Routledge
Taylor & Francis Group

Journal of Information Technology & Politics

ISSN: 1933-1681 (Print) 1933-169X (Online) Journal homepage: http://www.tandfonline.com/loi/witp20

A Policymaking Process "Tug-of-War": National Information Security Policies in Comparative Perspective

Kenneth Rogerson & Daniel Milton

To cite this article: Kenneth Rogerson & Daniel Milton (2013) A Policymaking Process "Tug-of-War": National Information Security Policies in Comparative Perspective, Journal of Information Technology & Politics, 10:4, 462-476, DOI: 10.1080/19331681.2013.843989

To link to this article: https://doi.org/10.1080/19331681.2013.843989

Accepted author version posted online: 18 Sep 2013.
Published online: 18 Sep 2013.

Journal of Information Technology & Politics, 10:462–476, 2013

ISSN: 1933-1681 print/1933-169X online
DOI: 10.1080/19331681.2013.843989

Routledge
Taylor & Francis Group

A Policymaking Process "Tug-of-War": National Information Security Policies in Comparative Perspective

Kenneth Rogerson
Daniel Milton

ABSTRACT. There is tension between the ideal of government transparency and the need to protect vital information. What types of information do governments protect on national security grounds? What arguments do governments use to justify the protection of this information? What will influence an open government information policy as opposed to a closed information policy? Through an examination of more than 250 information security–related policies from around the world, it is clear that (a) all governments limit the flows of information, (b) there are different reasons for this, and (c) the reasons are not always correlated to government type. In other words, sometimes democracies and authoritarian countries limit the same types of information issues. The policies and policy discussions are dependent on a variety of actors and which actor(s) wield the strongest influence at the time, which makes them often get caught up in a policy "tug-of-war" that most often results in incremental policy change and implementation.

KEYWORDS. Autocracy, democracy, free flow of information, information security policy, policy tug-of-war

In a networked and information-saturated world, information security is critical to states and policymakers. A confluence of factors and actors, including divergent political and economic interests, policy-making processes, government types, and technical expertise at the policy-making level, all combine to produce disparate information security polices among states. Scant attention has been paid in the information security literature to the important issue of differences in information security polices among states, especially to the differences between the information security polices of authoritarian and democratic states and how disparate policy-making processes contribute to those differences. Do authoritarian and democratic governments address information security policy similarly or differently, and, through the lens of the tension between the variety of actors and stakeholders in the different types

Kenneth Rogerson is a lecturer and Director of Undergraduate Studies at Duke University's Sanford School of Public Policy.

Daniel Milton is an assistant professor at the United States Military Academy and an associate at the Academy's Combating Terrorism Center.

The authors express gratitude to the anonymous reviewers for their extremely helpful comments and guidance.

Address correspondence to: Kenneth Rogerson, Sanford School of Public Policy, Duke University, Duke Box 90239, Durham, NC 27708-0239 (E-mail: rogerson@duke.edu).

of governments, what might best explain those similarities or differences?

Policies, in general, come in two broad categories: (a) specific policies that governments enact and (b) policies that are proposed, but may not be enacted, and the discussions surrounding these proposals. Both types of policy are relevant to this project. Within the context of information security, we ask the following: What classes of information do governments protect? What arguments do governments use to justify the protection of this information? Note that the answer to the second question is *not* simply that governments can do what they want to do as long as they relate it to national security. This is particularly true where more actors and interests are involved and more coordination is required to shift the status-quo policy.

There are two challenges in understanding how states address information security policy. The first is that there are a variety of actors, both public and private, interested in how information security policy functions. However, these actors do not operate in a vacuum. They are constrained by political, ideological, and institutional factors. This leads to the second challenge, which is that the institutional nature of the government (whether democratic or authoritarian) also affects how the government addresses these issues. While policy-makers and private actors in both democracies and authoritarian countries interact to address the securing of what they consider vital information, these interactions may differ across government types. Consequently, the policy-making process may resemble a "tug-of-war" in countries in which policy-making authority is diffuse. In these countries, interactions between policy-makers and private actors "tug" policies in one direction or another, depending on the political and ideological climate. In such an environment, it is rare to find that information security policies, as very broadly defined above, find themselves completely dominated by one way of thinking. However, this is less the case when policy-making power is concentrated, as it is in authoritarian governments. Even though multiple actors are interested, they are less capable of influencing policy, which looks less like a tug-of-war and is more focused on the state's own interests.

Governments deal with policy-making in different ways when it comes to securing information. In particular, the broad range of actors and interests involved in policy-making in democracies create unique tensions that are not found in authoritarian countries, where access can be more restricted and the policy-making process more centralized. Notwithstanding these ideals, there is literature that suggests that democracies may not always measure up to their own stated ideals, particularly those concerning information transparency and when facing threats (see, for example, the literature on information privacy: Klosek, 2007; Rosenzweig, 2013). To evaluate these ideas in the context of information security policy, this study examines a dataset of 250 actual and proposed information security policies from around the world in which governments have addressed information security policy. The findings suggest that information security policy-making in democracies resembles a multiple-actor tug-of-war, in which information security policy-making seldom results in large changes or policy adaptations (Anderson, 2011). This differs from the policy-making process in autocratic countries, which is still a tug-of-war, but involves fewer actors and a less diverse set of interests. These findings are consistent with general beliefs about democracies and autocracies. There are, however, exceptions to these general findings, particularly when democracies experience serious national security threats.

INFORMATION SECURITY POLICY-MAKING AND GOVERNMENT TYPE

Much of government intervention in information security has been in two large categories: (a) military and defense and (b) consumer protection/identity, though there are others as well. For example, in *Conquest in Cyberspace: National Security and Information Warfare* (2007), Libicki laid out the structure of how the U.S. Department of Defense understands information security, providing some important

broad concepts that could be applied in a variety of cases and possibly even countries. These categories help the reader understand what is happening, but not how they might change over time.

On the consumer side, Bob Sullivan provides an overview of the policy that protects (and often does not protect) a consumer's identity. In *Your Evil Twin: Behind the Identity Theft Epidemic* (2004), Sullivan presents what he calls the "Kafkaesque trials" that people face when their identity is stolen and, instead of helpful policy for some redress of grievances, they find "government ineffectiveness and law enforcement indifference" (p. xvi). Again, Sullivan provides a rich arena for understanding what is happening, and also proposes some policy changes to help. But, which actors and interests need to come together to nudge policy in a direction that will work? And what are the strategies and rationale they might use to do it?

With both democratic and authoritarian governments, there is a wide variety of factors that play a role in how the state makes information security policy. Such factors include those found in written documents, such as constitutions, as well as those cultural, political, and economic rules of engagement that are simply part of how the country functions. The fact that there are so many factors in so many different countries may lead some to conclude that an analysis of the way in which democracies and autocracies generally deal with information security policy is not useful. However, domestic intricacies notwithstanding, analyzing these general government types can serve meaningful academic and public policy purposes. Understanding how democracies and autocracies generally deal with information security policy provides a better context for understanding how country-specific differences play out. It also provides policymakers with a better understanding of the limits and constraints faced in these different types of governance structures.

When it comes to democracies and information, there is a general belief that democracies should seek transparency in their policies and actions to citizens and to other nations (Florini, 1998, 2004). Acting on these ideals, policymakers should build their information-security policies on the goal of an open-access society in which information is abundant and government processes are transparent. While advocating the benefits of this open-access approach to information security, such as the accountability of political agents to an electorate, some proponents of this view acknowledge that, even in democratic societies, a more stringent form of information security may be necessary in some circumstances to protect vital state interests, but that such control should be as limited as possible (Florini, 2004; Thompson, 1999, pp. 192–193).

One limitation of this argument is that it does not address the transitory period between norms and policy. Even if the assumption is made that democratic norms support complete—or nearly complete—transparency and stand in contrast to government secrecy, the question still remains: How do the norms find their way through the policy process and into enforceable laws? Even more, how do normative arguments account for the fact that governments still classify information at relatively high rates? It is not enough to wave the wand of national security at these questions. After all, the decision to classify information is made by actors with interests, whether for country or self.

Another limitation in some of the arguments regarding information security deals with the institutional origins of secretive government policy. There is an assumption that the executive branch of government, especially in the United States, is responsible for the increase or continued presence of government secrecy (Florini, 2004, pp. 20–21). While the executive branch may have an interest in maintaining secrecy, the argument misses the fact that, in a democracy, there are multiple actors that participate in the policy-making process. Making recommendations for policy based on an understanding of only one actor, instead of a more broad understanding of the policy-making process as it relates to information security, is incomplete. In general, the amount of research that directly addresses information security in its policy-making context is limited.

In contrast to the democratic ideal of transparency, authoritarian governments rely on the principle of self-preservation (see O'Donnell,

Schmitter, & Whitehead, 1986). Resultant information security policies normally reflect this principle, focusing on governmental access to the nodes of information flow and providing legal power for government representatives to request information with minimal recourse. One strength of this position is that government structures are set up to approve and implement information security policies without formal questioning. If there is an opposition, it is in a position of relative weakness.

Of course, authoritarian governments are not immune from debate and dissent about policies. In particular, authoritarian governments may face the threat of protest because of their policies. The institutional differences between democracy and authoritarian governments allow the latter to deal with the problem more directly. In other words, while this threat may be consistently real, some governments have found ways to prevent it. Peter Jones (2012) writes that while there is a trend in the recent "revolutions" in the Middle East, fewer have happened in monarchies. He reasons that this may be because of the societal control that the regimes have through a paternalistic "social contract" that the majority of citizens accept, or even that they "buy off" their citizens through financial incentives (Jones, 2012).

Comparing information security policy over the two types of governments, Helen Milner (2006) applied the idea of democratic exceptionalism to the spread of different means of technology, claiming that the factions in power in authoritarian governments can see and prevent the spread of technology that might undermine their power, while factions within democratic governments have many more institutional hurdles to overcome (pp. 178, 184, and 195).

It is not inconceivable to view authoritarian governments as desiring to limit the release of sensitive information, while viewing democratic institutions as encouraging openness. Both of these arguments appear in the preceding paragraphs. However, one of Milner's key points is the groups that desire to block technological diffusion within a democracy often do not have the support of political institutions (2006, 195). This may (or may not) be the case when dealing with information security. There are a number of actors—both institutional and individual—who wield great amounts of power and who might oppose policies designed to increase transparency.

Early research on information flows, especially concerning the World Wide Web, assumed a democratic imperative. That is, greater flows of information will lead to more openness. But scholars immediately began to test this proposition. From Robert McChesney's (1996) early work criticizing corporate control of the internet to Stephen Lax's (2001) edited volume exploring similar issues, academics have studied whether theories such as Milner's can be empirically supported. McChesney finds that democratic governments have more autocratic tendencies when it comes to information restriction, and Lax's contributors find that most governments at the time of the study seemed to be erring on the side of security rather than dissemination.

Other more recent scholarship by Ronald Diebert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain has provided a wealth of information about the ways that different countries control the flow of information. In *Access Denied* (2008) and *Access Controlled* (2010), this group of researchers catalogs the information-controlling activities of several countries. Similarly, Giacomello (2005) examines the different way in which democratic countries deal with control of the Internet. In particular, his analysis of democracies showed that while they often dealt with similar internet challenges, their methods of dealing with these challenges differed according to dialogue and culture.

Building on these conceptual and empirical works, a next research step would be to find some trends and patterns in this cataloguing, and to address how the ideals of a particular government type are represented in its policy-making. What types of information do governments protect? What arguments do governments use to justify the protection of this information? And what best explains the give-and-take, or the tug-of-war, in the formulation of these information security policies?

METHODOLOGY

To understand these competing policy-making interests, we surveyed examples of policies around the world that address the issue of information security. The data set contains approximately 250 policies (both proposed policies and those passed into law) that resulted in either changes to laws, new laws, or the creation of new governmental agencies addressing the issue of information security. The examples represent all regions of the world: Africa, the Americas, Asia, Europe, and the South Pacific. It covers the time period from 1998 to the present. While some of the laws and examples may seem outdated, the importance of this project is in the policy analysis over time, not only in its relevance to current events.

These policies do not represent randomly distributed events. Countries that have information security policies have them because circumstances are such that the policy has enough support that it can be adopted through the existing institutional process. However, the goal is not to look at the effect of information security policy on other variables. Rather, it is to explore the non-randomness itself. What variables, or factors, influence the type or focus of the information security policies that a given country will adopt?

The dataset is not exhaustive; certain countries are not represented. The primary sources for gathering the information were news and political databases, such as LEXIS/NEXIS, and country parliamentary document repositories. The policies were analyzed based on three questions. First, what type of information is secured or limited? The answers were meant to represent the policy issue area. Some laws overlap among categories. Second, what is the rationale that governments use for securing or limiting the information? This includes the goals of the policy, though these are not always explicitly stated. Third, what are the circumstances around which the policy is formulated? This is the most difficult question to answer, since the situations are not always specifically stated in the news articles or legislative archives. But, where possible, this context can provide a wealth of understanding about the extent to which governments go to secure information. The second and third questions speak specifically to the tug-of-war.

NATIONAL INFORMATION POLICIES FROM AROUND THE WORLD

While some information policies are designed to free the flow of information—such as sunshine laws or freedom of information acts—other policies are targeted at limiting, securing, or controlling the flow of information. The types of controlled information fall into the following categories: external threats (national security issues), internal threats (antigovernment or antistability information), infrastructure information, personal or individual information, commercial information, and news media information.

External Threats (National Security Issues)

Issues of national security policy have always been targets of policy-limiting information flows. In *Empire and Communications* (2007), Harold Innis makes the argument that the control of information (what he referred to as "monopolies of knowledge") was indispensable in the making of empires from the Egyptians to the British. Defense of national priorities against external threats is the most obvious—and often the most accepted—reason to limit the flows of information within a country. However, external threats, such as war and some forms of terrorism, differ from internal threats, such as antigovernment protests and seditious acts (which may include terrorist acts but are distinguished from others such as the U.S. "War on Terror"). While internal threats matter (addressed in the subsequent section), external threats and the policies designed to address them take on a different tenor that makes them an analytically separate category.

For example, the Patriot Act gave the U.S. government access to some information it had

not had before. While the U.S. military uses the Internet and other mass media to communicate with the Iraqis and Americans (Bernard, 2005) about the war (some have called this propaganda; see Sandoval, 2006), it also limits the use of specific types of media by soldiers, who may want to blog about or comment on the war, justified by the argument that such communication may potentially empower enemies or create disunity.

In addition to allowing governments to broaden the scope of information they monitor and regulate, external threats could reveal new vulnerabilities. War between nations also provides a powerful motivation for developing information security policies that can protect against foreign intrusion. Smith (2012) argues that this is the most enduring lesson of the Russian cyber efforts against Estonia in 2007 and Georgia in 2008. In particular, the tension between Russia and Georgia demonstrated the need to protect computer networks (civilian and military alike) in the case of armed conflict.

Such lessons are not unique to interactions among state actors. There has been an increased focus since 9/11 on the role of nonstate actors. The external threat of terrorism has figured prominently in shaping the types of information security policies that have emerged over the past decade or so. The 2001 attacks in New York City and Washington, DC, by al Qaeda, have spurred other countries to enact information controlling policies. Senator Chris Ellison of the Australian Parliament referenced the September 2001 events as being influential in the country's need to have modern laws and policing powers to investigate cybercrimes, and to prevent incidents of cyber-terrorism: "Previously if a terrorist attack had been carried out on Australia's national information infrastructure police did not have the power to compel suspects to assist in an investigation of complex computer systems protected by passwords or encryption, or to conduct searches on-line across different locations" (Australia's Attorney General's Department, 2001). The new policies gave Australian law enforcement broader authority to access and subsequently limit information flows if necessary.

Internal Threats (Antigovernment and Antistability Information)

Limiting information has been relatively common when dealing with threats to a country's internal stability. The Sedition Acts of 1798 in the United States criminalized treasonous language. More recently, changes in Russian media law during the 2000s made discussions that opposed the sitting administration more liable for prosecution.

Singapore, for example, has been recognized for programs that electronically connect its citizens and government. The government has claimed it wants to be a "paperless" society. However, in 2003, the parliament passed the Computer Misuse Act, which interpreters have called a response to the Internet as a "weapon of mass disruption." The government states it will judiciously use the power bestowed by the law, but "It could be misused to invade into the privacy of citizens to gather information,' said Sinapan Samydorai, president of Think Centre, a Singaporean civil liberties group. He said the new laws could be used as an "'instrument of oppression' by the government" (Singapore Cyberterrorism, 2003).

For China, combating threatening information flows is an implicit policy:

> For companies and individuals alike, understanding Chinese online political censorship is made more difficult by the secrecy in which it is shrouded. Officials routinely deny that it happens at all. "As I understand it, the censorship of web sites or online content is completely impossible," says Wang Guoqing, vice-minister of the State Council Information Office, the government body responsible for media monitoring. But top leaders have left no doubt that controlling the web is a political priority. "Whether or not we can actively use and effectively manage the internet . . . will affect national cultural information security and the long-term stability of the state," Hu Jintao, China's president, told a meeting of the Communist party's governing Politburo in January. It was necessary to

> "purify the internet environment." (Dickie, 2007)

Infrastructure Information

Information infrastructure development around the world has traditionally been a mixture of public and private initiatives, with some countries leaning toward one or the other. Those that tend to implement publicly funded programs might do so with the intent to control the information that goes through those networks.

For example, in 2006, Kenya, Uganda, and Tanzania began the process of adopting harmonized cyber laws to enable the establishment of e-government and e-commerce programs. The respective governments recognized the transborder flows of information that were already taking place, and wanted to assure that they had some type of control (and possibly income) from these existing connections (Ruiz, 2006). This type of control is not necessarily negative. Those in authority simply want to know what is happening.

Another example of infrastructure control is the debate over the liability of privately run Internet service providers (ISPs) in the flow of information over their networks. ISPs, organizations or companies providing the channels through which most Internet information flows, can be publicly or privately run. The truth is that, while the technology exists to monitor the information that flows through their networks, many ISPs, especially privately owned ones, do not. Governments have been engaged in policy debates about this issue of infrastructure control.

According to India's Information Technology Act of 2000, ISPs are not liable for criminal activity on their networks:

> For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. (India IT Act, 2000, p. 21)

But, complete autonomy is usually not possible. Subsequently, the law states that the police shall have authority to enter any establishment and search its electronic records (p. 22) if the situation merits.

The United States is addressing this same issue through proposed legislation to update the Foreign Surveillance Act of 1978. U.S. lawmakers have hesitated to protect ISPs in the name of civil liberties.

> The companies are hamstrung from defending themselves in court, however. The Bush administration is invoking the 'state secrets' privilege to block the companies from revealing secret documents that might bolster their argument that the eavesdropping program was legal. The House compromise bill would encourage the federal district judge hearing the telecommunications lawsuits to review those classified documents in secret to determine whether the companies acted legally. (Hess, 2008)

Personal/Individual Information

The privacy of personal information has long been a topic of discussion in national parliaments, especially in more democratic societies. Some have passed laws and others have not. Because cultures understand privacy from differing perspectives, it can be difficult to pass laws on this topic. The difference in the culture of privacy is readily apparent in information-related discussions between the United States and the European Union (see Rogerson & Strauss, 2002). In order to formulate and implement a privacy policy or program, governments must control information somehow, usually limiting the information that can be collected or stored by governments or private industries. For example, the European Union Convention on Cybercrime recognizes a right to privacy: "Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for

the Protection of Individuals with regard to Automatic Processing of Personal Data" (EU Convention on Cybercrime, 2001, Preamble, paragraphs 10 and 11).

This is not always the case, and in other countries, information on individuals does not receive the same type of protection. For example, Kazakhstan has passed the "On Protection of State Secrets of the Republic of Kazakhstan," which de-emphasizes individual privacy in favor of more official information.

Commercial Information

Countries may also have policies pertaining to commercial information, that is, financial transactions, e-commerce, online taxation, etc. In some cases, these policies may be deregulatory in nature and designed to stimulate growth according to free market principles. In other cases, they may be regulatory in order to provide stimulus or monetary infusions into a region. The East African Community has started a program called The E-Legislation Policy Development Initiative:

> The primary objective of the project is to create model electronic transactions laws piloted in Kenya that can be customized for the East African Community partner states of Uganda, Tanzania, Rwanda and Burundi. The initiative is in recognition of the fact that eTransactions laws have the potential to generate significant economic and political development for Kenya and East Africa as a whole. (Ouma, 2007)

This program recognizes both the nature of information to cross borders and the desire of governments to be involved in the development of the project, and thus have some control of the information that flows through the newly created networks.

News and Media Coverage

Information policies may also be initiatives to limit media coverage. For example, the Russian government attempted to control coverage of its conflict with the breakaway province of Chechnya, some of which was based on its existing media laws:

> On 4 November [1999], the Russian Information Centre and the military General Staff summoned executives of Russia's leading TV and radio companies to draw up plans for broadcasts to Chechnya and adjacent regions. All the reports, both from Moscow and locally, will be prepared under the aegis of the Russian Information Centre and will be transmitted in Russian and possibly, in time, also in Arabic, Russia TV reported. (Feuilherade, 1999)

Some countries have media laws that delineate the types of information that are or are not appropriate to publish or broadcast. Few countries have freedom of speech and press laws similar to those found in the U.S. Constitution.

Worms and Viruses

Finally, there is a category of laws that targets hackers and those who maliciously send worms, viruses, and Trojan horses across information networks. Japanese law enforcement reported that, in December 2002 alone, there were 58,000 hacker attacks against Japanese police computers. More than 40% of the attacks came from Israel, 20% from the United States, 9% from Japan, and 7% from South Korea. More than 90% of the attacks were simple preparatory attacks to see what programs were on the police computers, but the remaining attacks were serious attempts to close down the computers. So, in 2003, Japan passed a law that would criminalize these activities, even those that were simply preparatory in nature. In addition, it created a monitoring center to track down the offenders (Seeman, 2003).

RATIONALE FOR SECURING THE INFORMATION

The second research question is identifying the rationale—stated or inferred—for passing the law or implementing the policy. These fall

into three categories: (a) defending national interests, (b) protecting the citizens, and (c) facilitating cross-border information-sharing.

Defending national interests is the largest category and has a number of components. There is always an interest in using military and defense as a rationale for limiting the flow of information. Countries want to protect intelligence in times of conflict so that the "enemy" will not discover sensitive information and to protect—as much as possible—those who are on the ground fighting. In 2006, Chinese government officials published a report entitled "China's National Defense in 2006" that states that China is pursuing a three-step development strategy to modernize its national defense and armed forces that includes building "informationized armed forces" capable of winning "informationized wars" by 2050 (Greenemeier, 2007, p. 2).

Also in the arena of security issues is maintaining control within borders. Again, China provides the example. The Chinese government has a reputation for censoring speech that comes through the Internet, though it is not the only country to do so (see Kalathil & Boas, 2003).

> While the GFW [Great Firewall] protects the government from information assault from without, internally another system applies [also known as the Golden Shield]. Vaguely worded laws against any speech judged seditious, superstitious or merely "harmful to social order" give officials wide discretion to punish those who post or host sensitive content. But the main burden of routine censorship is left to internet service providers and suppliers of content. (Dickie, 2007)

And, since the latter groups can be targets of government crackdowns as easily as individuals, they are often willing participants. While not suppressing opposition completely, China has succeeded in limiting the impact of some societal groups through this censorship and monitoring, resulting in a tilt toward the ruling party's desired policy.

A second rationale is protecting citizens. This could be protection from worms and viruses, as in the Japanese example cited above. It can be in the form of regulating annoyances like spam (unsolicited commercial e-mail), as with the CanSpam Act of 2003 in the United States. But the language of protection has also been utilized more broadly. In South Africa, parliament passed the Electronic Communications and Transactions Bill, which was designed to protect citizens from cyber-terrorism. Given the broad language of the bill, there were bound to be critics: "The new law was strongly criticized, especially by the Democratic Alliance party, which voted against it, and by internet freedom organizations and private firms. The law allows telecommunications minister Ivy Matsepe-Casaburri to appoint inspectors to monitor telecommunications networks and their content, which they are authorised to seize" (Reporters Without Borders, 2003, p. 103).

In one case, a policy strongly reflected damage that was inflicted on citizens. In April and May 2007, the Estonian government was subjected to a number of denial-of-service attacks on the country's Internet infrastructure. The event incapacitated banks and government institutions (Finn, 2007, A1). The Estonian parliament responded later that fall, voting for a change to the country's penal code. "A computer attack would become an act of terrorism when committed with the same aims as a conventional act of terrorism. Under existing law, crimes of terror are crimes whose goal is to seriously upset or destroy the country's political, constitutional, economic or social order" (Estonia Gets Tough, 2007). The reaction of Estonians, and of the tech-savvy ones in particular, provided a pull toward citizen protection in subsequent policies.

In early 2012, negative citizen reaction to the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA) resulted in a number of policy-makers changing their minds about how they perceived the legislation. At least some of the credit for this change has been attributed to the citizen outcry (Schmitz, 2013, p. 213), which pulled the policy-makers away from what initially seemed to be easy passage of the legislation. This, in particular, provides a salient example of the role that citizens play in the tug-of-war, not just political figures.

A third category of explanations for information-securing policies is that they facilitate cross-border information sharing. As seen in the Kenyan and East African Community (EAC) examples, there is a desire to take advantage of already existing networks and connections for the benefit of the state. One reason is to exchange information about criminal activity. The EAC "began harmonizing its laws to prosecute cyber criminals operating across national boundaries" (Ouma, 2007). It is not always easy to get information about hackers or other cybercriminals who do not live within national boundaries. The EU Convention on Crime, for example, is particularly focused on tracking down those who distribute child pornography, the only content-related offense in the convention. Chapter III of the convention is entirely devoted to international cooperation and sharing of information. At the same time, the convention allows for countries to make individual decisions on bilateral arrangements with each other.

CIRCUMSTANCES AROUND WHICH INFORMATION IS SECURED

The rationale is the stated reason for which a policy has been proposed or adopted. The circumstances are the unique situations that might have led to the policy's proposal or adoption. While each circumstance or situation can be distinctive, there are some trends. At this point, most information policy adoption or change seems to be in response to some type of threat.

The most visible and most cited threat is terrorism, both online and offline. The Australian Cybercrime Act and the policy changes in Estonia, while not defining terrorism as others might, were proposed, adopted, and implemented because of what each interpreted as terrorist acts. The Australian parliamentarian explicitly stated that he proposed the bill because of the events of September 2001, and the Estonians were responding to what they felt was a terrorist attack from the Russians.

The expansion of cyber-related research funding is another type of policy reaction. Since September 2001, the United States and Israel have been working together on information security and monitoring programs, which, according to Mark Last of Ben-Gurion University of the Negev, are designed to predict future terrorist activities and targets by searching Web pages, e-mails, and other online data: "It may be nerdy mathematicians and computer scientists who have as much to do with victory in the War on Terror as conventional warriors. Perhaps in response to the shutdown of Terror Information Awareness, the US is quietly funding research in Israel designed to detect terrorist use of the Internet" (Abbey, 2004). Other programs include developing mathematical models to locate specific terrorists and their activities. The National Institute for Systems Test and Productivity, a U.S. government-funded research institute operated by the University of South Florida, is financing the research.

Some refer to these threats in a less provocative way, calling them antigovernment hackers. In 2000, the government in Azerbaijan claimed that Armenian hackers attacked the country's ISPs. During the Armenian–Azerbaijani "electronic war," the Web sites of all large Internet users, including humanitarian organizations, in Azerbaijan were hacked into and vandalized. The e-mail connections of all major Azerbaijani newspapers were severed. A site posting incorrect information about Azerbaijani President Heydar Aliyev appeared. Armenian State Television and Armenian Assembly in America sites were attacked in retaliation. In response to some pressure from these organizations, the government created a new technical council to deal with the matter. Members included experts from the National Security Ministry and owners and operators of ISPs (Azerbaijan to Secure, 2000). While the government itself was not attacked, policy-makers were persuaded that an attack on the institutions of Armenian civil society were a threat to the country and thus were pulled toward acting in the interests of those institutions. It might be argued that the creation of a council is not a very effective response, simply contributing to an increased bureaucracy. But, the council would not have been established without the pressure from the groups that were attacked.

Another threat is that to personal information. Some believe that governments can use legislation and programs to gather personal information about their citizens and use it against them. In Pakistan, the parliament passed a bill to "Make Provision for Prevention of Electronic Crimes." While much of the legislation mirrors other cybercrime laws from around the world, it also includes the creation of a new government agency: "The Federal Government shall establish a specialized investigation and prosecution cell within Federal Investigation Agency [FIA] to investigate and prosecute the offences under this Act" (Pakistan, 2007). An anonymous Pakistani blogger known as Teeth Maestro responded in this way:

> The FIA has been given complete and unrestricted control to arrest and confiscate material as they feel necessary, without forcing them to present a credible case before an arrest warrant is issued, if the FIA follows the law by the book they can pick up any person or property, hold them in custody for up to one year (extensions allowed) before even presenting the case in court. A very dangerous supposition as it opens the door for the rouge FIA agency to do as they please *without any safeguards and protection for the innocent.* (Maestro, 2007, emphasis in original)

While the blogger's commentary did not seem to result in any policy change in the end, the very existence of it exemplifies the attempt.

A final threat is not being at the cutting edge of economic competitiveness in an age of global information flows. A number of policies were aimed at opening up borders and sharing information, under very specific conditions. The interests involved were represented by the private sector. In these cases, governments seem to see the value of more open information flows with the goal of economic development. They are open to partnerships with business to encourage and facilitate this. While there was no immediate evidence of private sector pull on policy change, research has provided some empirical and theoretical support that this could be the case (see Browne, 1998).

THE INFORMATION POLICY TUG-OF-WAR

What, then, best explains the processes that result in the formation of information security policy? Information security policy is the result of the choices of a conglomeration of independent political actors, having their own set of interests and goals. By understanding how these forces act and counteract each other, the end result is clearer, i.e., the actual information security policy adopted by a particular county. There may be a wide variety of actors in play, but the policy results differ depending on the institutions that empower those actors.

Imagine a game of tug-of-war between two actors. There is usually a flag somewhere in the middle of the rope, which helps signal when one player wins. To determine the actual location of the policy, in our case the information security policy, we should look at the location of the flag in the game. Once the tugging begins, how is the location of the policy determined? It could be a result of the relative strengths of the actors or the geography of the terrain upon which they stand. Indeed, there is a variety of factors that would determine how the policy will fluctuate as the competition continues.

Now imagine that more actors are added to both sides. The location of the flag shows where the policy stands. Figuring out what influences the location of the flag entails analysis similar to the discussion above, but more detailed. The actors pull from different directions because, presumably, not all actors share the same point of view. Instead of a straight line of competing actors, there is now a web of forces that compete to move the policy closer to their preferred point. The more the policy-making process resembles a web, the more subtle changes in the location of the flag might not be noticeable in such an atmosphere. This is interesting, because when there are noticeable changes in the location of a policy, it is a signal that a number of actors were able to move their ideal points close enough to each other such that they had enough political

strength to move the location of the policy. To understand what has affected the location of policy, multiple factors come into play, not just the number of voters for or against the policy proposal.

This model posits that the location of actors and information security policy in a policy space is not directly contingent on the type of government. If this were the case, democracies should have information policies similar to other democracies and autocracies to other autocracies. While the type of government does influence the ability of actors to shift the local of information security policy, both have a variety of types of policies, even though democracies have many actors and factors that can affect the process, as opposed to the relatively fewer actors that may exist in an authoritarian government. The type of policy in a democracy might, therefore, also be the result of international and domestic factors that result in the "lining up" of actors on either side of the tug-of-war policy game. The lax or strict nature of information security policy in a given country seems to reflect more the relative strength of one policy position versus another.

Who are these actors? A principal actor is the executive of a government. The theoretical assumption is that the executive in a democracy has an interest in promoting and adopting a policy that results in flexible regulations regarding information security. Flexible regulation gives the executive more discretion on whether to release sensitive information. This does not mean tht the executive will always choose to be secretive rather than to be open, but merely reflects the fact that the executive would prefer to have the choice rather than having the limit defined by the legislature. Executives have the desire to retain their office and to work effectively within it. To do so, they must maintain public support, which may be damaged by a more complete disclosure of his policy actions. The executive in an autocracy is worried about long-term self-preservation, so policy decisions made at the top level could be described in a similar way: wanting the choice to reside there, regardless of the substance of the choice.

Other branches of government are also participating in the tug-of-war. Each separate actor represents a separate point in the policy contest. The role of the legislature is paramount, as it passes the laws that define the rules regarding information security. Within the legislature, ideological and social factions exist that have important functions. Some may agree with the executive and not want to place limits on the office itself, while others may want to offer a more concrete check on executive power. In this case, less flexible standards regarding information security may assist them in exercising an oversight role more effectively. When the standards are less flexible, or more defined, then it is easier to detect violations of the standard. While the legislative branch in an autocracy may fill the role of a "rubber stamp," its existence still provides a visible and publicized action to which the autocrat can refer to for legitimacy.

Interest groups may also play a role in the policy-making process regarding information security policy. These groups can be represented by media organizations that exist in single or multiple markets. International organizations such as Amnesty International and Human Rights Watch also have desires for favorable information security policies. The role of these groups is twofold. First, they desire and press for laws that allow for access to information. Second, they act as watchdogs that call attention to excessive government secrecy or lack of information on important issues. Other institutions that take part in this tug-of-war include the media and other representatives of civil society, such as religions or ethnic groups or ad hoc citizens groups.

CONCLUSION

This article illustrates a paradox: The countries that should be the most interested in protecting information are those who (under certain conditions) will abuse information just like every other nation. While this analysis has illustrated some of these conditions, these findings certainly do not represent the final word. Rather, they provide concepts that can illuminate some of the nuances of the tug of war.

Understanding policy give and take, or tug-of-war, has vexed scholars for some time. The

results have begun to converge onto processes that fold back on themselves, responding to feedback and playing off other actors' actions, such as James Anderson's (2011) policy cycles or John Kingdon's *Policy Primeval Soup* (2011, Chap. 6). While the "tug-of-war" we propose does not encompass every part of the policy process, it sheds some light on the actors' actions, especially in the context of information and technology.

First, even though the multiple-actor tug-of-war is an appropriate visualization, outcomes differ depending on the types of information that governments are trying to control. The Singaporean case illustrates the fact that even though there is sufficient political will to extend information access to all citizens, there is still little expectation that the desire for openness in this area will lead to less security in terms of how the government chooses to monitor this extended information access. Labeling countries as "open" or "secretive" must be done very cautiously, as this designation might be more fitting in some circumstances as opposed to others.

Also, this tug-of-war usually means that incrementalist policy-making is the norm (Birkland, 2005, p. 216): small changes and adjustments in existing policy or new policy that does not create a lot that is new. For example, the U.S. anti-spamming policy only criminalizes misleading subject lines (Can Spam Act of 2003) and the 2006 amendments to the India IT Bill that limit its impact. But, there are exceptions when one group in the tug-of-war is stronger, such as with China's censorship policies or when multiple groups come together, such as with post–September 2001 U.S. policy.

A second related point addresses the impact of democratic principles and ideals and addresses the normative question brought up earlier. The results are definitely mixed. Democracies, when faced with threats from others, limit their openness in favor of greater protection. This conclusion is not robust and may depend on other factors, as demonstrated by the debate of updating the Foreign Intelligence Surveillance Act (FISA) statutes. There is a clear opposition in the U.S. Congress toward limiting civil liberties, although it is hard to say whether or not this opposition represents a normative distinction between actors trying to influence the location of the policy or whether it represents a simple political fight. Generally it seems that even democracies exhibit closed-society tendencies from time to time, despite the continual debate over openness vs. secrecy.

Third, there appears to be a clear connection between the ability to effect change in information security policy and the threat of terrorism or war. Issues of national security have a strong influence. There is a tendency by governments and other interest groups to believe that information security policies can be instrumental in securing whatever stability or victory is sought in a conflict. This connection begs the questions of how and why this is the case, and would require greater study into the implementation phase of the information-related policies and programs.

Finally, there are some countries that place more of a cultural value on individual privacy than others, sometimes to the detriment of other global or national issues—and vice versa. These types of policies tend to ask implicitly that citizens give up some of their information control for the interests of the state. For example, the Electronic Crimes Act in Pakistan is designed to protect citizens from the consequences of online crime, but it also gives law enforcement greater latitude to intrude into citizen activities. The EU Convention on Cybercrime is an exception to this, but the European cultural commitment to privacy also seems to be different from the rest of the world.

Conceptually, then, a model of information policy-making along these lines would need to take into account the actors who have an interest in the formulation of the policy, the arguments that the actors are using to support their positions, and the circumstances under which the policy formulation is happening. First, as defined here, the actors include a broad range of political, economic, and societal groups, not all of which will be interested in every piece of information security–related policy. But, it is not too difficult to identify interested parties through a study of legislative hearings and media coverage. Second, the rationale or arguments in policy positioning can be identified through similar

sources: cataloguing statements and utilizing content analysis to uncover and understand them. Third, the circumstances require some historical and contextual research through archives and media coverage.

Throughout the policy-making process, there can be tension between actors and stakeholders: the policy-makers, interest groups, those in the private sector, citizens, and what Hsu, Liang, and Chen (2007) refer to as "technical elites," those practitioners who understand how the technology works. Some of these actors—especially the policy-makers—may have difficulty grasping the nuances of information security policy or even information policy more broadly defined. In 2012, Rose Gottemoeller, U.S. Acting Undersecretary for Arms Control and International Security, said that cyber-defense policy has been "slow moving due to the current generation of policy-maker's lack of technological understanding" (Kaiser, 2012). At a broader level, information security policies are also an example of the tension between decisions that are made in response very specific situations but whose consequences might be unforeseen. These two tensions inspire a potentially rich research agenda about the dynamic nature of information technology and its resultant security and/or transparency requirements.

REFERENCES

Abbey, A. (2004, May 6). Virtual Jihad. *Jerusalem Post.* Retrieved from http://www.globalsecurity.org/org/news/2004/040506-virtual-jihad.htm

Anderson, J. (2011). *Public policymaking*. Boston: Wadsworth Publishing.

Australia's Attorney General's Department. (2001, September 27). *New laws combat cyber terrorism* [Press Release]. Retrieved from http://www.crimeprevention.gov.au/Pages/default.aspx

Azerbaijan to secure Internet sites from Armenian Hackers. (2000, February 15). *Armenian Daily Digest.* Retrieved from http://www.eurasianet.org/resource/armenia/hypermail/200002/0021.html

Bernard, R. L. (2005, January 9). *IO Marines fight insurgency through interaction* [U.S. Military Press Release]. Retrieved from http://www.iwar.org.uk/news-archive/2005/01-09.htm

Birkland, T. A. (2005). *Theories, concepts, and models of public policy making*. Armonk, NY: M.E. Sharpe.

Browne, W. P. (1998). *Groups, interests and U.S. public policy*. Washington, DC: Georgetown University Press.

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (Can Spam Act). (2003). Pub. L. 108–187, §1, 117, Stat. 2699.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2008). *Access denied: The practice and policy of global Internet filtering*. Cambridge, MA: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2010). *Access controlled: The shaping of power, rights and rule in cyberspace*. Cambridge, MA: MIT Press.

Dickie, M. (2007, November 12). China traps online dissent. *The Financial Times.* Retrieved from http://www.ft.com/cms/s/0/ef0e7d64-9138-11dc-9590-0000779fd2ac.html#axzz28598ORX8

Estonia gets tough on cybercrime. (2007, September 17). *The Baltic Times.* Retrieved from http://www.baltictimes.com/news/articles/18815/

European Union Convention on Cybercrime. (2001, November 23). Retrieved from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Feuilherade, P. (1999, November 19). Russia's media war over Chechnya. *BBC News.* Retrieved from http://news.bbc.co.uk/2/hi/world/monitoring/528620.stm

Finn, P. (2007, May 19). Cyber assaults on Estonia typify a new battle tactic. *Washington Post*, p. A01. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html

Florini, A. (1998). The end of secrecy. *Foreign Policy*, *111*, 50–63.

Florini, A. (2004). Behind closed doors: Governmental transparency gives way to secrecy. *Harvard International Review*, *26*, 18–21.

Giacomello, G. (2005). *National governments and the control of the Internet: A digital challenge*. New York: Routledge.

Greenemeier, L. (2007, September 18). China's cyber attacks signal new battlefield is online. *Scientific American.* Retrieved from http://www.sciam.com/article.cfm?id=1A9C210F-E7F2-99DF-3C85F17B1680980D&page=2

Hess, P. (2008, March 11). House Democrats refuse to give telecoms immunity. *Associated Press.* Retrieved from http://www.law.com/jsp/article.jsp?id=900005560729&House_Democrats_Refuse_to_Give_Telecoms_Immunity

Hsu, N., Liang, J., & Chen, Y. (2007). Taiwan's information security policy enhancement: n analysis of patent indicators and patent documents. In T. E. Simos & G. Maroulis (eds.), *Computation in modern science and engineering: Proceedings of the International Conference in Science and Engineering* (Vol. 2, Part B; pp. 1228–1231). College Park, MD: American Institute of Physics.

India Information Technology Act of 2000. (2000). Retrieved from http://www.cyberlawsindia.net/itbill 2000.pdf

Innis, H. (2007). *Empire and communications*. Lanham, MD: Rowman and Littlefield.

Jones, P. (2012). The Arab Spring. *International Journal*, *67*, 447–463.

Kaiser, T. (2012, April 4). U.S. gov official: Current generation of policymakers lack understanding of technology. *Dailytech*. Retrieved from http://www.freerepublic.com/focus/f-news/2868152/posts

Kalathil, S., & Boas, T. C. (2003). *Open networks, closed regimes: The impact of the Internet on authoritarian rule*. Washington, DC: Carnegie Endowment for International Peace.

Kingdon, J. (2011). *Agendas, alternatives and public policies*. Boston: Longman.

Klosek, J. (2007). *The war on privacy*. Westport, CT: Praeger Publishers.

Lax, S. (2001). *Access denied in the Information Age*. New York: Palgrave.

Libicki, M. C. (2007). *Conquest in cyberspace: National security and information warfare*. Cambridge, MA: Cambridge University Press.

Maestro, T. (2007, September 8). *Draconian cyber crime law in Pakistan*. Retrieved from http://www.teeth.com.pk/blog/2007/09/08/draconian-cyber-crime-law-in-pakistan/

McChesney, R. W. (1996). The Internet and U.S. communication policy-making in historical and critical perspective. *Journal of Communication*, *46*, 98–124.

Milner, H. V. (2006). The digital divide: The role of political institutions in technology diffusion. *Comparative Political Studies*, *39*, 176–199.

O'Donnell, G., Schmitter, P. C., & Whitehead, L. (1986). *Transitions from authoritarian rule: Southern Europe*. Baltimore, MD: The Johns Hopkins University Press.

Ouma, M. (2007, August 5). Kenya's cyber law being developed. *East Africa Standard*. Retrieved from http://www.ifg.cc/index.php?option=com_content&task=view&id=23641

Pakistan: Bill to make provision for prevention of the electronic crimes. (2007). Retrieved from http://www.t2f.biz/events/wp-content/prevention-of-electronic-crimes-act.pdf

Reporters Without Borders. (2003). *The Internet under surveillance.* Paris: Author. Retrieved from http://en.rsf.org/IMG/pdf/doc-2236.pdf

Rogerson, K., & Strauss, J. (2002). Policies for online privacy in the United States and the European Union. *Telematics and Informatics*, *19*, 175–209.

Rosenzweig, P. (2013). *Cyber warfare: How conflicts in cyberspace are challenging America and changing the world*. Westport, CT: Praeger Publishers.

Ruiz, M. (2006, July 12). Internet law—Kenya, Uganda and Tanzania adopt cyber laws. *Internet Business Law Services.* Retrieved from http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1539

Sandoval, G. (2006, August 22). Now playing on the Net: War propaganda. *CNET News.com.* Retrieved from http://www.news.com/Now-playing-on-the-Net-War propaganda/2100-1038_3-6108004.html

Schmitz, S. (2013). The US SOPA and PIPA—a European Perspective. *International Review of Law, Computers & Technology*, *27*, 213–229.

Seeman, R. H. (2003). *2003 Japan law: Cybercrime cyberterrorism*. Retrieved from http://www.japanlaw.info/law2003/2003_CYBERCRIME_CYBERTERRORISM.html

Singapore cyberterrorism law raises fears of abuse. (2003, November). *The Hindustan Times.* Retrieved from http://www.crime-research.org/news/2003/11/Mess2401.html

Smith, D. (2012). *Russia cyber operations*. Washington, DC: Potomac Institute for Policy Studies.

Sullivan, B. (2004). *Your evil twin: Behind the identity theft epidemic*. New York: John Wiley and Sons, Inc.

Thompson, D. F. (1999). Democratic secrecy. *Political Science Quarterly*, *114*, 181–193.