SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015 ARTICLE 2, PAGE 39

TRAGEDY OF THE COMMONS: SNOWDEN'S REFORMATION AND THE BALKANIZATION OF THE INTERNET

MATTHEW FUNK

"Thou hast loosed an Act upon the world, and as a stone thrown into a pool so spread the consequences thou canst not tell how far." –Rudyard Kipling[1]

INTRODUCTION

In 1517, Martin Luther put into motion events that would uproot the hegemony of the Catholic Church in Western religion.[2] His *Ninety-Five Theses* would be the basis for an enormous upheaval of the sacred status quo, and challenge centuries of religious ordering. His "protest" of the practices of the Catholic Church would be disseminated with the power of the printing press, the pinnacle of information technology at the time, and lead to a great fork in the history of Christianity. Protestantism, with unique movements springing up throughout Europe, would ultimately separate from the oversight of the Catholic Church and create a new religious paradigm.

No different in principle, but perhaps in scale, has been the upheaval caused by the confessions of former National Security Agency contractor Edward Snowden. His "leak of [National Security] [A]gency documents has set off a . . . debate over the proper limits of

[1] RUDYARD KIPLING, KIM: AUTHORITATIVE TEXT, BACKGROUNDS, CRITICISM 176 (Zohreh T. Sullivan ed., 2002).

[2] *See generally*, Geoffrey Parker, *Success and Failure during the First Century of the Reformation*, 136 PAST & PRESENT 43, 82 (1992), *available at http*://past.oxfordjournals.org/content/136/1/43.full.pdf+html (describing the early developments of the Protestant Reformation).

government surveillance."[3] These leaks have "opened an unprecedented window on the details of surveillance by the NSA, including its compilation of logs of virtually all telephone companies in the United States and its collection of e-mails of foreigners from the major American Internet companies."[4] This, in turn, has rippled into raucous calls for a new Reformation—one of Internet, not religious, sovereignty and sensibilities. Such calls implicate the principles undergirding the purposes, governance, and even geography of the Internet. And while the calls may not lead to a catastrophic schism on the scale of Christianity's division in the 16th century, they are certainly loud enough not only to question policy choices regarding the defining information technology of the new millennium thus far, but also to challenge the traditional dynamics of sovereignty-retention in the face of a global online commons.

States, and their behavior in the modern world, are geopolitically defined in territorial terms. This territorial approach was "accepted as the primary political strategy after the anarchic implications of a negative-sum game . . . became widely appreciated."[5] At the state level, "the content of a territory can be manipulated and its character designed," and this territory can be used "as the instrument for securing a particular outcome."[6] The modern territorial state, forged by trial-and-error over the past two centuries, seeks to maximize if not monopolize control and power over achieving these particular outcomes. It has thus emerged as a "power container," predicated on the "domination of political practice in the world by territoriality" as a

---

[3] Scott Shane, *Ex-Contractor Is Charged in Leaks on N.S.A. Surveillance*, N. Y. TIMES (June 21, 2013), http://www.nytimes.com/2013/06/22/us/snowden-espionage-act.html?adxnnl=1&adxnnlx= 1385312525-3kfeFqdcTH4zPWJ2P5KjTg.

[4] *Id.*

[5] Peter Taylor, *The state as container: territoriality in the modern world-system*, 18 PROGRESS IN HUMAN GEOGRAPHY, 151, 161 (1994), *available at* http://phg.sagepub.com/content/18/2/151.full.pdf+html.

[6] *Id.* at 151.

"consequence of [the] territorial link between sovereign territory and national homeland."[7] States as power containers can be "filled" or "leak," by the successes or failures, respectively, of their four basic tasks: waging war, managing the economy, giving national identity, and providing social services.[8] These successes or failures amount to state "containment of power, wealth, culture, and society"[9] respectively.

The modern state's relationship with the Internet fits neatly within territoriality theory. Despite its origins in the security apparatus of the United States, and its initial purpose as a tool for war-making power accumulation, the Internet has come to represent, in some respects, a leak in the power container of the modern state. This is, for the most part, due to its nature as a globally accessible information technology and its continued development away from traditional norms of territoriality and the physical geopolitical borders observed by states. For many states and individuals alike, this globalization pushes away from the constructed and imagined communities that exist at the state level.[10]

The Internet will continue, consequently, to poke holes in the modern state as a power container unless respective sovereign authorities are able to plug them and recapture the true filling potential of the Internet by maximizing their own control locally while minimizing influence from beyond their borders. The Internet today has no fewer than 2.4 billion users (roughly 34% of the world's population),[11] and is a tool that has truly interpenetrated the border

---

[7] *Id.*

[8] *See id.* at 152 (citing the four basic tasks of the modern nation-state).

[9] *Id.*

[10] *See* Taylor, *supra* note 5, at 155 (discussing nations, in Benedict Anderson's famous phrase, as "imagined communities").

[11] *See Internet Usage Statistics*, INTERNET WORLD STATS, http://internetworldstats.com/stats.htm (last updated Dec. 31, 2013) (providing global Internet usage statistics).

between the real and the virtual."[12] For some, this "conflict between states as containers and the global ecosystem is interpreted as leading to a future end of the state," while for others, "territoriality is too good a strategy to dispatch to history."[13]

The viability of either theory and either outcome is not yet clear, but the importance of state responses to the Snowden leaks certainly is. States are realizing diminished levels of sovereignty and control over domestic online activity via third-party surveillance actors – holes in their power containers. In addition to the traditional practice of censorship, there is now another half of the equation when it comes to maintaining territoriality online: containment of local resources and data to the preclusion of prying eyes. Whether an ultimate balkanization of online interests is to befall the Internet as a result of these containment efforts will be determined by the subsequent choices states have, and will continue to make in response to such realizations of susceptibility.

I. HISTORICAL DEVELOPMENT OF THE INTERNET

Before the implications of the Snowden leaks can be assessed, the guiding principles adopted and policy choices made by the U.S. Department of Defense in the early development of the Internet must be understood. At the most basic level, the Internet is a "packet switched communications facility in which a number of distinguishable networks are connected together using packet communications processors called gateways which implement a store and forward packet forwarding algorithm."[14] ARPANET, the first iteration of today's Internet, was designed

---

[12] Barney Warf, *Geographies of Global Internet Censorship*, 76 GEOJOURNAL, 1, 1 (2011) *available at* http://link.springer.com/article/10.1007%2Fs10708-010-9393-3#page-1.

[13] Taylor, *supra* note 5, at 152.

[14] David Clark, *The Design Philosophy of the DARPA Internet Protocols*, ACM SIGCOMM, 2 (1988), http://ccr.sigcomm.org/archive/1995/jan95/ccr-9501-clark.pdf.

"to come to grips with the problem of integrating a number of separately administered entities into a common utility"[15] and develop "an effective technique for multiplexed utilization of existing interconnected networks."[16]

Notwithstanding the fundamental goal of connecting preexisting networks, early policy decisions within the Department of Defense prioritized some features over others.[17] In order of importance:

> 1. Internet communications must continue despite loss of networks or gateways; 2. The Internet must support multiple types of communications service; 3. The Internet architecture must accommodate a variety of networks; 4. The Internet architecture must permit distributed management of its resources; 5. The Internet architecture must be cost effective; 6. The Internet architecture must permit host attachment with a low level of effort; 7. The resources used in the Internet architecture must be accountable.[18]

A commercial network would certainly reorder such goals, but it is always worth remembering ARPANET "was designed to operate in a military context."[19]

In terms of the Internet developing as a commons that was to depart from traditional notions of territoriality, goals two, three, four, and five are the most pertinent. These represent the accommodation of a variety of communications services and networks, distribution of resource management, and cost-effectiveness. Such features, though originally military-minded priorities, created the basis for a thriving, global Internet in a setting where approaches, standards, and allocable resources would come to vary widely.

---

[15] *Id.*

[16] *Id.* at 1.

[17] *Id.* at 2.

[18] *Id.*

[19] Clark, *supra* note 13, at 2

Because ARPANET was developed along guiding principles that fostered a global-commons model, state power containers leaked politically, economically, and socially as adoption of the Internet progressed. Politically, the Internet "necessarily and inevitably promotes democracy by giving voice to those who lack political power."[20] Economically, commercial actors around the world embraced "convenient access to worldwide information," the possibility of "establishing a global presence," and "extending world market reach,"[21] resulting in "rapid globalization of economic activities that has made territorial economic containment"[22] increasingly difficult. Socially, global adoption has led to rampant cultural diffusion, cutting severely against the idea of roughly two hundred distinct cultural containers, "within which national ideals are being reproduced in schooling, the mass media and all manner of other social institutions."[23] The Internet, from the start, has come to represent a leaky reality for the modern power container.

Despite these realities, the Internet was and is celebrated at for its decentralized, multi-stakeholder model, named so because "businesses, organizations, governments, and users all play their part"[24] in Internet governance. For about ten years, the Internet "completely overcame the telecommunications system of national boundaries . . . a virtual space that was completely interconnected and globalized, and governments had to react to that after the fact."[25] With only

[20] Warf, *supra* note 12, at 2.

[21] Margaret Tan and Thompson S.H. Teo, *Factors Influencing the Adoption of the Internet*, INT'L J. OF ELECTRONIC COM. 5, 10 (Spring 1998), *available at* http://www.jstor.org/stable/pdfplus/27750854.pdf?acceptTC=true&acceptTC=true&jpdConfirm=true.

[22] Taylor, *supra* note 5, at 158.

[23] *Id.* at 156.

[24] Marietje Schaake, *Stop Balkanizing the Internet*, HUFFINGTON POST (July 17, 2012, 10:59 AM), http://www.huffingtonpost.com/marietje-schaake/stop-balkanizing-the-internet_b_1661164.html.

one organization, ICANN, in a significant position of governance, the multi-stakeholder model "defies top-down control"[26] and "simply does not care about traditional borders."[27] This has been the status quo since the mass adoption of the Internet as an information technology, and is not to say that states have not attempted, vehemently even, to territorialize online spaces and stop the leaking.

II. STATE ASSERTIONS OF SOVEREIGNTY OVER DIGITAL TERRITORY

Given the leaky potential of the Internet as an information technology, it is no surprise that state sovereign authorities have attempted to use it instead to fill their containers. Traditionally, this has been in the form of state governments restricting what *outside* information users *inside* their territory have access to (i.e. censorship), to better control what information can be disseminated to and among their citizens. However, after watershed revelations regarding NSA practices, states are now looking to restrict what *inside* information users *outside* their territory have access to (i.e. containment), an attempt to reestablish sovereignty over content produced within their borders by citizens susceptible to surveillance by third parties. While not necessarily employed by all states, both mechanisms, censorship and containment, are two sides

[25] Tom Gjelten, *Are We Moving To A World With More Online Surveillance?*, NPR (Oct. 16, 2013, 2:56 AM), http://www.npr.org/blogs/parallels/2013/10/16/232181204/are-we-moving-to-a-world-with-more-online-surveillance?sc=17&f=1001.

[26] Steven Titch, *We Must Take UN's Internet Grab Seriously*, REASON FOUNDATION (June 21, 2012, 5:06 PM), http://reason.org/blog/show/1012962.html. That is not to discount the importance of regulation at some level. *See* Zoë Baird, *Governing the Internet- Engaging Government, Business, and Nonprofits*, FOREIGN AFFAIRS, 18 (Dec. 2002), *available at* http://www.jstor.org/stable/pdfplus/20033341.pdf?acceptTC=true&acceptTC=true&jpdConfirm=true (noting the importance of bureaucratic administration on the part of ICANN).

[27] Schaake, *supra* note 24.

of the same coin and together represent the complete picture of territorial practices in digital spaces.[28]

A. The Era of Censorship: Territoriality Before Snowden

Traditional manifestations of online territorial behavior by states are most often reflected in attempts by governments to control virtual behavior within their borders, just as they might attempt to control physical behavior. Authoritarian and politically repressive governments most "often fear the emancipatory potential of the Internet, which allows individuals," to some extent, "to circumvent tightly controlled media."[29] In this sense, the "world's authoritarians have shown just as much aptitude for technology as their discontented citizens"[30] as they move to centralize power online for political, religious, economic, and moral reasons. However restrictive censorship policies may be, whether they are more like Denmark's with a completely unrestricted Internet or North Korea's with no access whatsoever,[31] it remains true that "only 13% of the world's people . . . live in countries with minimal censorship," while "one quarter of the world's people and Internet users live under governments that engage in very heavy censorship."[32]

At the most basic level, censorship entails control over Internet "access, functionality, and contents."[33] Because precise filtering is relatively difficult, censorship tends to take on many

[28] States, of course, make value judgments in theory about what type of regime they wish to employ in practice, so levels of censorship and containment operate on a sliding scale depending on levels of desired involvement, protectionism, or involvement.

[29] Warf, *supra* note 12, at 3.

[30] *Id.*

[31] *Id.* at 4.

[32] *Id.* at 5.

forms, including content filtering based on keywords, redirection, website blocking, discriminatory pricing, hardware and software manipulation, spreading viruses, denial-of-service attacks, and even just-in-time blocking at moments when political information is critical.[34] Almost ubiquitous, however, is "self-censorship," where users police their own behavior out of fear of repercussions, or even out of habit.[35] Censorship could also conceivably be used as a means of containment, where access to services known to be bugged could be blocked. No matter the form it takes, however, censorship is and always will be susceptible to mission creep; "[o]nce formal censorship is initiated, no matter how benign or transparent, the temptation to enlarge its scope . . . is always there."[36]

The same various methods of censorship may be employed across countries, but states each take their own unique approach to the traditional, censorship-based attempts at territoriality online. To use the United States as an example, sanctioned censorship efforts in the U.S. largely revolve around controlling negative externalities "such as Internet crime and pornography that the market, left to its own devices, would fail to control."[37] Additionally, the FBI "encourages ISP's to censor websites that are not consonant with the public interest and to turn over information about users whose email reveals suspicious intent."[38]

China, on the other hand, with more than 420 million Internet users arguably has the world's most severe Internet censorship.[39] Since 2006, China's "Great Firewall" has been the

---

[33] *Id.* at 4.

[34] *See* Warf, *supra* note 12, at 4 (explaining the various methods of Internet censorship).

[35] *Id.*

[36] *Id.*

[37] *Id.* at 8.

[38] *Id.*

"most extensive, technologically sophisticated, and broad-reaching system of Internet filtering in the world."[40] State controlled backbone networks control all international Internet connections, while monitors and citizen volunteers (Beijing alone has 10,000) screen "blogs and email messages for potential threats to the established political order," and access to popular services like Yahoo! and Google is heavily restricted.[41]

Russia, too, was "never all that supportive of Internet freedom."[42] While it certainly lacks the extensive infrastructure that Chinese censorship programs employ, the Russian system relies heavily, as many censorship regimes do, on self-censorship. "Russia's Internet surveillance law . . . allows state security services unfettered physical access to ISPs and requires them to report statistics about users."[43] This is all supposedly in the name of "fighting corruption."[44] Reported statistics create self-policing behavior on the part of users who fear that their activities online have the potential of becoming known to government authorities.

While China relies heavily on infrastructure at the state level and Russia relies on self-censorship at the individual level, Iran "manages its censorship at the level of the ISP."[45] Not only has the government "assumed control over all international traffic entering or leaving the country," but ISP's must also prohibit access to all "non-Islamic" websites. Together, these three regimes represent the various levels at which online censorship can be executed: state, individual,

[39] Warf, *supra* note 12, at 8.

[40] *Id.*

[41] *Id.*

[42] Gjelten, *supra* note 25.

[43] Warf, *supra* note 12, at 11.

[44] *Id.*

[45] *Id.* at 10.

and ISP. This was the traditional approach to territoriality and power container theory online, but after Snowden, another side of the coin was revealed.

B. Watershed: What the NSA Did and Why It Matters

The documents leaked by Edward Snowden in the summer of 2013 set off a chain of events that would lead to a dramatic change in the way both individuals and states look at the Internet. This involved the exposure of "hundreds of classified documents" pointing to what Snowden believed to be a shocking "invasion of Americans' and foreigners' privacy."[46] Snowden has since sought asylum abroad, but the effects of his disclosures remain.

Documents he provided reveal that the NSA employed an elaborate surveillance network that "cracked much of the online encryption relied upon by hundreds of millions of people to protect the privacy of their personal data, online transactions and emails."[47] To achieve this, the NSA uses Computer Network Exploitation (CNE), the "secret infiltration of computer systems achieved by installing malware."[48] CNE was used on "more than 50,000 computer networks worldwide," specifically "designed to steal sensitive information."[49] Thousands of officers, housed within the NSA's TAO (Tailored Access Operations) division execute the agency's CNE surveillance, some of which has been ongoing since as early as 1998 and reached users as far away as Brazil and Venezuela.[50] The documents also implicate the NSA's use of

---

[46] Shane*, supra* note 3.

[47] James Ball, Julian Borger & Glenn Greenwald, *Revealed: how US and UK spy agencies defeat internet privacy and security*, THE GUARDIAN (Sept. 5, 2013), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (noting the NSA's high cyber-surveillance budget).

[48] Floor Boon, Steven Derix & Huib Modderkolk, *NSA infected 50,000 computer networks with malicious software*, NRC (Nov. 23, 2013, 2:40 AM), http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/.

[49] *Id.*

[50] *See id.* (noting the long history of the NSA's surveillance program).

"supercomputers to break encryption with 'brute force'" and NSA collaboration with technology companies and service providers" to insert exploitable vulnerabilities.[51] Aside from the undoubtedly large personnel costs, such methods of surveillance are "relatively inexpensive" yet "provide the NSA with opportunities to obtain information that they otherwise would not have access to."[52]

Smartphones, however, are the NSA's goldmine. Notwithstanding the fact that half of American, half of German, and two-thirds of British citizens have one, smartphones combine "in a single device almost all the information that would interest an intelligence agency: social contacts, details about the user's behavior and location, interests (through search terms, for example), photos and sometimes credit card numbers and passwords."[53] Realizing the surveillance potential of the smartphone's meteoric rise in popularity, the NSA set up task forces for tapping "leading smartphone manufacturers and operating systems," like Blackberry, Apple's iOS, and Google's Android.[54] Such surveillance programs are also not solely limited to United States government agencies—they have also been revealed, for example, in Great Britain, Sweden, and the Netherlands.[55]

---

[51] *See* Ball, *supra* note 47 (explaining the various NSA surveillance techniques).
[52] *Id.*

[53] Marcel Rosenbach, *How the NSA Accesses Smartphone Data*, SPIEGEL ONLINE (Sept. 9. 2013, 12:25 PM), http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html.

[54] *Id.*

[55] *See* Ball, *supra* note 47 (noting the existence of the British surveillance program); Gunnar Rensfeldt, *FRA has access to controversial surveillance system*, SVT (Dec. 11, 2013, 2:39 PM), http://www.svt.se/ug/fra-has-access-to-controversial-surveillance-system (Swedish program); Steven Derix, Glenn Greenwald & Huib Modderkolk, *Dutch intelligence agency AIVD hacks internet forums*, NRC (Nov. 30, 2013, 3:00 AM), http://www.nrc.nl/nieuws/2013/11/30/dutch-intelligence-agency-aivd-hacks-internet-fora/?ref=twt2 (Dutch program).

The fruits of these labors are quite intrusive—"an image of a former defense secretary with his arm around a young woman;" images depicting "young men and women in crisis zones, including an armed man in the mountains of Afghanistan;" and "an Afghan with friends and a suspect in Thailand."[56] These cited examples all implicate private individuals, but it seems officials of foreign governments have been targeted as well. The German government recently "awarded a major contract for secure mobile communications within federal agencies" to Blackberry, one of the operating systems cracked by NSA task forces. Whether created by individuals in a private or public capacity, smartphone data can be tapped either from the phone itself, or from backup files created by users on their computer.[57] The documents leaked by Snowden certainly paint a startling picture of what modern surveillance techniques can accomplish when agencies are given access to copious resources.[58]

Symbolically, however, the unveiling of extensive government surveillance programs has and will continue to have far-reaching implications. The NSA and similar programs have subverted "the internet and turn[ed] it into a massive surveillance tool." This has both challenged previous beliefs that cryptography could be used to create a "basis for trust online," and undermined "the very fabric of the internet."[59] This lack of trust will, in turn, drive countries towards domestic technology companies that "require citizen data to stay within their borders."[60] Not to mention the fact that all users, and no longer just those in known surveillance states, will

---

[56] Rosenbach, *supra* note 53.
[57] See *id.* (explaining how such tactics are employed).

[58] *See* Ball, *supra* note 47 (citing the $250 million dollar annual budget of a single NSA program).

[59] *Id.*

[60] Grant Gross, *US faces major Internet image problem, former gov't official says*, COMPUTERWORLD (Dec. 5, 2013, 4:48 PM), http://www.computerworld.com.au/article/533605/us_faces_major_internet_image_problem_former_gov_t_official_says/.

"think twice about what opinions to express" online.[61] While the constitutionality of the NSA programs is still unclear,[62] the existence of palpable effects on user behavior in digital spaces is undoubted. Internet users in all corners of the globe are potentially vulnerable to surveillance as long as NSA and similar government programs remain in effect.

C. A New Era: Territoriality Online After Snowden

These leaky vulnerabilities have inspired responses from private and public actors alike, new approaches to protecting the integrity of the territorial state as power container in the digital age. Such realizations of vulnerability, though, have prompted territorial behavior most visibly in liberal governments and only residually in more repressive states.[63] This type of behavior was traditionally reserved for authoritarian regimes engaging in censorship. Regardless of practitioner, though, the NSA-effected containment efforts have brought into existence a new manifestation of territorialism online. Snowden's confession turned over the coin of digital territoriality from censorship to containment.

Since Snowden's disclosures, Brazil has been out in front of online containment efforts. The Brazilian government learned that the NSA has led extensive surveillance efforts there,[64] going so far as to target private emails and calls,[65] the Brazilian president, Dilma Rousseff,[66] and

---

[61] *Id.*

[62] *See* Josh Gerstin, *Judge: NSA phone program likely unconstitutional*, POLITICO (Dec. 16, 2013, 1:36 PM), http://www.politico.com/story/2013/12/national-security-agency-phones-judge-101203.html (predicting that U.S. constitutional issues will go unresolved until a case on point goes before the Supreme Court).

[63] *See* Scott J. Shackelford, *The Coming Age of Internet Sovereignty?*, HUFFINGTON POST (Jan. 10, 2013 6:59 PM), http://www.huffingtonpost.com/scott-j-shackelford/internet-sovereignty_b_2420719.html (discussing Iran's recent containment policies); Gjelten, *supra* note 25 (discussing Russia and China's recent containment policies).

[64] *See* Boon, *supra* note 48 (citing an NSA presentation that revealed CNE surveillance targets).

[65] *See* Leo Kelion, *Brazil plans secure email service to thwart cyber-spies*, BBC NEWS (Oct. 14, 2013), http://www.bbc.co.uk/news/technology-24519969 (explaining the NSA's targeting of private Brazilian communications).

domestic oil giant Petrobas.[67] President Rousseff herself has led the charge, "fast-tracking a vote on a once-dormant bill that could require that data about Brazilians be stored on servers in the country."[68] This would involve the Brazilian government requiring service providers to "keep the servers in Brazil, encrypt all the traffic inside or outside the country, and only give access to Brazilian police and intelligence services."[69] While it is clear that many state actors find NSA practices unpalatable, it "has touched a real nerve in Brazil, a country that prizes its sovereignty and is understandably sensitive about such abuses."[70] In Rousseff's own words, "the relationship [Brazil has with the U.S.], based on the fact that [they] are big democracies in this part of the world, is incompatible with the act of spying."[71] Brazil has consequently sought to reestablish territoriality over its digital spaces, not with censorship, but with containment.

While Brazil has been weighing its options south of the equator, Europeans in the northern hemisphere are making similar containment-oriented decisions. Like in Brazil, the Finnish public sector has stepped in to mollify concerns of foreign data surveillance. The Finnish government has announced plans to "build a fast, high-quality and cyber-secure connection to European and global networks from Finland to Germany via an underwater fibre optic cable."[72]

---

[66] *See* Gjelten, *supra* note 25 (discussing the reactions of various states and leaders to the extent of NSA programs).

[67] Juan Forero, *Brazilian TV show says U.S. spied on state-run Petrobras oil firm, cites NSA*, WASH. POST (Sept. 8, 2013), *available at* http://articles.washingtonpost.com/2013-09-08/world/41880912_1_petrobras-obama-administration-president-obama.

[68] Elizabeth Dwoskin & Frances Robinson, *NSA Internet Spying Sparks Race to Create Offshore Havens for Data Privacy*, WALL ST. J. (Sept. 27, 2013, 12:15 PM), http://online.wsj.com/news/articles/SB10001424052702303983904579096082938662594.

[69] Kelion, *supra* note 65.

[70] Dwoskin, *supra* note 68.

[71] *Id.*

[72] *New data cable to make Finland's one of the world's most attractive ICT regions*, FINNISH GOV'T. (Nov. 12, 2013, 2:30 PM), http://government.fi/ajankohtaista/tiedotteet/tiedote/en.jsp?oid=402176.

Such a cable would "raise the protection of Finland's international connections and data security to a new level"[73] through preclusive containment measures.

In Germany, it has been the private, not public sector that has responded to security concerns after the surveillance susceptibilities of citizens' user data became known.[74] Three of the largest email providers in Germany, recognizing the potential market for such a service, jointly developed "Email Made in Germany. The companies promise that by encrypting email through German servers and hewing to the country's strict privacy laws, U.S. authorities won't easily be able to pry inside."[75] Within two months of Email Made in Germany's release, more "than a hundred thousand Germans [had] flocked to the service."[76]

In addition to the liberal-state public and private sectors, there is also a third flavor of containment advocate: bandwagon authoritarian states trying to capitalize on the growing balkanization movement. Known traditionally for their censorship practices, these states would benefit from containment in that with greater balkanization and a rise in the popularity of territorial containment practices online there would be less transparency from the outside looking in on their regulation of digital spaces should they also choose to adopt such policies. Iran, considering perhaps the most extreme approach, is reportedly "building a national network detached from the global Internet to enhance government control of information and potentially better guard against cyber attacks."[77] Russia and China are also pushing to "centralize their

---

[73] *Id.*

[74] *See* Rosenbach, *supra* note 53 (noting the vulnerabilities of German public officials, who use NSA-cracked Blackberry devices and software)

[75] Dwoskin, *supra* note 68. *See also Verschlüsselung*, EMAIL MADE IN GER., http://www.e-mail-made-in-germany.de/ (last visited Mar. 9, 2015) (describing the service's encoding mechanism).

[76] Dwoskin, *supra* note 68.

[77] Shackelford, *supra* note 63.

[Internet] infrastructures and get the U.S. out of the picture."[78] With increased balkanization among capitalizing repressive states, such practices could "have negative consequences for free speech as well as for protection of privacy."[79] The Internet would move away from the auspices of the vulnerable, yet free-speech driven, U.S. dominated model and towards individualized centralization under authoritarian regimes like those of Iran, Russia, and China already employing and benefiting from digitally restrictive policies.

Regardless of actor, regime, or motivation, reactionary containment efforts have already catalyzed the potential balkanization of online resources. This represents a straying from the idea of a global commons that has flourished since the early days of the Internet and towards the colonization and retainment of digital spaces spaces under individualized regimes. As states move to stake their claim in the digital commons, asserting territoriality in twenty-first century fashion, it remains to be seen how far states will go to protect the integrity of their power containers against the draining practices used by those beyond.

III. FUTURE DEVELOPMENTS

Balkanization efforts by states seeking to contain proprietary digital resources put the traditional, multi-stakeholder model of the Internet at risk. Many states, like Brazil, Finland, and Germany, would like to see an expansion of the twentieth-century power container to include a more rigorous exaction of control over twenty-first century digital resources. For these states, policy choices have laid the groundwork for a more state-centric approach to the geography of online spaces, data, and politics, leading to a dramatic evaluation of the state of the Internet today. States have called into question that ordering of priorities affected by the Department of

[78] Gjelten, *supra* note 25.
[79] *Id.*

Defense in the creation of ARPANET, and the subsequent development of a decentralized, colonized global commons. Whether the state-centric model succeeds in its usurpation or the multi-stakeholder model manages to retain its preeminence will be determined ultimately by evaluations of the two approaches.

At its heart, the state-centric model aims to apply power container and territoriality theory to achieve the centralization of Internet resources under a particular regime. This would result in an increased balkanization of digital spaces among individual sovereigns. The states employing reactionary measures do so in the belief that "everyone's data and privacy are more vulnerable to hackers, governments, terrorists, and criminals of all kinds" due to NSA installation of not only secret back doors in online services, but also manufactured weaknesses in global encryption standards.[80] Responses like those of the Brazilian and Finnish governments are "touted as a way to protect . . . citizens . . . and sovereignty"[81] by limiting the power and influence of outside actors through networked insulation. The state-centric model would trade off perceived efficiencies created by a freely discursive global marketplace for protection of domestic digital, proprietary resources that have been increasingly threatened since the advent of the Internet.

The state-centric model, though, leaves some questions unanswered. For example, "what costs will this impose in terms of innovation an interconnectedness, and how can we manage the growing reach of the leviathan to minimize distortions and protect civil liberties?"[82] Containment policies could "raise the cost of computing"[83] by establishing a system similar to "the European train system, where varying voltage and 20 different types of signaling technologies force

[80] T.A. Ridout, *Marco Civil: Brazil's Push to Govern the Internet*, HUFFINGTON POST (Oct. 22, 2013, 1:47 PM), http://www.huffingtonpost.com/t-a-ridout/brazils-push-to-govern-the-internet_b_4133811.html.

[81] *Id.*

[82] Shackelford, *supra* note 63.

[83] Dwoskin, *supra* note 68.

operators to stop and switch systems or even to another locomotive, resulting in delays, inefficiencies, and higher costs."[84] A system of countries advocating for domestic hosting like Brazil "could have trouble competing with the economies of scale enjoyed by big U.S. companies."[85]

In addition to raising costs, the varying jurisdictions of a balkanized Internet would create a new set of privacy concerns and potential rights abuses.[86] In the countries that "don't protect the privacy of citizens' Internet data" to begin with, Internet users could be safer from the eyes of outsiders, but they "wouldn't be safe from their own governments' eyes."[87] In states like Iran, Russia, and China where censorship-based territorial policies are already in effect, there could be "even less access to basic communications, hampering the ability to interact online outside of [a] regime's control and censorship"[88] with the addition of containment policies. Even Brazil, ironically enough, makes hundreds of requests for Facebook user data each year, and it would be the Brazilian government in charge of the domestic data servers. [89]

For many, though, the answer is simply to curb the use of unlawful outside surveillance. As a solution, it would theoretically maintain the integrity of states' sovereignty and reduce threats to digital power containment within a given territory. The UN, for example, recently created a right to privacy, establishing "that human rights should prevail irrespective of the

---

[84] Sascha Meinrath, *The Balkanized Internet and the Vitamin C Cartel*, THE WEEKLY WONK (Oct. 10, 2013), http://weeklywonk.newamerica.net/editions/the-balkanized-internet-the-vitamin-c-cartel/.

[85] Dwoskin, *supra* note 68.

[86] *See* Meinrath, *supra* note 84 (discussing the rights-based costs of Internet balkanization); Dwoskin, *supra* note 68 (commenting on privacy risks).

[87] Dwoskin, *supra* note 68.

[88] Meinrath, *supra* note 84.

[89] *See* Dwoskin, *supra* note 68 (discussing the Brazilian government's current data surveillance practices and proposed containment policies).

medium and therefore need to be protected both offline and online."[90] A "restoration of balance that prioritizes civil rights, not surveillance, as vital to (inter)national security"[91] could mollify the concerns of those states pushing for greater balkanization and prevent the degradation of those benefits the Internet confers as a common space under the multi-stakeholder model. At least in the case of the United States, policy-makers should ask themselves whether "the benefit of spying on Brazil's oil company [is] worth the cost of antagonizing the people of [the Western] hemisphere's second-largest democracy and giving China and Russia the moral high ground in debates over how people around the world should access information."[92] Like nuclear non-proliferation, transparently coordinating a reduction of international surveillance practices could remove the perverse incentives to balkanize and preserve the integrity of shared digital resources against containment.

CONCLUSION

The territorial approach to modern statehood was developed, as described above, in response to a "negative-sum game."[93] That negative-sum game was the Thirty-Years War that ravaged Europe, in the name of religion, a hundred years after Martin Luther catalyzed the Protestant Reformation. It was only in 1648 at the Treaty of Westphalia that the war came to an end, and where "state centralization was accepted through the principal of noninterference in each other's internal affairs, thus formally eliminating all rival power centres in [state]

---

[90] United Nations, *Third Committee Approves Text Titled 'Right to Privacy in the Digital Age', As it Takes Action on 18 Draft Resolutions*, UNITED NATIONS MEETINGS COVERAGE AND PRESS RELEASES (Nov. 26, 2013), http://www.un.org/press/en/2013/gashc4094.doc.htm.

[91] Meinrath, *supra* note 84.

[92] *Id.*

[93] Taylor, *supra* note 5, at 161.

territories."[94] With these formal recognitions, the modern sovereign state as power container could come into fruition and freely govern those territories within its borders.

Not only has the second decade of the twenty-first century seen the advent of a crystallizing digital reformation, but also the same competitively disrespectful and meddlesome state of affairs that instigates bloody, rivalrous conflicts. In order to preserve the wondrously successful sprawling commons model of the Internet, the necessity for a new Treaty of Westphalia is painfully clear. Without the same principles of restraint and noninterference governing surveillance temptations, states will have no option but to push away from each other, colonizing and centralizing digital spaces under their own regimes. It is not just the modern power container that is leaking—the limitless potential of perhaps the greatest technology the world has ever seen leaks too. To stop the leaking we must look into our past, and thus preserve our future.

[94] *Id.*