "foreignness requirement."[65] Foreignness is important, because under the international governance system, the US surveillance of its own citizens is legal as a matter of sovereignty. It is foreign surveillance of individuals in territories outside of US jurisdiction that seems to be most problematic within international political geography.

It is not exceptional that a portion of the Bill of Rights does not extend outside the borders of the US as it is a guarantee of rights in the US, and the 4th Amendment is one of the rights that is guaranteed only to citizens and to noncitizens within US borders.[66] This presents a somewhat dichotomous position for the US. On one hand, former Secretary of State Clinton argued for the extension of First Amendment rights to Cyberspace, and on the other hand the government is secretly not extending Fourth Amendment rights.[67] The dichotomy exists because the freedom of speech that the government asserts should be extended is protected by the 4th Amendment impediment to

government interference in one's private life. So, the "universal" rights that Clinton offers are extended unevenly based on a political identity.

The hallmark of the activities exposed by Snowden is the replacement of individualized suspicion of criminality, critical to the U.S. Constitution 4th Amendment warrant requirement, with a permanently suspect political identity of "foreign."[68] As a result, FISC does not make determinations as to whether particular foreign individuals will be surveilled. Judicial review is instead limited to determining whether the procedures, which are adopted and authorized secretly, "are reasonably designed" to prevent surveillance of US persons or of individuals within the borders of the US.[69] What is exceptional is the US government's power to actively transform political space outside of its borders. It is able to do this because "much of the world's communications flow through the US."[70] This means that it is able to leverage its territory into the territory of other states.[71]

What Snowden revealed was not just a surveillance program, but a fundamental shift, from the state's point of view, in the extent to which a state can shape the political geography outside its own borders. It has long been understood that surveillance reshapes space, and that "[p]rivacy has a spatial dimension."[72] This is the core idea in Jeremy Bentham's Panopticon, and Cohen argues that modern rhizomatic surveillance systems dramatically change public and private space.[73] Surveillance "alters the experience of places in ways that do not depend entirely on whether anyone is actually watching."[74] Lessig terms it a "burden" that is imposed on the individual,[75] and Greenwald notes that a citizenry that is aware of always being watched quickly becomes a compliant and fearful one."[76] Transnational surveillance, then, exerts a new political geography on the individual by placing burdens on him or her that "alters the balance of powers and disabilities" within Cyberspace.[77] As a result, despite the fact that this is a government action, it is one that erodes the borders of international geography, because borders historically inhibited extraterritorial surveillance of this scale and scope. This loss of "political independence" is exhibited in Snowden's testimony before the European Parliament in which he states that "without getting out of my chair, I could have read the private communications of any member of this committee, as well as any ordinary citizen."[78] In fact, Snowden's leaks confirm that the US engaged in just this sort of surveillance,[79] which bears "implications for our assumptions of how international relations unfold."[80] The ability of the US to surveil the communications of foreign politicians indicates a change in their political geography, since "[s]paces exposed by surveillance function differently than spaces that are not so exposed."[81]

It should also be emphasized that the state's ability to transform political geography outside of its borders is based on its ceding of authority to corporate intermediaries as discussed in the previous chapter.[82] The ability of these networks to expand their reach extends the reach of the state to data, and corporations incentivize individuals to enroll in the "surveillant assemblage" using "benefits and pleasures, including price discounts, social status, and voyeuristic entertainment."[83] The state benefits from the corporate goal "to harness raw power of data."[84] Indeed, the reliance on "private intermediaries has equipped states with new forms of sometimes unaccountable and nontransparent power over information flows."[85] It should also be noted that these activities are not limited to the US, and Snowden revealed a "surveillant assemblage" that includes the UK,[86] France,[87] Australia,[88] and Germany.[89]

The state's ability to transform political geography should also be considered within the context of the ability to transform territorial geography discussed in Chapter 6. IoT allows states to control physical infrastructure in foreign domains as shown with Stuxnet. It also enables digitized violence as found in the US use of drones. The Predator drone was first developed as a surveillance tool for the Air Force, a purpose it served until the 2000s when it was fitted with munitions to carry out targeted killings in foreign countries.[90] The Predator is connected to a user in the US via a communications link built on Internet technology and relayed by a commercial telecommunications satellite.[91] If the drone is understood as a 'thing' on the IoT, then it is the embodiment of digitized violence. The political geography ascribed to the targets of drones by the international system is transformed dramatically through Cyberspace as the state mediates the right to fair trial and the right to life.

Networked Global Politics

What has been described in the previous two sections is a cross reaching of power, and they both describe changes

in the political geography at a localized perspective. A further inquiry should be made into what this does to the political geography of international space. This inquiry will reveal borders are shifted when other entities are networked in at a power level that can directly contest states. One of the implications of the previous two sections is that states have ceded authority in Internet governance, and that they rely on their ability to blend in with non-state actors online. This section will examine hackivists as evidence of a world-scale political geography that networks in non-state actors. The term itself invokes the idea of changing technology (i.e. hacking) for political change (i.e. activism). Hacktivists "use cryptography to effect political change," as a means of giving power "to the people."[92] This section will trace a narrative of hacktivism that will illustrate this transformation in global political geography.

In November of 2010, the website WikiLeaks began to publish leaked US State Department Diplomatic cables onto the Internet, in an incident that came to be known as Cablegate. WikiLeaks is a website founded by Julian Assange that is, in its own words, a "multi-national media organization and associated library" that has a perfect record in "resistance to all censorship attempts."[93] The website "specializes in the analysis and publication of large datasets of censored or otherwise restricted official materials involving war, spying and corruption" (again in its own words).[94] Assange has gone so far as to put this in diplomatic terms, stating "WikiLeaks is a giant library of the world's most persecuted documents. We give asylum to these documents, we analyze them, we promote them and we obtain more."[95] According to Domscheit-Berg, Assange focused on the US specifically "seeking out the biggest possible adversary."[96]

The Cablegate releases were the catalyst for WikiLeaks' and Assange's quick rise to global prominence. This led to Assange being characterized in the rhetoric of the state as a "terrorist" and "outrageous, reckless, and despicable."[97] The releases were unprecedented in nature and caused serious embarrassment for the US as well as security concerns globally, though WikiLeaks did attempt to minimize the exposure of human life. The 251,287 documents gave an unparalleled glimpse into the international relations of the United States and exposed to the public eye government processes that in general remain closed. They were leaked by a young army soldier named Chelsea Manning, who was later prosecuted in the United States for releasing the documents.[98] The US began to mount a case against Assange, and began to apply diplomatic pressure in order to find a way to get to Assange .[99] Then in August of 2010, a warrant for Assange's arrest was issued in Sweden on the basis of rape allegations.[100] The UK placed Assange under house arrest while it determined whether or not extradition was proper with the UK Supreme Court making an affirmative decision in May of 2012.[101] Assange then fled to the Ecuadorian Embassy in London where he was granted asylum. The UN Human Rights Council's Working Group on Arbitrary Detention released an opinion in February of 2016 that ruled the detention "arbitrary."[102]

As of this writing, Assange has been expelled from the Ecuadorian Embassy as the result of an internal change in leadership in Ecuador. The leadership accused Assange of using his refuge in the embassy to meddle in internal affairs of other states and revoked his asylum status for "the trangression of international treaties."[103] He is serving a short sentence for failing to surrender to court and is facing possible extradition to either Sweden or the United States.[104]

Diplomatic pressure was not the only pressure that the United States mounted. It also attempted to get the corporations within their borders to put pressure on Assange by ceasing to allow their services to be used to support WikiLeaks. Several major companies, such as Amazon, PayPal, and Mastercard, succumbed to this pressure displaying the corporate authority over the Internet. There was no public legal action taken against these corporations, and the government denied such actions.[105] This cued the entrance of the hacktivist group Anonymous.

Anonymous is a hacker collective that is geographically distributed and whose identities are as secret as code can keep them. In the group's own words, "Anonymous is a loose collection of individual people around the world. […] Anonymous is notoriously associated with hacking and hacking operations, but over the years has evolved into a majority protest/civil activist movement."[106] Significantly, Anonymous has no leader and anyone can join.[107] The "nihilistic" group has been associated with a number of high profile hacks that generally have some variety of social justice motive.[108] They have declared operations against groups like the CIA,[109] Westboro Baptist Church,[110] Mexican drug cartels,[111] the Church of Scientology,[112] the Islamic State,[113] and even Kanye West.[114] As

Cablegate unfolded, Anonymous employed DDoS attacks against the corporations that they claimed were censoring WikiLeaks.[115] In addition to corporations, Anonymous also attacked governments such as Zimbabwe and Tunisia that were censoring the documents.[116] Anonymous' actions were undergirded by a philosophy that "knowledge is free," a phrase that resonates with the political geography described in Chapter 4.[117]

A third, but unlikely to be final, act in this leaking drama are the leaks of Edward Snowden. Snowden, it must be assumed, was to some extent inspired by this global drama over government transparency, and like Manning he released a trove of government documents to the press. Several days after the first leak, the same journalists that broke the leaks also broke the identity of the leaker by publishing an interview with Snowden. In this interview he stated that he hoped his leaks "will trigger [debate] among citizens around the globe about what kind of world we want to live in."[118] Snowden's interview was from a hotel room in Hong Kong. While the United States scrambled to put in motion the legal process for getting to Snowden, he was quietly shuttled onto a plane that took him to the international terminal of the Moscow airport before the US could cancel his passport.[119] He lived in the international zone of the airport, outside the legal and political borders of any state, for more than a month.[120] During this time, it was rumored that he was going to be given asylum in Bolivia and that he was aboard a diplomatic flight transporting the president of Bolivia.[121] The United States applied a great deal of diplomatic pressure, and as a result Portugal, France, Italy, and Spain denied access of this plane to their airspace.[122] The plane was eventually rerouted to Vienna, where it was searched and the Austrian Foreign Minister confirmed that Snowden was not aboard.[123] Snowden was granted temporary asylum for one year in Russia, which has since been renewed.[124] He was represented by WikiLeaks attorneys in the negotiations with the Russian government. In fact, WikiLeaks contributed a great deal of resources to ensure that Snowden did not fall back within the jurisdiction of the US.[125] From a legal and political enclave of Ecuador in the territory of the UK, Assange was able to wield global political power to subvert the international power of the US.

This narrative is not intended to lionize Assange, Manning, Snowden, or the members of Anonymous. The facts surrounding each require particularized ethical reflection. Instead, this narrative is used to expose a new form of global networked power that is pushing up against the territorially ordered international political system. Three observations of this narrative illustrate aspects of the new political geography formed as cybergeography comes into proximity with international geography. The first observation is the role of encryption technologies within this narrative. Greenberg notes that "the technology that enables the spillers of secrets has been accelerating with the dawn of the computer" and that the Internet caused a "Cambrian explosion" of tools to empower the individual.[126] Encryption technologies are foundational to the WikiLeaks platform, critical to hiding the identity of Anonymous activists, and were the tool used by Snowden to transfer his leaks to the press. In the Cablegate episode, Manning may never have been caught except that she revealed herself to a fellow hacker that turned her in,[127] and Snowden revealed his own identity. Encryption allows the leaker to transform politics within the global space by transforming their own identity, a function enabled within the communicative conditions of Cyberspace.

The second observation is the role of borders within this narrative. Borders are freely deconstructed and reconstructed at will by states creating ripples in the construction of the International system. Borders themselves are recoded to hold both traditional content as well as new fluid geographies. For instance, at numerous points we see borders serving traditional functions. Assange was subject to the international process of extradition, but he claimed asylum within the diplomatic borders of Ecuador. Assange was thus protected through established international governance mechanisms, so long as Ecuador wanted to protect him (they eventually withdrew their protection and handed him over to the British police in April 2019). Similarly, Hong Kong allowed Snowden to leave for Moscow claiming that "documents filed by the US did not fully comply with legal requirements."[128] In addition, we see a display of states flexing their territorial authority in denying their airspace to a plane that potentially carried Snowden. At the same time, borders are reinscribed in different ways that reveal their imaginariness. Assange's exile reveals the legal fiction of territory, which gets highlighted when the same type of diplomatic territory is so easily violated in the case of the Austrian search of Bolivia's diplomatic flight. Similarly, Snowden's existence in the nowhere of an airport displays the fictions in territory. While Assange and Snowden are relying on international geography for protection, they at the same time reveal the imaginaries that surround the individual and hack together new spatial realities for themselves. The role of territorial, legal, and political borders across this narrative arc is indicative of geographic duality that Cyberspace enables. Individuals can exploit the geography of Cyberspace and

remain unconfined in their ability to reach out and affect processes outside the territory in which they exist, so long as they have access to the network.[129]

Finally, the articulation of power within this narrative shows new patterns that reflect a new shape of world-scale political geography. Within this narrative, states are engaged in international politics in order to resolve the issues caused by transnational actors. This power though is often inflected through corporate power structures as can be seen in the Cablegate episode and in the programs such as PRISM that Snowden unveiled. The state's power is now part of a, pardon the pun, diversified portfolio. Power is inflected back at the state through individuals that assert themselves as adversaries on equal footing with the state and become "global political player[s]."[130] Though each has their own interesting spatial standing, each is able to leverage themselves in such a way that they challenge the political space of the state from outside its political geography. Interestingly, Assange is reported to have "adopted the language of the power mongers he claimed to be combatting," which shows how he was positioning WikiLeaks as an adversary of equal standing to the state.[131] These acts are beyond civil disobedience, which is "a public nonviolent conscientious yet political act contrary to law" with the goal of changing the status quo.[132] These technologies remove the "price" of legal consequences through the use of encryption technologies.[133] Instead, as an anonymous author stated in 2600: The Hacker Quarterly "[h]ackers are no longer anonymous independent operators or groups: We are now a known and calculated factor" in power structures.[134] While this is easily read as boastful, it is hard to ignore the attention that cybersecurity is receiving at the top levels of governments and corporations, among others. Indeed, governments, corporations, and hacktivists must be examined together to reveal "the baroque workings of power" in global politics.[135] These "baroque workings" are highlighted not just by attacks on corporations and states by groups like Anonymous, but also in cases of attacks on corporations by states such as North Korea and Sony.

Geographic duality is maybe the best way to describe the situation in which Cyberspace exists within international space and international space exists within Cyberspace creating a unified world-scale geography in which neither is dominant. While this rings like an attempt at empty metaphysics, we find it reflected in the architecture of Cyberspace. The physical layers of Cyberspace and the users in Cyberspace exist within the borders of the state and therefore within the borders of the international. But, the logical layer of the Internet is made of algorithms, and these are ideas operationalized through machinery.[136] This means that the logical layer is a manifestation of human consciousness. Or in simpler terms, the logical layer is ideas, and ideas are notoriously hard to control.

—

This chapter has shown how world-scale political geography is shifting as new actors become mediums for power within the system and serves as a capstone for Part II, which highlights encounters where cybergeographies come into proximity of international geographies. The various cases and incidents addressed in this section are meant to reveal complexity within the system by layering the spatial, legal, and political geography of Cyberspace onto the spatial, legal, and political geography of international space. This layering shows the junctures and disjunctures of these two intermingled geographies. The following final chapter will pull these various threads together and posit that Cyberspace short circuits international governance processes and allows actors to reprogram the world.

Notes

[1] *Covenant of the League of Nations* (1919).

[2] Woodrow Wilson, "Fourteen Points" (1918).

[3] Manela, *The Wilsonian Moment* (2007) 59–60.

[4] UN Charter (1945) Art 1(1)

[5] *Id.* at Art. 1(2)

[6] *See generally* Pompe, *Aggressive War* (1953) and Cassese, *International Criminal Law* (2003).

[7] Borgwardt, *A New Deal for the World* (2005) 191–192.

[8] *For example compare* US Constitution, Amend. 1 *with* Korea (Democratic People's Republic of)'s Constitution of 1972 with Amendments through 1998, Art. 67.

[9] Habermas, *The Postnational Constellation* (2001) 114.

[10] *Id.*

[11] On Turing *see generally* Brate, *Technomanifestos* (2002) 53–84. For fictionalized accounts *see The Imitation Game* (Black Bear Pictures/Bristol Automotive 2014) and Stephenson, *Cryptonomicon* (1999).

[12] *See* Berlinski, *The Advent of the Algorithm* (2000) 187.

[13] DeNardis, *The Global War for Internet Governance* (2014) 93.

[14] Lessig, *Code 2.0* (2006) 236.

[15] Greenberg, *This Machine Kills Secrets* (2012) 65 and Davis, "The Internet As a Source of Political Change in Egypt and Saudi Arabia" (2008) 35.

[16] Tor is an "onion routing" network that conceals the IP addresses of individuals using the software. *See generally* Greenberg, *This Machine Kills Secrets* (2012) 135–168.

[17] *See generally* Fielder, "The Internet and Dissent in Authoritarian States" (2013) 161–91 and Castells, "Communication, Power and Counter-Power in the Network Society" (2007).

[18] Fielder, "The Internet and Dissent in Authoritarian States" (2013) 162.

[19] *See, for example*, Organization for Security and Co-operation in Europe, "Freedom of Expression on the Internet" (2011).

[20] Greenberg, *This Machine Kills Secrets* (2012) 148; Domscheit-Berg, *Inside WikiLeaks* (2011) 189; and Assange, *Cypherpunks* (2012) 1.

[21] *Id.*

[22] Greenberg, *This Machine Kills Secrets* (2012) 126–27.

[23] Greenberg, *This Machine Kills Secrets* (2012) 136, 3.

[24] *For example* Moore & Rid, "Cryptopolitik and the Darknet" (2016) 21–25.

[25] *See generally* National Center for Justice and the Rule of Law, *Combating Cyber Crime* (2007).

[26] *See generally* "Paris Attacks: What Happened on the Night" (2015) and "Everything We Know about the San Bernardino Terror Attack Investigation so Far" (2015).

[27] *For example* Gallagher, "NSA's Director Says Paris Attacks 'would Not Have Happened' without Crypto" (2016); O'Neil, "Edward Snowden and Spread of Encryption Blamed after Paris Terror Attacks" (2015); and Knight, "Controlling Encryption Will Not Stop Terrorists" (2016).

[28] Lewis, *The Crisis of Islam* (2004) 147.

[29] Princeton Project on National Security, "Report of the Working Group on State Security and Transnational Threats" (2008) 10–11.

[30] Bergen & Hoffman, *Assessing the Terrorist Threat* (2010).

[31] Stewart & Mueller, "Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening" (2011) 2.

[32] Clapham, "Degrees of Statehood" (1998) 150.

[33] *See also* Clinton, "Internet Rights and Wrongs" (2011) and Dunn, "Unplugging a Nation" (2011) 15.

[34] Greenberg, *This Machine Kills Secrets* (2012) 154

[35] Habermas, *The Postnational Constellation* (2001) 118.

[36] *See* Berkman Center, *Don't Panic Making Progress on the "Going Dark" Debate* (2016).

[37] Cohen, "Privacy, Visibility, Transparency, and Exposure" (2008) 200.

[38] Habermas, *The Postnational Constellation* (2001) 17.

[39] Clinton, "Internet Rights and Wrongs" (2011).

[40] *See generally* Arendt, *Eichmann in Jerusalem* (1963).

[41] United Nations Security Council, S/RES/138 Question relating to the case of Adolf Eichmann (1960).

[42] UN Charter (1945) Art. 1(2), 2(4).

[43] *For example* Bowman, "Thinking Outside the Border" (2007) 189–251.

[44] Lessig, *Code 2.0* (2006) 209.

[45] *Id.* at 216.

[46] Riley v. California (2014) 18.

[47] *See* US v. Jones, 132 S. Ct. 945 (Sotomayor concurring) (2012).

[48] Lessig, *Free Culture* (2004) 278.

[49] Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily" (2013).

[50] Greenwald, *No Place to Hide* (2014) 2.

[51] Specific companies noted are Microsoft, Google, Facebook, Pal Talk, YouTube, Skype, AOL, and Apple. Greenwald & MacAskill, "NSA PRISM Program Taps in to User Data of Apple, Google and Others" (2013); National Security Agency, "PRISM/US-984XN Overview of the SIGAD Used Most in NSA Reporting Overview" (2013); Gellman & Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program" (2013); Greenwald *et al*, "Microsoft Handed the NSA Access to Encrypted Messages" (2013); and

MacAskill, "NSA Paid Millions to Cover Prism Compliance Costs for Tech Companies" (2013).

[52] Privacy and Civil Liberties Oversight Board (PCLOB), "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (2014) 33–34. *See also* Greenwald & MacAskill, "NSA PRISM Program Taps in to User Data of Apple, Google and Others" (2013).

[53] PCLOB, "Report on the Surveillance Program" (2014) 35; National Security Agency, "(TS//SI/NF) FAA Certification Renewals With Caveats" (2011).

[54] PCLOB, "Report on the Surveillance Program" (2014) 37, 39.

[55] Greenwald & MacAskill, "Boundless Informant" (2014) and National Security Agency, "BOUNDLESSINFORMANT – Frequently Asked Questions" (2012). *See also* Greenwald, "XKEYSCORE" (2013).

[56] Executive Order 12333: United States Intelligence Activities (2001). *See* National Security Agency Office of Inspector General, "Working Draft Report from March 24, 2009 on Stellar Wind (PSP)" 1–3; PCLOB, "Report on the Surveillance Program" (2014) 16–18; and Gallington, "Perspectives on Collection, Retention, and Dissemination of Intelligence" (2014) 2.

[57] Nincic & Ramos, "Torture in the Public Mind" (2011) 231–49, 233. *See also* Stewart & Mueller, "Cost-Benefit Analysis of Advanced Imaging Technology" (2011); Gallington, "Perspectives on Collection, Retention, and Dissemination of Intelligence" (2014) 10; Wittes, "The Intelligence Legitimacy Paradox" (2014); Princeton Project on National Security, "Report of the Working Group" (2008); and Greenwald, *No Place to Hide* (2014) 5.

[58] NSA OIG, "Working Draft Report from March 24, 2009" 36–37; PCLOB, "Report on the Surveillance Program" (2014) 16–18, 42; and United States Department of Justice, "Exhibit A: Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to Be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" (2009). *See also* Gallington, "Perspectives on Collection, Retention, and Dissemination of Intelligence" (2014) 5–6 and PCLOB, "Report on the Surveillance Program" (2014) 26–27.

[59] Foreign Intelligence Surveillance Act of 1978, 95 Pub.L. 511; Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 110 Pub. L. 261; and PCLOB, "Report on the Surveillance Program" (2014) 19, 81–84. *See also* Greenwald & MacAskill, "NSA PRISM Program Taps in to User Data of Apple, Google and Others" (2013).

[60] PCLOB, "Report on the Surveillance Program" (2014) 89–90.

[61] PCLOB "Report on the Surveillance Program" (2014) 20–21. Foreign intelligence is "information that relates to the ability of the United States to protect against actual or potential attack by a foreign power; sabotage, international terrorism, or the proliferation of weapons of mass destruction by a foreign power; or clandestine activities by a foreign power." *Id.* at 22. *See also* Gallington, "Perspectives on Collection, Retention, and Dissemination of Intelligence" (2014) 5.

[62] Snowden, "Testimony before the Parliament of the European Union" (2014).

[63] Gellman & Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program" (2013); Greenwald & Ackerman, "How the NSA Is Still Harvesting Your Online Data" (2013); Greenwald & Ball, "The Top Secret Rules That Allow NSA to Use US Data without a Warrant" (2014); Greenwald & Ackerman, "NSA Collected Americans' Email Records in Bulk for Two Years under Obama" (2013); Ball & Ackerman, "NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls" (2013); Gellman, "NSA Broke Privacy Rules Thousands of Times per Year, Audit Finds" (2013); and National Security Agency, "(U//FOUO) NSAW SID Intelligence Oversight (IO) Quarterly Report – First Quarter Calendar Year 2012 (1 January – 31 March 2012 – EXECUTIVE SUMMARY" (2012).

[64] Greenberg, *This Machine Kills Secrets* (2012) 223. *See also* Wittes, "The Intelligence Legitimacy Paradox" (2014). *See also* PCLOB, "Report on the Surveillance Program" (2014) 23, 42, 85.

[65] Snowden, "Testimony before the Parliament of the European Union" (2014) 5 and PCLOB, "Report on the Surveillance Program" (2014) 21, 43–52.

[66] *Id. at* 86–7, 100–102.

[67] Clinton, "Internet Rights and Wrongs" (2011) *See also* US DoD, "Department of Defense Strategy for Operating in Cyberspace" (2011).

[68] PCLOB, "Report on the Surveillance Program" (2014) 18.

[69] *For example see* United States Department of Justice, "Memorandum for the Attorney General" (2007); United States Department of Justice, "Exhibit A" (2009); and PCLOB, "Report on the Surveillance Program" (2014) 26–27.

[70] NSA, "PRISM/US-984XN" (2013).

[71] Lam, "EXCLUSIVE: US Hacked Pacnet, Asia Pacific Fibre-Optic Network Operator, in 2009" (2013); Lam & Chen, "EXCLUSIVE: US Spies on Chinese Mobile Phone Companies, Steals SMS Data" (2013); Poitras, Rosenbach, & Stark, "NSA Spies on 500 Million German Data Connections" (2013).

[72] Cohen, "Privacy, Visibility, Transparency, and Exposure" (2008) 181. *See also* Kirby, "Minding the Gap" (2013) 10–11.

[73] Cohen, "Privacy, Visibility, Transparency, and Exposure" (2008) 184–186

[74] *Id.* at 192

[75] Lessig, *Code 2.0* (2006) 218.

[76] Greenwald, *No Place to Hide* (2014) 3.

[77] Cohen, "Privacy, Visibility, Transparency, and Exposure" (2008) 193.

[78] Snowden, "Testimony before the Parliament of the European Union" (2014) 2.

[79] MacAskill *et al*., "GCHQ Intercepted Foreign Politicians' Communications at G20 Summits" (2013); Poitras *et al*., "NSA Spied on European Union Offices" (2013); MacAskill & Borger, "New NSA Leaks Show How US Is Bugging Its European Allies" (2013); "NSA Hacked UN Videocalls as Part of Surveillance Program, Claims Report" (2013).

[80] Dittmer, "Everyday Diplomacy" (2015) 604–05.

[81] Cohen, "Privacy, Visibility, Transparency, and Exposure" (2008) 194. *See also* Dittmer, "Everyday Diplomacy" (2015) 604–19.

[82] *See* Rushe, "Skype's Secret Project Chess Reportedly Helped NSA Access Customers' Data" (2013); Risen & Wingfield, "Web's Reach Binds N.S.A. and Silicon Valley Leaders" (2013); Greenwald *et al*., "Microsoft Handed the NSA Access to Encrypted Messages" (2013); Timberg & Nakashima, "Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance" (2013); Ball, Harding, & Garside, "BT and Vodafone among Telecoms Companies Passing Details to GCHQ" (2013); and Greenet Ltd. *et al* v. GCHQ – Statement of Grounds (2014).

[83] Cohen, "Privacy, Visibility, Transparency, and Exposure" (2008) 187.

[84] *Id.* at 186.

[85] DeNardis, *The Global War for Internet Governance* (2014) 15.

[86] Hopkins & Borger, "Exclusive: NSA Pays £100m in Secret Funding for GCHQ" (2013); Hopkins, Borger, & Harding, "GCHQ: Inside the Top Secret World of Britain's Biggest Spy Agency" (2013); and Dittmer, "Everyday Diplomacy" (2015) 604–19.

[87] Chrisafis, "France 'Runs Vast Electronic Spying Operation Using NSA-Style Methods'" (2013).

[88] Dorling, "Snowden Reveals Australia's Links to US Spy Web" (2013).

[89] "German Intelligence Agencies Used NSA Spying Program" (2013).

[90] Michel, "A History of Violence" (2015).

[91] *Id.*

[92] Greenberg, *This Machine Kills Secrets* (2012) 131, 168.

[93] WikiLeaks, "What is WikiLeaks" (2015).

[94] *Id.*

[95] *Id.*

[96] Domscheit-Berg, *Inside WikiLeaks* (2011) 189, 160.

[97] Greenberg, *This Machine Kills Secrets* (2012) 177

[98] Tate, "Bradley Manning Sentenced to 35 Years in WikiLeaks Case" (2013).

[99] Greenwald & Gallagher, "Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters" (2014).

[100] Domscheit-Berg, *Inside WikiLeaks* (2011) 203–215.

[101] Bowcott, "Julian Assange Loses Appeal against Extradition" (2012).

[102] UN Human Rights Council's Working Group on Arbitrary Detention, Opinion No. 54/2015 concerning Julian Assange (2015) Para 99.

[103] Dillet & Lomas, "Julian Assange arrested in London after Ecuador withdraws asylum" (2019).

[104] *Id.*

[105] Greenwald & Gallagher, "Snowden Documents Reveal Covert Surveillance" (2014) and Clinton, "Internet Rights and Wrongs" (2011)

[106] AnonHQ, "The Most Frequently Asked Questions People Have About Anonymous" (2016).

[107] *Id.*

[108] Greenberg, *This Machine Kills Secrets* (2012) 185.

[109] Albanesius, "Anonymous Takes Down CIA Web Site" (2012).

[110] Popkin, "Anonymous 'Brandjacks' Westboro Baptist Church on Facebook" (2013).

[111] Associated Press, "'Anonymous' Hackers Threaten Drug Cartel" (2011).

[112] *See* Daniel Domscheit-Berg, *Inside WikiLeaks* (2011) 35.

[113] Brooking, "Anonymous vs. the Islamic State" (2015).

[114] "Kanye West Targeted by 'Anonymous' in Searing Video" (2015).

[115] Mackey, "'Operation Payback' Attacks Target MasterCard and PayPal Sites to Avenge WikiLeaks" (2010).

[116] "Anonymous Activists Target Tunisian Government Sites" (2014).

[117] Greenberg, *This Machine Kills Secrets* (2012) 185.

[118] Greenwald, MacAskill, & Poitras, "Edward Snowden" (2013) and *Citizen Four* (HBO Films 2014).

[119] Branigan & Elder, "Edward Snowden Leaves Hong Kong for Moscow" (2013).

[120] Luhn, "Edward Snowden Leaves Moscow Airport after Russia Grants Asylum" (2013).

[121] Roberts, "Bolivian President's Jet Rerouted amid Suspicions Edward Snowden on Board" (2013) and Lally & Forero, "Bolivian President's Plane Forced to Land in Austria in Hunt for Snowden" (2013).

[122] *Id.*

[123] *Id.*

[124] Branigan & Elder, "Edward Snowden Leaves Hong Kong for Moscow" (2013).

[125] Kelley, "Edward Snowden's Relationship With WikiLeaks Should Concern Everyone" (2014) and Sledge, "Edward Snowden Gambles On Alliance With WikiLeaks" (2013).

[126] Greenberg, *This Machine Kills Secrets* (2012) 6.

[127] *Id.* at 31–32.

[128] Branigan & Elder, "Edward Snowden Leaves Hong Kong for Moscow" (2013).

[129] Henley, "Ecuador cuts off Julian Assange's internet access at London embassy" (2018).

[130] Domscheit-Berg, *Inside WikiLeaks* (2011) 270.

[131] *Id.* at 200–201.

[132] Rawls, *A Theory of Justice* (1971) 364.

[133] *Id.* at 367.

[134] Prisoner #6, “The 21st Century Hacker Manifesto” (2014–2015) 50.

[135] Dittmer “Everyday Diplomacy” (2015) 616.

[136] Berlinski, *The Advent of the Algorithm* (2000) xii.

About the author:

P.J. Blount is a Post-doctoral researcher at the University of Luxembourg in the Faculty of Law, Economics, and Finance. His research focuses on space and communications law. Previously he served as a Research Counsel and Instructor at the University of Mississippi School of Law; was a Visiting Scholar at the Beijing Institute of Technology, School of Law; and an Adjunct Professor at Montclair State University, Department of Political Science and Law.