Journal of Conflict Studies

Unlocking the Key to Authority: The Contest Over Encryption Regulation

Jeffrey W. Seifert

Volume 20, numéro 1, spring 2000

URI : https://id.erudit.org/iderudit/jcs20_01art08

Aller au sommaire du numéro

Éditeur(s)

The University of New Brunswick

ISSN

1198-8614 (imprimé)
1715-5673 (numérique)

Découvrir la revue

Citer cet article

Seifert, J. W. (2000). Unlocking the Key to Authority: The Contest Over Encryption Regulation. *Journal of Conflict Studies*, *20*(1), 140–172.

Unlocking the Key to Authority: The Contest Over Encryption Regulation

by

Jeffrey W. Seifert

INTRODUCTION

Advances in technology, and especially the development of the Internet, contribute to an increasingly fractured and competitive global political economy (GPE) by allowing for the rise of claims to legitimate rule-making authority by non-state actors. The motivating force behind these claims involves the protection of property rights. The new forms of property created in a bit-based political economy are not afforded protection by atom-oriented laws based on principles, such as scarcity and right of exclusion. Moreover, there is a very deep sense among the creators and owners of these new forms of property that actors and institutions other than states are the legitimate protectors of rights and promulgators of rules. The result has been increased activity by non-state actors to act as creators of rules and institutions, a role formerly thought of as reserved for nation-states. This, in turn, raises a number of questions about the changing nature of authority in the GPE. How will the Internet be regulated? Who will make the rules? How will they be enforced? How do we explain non-state groups' unwillingness to allow governments alone to make rules about electronic commerce and the Internet, and the apparent inability of states to do so? What is the relationship between state and non-state actors in developing rules for cyberspace in the GPE?

The international relations (IR) literature offers many competing and often contradictory answers to these questions. The qualitative changes in the GPE, brought about in part by the development and proliferation of information technology, as well as other contributing factors, such as the heightened role of finance, and increased mobility of people, have outpaced advances in theory. Much of modern IR theory development occurred as a result of the Cold War, a period of bipolarity rife with military tensions colored by the constant (even if at times unlikely) threat of nuclear war. It should not surprise us then that many of our conceptual tools are ill-equipped to explain phenomena in a post-Cold War world characterized by economic multipolarity but military unipolarity where strength is measured in initial public offerings (IPOs) instead of intercontinental ballistic missiles (ICBMs), and security threats comes less from nation-states than from terrorists. The proliferation of actors and the means to organize confounds many of the major principles of IR theory, including nation-state sovereignty, unitary actor decision-making and power. How then do we explain international cooperation, policy formation and coordination? To answer this question this article examines the regulation of encryption technology through a synthesis of two competing but complementary theoretical approaches; international regimes and epistemic communities. The goal of this article is to investigate the conditions under which the practices of non-state actors converge to form rules and institutions, especially when they

potentially conflict with the interests of state. In doing so, it will demonstrate how non-state actors have the potential to capture legitimate rule-making authority from states in specific issue areas, and will evaluate the implications of this process both for the state, and the GPE as a whole.

To that end, the rest of the article is organized in the following manner. The first section illustrates the policy parallels between the creation of the "rules of the road" at sea in the eighteenth and nineteenth centuries and the formation of the rules of the Information Superhighway. In the second section I locate the competing approaches used in this paper along a continuum of models of Internet governance and discuss why the regime and epistemic community approaches are the most practical and theoretically viable options for resolving global policy conflicts. The following three sections review the international regimes and epistemic community literatures and discuss the possibilities for future research by focusing on the role of rules in institution formation. The sixth section takes a more in-depth look at encryption regulation, including a brief history and technical review, focusing on the Clipper chip debate and export controls. The findings of these two issues are summarized in the conclusion, along with some suggestions for future research.

POLICY PARALLELS Rules of the Road at Sea

Although the continued development of the Internet as both a communications infrastructure as well as a locus point for political and economic activities presents new challenges to the rule-making authority of governments, it is not unprecedented. As developments in technology enhance an actor's capabilities, we often encounter situations where actors interact with other actors under new circumstances that necessitate the formation of rules and/or regimes to guide/regulate behavior. An example of such a scenario is the development of the rules of the road at sea by the international shipping industry, summarized below by James C. Roberts.

The dramatic growth of oceanic shipping in the eighteenth and nineteenth centuries sparked a direct regulatory interest in preventing collisions and determining fault when a collision occurred. In turn, governments developed legal interests in international efforts to codify a set of "rules of the road" for ocean vessels. Thus, a movement toward assessing civil damages generated a ruler of the waves during the last half of the nineteenth century.

Great Britain's Parliament enacted the first comprehensive rules of the road in 1862, but the rules affected only British ships or ships within British jurisdictions. The insurer, Lloyds of London, sponsored an international conference of private shipowners, shippers, and underwriters in 1864 to draw up rules of the road and insurance processing (McFee 1950:283). British representatives urged other nations to accept British laws as standard for their ships and sailing conduct. For the same purpose the United States (1890) sponsored an international conference in 1889. British agents drafted the shipping rules considered at the conference, which produced not a treaty but an agreement that formed the basis for many national laws on the rules of the road. Subsequent changes in the rules

introduced by Great Britain were often copied by other maritime powers. If Britannia did not rule the waves, it did at least rule the rules of the waves.

He continues,

In the formation of the navigation rules, practices developed among autonomous actors pursuing their own interests without the aid of an overarching government or coordinating institutions. Instruction rules constituted these practices that involved avoiding collisions, determining liabilities, calling conferences, and the like. Great Britain, the nation most vested in the rules because of its enormous fleet (McFee, 1950:279), actively argued to other nations that following the rules would lead to higher utility for each participant. In short, Britain attempted to make the rules regulative. Simultaneously, insurers strenuously pressured national governments to codify international rules to better enable the insurance carriers to resolve claim disputes. Thus, by making and following rules, international actors structured their relations, yet simultaneously, the actors were constituted by the relations and practices. A lone ship at sea is not constituted as an actor in the practice of the international rules. Only when the ship encounters another is it then constituted as an actor by those rules, for only then can it act vis-a-vis the structure of the system.[1]

Today the rules of the road at sea are governed by a combination of private agreements, national policies and international conventions. The fact that these rules evolved largely absent of government regulation can be attributed to several factors. One is the entrepreneurial spirit and colonial ambitions driving the early growth of oceanic shipping. Another factor is the geographic and product diversity inherent in the industry. A third factor is the lack of a natural monopoly that would stimulate the intervention of state regulation.[2]

Just as the growth of oceanic traffic in the 1700s and 1800s created the need, and ultimately the codification of the rules of the road at sea, the growth of the Internet as an infrastructure to support social, political and economic activities in the twentieth and twenty-first centuries is also creating the need to develop rules to govern the Information Superhighway. In this case, the entrepreneurs and activists of e-commerce, the geographic and substantive complexity, and the speed of change and influx of new actors, favor the creation of rules through private means.

There are currently several Internet policy issues that exemplify the struggle between states and non-states to establish and maintain legitimate rule-making authority in the global political economy. Some of these issues include taxation, oversight of the Domain Name Server (DNS), content regulation, privacy protections, online gambling and encryption regulation. The primary reason why Internet-related issues are so challenging to solve and interesting to study is the double anarchy of the medium. The Internet itself is an anarchical medium, controlled by no one. The Internet empowers users as effectively autonomous actors who engage in practices that converge to form rules that are applied across this anarchical medium within the anarchy of the international system. The transnational nature of Internet issues renders attempts to address them at the

national level largely ineffective. Moreover, these national efforts contribute to the obstacles that stymie efforts to promote cooperation between countries. To illustrate this struggle, below I summarize the circumstances surrounding privacy regulation and briefly introduce the central issue of this article: the regulation of encryption technology.

Privacy

Currently privacy rules in the GPE are represented by a patchwork of local, national and regional laws, and self-regulation practices. Many countries in Europe, such as Sweden, Germany and the Netherlands, have very strict privacy laws.[3] Indeed the European Union as a whole instituted its Privacy Directive on 23 October 1998. Under this law companies are prohibited from using customer information in ways not intended by the customer, such as selling the information as a marketing tool or the "processing" of health data by non-medical personnel.[4] In addition, the law mandates that companies must inform people when and what information is being collected and what it will be used for. They also must provide a person with a copy of the collected information "in an intelligible form."[5] Perhaps the most controversial provision of the Privacy Directive is Article 26, which restricts the transfer of personal data (with some well-defined exceptions) to third countries that do not provide "adequate" protections.[6]

With the potential to disrupt electronic commerce, Article 26 raises a number of questions about data transfer to countries, such as the United States and Japan, which take a self-regulation approach to privacy. Pressured by industry organizations and lobbyists, who argue that strict privacy measures would post an undue burden and expense, and would hinder economic development, the US has so far chosen to maintain its self-regulation position. However, a series of surveys of popular web sites by the Federal Trade Commission (FTC) has consistently shown lax privacy policies regarding the collection of personal information with little improvement over time.[7] The appearance that self regulation is not working has been reinforced by incidents, such as the discovery of a Global Unique Identifier (GUI) tracking number in Microsoft Windows 98 and the recent revelation that RealNetworks's popular program RealJukebox, used to listen to CDs and MP3 files on computers, was surreptitiously monitoring and transmitting the listening habits of its users back to the company.[8]

These results spurred some privacy advocacy groups to renew their call for formal regulations while industry groups, such as the Online Privacy Alliance, promoted new guidelines for self-regulation and technical solutions, such as the use of encryption.[9] In an effort to rehabilitate the practice of self-regulation, the Council of Better Business Bureaus' Internet subsidiary, BBBOnLine, is now administering a privacy certification program. With the support of nearly 300 e-commerce companies, the hope is that the BBBOnLine program will satisfy the demands of the European Union without requiring new laws.[10]

At the other extreme is the "Big Brother" approach to privacy, favored by less democratic countries, such as Russia and China. In these cases, where governments actively eavesdrop on all forms of communication, electronic privacy is virtually non-existent. In

China, the government tries to monitor the content of e-mail through electronic means by requiring all Internet services to connect to the Internet through four interconnected, state-run, networks. Two are commercial networks; ChinaNet and China Golden Bridge Network (ChinaBGN) and two are academic networks; China Education and Research Network (CERNet) and the China Science and Technology Network (CSTNet). These networks, in turn, are under the full regulatory control of the Ministry of Information Industry, established in March 1998.[11]

The divergence of goals, perspectives and laws (or lack thereof), as well as continual technological developments, undermine attempts to harmonize national laws and coordinate international privacy rules. Since electronic flows, such as e-mail do not follow fixed routes, but instead stream through a random number of countries and servers, there is a great deal of uncertainty about the privacy protections actually afforded one's data.[12] Finally, the emergence of new actors and technological developments has so far mitigated against international coordination through traditional means and organizations, such as the United Nations.

Encryption

In contrast to the other two issues described, the encryption debate is about much more than just property and privacy rights. It also encompasses issues related to law enforcement and national security concerns, such as countering terrorism or preventing the proliferation of Weapons of Mass Destruction. Consequently, a larger and more diverse group of state and non-state actors compose the active encryption policy community. Some of these actors try to influence the debate not only through the more traditional policy means, but also through the development of technologies that support their policy goals. The encryption issue is also remarkable because it represents a technology that until the 1970s has been monopolized by military and intelligence services in the name of national security for most of this century. Since that time commercial interests, privacy advocates and civil liberties organizations have gained a sizable stake in the technological and legal development of encryption techniques, challenging the authority of the nation-state. However, before we can investigate this issue in more detail, we must first examine the conceptual tools used to try to explain the changes in rulemaking in the global political economy.

A CONTINUUM OF INTERNET GOVERNANCE

There are numerous models of Internet governance. Using James Rosenau's broad conceptualization of governance, we can think of Internet governance as the authority structures/relationships between actors (both state and non-state) "that amount to systems of rule in which goals are pursued through the exercise of control."[13] To capture the range of possible rule systems, I have created a scale of Internet governance models[14] (rule systems) ranging from highly informal rule systems at one end (markets, self-regulation schemes), to highly formalized rules systems (world government), at the opposite extreme (see figure 1). Between these two extremes lie a variety of rule systems including different forms of regimes, epistemic communities and national law. Due to

space limitations, it is not possible to compare the merits of each rule system in detail here. However, a very brief review of the major points on the continuum is provided to locate the models in context to the larger argument of the article.

Informal Rule Systems									Formal Rule Systems
	Markets	Self Regulation	Epistemic Communities	Private Regimes	Mixed Regimes	National Laws	Interstate Regimes	World Government	

Figure 1. Internet Rule System Scale

The cyberspace as anarchical space model views the Internet as a separate space with its own unique properties of sovereignty/authority. This model, put forward by David Johnson and David Post, attorneys who specialize in "cyber law," argues that a new type of space, Cyberspace, has been/is being created by "screens and passwords that separate the virtual world from the Ôreal world'."[15] The boundary is represented by the password/screen, comparable to crossing a state line or a custom's post between two countries. It delineates a new space that needs to create its own new laws and legal institutions that will differ from territorially based laws. If we follow this model to its logical conclusion, then countries do not have the power to enforce laws in Cyberspace, just as they do not have the power to enforce their laws outside their geographic borders.

At the other end of the spectrum, the cyberspace as supranational space model assumes the existence of some form of a world government, arising from nation-states. Although more of a theoretical possibility than a realistic probability, this model is a hybrid of the cyberspace as anarchical space model and the cyberspace as national space model. On the one hand, this model treats cyberspace as international space, although not separate from the "real world," but beyond the control of any single sovereign nation-state. On the other hand, this model assumes that a single governing body can subsume and mollify the various competing, and at times intense, ideologies and rule systems into a coherent whole. The form such a government would take can only be speculated. One possibility is that some part of the United Nations, such as the International Telecommunications Union (ITU), is vested with the authority to decide Internet issues. This is more of a state-based scenario that is unlikely to emerge in the foreseeable future, if for no other reason, than there are numerous other non-state groups that claim some authority to decide different facts of Internet governance, e.g., Internet Engineering Task Force (IETF), Internet Architecture Board (IAB), Internet Corporation for Assigned Names and Numbers (ICANN). An alternative scenario for this world governing body model is that it could develop out of ICANN. Indeed, that is a fear of some Internet constituencies. However, at the present, the inability of ICANN to effectively manage the issues it was originally mandated to do mitigates against the chance it will be able to expand its influence to other areas of Internet governance.

Compared to the second model, the cyberspace as national space model is more probabilistic but no more likely to succeed. In contrast to the first model, the cyberspace

as national spaces model views the Internet as another technology to be regulated by national laws. This is a model advocated most often by national governments, especially authoritarian governments such as China, Singapore and Guatemala, but also by more democratic governments, such as the United States. However, it is also the least suited to a global technology, such as the Internet.

On the one hand people do not live "virtual" lives, they live "real" lives. A person logs on to the Internet from a real, physical location. As such, these activities are subject to the laws and regulations of the city, state or country where the person is located. On the other hand, the problem with this model is that the Internet is a global medium. Laws imposed by one city, state or country, can affect users in other parts of the world, which in turn is a challenge to the sovereignty of the other countries.[16] For example, if country A outlawed all pornography websites, then people in country B, where pornography is legal, are having restrictions imposed on their free speech. However, if country B does not enforce country A's law on pornographic websites and allows people in its country to establish such sites, then country A's law is effectively undermined because the Internet is a global medium that can be accessed from nearly anywhere in the world. So, it is both impractical and unacceptable to other countries for one country to try to impose its laws over the Internet.

A fourth governing model for the Internet is the creation of international regimes to regulate various aspects of the Internet. A common feature in international relations, regimes are developed to address transnational problems/issues that require the cooperation of many countries (and non-state actors), and that cannot be solved by any one country/actor alone. For example, many people and countries cause environmental damage to the ozone layer. If only one country imposed strict environmental controls, while that would help the problem to a small degree, it would not address the core issue that everyone needs to cut down on emissions. Moreover, the one country that did enact strict regulations would probably not realize the benefits of its actions because environmental problems, such as a hole in the ozone layer, do not respect country borders. Other issue areas that have been the subject of international regimes include the use of oceanic resources, nuclear proliferation, technical standards and human rights.

The Internet, being a global medium that is not "owned" by any one country, company or organization, lends itself to being governed by some kind of a regime. There are already some attempts to regulate certain aspects of the Internet through the use of a regime, such as the DNS and digital certificate authorities.[17]

Related to international regimes, a fifth governing model for the Internet is the mobilization of epistemic communities. "An epistemic community is a network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area."[18] These knowledge communities could create policy or at least influence the process. The impact of epistemic communities in international relations has been well documented, especially in environmental issues.[19] However, epistemic communities are also likely to play a role in science and technology issues generally due to their highly complex and

technical nature, which contributes to a high degree of "irresolution" among policy makers.[20] Driven by this irresolution and the growth of the administrative state, decision makers who are required to address a larger range of issues, such as macroeconomic, health and population concerns, can be expected to look to epistemic communities for information and guidance in policy decisions.[21]

It is not hard to imagine how the Internet, which was created and developed by a loosely organized group of like-minded, talented individuals, could be governed through an epistemically influenced governance structure. An example of this can be seen in the development of standards for making web content accessible to people with disabilities. Within the Internet population exists an epistemic community of web content developers, programmers, academics and concerned individuals who share the normative view that the Internet should be accessible to all users, regardless of visual, audio or other physical impairment. This community works to develop standards and technology to overcome the barriers to access. While they utilize a variety of methods, their overarching goal of accessibility is advocated through the World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines.[22] Based on their research and technology development, the Web Accessibility Initiative (WAI) serves as the central authoritative locus of expertise on access issues. The WAI promotes its ideals of accessibility through a list of "checkpoints" designed to help web content developers create accessible websites. The WAI also strives to use its guidelines, which were developed through an open-consensus forum, to educate policy makers to ensure not only that government information and services delivered over the Internet are accessible, but also to encourage legislation that promotes its objectives. As the issue of Internet accessibility moves up the policy agenda, we can expect policy makers to look to this community for information that will be used to guide policy decisions.

Summary

From this brief review of Internet governance models it is clear that neither all-public nor all-private governance systems are likely to produce long-term stable results. Regulating the Internet involves the cooperation of many different actors including countries, businesses, interest groups, etc. Moreover, the world's Internet users must view the process as legitimate. The question then is what combination of private/public cooperation is likely to prevail in rule making. The regimes and epistemic communities models identified in this section provide a means to explore this question and develop a more comprehensive understanding of international policy cooperation and conflict. In the next two sections I review the basic tenets of regime theory and epistemic communities in more depth and demonstrate how these conceptual tools can be applied to studying the role of rules in policy coordination.

REGIME THEORY: A PROMISING BUT INCOMPLETE APPROACH

The widely accepted definition of international regimes was put forth by Stephen Krasner in his influential 1983 edited volume, International Regimes. Here, he and the contributors to the volume define regimes "as sets of implicit or explicit principles,

norms, rules, and decision-making practices around which actors' expectations converge in a given area of international relations." Krasner goes on to define principles as "beliefs of fact, causation, and rectitude," norms as "standards of behavior defined in terms of rights and obligations," rules as "specific prescriptions or proscriptions for action," and decision-making procedures as "prevailing practices for making and implementing collective choice."[23]

Many different schemas have been used to categorize the various disparate approaches to international regimes.[24] However, it is Oran Young's work on institutional bargaining - "bargaining with the objective to create an institution" - that serves as the best regime approach to explain rule formation in the GPE.[25] He is one of the few regime theorists who has focused heavily on developing a model of regime formation. One of the primary advantages of his approach is that it prioritizes process over structure, in contrast to rational choice approaches, which emphasize structures. While structural factors are not entirely unimportant, a process-focused approach gives the opportunity to examine actors' actions that structural approaches assume away. The institutional bargaining model "treats states as selfish actors confronted with both the possibility of achieving joint gains through cooperation and the difficulty of settling on specific norms and rules."[26] Young's model is based on several assumptions about the bargaining environment. One of these assumptions is that institutional bargaining will succeed only if it takes place under contractarian terms. In other words, in order to avoid positional deadlocks, there must be a presence of a veil of uncertainty in which the actors are unsure of whether they will be in an advantageous or disadvantageous position if the problem is not solved to benefit the common good.[27] Young's model also assumes that exogenous shocks or crises will increase the chances of negotiating successful terms for the regime.[28]

Alternatives to Interstate Regimes

Despite the more progressive attitude of interest-based regime approaches toward non-state actors, they still ignore the possibility of non-interstate regimes. As Rosenau points out, the term Ôinternational regimes' is really "a misnomer because the rules, norms, principles, and procedures of many regimes . . . often involve a sharing of authority among NGOs as well as national governments."[29] Instead, it is more accurate to refer to regimes by the composition of their actors/members. Given the nature and secrecy of national security regimes, such as the START and SALT treaties, we would expect most of these types of agreements to be interstate regimes. However, there are many other issue areas in which non-state actors play a significant role, such as the environment, technology standards and banking. Haufler refers to regimes that are wholly or primarily dominated by private sector actors as "private regimes."[30] While there are numerous examples of purely inter-state regimes, very few purely private regimes exist. One that Haufler identifies is the global insurance industry.[31] More commonly found though are two types of mixed private-inter-state regimes. The first type involves states as the dominant players with non-states as either the target of regulatory action or functioning as subordinate partners. The second type occurs when non-state actors generate a regime of rules, norms and possibly even informal laws sanctioned by state authority.[32] It is important to note that private regimes do not include oligopolies or cartels since they are

generally considered illegitimate and illegal in most countries. Private regimes, on the other hand, "seek and maintain a degree of legitimacy and accepted authority for their rule within the larger society" through the development of norms and principles.[33]

Private regimes, as Haufler describes them, "exist when firms cooperate over issues beyond price, supply, and market share alone."[34] In other words, private regimes are formed to establish common practices, standards and/or goals. Given this broader set of objectives, it would be appropriate to speak of non-business actors, such as NGOs, interest groups and scientific organizations as possible originators and members of private regimes.[35] The successfulness/authority of a regime can be gauged by its ability to influence or govern "a wide range of behavior among those who created it and among many actors outside of it."[36] However, despite the utility of these more advanced regime explanations, we still lack a mechanism to describe how non-state actors join and affect the policy community. To that end, the epistemic communities literature provides some answers.

EPISTEMIC COMMUNITIES

Epistemic communities are defined as "networks of knowledge-based communities with an authoritative claim to policy-relevant knowledge within their domain of expertise."[37] What brings individuals together as an epistemic community is their shared "knowledge about the causation of social or physical phenomena" and a "common set of normative beliefs about what actions will benefit human welfare" within a specific issue area. Although often drawn from a variety of disciplines, these professionals share a common set of characteristics:

1) Shared consummatory values or principled beliefs;

2) Shared causal belief or professional judgement;

3) Common notions of validity;

4) A common policy enterprise.[38]

Additional characteristics of an epistemic community include shared-intersubjective understandings, a shared way of knowing, shared patterns of reasoning, shared discursive practices, and a shared commitment to the application and production of knowledge.[39]

While often associated with the scientific community, members of an epistemic community need not be natural scientists. They can be "social scientists or individuals from any discipline or profession who have a sufficiently strong claim to a body of knowledge that is valued by society."[40] In addition, epistemic communities can be (but are not always) transnational and do not need to meet regularly in a formal setting to promote their ideals. Instead, epistemic communities can diffuse its ideas worldwide "through conferences, journals, research collaboration, and a variety of informal communications and contacts."[41]

Contrary to the conventional view that epistemic communities must become part of the bureaucratic apparatus of the state to influence policy,[42] I posit that they can work either within or outside of the bureaucratic state structure. In the case of extremely technical issues for example, such as modem handshake standards and Internet protocols, where the state has no formal interest, or perhaps is even unaware that a standard is being developed, we could expect to see an epistemic community form and implement rules without involving the state. Moreover, while largely overlooked in the literature, it is possible to have competing epistemic communities trying to influence rule formation over a particular issue. We are especially likely to see this occur with issues that cross both technical, political, economic and/or social boundaries. Epistemic communities concerned with the best technical solution may come into conflict with an epistemic community more concerned with the social ramifications of a rule choice.

There are two primary reasons why epistemic communities arise. The most well-known reason is when the policies of one state export the costs of the policies to other states, requiring international cooperation. The second reason is the interest to learn and draw lessons from the experiences of others. Here the motivation is to increase the export of information instead of decreasing the export of costs.[43] In the case of many, although not all Internet regulation issues, it is this second motivation that drives the creation of epistemic communities. In the case of states, there is a interest in re-engineering governance mechanisms as some of their standard practices become less and less effective. In the case of non-state actors, they have a desire to learn governing techniques as they assume some of the regulatory authority once held solely by states. For example, in the issue of encryption export controls, there is an epistemic community of states that believes that national security issues override economic ones, and that economic goals can be adequately achieved even under heavy regulation. In contrast, there is an epistemic community of countries that believes economic concerns are of greater value than national security concerns and that export controls should be relaxed so that economic development may spread to other areas of the world. In the case of non-state actors, there is an epistemic community that strongly believes that privacy needs to be better protected and that strong encryption technology is the solution. Similarly, there is an epistemic community of business actors that believes strong encryption technology is necessary to ensure consumer confidence in online transactions and that this technology should not be regulated. There is yet another epistemic community of private actors who believes that export controls are a bad idea because of the technical flaws of weaker algorithms and escrow systems. We can gather from this simple example that there can be many competing epistemic communities that may join together on some issues for entirely different reasons while competing against other epistemic communities in an effort to influence policy outcomes through rule creation. In the next section I outline a strategy that explains how epistemic communities try to establish rules, and perhaps even regimes, in order to influence global public policy.[44]

THE ROLE OF RULES IN POLICY COORDINATION

Rules have been at the center of global relations for thousands of years. As Edgar Gold points out, the rules of the road at sea date back to Babylonian Law, codified by

Hammurabi around 2200 BC.[45] The growth and acceptance of rules contributes to the formation of regimes. The traditional and most widely accepted notion of regimes is that they are constituted by principles, norms, rules and decision-making procedures. However, an alternative approach is to utilize a model of regimes based on a conceptualization of different rule types drawn from Max Black's influential work on rules and their meanings.[46] Interpreting regimes as a product of rules and associated practices "that result from agents' choices in the face of these rules," is not a radical departure from the traditional notion of regimes. As Nicholas Onuf argues, principles, norms, rules and decision-making procedures are all rules. They are differentiated by their degree of "generality (principles and procedures) and formality (rules and norms)."[47] By drawing on Black's comprehensive categorization of rules, we address the first critique mentioned above by avoiding what Onuf refers to as the "uselessly imprecise definitions offered for principle, norm, rule, and decision-making procedure."[48]

According to Black, there are four main types or senses of "rule;" instruction, regulation, precept and principles, or general truths.[49] For the purposes of this article, I will only discuss the first two types of rule. The first, and most important is the instruction-sense rule. Instruction-sense rules are meant to provide direction or instruction on how to achieve some end or purpose. Perhaps the most well-known example of such a rule, put forth by Black, is "Do not plant tomatoes until after the last frost."[50] One of the defining aspects of instruction-sense rules is that unlike regulation-sense rules, there is no "penalty" for breaking the rule. Contrary to Black's belief[51] that these rules "have neither authors nor histories," Onuf argues that since all rules must be stated or are statable, and all statements have authors, then instruction-sense rules must be able to have authors. However, that does not mean we know the identity of the author. As Onuf notes, "People decide on the action indicated [in the instruction-sense rule] or not, and bear the consequences. The rules registers a long history of such decisions and thus has innumerable authors."[52]

The second type, or sense, of rule identified by Black is the regulation-sense rule. Unlike instruction-sense rules, regulation-sense rules have specific authors by virtue of the actor(s) who announce and enforce the rule. Examples of regulation-sense rules include traffic regulations and laws banning the exportation of specific items.[53] Regulation-sense rules are normative in that they specify what an actor must do (or not do) and the sanctions for breaking the rule.[54]

The purpose of focusing on instruction-sense and regulation-sense rules is to show the regime formation process more clearly, and account for the existence of private and informal regimes as well as inter-state regimes. The key to this approach is the use of instruction-sense rules. Instruction-sense rules are especially important to the formation of regimes in regard to issues where more formalized rules are weak, ill developed, or non-existent. As noted earlier in the rules of the road at sea example, instruction-sense rules played a pivotal role in the evolving regulation of oceanic shipping.

In a regime composed primarily of instruction-sense rules, we could say that actors are part of a "network of rules and related practices."[55] In this case the power of the rule comes from its utility, not from its author, unlike regulation-sense rules. This is why instruction-sense rules can have multiple authors, such as an epistemic community. Either non-state or state actors can author instruction-sense rules. In an instruction-sense rule regime there are no rules about rules. This allows relatively minor actors, actors who may not possess great power or wealth but instead have a useful solution to a problem, to be the authors of rules. In the case of Internet problems, technical solutions are often preferable to legal solutions because of their efficiency and/or low cost. This is one of the reasons why non-state actors have played such a prominent role in Internet regulation compared to other issue areas. Viewed from this perspective, it is not surprising that the Internet appears to be predisposed to being regulated by a "network of rules and practices" rather than a hierarchical rule system favored by states.

Instruction-sense rules represent the same function as norms in that instruction-sense rules are guideposts for standards of behavior that cannot be enforced in an official manner. If one were to break Black's most oft-cited example of an instruction-sense rule, "Do not plant tomatoes until after the last frost" one would not receive a fine from the plant police. However, the non-conformist may not have a very successful garden. As more actors adhere to an instruction-sense rule, we can speak of a convergence of behavior. We can also say that the rule is strengthened every time an actor chooses to follow a rule "by making it more likely that they and others will follow the rule in the future."[56] When this occurs, both the rule and the authors (if known) gain legitimacy over time, contributing to the formation of an informal regime. We can also speak of the authors of a popularly followed instruction-sense rule as having authority because other actors are following a rule they perceive to be legitimate but are not otherwise forced to follow.

The second part of the regime formation process involves the development of regulation-sense rules. It is then that the regime is formalized with specific duties, responsibilities and punishments outlined. The regulation-sense rules may represent a codification of existing instruction-sense rules or they may represent an attempt by an actor(s) to re-assert authority over an issue by authoring a new set of rules. Even if the regulation-sense rules merely re-affirm existing instruction-sense rules, we speak of the rules as being re-authored by the authors of the regulation-sense rules. However, this can also be interpreted as an acknowledgement of the legitimacy of the original instruction-sense rules and their authors by the authors of the regulation-sense rules. In a regime dominated by regulation-sense rules, actors are assigned a place or an office, relative to other actors in the regime. In other words, a hierarchy of some form exists where the lead actor (acting as the hegemon) can regulate/influence the behavior of the other actors.[57]

There are several advantages to this approach to understanding the formation of rule institutions, such as regimes. First, by utilizing a simpler, more straightforward model that relies on clearly differentiated stages of rule development, we avoid much of the conceptual ambiguity inherent in the dominant definition of regimes. Second, by accounting for different stages of rule and regime development (informal -> formal) and

different types of regimes (private, mixed, inter-state/public) we can better determine if an actor's behavior is in fact rule-governed or not, and we can better ascertain the effectiveness of the rule system by looking for deviations from the expected rule-governed behavior. Third, by including both state actors and non-state actors, such as non-governmental organizations (NGOs), transnational corporations (TNCs) and lobbying organizations, we enhance the explanatory potential of the regime and epistemic communities literatures to address the transnational issues that characterize the post-Cold War political economy, such as the environment, cultural conflict and Internet-related policies.

THE ENCRYPTION ISSUE - A STRUGGLE OVER PROPERTY RIGHTS

The heightened awareness and need to resolve Internet-related policy conflicts represents an ideal scenario to examine global rule formation. The enhanced role of information technology (IT) in global socio-politico-economic issues is revitalizing an interest in property rights. An increasing number of nation-states currently face the challenge of protecting the new forms of property being produced by the information economy while striking a balance with national security concerns. The rapid development and proliferation of IT in the last 20-30 years led to the revitalization or invention of many forms of mobile property, such as information and knowledge, credit, aliases and cybercash, to name a few. Today's "land, labor, and capital" are being replaced by new (often intangible) forms of capital, such as knowledge, as the principal economic resource.[58] IT spending by business increases each year. The information sector is one of the leading growth areas in the world economy and is revolutionizing almost all other industries. In manufacturing, information has become a new source of cost savings and profits. Inventory control, accounting methods and marketing is being made more efficient and effective through information controls. To compete in the information age businesses must invest in hardware, software, Internet websites and computer training. As part of this investment, business needs to ensure the security of their products and information, as well as that of their customers. The way they are doing this is to use encryption technology.[59] In the health care industry, the increasingly integrated systems of insurance records, hospital files and doctors' files have created the need to better protect confidentiality while not hindering access by authorized users. The entertainment industry has also developed a need for encryption technology to protect copyright.[60]

As the number of people on the Internet increases each year, so does the volume of online purchases. A person can now purchase and download intellectual property such as music, books, videos, software, technical reports, investment information, newspapers and other services via a website. Initially, the physical form of these products (books, CDs, tapes, etc.) contained inherent barriers (although certainly not insurmountable) to prevent, or at least make inconvenient, the illegal distribution or alteration of the product. Now that they are available in a raw digital format, many of these barriers have disappeared. Copying and distribution costs have decreased significantly, as represented by the robust market for pirated software in China, the growth of websites illegally hosting downloadable MP3 music files, and the mirroring of content from websites that charge a

fee for access. The ineffectiveness of legal solutions has increased the urgency for technical ones.

Whether for internal use or external distribution, the creators, owners and users of these new forms of mobile property - information, knowledge, intellectual capital - must be assured that their data is secure and their privacy is protected. Likewise, the consumers of these digital goods are concerned about the security of their transactions. They do not want their credit card numbers or other personal information to fall into the wrong hands. These merchants and customers, "like the cannon-carrying merchant ships of two centuries ago, must provide security themselves."[61]

However, in contradistinction to non-state actors' interest in data security and privacy, many states find that their interests in national security and law enforcement are being threatened, undermining their authority and sovereignty. Dyson highlights a number of potential scenarios, including drug dealers doing business on the Internet, money laundering, global criminal organizations operating across borders in secret, and terrorists attacking a target, such as a bank or government installation from a secure location in a renegade country.[62]

The United States government is one of the leading proponents of this view. Although the law enforcement and national security interests are very closely related and rely on the same basic rationale - unregulated strong encryption impairs our ability to protect ourselves as a country - there are some differences that affect which actors and epistemic communities may become active in trying to influence the policy community surrounding a particular issue within the encryption debate. Law enforcement has two primary concerns in regard to encryption. The first is their ability to wiretap telephone, fax, e-mail and other communications in real time. Wiretapping is one of law enforcement's most important tools, not only in investigation and prosecuting crimes after they have occurred, but also to prevent crimes before they happen.[63] One of the most oft cited examples by the US Federal Bureau of Investigation (FBI) was the importance of unimpeded electronic surveillance in breaking up a terrorist plot to "bomb the United Nations building, the Lincoln and Holland tunnels, and 26 Federal Plaza as well as conduct assassinations of political figures."[64] The catastrophe at the World Trade Center serves as a reminder of what can happen. The second concern of law enforcement is their ability to access and read data discovered under a search warrant. If captured information cannot be read then the value of such searches to help in prosecutions and crime prevention decreases.[65] Even with the encryption restrictions in place, due to limited resources and lack of qualified experts it can sometimes take years for federal investigators to evaluate data collected from hard drives and other seized equipment. There are currently over 100 hard drives waiting to be examined in the Dallas, Texas labs of a federal cybercrime taskforce and only three forensic experts able to look at them.[66]

The national security community also has similar concerns about encryption diluting their capabilities. Its primary concern is over signals intelligence (SIGINT). SIGINT represents "the most important source of foreign intelligence for our national policymakers."[67] One example of this is Echelon, a computerized communications

surveillance system established after World War II by Britain, Canada, Australia, New Zealand and the United States, although not publicly acknowledged until this past May. Echelon is capable of monitoring "millions of e-mail, fax, telex, and phone messages sent over satellite-based communications systems as well as terrestrial-based data communications."[68] As a result, the national security community wants to prevent the easy export of strong encryption technology, especially that embedded in shrink-wrapped applications (i.e., e-mail programs) and hardware.[69] The national security community is concerned that ubiquitous encryption technology abroad will make it more difficult to fight against drugs and terrorism, and in turn will lead to a decline in the US position in the world.

Taken together, law enforcement and national security interests are in conflict with the competing interests of civil liberties groups (privacy), industry (protection of intellectual property), and technologists (protection of information networks, including critical national information systems and networks).[70] Two issues that illustrate this conflict are the Clipper chip and the debate over export restrictions. However, before we can examine these issues, we first should have a brief understanding of the history of encryption technology and how it works.

Brief History of Encryption

While the encryption debate is relatively new, the encoding of communications was in use long before the computer was invented. Cryptography is the encoding of plain text messages into ciphertext, or codetext, rendering it unintelligible to unintended recipients of the message. In contrast to steganography, which conceals "the very existence of the message," cryptography does not. The first known existence of encoded text dates back to 1900 BC in Egyptian culture when a scribe used hieroglyphic symbol substitutions when recording his master's history. For the next 3,000 years, mirroring the development history of mankind, cryptography appeared and disappeared in many places of the world, but never became well developed. It was not until the fourteenth century that cryptography was used "uninterrupted to the present as it emerged from the feudalism of the Middle Ages."[71]

During the twentieth century, government involvement in cryptography development (both US and other national governments) appears to have waxed and waned with the occurrence of wars. Over time cryptography equipment became increasingly mechanized and more complex. In 1911, the US began its first concentrated efforts in military cryptoanalysis, although it did not have an official codemaking or codebreaking agency. However, as World War I progressed, the US was soon able to create and distribute codes to the American Expeditionary Force (AEF) more quickly than either its allies or its enemies, including the Germans. It was a French cryptoanalyst though that broke the German ADFGVX system in 1918 so that the Allies could counter the German assaults and ultimately win the war. By the end of World War I the field of cryptography had begun to come in to its own, due in no small part to the rapid growth of radio communications.[72] By World War II, cryptography had become an integral part of national security. In the case of the Germans, the Enigma machine was critical to its

success, and ultimately its defeat.[73] Japan also had its own secret encryption system, PURPLE. Although PURPLE messages were easier to follow once the code was broken, PURPLE proved to be much more difficult to originally crack.[74] Following World War II cryptography development became largely concentrated in the national military and intelligence services, such as the United States' National Security Agency (NSA) and the United Kingdom's Government Communications Headquarters (GCHQ). However, this monopoly began to be challenged in the 1970s when cryptographic innovations started to emerge from researchers at universities and corporations working independently of the government. In the late 1960s IBM began cryptographic research at its Watson Research Lab for automatic teller machines for Lloyds Bank of London. A researcher at these labs, Horst Feistel, developed a cipher called Lucifer, from which the US Data Encryption Standard (DES) was later created (with the influence of the NSA). DES has served as the worldwide standard ever since.[75] However, breakthroughs in computing power have rendered DES ineffective against today's attacks. To extend its life, 3-key triple DES is being used while a new standard, known as the American Encryption Standard (AES) is developed. AES is expected to be finalized sometime in 2000.

Another breakthrough occurred in 1974-75 when Whitfield Diffie, Martin Hellman and Ralph Merkle develop the concept of public key cryptography. Public key cryptography allows a user to have two keys, one that is private and kept secret, and another that is public and given out. This allows others to encrypt a message with your public key so that it can be decrypted only by the private key.[76] In 1977, three MIT researchers, Ron Rivest, Adi Shamir and Len Adleman were able to turn this concept into a working encryption system they called RSA Public Key Cryptosystem, after their initials. They went on to form a company, RSA Data Security Inc. in 1982, which is the world's leading cryptography company today.[77] Throughout the 1980s and 1990s, encryption development and technology became increasingly widespread around the world. By the mid-1980s, the NSA was very concerned about this situation and its ability to maintain superior codebreaking capabilities. The NSA made numerous attempts to stymie the outside development and proliferation of encryption technology. In the 1970s, the NSA had tried to stunt encryption research through secrecy orders against researchers, preventing the delivery of conference papers and the use of patents received. The NSA also tried to pressure the National Science Foundation (NSF) to discontinue funding of encryption research. However, neither tactic was very successful.[78] Later, the NSA announced it would not support the 1988 recertification of the DES standard, in an attempt to replace it with its own standard. This brought a tremendous protest from the banking and computer industries, which had recently invested large amounts of money and resources to use DES. Ultimately, DES was recertified by the National Bureau of Standards (NBS) over the objections of the NSA.[79]

Having little luck on its own, the NSA tried to enlist the support of the FBI. After much lobbying, the NSA convinced the FBI that encryption posed a significant threat to its electronic surveillance capabilities, especially wiretapping. By 1991, the FBI was formulating a policy for the support of key escrow. That same year Pretty Good Privacy (PGP), a public key encryption program written by Philip Zimmerman, appeared as freeware and quickly became the most widely used e-mail encryption software in the

world. In response, the US federal government filed a criminal suit against Zimmerman for violating the Arms Export Control Act. At that time encryption technology was still classified as munitions by the State Department. In 1995, MIT Press took a decisive step and published the code of PGP as a 600-page book, which it sold worldwide. This left the Justice Department in the awkward position of having to prosecute MIT if it was going to continue to pursue the Zimmerman case. In 1996, the case was dropped and Zimmerman founded PGP, Inc.[80]

It is evident from this very incomplete history of encryption that it involves some very strong and often contradictory interests. It is not surprising then that efforts to regulate encryption are hotly contested. It is also clear that the authority of national governments is at stake. For these reasons, encryption regulation is a very interesting case to analyze. However, to better understand the issues being examined, we first need to have some familiarity with how today's encryption works.

Technical Aspects of Encryption

The encryption technology of the World War II era consisted of clunky mechanical machines, codebooks and keys. Keys could be words, phrases or numbers specifying "such things as the arrangement of letters within a cipher alphabet for the pattern of shuffling in a transposition or the settings on a cipher machine." A cipher alphabet is a list of equivalents used to transform the plaintext into coded text.[81] Today the encryption technology under scrutiny involves the use of mathematical formulae to encode electronic transmissions, such as e-mail, credit card orders and other data transfers from being read if intercepted by a third party, such as a spy or a hacker. An algorithm encodes a message so the receiver cannot read it unless s/he has a "key" that can decrypt the message. A key functions as a "map" that allows users to decipher the transcription code or mathematical algorithm to access the encrypted data.[82] The longer the key used to encrypt the message originally, the exponentially more difficult it is for an eavesdropper to decode an intercepted message. For example, a 41 bit key could take up to twice as long to break than a 40 bit key because each bit doubles the number of possible keys and hence the amount of time to randomly decode it. This method of trying all the possible keys is also referred to as brute force search. The chart below shows the relative strength of different key lengths (see figure 2).

Key Length	**Possible Keys**
40 bits	1,099,511,627,776
56 bits	72,057,594,037,927,900
90 bits	1,237,940,039,285,380,000,000,000,000
128 bits	340,282,366,920,938,000,000,000,000,000,000,000,000

Figure 2. Encryption Key Chart[83]

The key length a person would want to use depends on the information being transmitted. A generic e-mail message or even some sensitive financial or trading information, valuable only for a couple of hours due to changing market conditions, may require just a smaller key. However, more important information with a longer shelf life, such as a credit card number, social security number, trade secrets or intellectual property would merit a much stronger encryption code.[84]

Presently, 128-bit encryption is considered "unbreakable." "This means that it is computationally infeasible to construct the system and key in use to read the message it is protecting."[85] However, what is "unbreakable" today may not be so tomorrow. For example, in the first edition of Bruce Schneier's book Applied Cryptography, published in 1994, he says that assuming a supercomputer that can try one million keys a second, it will take 2000 years to find the correct key that is 56 bits long.[86] Schneier, a very highly respected cryptographer, could not have known then how quickly computing power would increase in capability and decrease in price in just a few years. In July 1998, a 56-bit key was broken in 56 hours with a homemade supercomputer that cost only $250,000 in equipment, a small price for organized crime rings, terrorists or unfriendly governments.[87] Given Moore's Law, which says that the performance of semiconductor technology doubles every 18 months, we cannot expect 128-bit encryption to stay unbreakable for long. In no small part, it is the speed of innovation that contributes to the clash of actors' interests. A law made today could be made completely irrelevant in a couple of years by advances in technology. Given the rather lengthy and bureaucratic process of lawmaking by states, it is little wonder that non-state actors feel they are better equipped to make the rules.

The Clipper Chip Debate

As mentioned earlier in the article, of the various encryption issues battled between competing epistemic communities, two stand out; key escrow requirements and export controls. The Clipper chip debate of the early 1990s revolved around a proposed US government-mandated and regulated key escrow system. As part of its ongoing struggle to prevent law enforcement's electronic surveillance capabilities from being eviscerated by advances in technology, the NSA developed its own alternative to DES. The goal was to create a cryptographic system strong enough to satisfy exporters' needs while making it easy for law enforcement officials to intercept and read the encrypted communications. The result was the Escrowed Encryption Standard (EES). EES utilized a classified algorithm named Skipjack, which in turn was embedded in a tamper-resistant computer chip called the Clipper. Skipjack used an 80-bit key, considered strong at the time. Also embedded in the Clipper chip was a key escrow function. In other words, each Clipper chip has a special key, not used to encrypt messages but instead to encrypt a copy of the user's message key. As part of the escrow system, a copy of each special key is split into two parts, with each part being put in separate databases established by the US Attorney General.[88] The Clipper chip was designed to be installed in telecommunications equipment, such as telephones and fax machines. However, a very similar chip called Capstone, which uses the same EES standard, was made to go into computers as well.[89]

On 16 April 1993, barely three months into his first term, President Clinton announced the Escrowed Encryption Initiative in which the EES was proposed as the new encryption standard.[90] Reaction to the proposal was swift and nearly unanimously negative. Three distinct, but complementary communities can be identified among those critical of the Clipper chip. The first community consisted of privacy advocates and civil liberties groups. Their primary argument was that even if not actually used, the mere existence of a government capability to read messages "creates the perception that no communication is private."[91] The second community consisted of cryptographers and technology developers. Their opposition to the EES focused primarily on technical weaknesses of the plan. One of the weaknesses they highlighted was that the EES represented a step backward to the mid-1970s. What public key cryptography achieved by decentralizing the key function, would be undone by the creation of key escrow databases called for in the proposal. In effect then, the EES proposal challenged an instruction-sense rule that had guided the development of encryption technology since the 1970s, which said secure communication is facilitated by "reducing the trust that must be placed in centralized resources."[92] The EES proposal also challenged an instruction-sense rule regarding the importance of promoting the open development of interoperability among products. Instead, the Clipper chip would be manufactured by only a few authorized suppliers and could only be purchased with government permission.[93] The third community consisted of industry groups whose primary interest was the marketability of their products for export. Industry groups followed a very basic instruction-sense rule about demand - do not produce products that do not meet demand. In this case, foreign companies wanted products that provided strong security that could not be tapped into by the US government. Likewise, foreign governments would not want to purchase technology that left them more vulnerable to the world's remaining superpower. However, the EES proposal challenged that rule by implicitly saying that consumers will be satisfied by a limited set of choices that do not meet their wants and needs.

Although coming from different perspectives, these three communities joined in opposition to the EES proposal to protect their complementary interests.[94] Less than a month after the EES proposal was announced, a self described "coalition of communication and computer companies and associations and consumer and privacy advocates" known as the Digital Privacy and Security Working Group (DPSWG) formed and sent a letter to President Clinton detailing their opposition to the plan. In June 1993, the DPSWG presented public testimony at Congressional hearings. Five days later the National Institute of Standards and Technology (NIST), which was in charge of implementing the EES, announced it would delay and review the plan until the fall. However, in September the Clinton administration announced that NIST and a non-law enforcement agency in the Treasury Department would serve as the two key escrow agents. Incensed by the lack of independence of the escrow agents from the federal government, the DPSWG continued to fight the proposal. In December, the DPSWG proposed it would accept the Clipper chip as a voluntary standard if the strict export controls were dropped. Although willing to agree to Clipper as a voluntary standard, the US government would not ease the export rules. In January 1994, several companies announced they would not use the Clipper chip and instead would use a commercially developed encryption standard called RSA, which reinforced their instruction rules. In

addition, a letter "signed by forty-one computer privacy advocates, cryptography experts, and technical specialists" was sent to President Clinton calling for the complete withdrawal of the Clipper proposal.[95] Despite this strong opposition, on 4 February 1994, the US federal government adopted the EES as a Federal Information Processing Standard. Although mandated as a governmental standard that would have to be used by anyone wanting to do business with the federal government, the Clipper was voluntary for the private sector. The standard was to be used for voice, fax and computer information carried over telephone lines and was made available in various models of the AT&T Telephone Security Device Model 3600 (TSD 3600). Although the government tried to seed the market by buying several thousand of these units, almost none were sold commercially.[96] With the Clipper chip largely unpopular and unused, and US efforts to get other countries to adopt the standard unsuccessful, the US government changed tactics and tried to leverage its control over export controls to induce the computer industry to develop and implement key escrow/key recovery systems on their own.

Export Controls

Having failed to establish the Clipper chip as an international standard in 1996, the US government began to focus its efforts on using export controls as a camouflage for pushing a reformed version of its software key escrow proposal. One of the first things it did was to blur the distinction between real-time communications and information storage. By using the term "key recovery" instead of "key escrow," the US government emphasized the idea that having a spare set of keys is a good information management practice. "If you lose the keys, you lose the information." This argument was coupled with the notion that key recovery is an important tool for ensuring customer trust that they can retrieve their data. On 1 October 1996, the White House proposed that "for two years, beginning on 1 January 1997, the government would allow export of unescrowed systems with 56-bit keys (mostly DES keys, presumably) in return for promises from the exporters that they would implement key recovery systems in their products."[97] In other words, the government was proposing a form of self-regulation, as long as it met certain standards. Although a consortium of computer companies, led by IBM, initially endorsed this proposal, preferring a market approach to developing key recovery systems, this support quickly evaporated when the administration seemed to be taking further steps toward restricting exports. On 15 November 1996, President Clinton issued an executive order turning jurisdiction over encryption technology from the State Department to the Commerce Department. This removed encryption technology from the munitions list. However, the executive order also gave the FBI new authority over export controls.[98] During the next year the FBI stepped up its calls for strict export controls, as well as domestic controls over encryption.[99]Meanwhile, numerous bills were proposed and counter-proposed in Congress throughout 1997 with no progress made by either side.[100] In 1998 though, the computer industry started taking more aggressive action toward the export of encryption technology. Sun Microsystems made steps toward marketing Russian-made encryption, through a Russian company in which it held a ten percent ownership stake, in order to avoid US regulatory agencies. Network Associates began allowing its Dutch subsidiary to sell an international version of PGP that did not have a key recovery mechanism.[101] In April 1998, the Economic Strategy Institute

released a report estimating that direct and indirect losses due to export controls could reach between $34-65 billion over the following five years.[102] Relenting somewhat to the pressure of the software and financial industries, the Clinton administration agreed to allow the export of strong encryption software without key escrow features for banks and financial institutions.[103] After further pressure and the announcement of a $1 million advertising campaign by Americans for Computer Privacy (ACP), a coalition of computer companies that supports the export of strong encryption products, the Clinton administration expanded its exemption on encryption exports to include medical, insurance and electronic commerce businesses in 45 countries.[104]

However, despite these policy changes, the US had still not given up on its goal to bring encryption exports under control. In December 1998, after many years of unsuccessfully advocating for a formal multilateral regime on encryption, the US turned to an informal state mechanism, the Wassenaar Arrangement, in an attempt to establish its rules as the basis for a more formal agreement. The Wassenaar Arrangement is a coalition of 33 countries[105] whose purpose is to "contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies."[106] The encryption pact among the member countries removes all restrictions "including licensing and reporting requirements" on encryption products below 64 bits.[107] Encryption products of 64 bits and higher are to be subject to export restrictions. However, the pact contains a significant loophole that weakens its effectiveness considerably. Compliance with the agreement is voluntary, as it is up to the discretion of each individual country on how strongly to enforce it. In countries such as the United Kingdom, Japan and the United States, who already have relatively strict laws, the pact may just reinforce the status quo, though in countries such as Australia and Germany, which favor the use of strong encryption, compliance is expected to be low. Australia, for example, uses loose restrictions to attract encryption development companies, such as the US-based RSA Data Security, the leading developer of encryption technology, to establish subsidiaries in its country. Germany, which already had weak export controls on encryption technology, recently announced plans to give a grant of 318,00 marks (about $170,000 US) to a grass roots users group to develop new encryption software.[108] Even France, which until recently strictly regulated encryption technology over 40 bits and required all encryption keys of any strength to be registered with a key escrow system run by the state, recently announced it plans to allow the use of up to 128 bit encryption technology in an effort to promote electronic commerce and protect privacy.[109]

With the new rules of the Wassenaar Arrangement expected to have little effect in practice, and even US Secretary of Commerce William Daley noting the importance of global standards for encryption and privacy to the success of electronic commerce, there appears to be increasing support for lifting export controls on encryption software, both in the US and in other countries.[110] According to a study released by the Electronic Privacy Information Center in June 1999, fewer countries placed restrictions on encryption and more industrialized countries relaxed restrictions over the past year.[111]111 At the same time, researchers at the Cyberspace Policy Institute at George Washington University have shown that commercial encryption technology has become

"significantly more available in the last 18 months." Of the 805 encryption products available in 35 countries outside the United States, 167 of these products are "unbreakable."[112] Further evidence of the sea change in encryption is that of the 15 original algorithms submitted for consideration as the new American Encryption Standard (AES), ten were created outside the United States.

Bowing to the increased pressure by industry and civil liberties groups, the Clinton administration announced on 16 September that it planned to loosen export controls significantly. On 23 November 1999, the administration released a draft of its new encryption export rules for review by interested parties. The response was so great that release of the final rules was postponed a month from the original 15 December due date. On 12 January 2000, the US Department of Commerce Bureau of Export Administration (BXA) issued its new encryption export regulations. Moving from what Marc Rotenberg[113] calls a "gatekeeper model to a surveillance model," the new regulations replace many of the licensing requirements with one-time technical reviews and/or notification obligations.[114] In an effort to accommodate the competing demands of the various national security/law enforcement agencies, industry associations and civil liberties groups, the new policy is a complex web of regulations that makes distinctions based on a combination of factors, including the actor and country to whom the product is being exported, whether or not the product is classified as a retail commodity, and if the source code is "open source," "community source," or "private source." While a detailed explanation and analysis of the revised export regulations[115] could fill its own journal-length article space, a review of the highlights of the new rules can give the reader a sense of the changed regulatory environment.

- Under the new rules, "any encryption commodity or software, including components, of any key length can now be exported, under a license exception after a technical review, to any non-government end-user in any country except for the seven state supporters of terrorism." However exports to government end-users still require a license.
- Retail encryption products (as determined by the BXA based on a review of their functionality, sales volume and distribution methods) can also be exported to non-government end-users (including Internet and telecommunications service providers) without a license, although exports of these same products for services from foreign governments requires a license.
- Open source code can be exported under a license exception without technical review, provided a copy of the source code, or its Internet location, is provided to the BXA. Source code not open to the public can be exported to any non-government end-user after a technical review.
- Encryption products of any key length can be exported to foreign subsidiaries of US firms without a technical review while products with encryption commodities, software and technology exported by US firms or their foreign subsidiaries employing foreign nationals require a technical review before being exported under the license exception. "Post-export reporting is required for certain exports to a non-US entity of products above 64 bits. However, no reporting is required if the item is a finance-specific product or is a retail product reported to individual consumers. Additionally, no reporting is required if the product is exported via free or anonymous download, or is exported from a

US bank, financial institution or their subsidiaries, affiliates, customers or contractors for banking or financial use."

- The new regulations also implement the December 1998 Wassenaar Arrangement revisions, allowing "exports without a license of 56 bit DES and equivalent products, including toolkits and chips, to all users and destinations (except the seven state supporters of terrorism) after a technical review. Encryption commodities and software with key lengths of 64-bit or less which meet the mass market requirements of Wassenaar's new cryptography note are also eligible for export without a license after a technical review."[116]

Although complicated and filled with various exceptions and notification requirements, the new rules appear to favor (albeit not completely) the instruction-sense rules promoted by industry groups. Notably, the lack of a mandatory key escrow system and the ability to export strong encryption products with comparatively fewer restrictions represent a victory for industry. Civil liberties groups, however, are less satisfied with the new regulations, which only partially fulfill their instruction rules. On the other hand, requirements to turn over the source code of encryption products, submission of products for technical reviews, and tracking the end-users of encryption products address some of the concerns of the national security and law enforcement communities by providing them with information that will enhance their ability to crack messages and stay abreast of developments in encryption technology. At the close of this latest round in the encryption policy debate, no group of actors achieved a complete victory. The industry associations appear to have made the greatest gains while the civil liberties groups accomplished some of their goals and the national security/law enforcement community preserved some of their ground. As the new regulations are more fully exercised and their implications become more clear, we can expect to see the outlines for the new arguments in the contest to create the rules that will rule the Internet.

CONCLUSION

This is a particularly opportune time to examine changes in rule-making in the international system. The global political economy is undergoing significant change, fueled by advances in information technology, the heightened importance of international finance, and the development of the Internet as the new global infrastructure for facilitating political, economic and social interactions. The digitalization of commerce and politics has led to renewed concerns about property rights among non-state actors. The perceived failure of states to adequately protect these property rights has perpetuated a crisis of legitimacy in international relations. This dynamic is most clearly played out in regard to Internet regulation, especially encryption regulation, where age-old concerns of national security, law and order are being challenged by concerns over privacy, principles and profits.

The preliminary results of the two encryption issues examined in this article are mixed. In the case of the Clipper chip, the US government asserted its authority and enacted the EES as a federal standard over the objections of several non-state epistemic communities. However, as a voluntary standard for the private sector, EES was overwhelmingly

rejected in favor of a competing standard that has been distributed and used worldwide. This suggests the private sector has the capability to implement its own rules over the objections of national governments. In the case of export controls, after several years of a stalemate, the non-state actors appear to be gaining the upper hand in establishing encryption export rules in the global economy, as evidenced by the greater availability of strong encryption products and the gradual loosening of export laws in other countries.

The encryption debate is far from being resolved. Indeed, there may never be a true endpoint or resolution. If the US tries to mandate a key escrow function as a condition of approving the new AES in 2000, then a new battle between national law and private interests will erupt. The symbiosis between rules and technology cannot be separated. New developments in technology impact which laws are relevant while at the same time rules can impact what kinds of technology are developed. However, by considering alternative models of Internet governance, we can gain a better understanding of this new and complex area of rule formation.

Endnotes The author wishes to thank G. Matthew Bonham, David Charters, Margaret Hermann, James Roberts, Stuart Thorson, and the anonymous referees for their helpful comments and insights. Any errors of fact and interpretation that remain, however, are entirely the fault of the author. Comments and suggestions are welcome and can be sent to the author via e-mail at jwseifer@syr.edu.

1. James C. Roberts, "The Rational Constitution of Agents and Structures," in Kurt Burch and Robert A Denemark, eds., Constituting International Political Economy (Boulder, CO: Lynne Rienner), pp. 156-57.

2. Lee E. Preston and Duane Windsor, The Rules of the Game in the Global Economy: Policy Regimes for International Business (Boston, MA: Kluwer Academic Publishers, 1997), p. 149.

3. Judith Wagner DeCew, "The Priority of Privacy in a Technological Age," (Boston, MA: American Political Science Association, 1998), p. 2.

4. "Processing" is a broad term that means "any operation or set of operations which is performed upon personal data, whether or not by automatic means (Article 2(b)). Processing includes any collection, recording, use, or storage of personal information." Peter P. Swire and Robert E. Litan, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive (Washington DC: Brookings Institution Press, 1998), pp. 26 and 30.

5. Ibid.

6. Edmund L. Andrews, "European Law Aims to Protect Privacy of Personal Data," New York Times, 26 October 1998, p. A1; Swire and Litan, None of Your Business, p. 31.

7. Jeri Clausing, "Gains Seen in Consumer Privacy on Internet," New York Times, 12 May 1999, p. A20.

8. Jeri Clausing, " On-Line Privacy Group Decides Not to Pursue Microsoft Case," New York Times, 22 March 1999, p. C-5; Sara Robinson, "CD Software Said to Gather Data on Users," New York Times, 1 November 1999, p. C5.

9. Jeri Clausing, "Administration Seeks Input on Privacy Policy," New York Times, 6 November 1998.

10. Jeri Clausing, "Business Group Unveils Plan for Online Privacy," New York Times, 18 March 1999; Saroja Girishankar, "Sellers Make Privacy Vow," InternetWeek, 22 March 1999, p. 8.

11. Ziziang (Alex) Tan, William Foster, and Seymour Goodman, "China's State Coordinated Internet Infrastructure," Communications of the ACM 42, no. 6 (June 1999), pp. 44-45.

12. Robert Gellman, "Conflict and Overlap in Privacy Regulation: National, International, and Private," in Brian Kahin and Charles Neeson, eds., Borders in Cyberspace: Information Policy and the Global Information Infrastructure (Cambridge, MA: The MIT Press, 1997), p. 269.

13. James N. Rosenau, Along the Domestic-Foreign Frontier: Exploring Governance in a Turbulent World. (Cambridge, MA: Cambridge University Press, 1997), p. 145.

14. I envision this as an infinite scale with an infinite number of possible points. I do not assume that the points marked here are the only points imaginable. Rather, they are meant to represent the flow of the continuum based on the predominant models described in the literature.

15. David Johnson and David Post, "The Rise of Law on the Global Network," in Kahin and Neeson, eds., Borders in Cyberspace, p. 3. Johnson and Post are Co-Directors of the Cyberspace Law Institute http://www.w3.org

23. Stephen Krasner, ed., International Regimes (Ithaca, NY: Cornell University Press, 1983) , p. 2.

24. Robert M.A. Crawford, Regime Theory in the Post-Cold War World: Rethinking Neoliberal Approaches to International Relations (Brookfield, MA: Dartmouth Publishers, 1996); Robert Keohane, After Hegemony: Cooperation and Discord in the World Political Economy (Princeton, NJ: Princeton University Press, 1984); Krasner, International Regimes, p. 6; Mark W. Zacher with Brent A. Sutton, Governing Global Networks: International Regimes for Transportation and Communications (Cambridge, UK: Cambridge University Press, 1996).

25. Oran R. Young, "Political Leadership and Regime Formation: Managing Natural Resources and the Environment," International Organization 45, no. 3 (Summer 1991) p. 282.

26. Andreas Hasenclever, Peter Mayer, and Volker Rittberger, "Interests, Power, Knowledge: The Study of International Regimes," Mershon International Studies Review 40, no. 2 (1996) p. 193.

27. Hasenclever, Mayer, and Rittberger, "Interests, Power, Knowledge," p. 194; Oran R. Young, International Cooperation: Building Regimes for Natural Resources and the Environment (Ithaca, NY: Cornell University Press, 1989), p. 148; Oran R. Young, International Governance: Protecting the Environment in a Stateless Society (Ithaca, NY: Cornell University Press, 1994) p. 107; Young and Osherenko, Polar Politics, p. 264.

28. Hasenclever, Mayer, and Rittberger, "Interests, Power, Knowledge," p. 194; Oran R. Young, "The Politics of International Regime Formation: Managing Natural Resources and the Environment," International Organization 43, no. 3 (Summer 1989), p. 371; Young, International Governance, p. 112; Young and Osherenko, eds., Polar Politics, p. 264.

29. Rosenau, Along the Domestic-Foreign Frontier, p. 160.

30. Virginia Haufler, "Crossing the Boundary between Public and Private," in Volker Rittberger, ed., Regime Theory and International Relations (Oxford, UK: Clarendon Press, 1993), p. 97; Virginia Haufler, Dangerous Commerce: Insurance and the Management of International Risk (Ithaca, NY: Cornell University Press, 1997), pp. 30-31.

31. Ibid.

32. Ibid, p. 31.

33. Ibid, p. 33 (emphasis added).

34. Ibid, p. 32.

35. See Haufler, Dangerous Commerce, p. 30 fn 5 for relevant works by Oran Young, Ernst Haas, Peter Haas, and Martha Finnemore on the role of various types of non-state actors to "act as catalysts of change within regimes."

36. Ibid, p. 32.

37. Haas, "Epistemic Communities and the Dynamics," p. 179.

38. Ibid, pp. 179-80.

39. Haas, "Introduction: Epistemic Communities," p. 3, fn5.

40. Ibid, p. 16.

41. Ibid, p. 17.

42. Emmanuel Adler and Peter M. Haas, "Epistemic Communities, World Order, and the Creation of a Reflective Research Program," International Organization 46, no. 1 (Winter 1992); Haas, "Introduction: Epistemic Communities;" Haas, "Epistemic Communities and the Dynamics;" Andreas Hasenclever, Peter Mayer, and Volker Rittberger, Theories of International Regimes (Cambridge, MA: Cambridge University Press, 1997), pp. 150-51.

43. Colin J. Bennett, "The International Regulation of Personal Data: From Epistemic Community to Policy Sector," (Annual Meeting of the Canadian Political Science Association, 1992), p. 2; Colin J. Bennett, "Understanding Ripple Effects: The Cross-National Adoption of Policy Instruments for Bureaucratic Accountability," Governance: An International Journal of Policy and Administration 10 (1997), p. 227; George Hoberg, "Sleeping with an Elephant: The American Influence on Canadian Environmental Regulation," Journal of Public Policy 11, no. 1 (1991), pp. 107-32.

44. See Wolfgang H. Reinicke, Global Public Policy: Governing without Government (Washington, DC: Brookings Institution Press, 1998) for a detailed discussion of global public policy.

45. Edgar Gold, Maritime Transport: The Evolution of International Marine Policy and Shipping Law (Lexington, MA: Lexington, 1981), p. 5.

46. Max Black, "Notes on the Meaning of Rule," Theoria XXIV (1958); Max Black, Models and Metaphors: Studies in Language and Philosophy (Ithaca, NY: Cornell University Press, 1962).

47. Nicholas Greenwood Onuf, "A Constructivist Manifesto," in Kurt Burch and Robert A Denemark, eds., Constituting International Political Economy (Boulder, CO: Lynne Rienner).

48. Nicolas Greenwood Onuf, World of Our Making: Rules and Rule in Social Theory and International Relations (Columbia, SC: University of South Carolina Press, 1989), p. 144, fn. 14.

49. Black, Models and Metaphors.

50. Black, "Notes on the Meaning of Rule," p. 121.

51. Black, Models and Metaphors, p. 110.

52. Onuf, World of Our Making, p. 80.

53. Black, Models and Metaphors, p. 109.

54. Onuf, "A Constructivist Manifesto," p. 10.

55. Ibid., p. 13.

56. Nicolas Greenwood Onuf, The Republican Legacy in International Thought (Cambridge, MA: Cambridge University Press, 1998), p. 188.

57. Onuf, "A Constructivist Manifesto," p. 13.

58. Peter F. Drucker, "The Global Economy and the Nation-State," Foreign Affairs 76, no. 5 (1997), p. 166.

59. Walter B. Wriston, The Twilight of Sovereignty: How the Information Revolution is Transforming the World (New York: Charles Scribner's Sons, 1992), p. 24-25.

60. Whitfield Diffie and Susan Landau, Privacy on the Line: The Politics of Wiretapping and Encryption (Cambridge, MA: The MIT Press, 1998), p. 43.

61. Ibid., p. 48.

62. Esther Dyson, Release 2.0: A Design for Living in the Digital Age (New York: Broadway Books, 1997), p. 266.

63. Kenneth W. Dam, "The Role of Private Groups in Public Policy: Cryptography and the National Research Council," Occasional Papers no. 38 (Chicago, IL: University of Chicago Law School, 1996), p. 7.

64. Louis Freeh, Testimony to US Congress, 105th Congress, 1st Session, "The Impact of Encryption on Public Safety," US House of Representative Permanent Select Committee on Intelligence, Hearings held 9 September 1997, http://www.fbi.gov/pressrm/congress/97archives/encrypt4.htm

65. Dam, "The Role of Private Groups in Public Policy," pp. 7-8.

66. Matt Richtel, "Investigators Face a Glut of Confiscated Computers," New York Times, 27 August 1999.

67. Dam, "The Role of Private Groups," p. 8.

68. Niall McKay, "Lawmakers Raise Questions About International Spy Network," New York Times, 27 May 1999.

69. Kenneth W. Dam and Herbet S. Lin, eds., Cryptography's Role in Securing the Information Society (Washington, DC: National Research Council, 1996), p. 73; Diffie and Landau, Privacy on the Line, p. 47.

70. Dam, "The Role of Private Groups," p. 8.

71. David Kahn, The Codebreakers: The Story of Secret Writing, 2nd ed. (New York: Scribner, 1996), pp. xv, 71-73 and 106.

72. Office of Naval Intelligence, "Strategic Use of Communications During the World War," in Monthly Information Bulletin, (August 1928) reprinted in Cryptologia XVI, no. 4 (October 1992), pp. 325-26, 329, and 347-48.

73. Ralph Erskine, "The German Naval Grid in World War II," Cryptologia XVI, no. 1 (January 1992), pp. 39-51.

74. Kahn, Codebreakers, p. 18.

75. Diffie and Landau, Privacy on the Line, p. 58-59.

76. It has since been revealed that James Ellis, a senior scientist at Britain's GCHQ, had developed the same idea back in 1969 but that the British intelligence agency felt it would be impossible to implement and decided not to act on it. J.H. Ellis, "The History of Non-Secret Encryption," Cryptologia XXIII, no. 3 (July 1999); Steven Levy, "The Open Secret," Wired (April 1999), p. 108.

77. Diffie and Landau, Privacy on the Line, p. 60-61.

78. Ibid, p. 62.

79. Ibid, p. 65.

80. Ibid, pp. 205-06.

81. Kahn, Codebreakers, p. xvii.

82. Dyson, Release 2.0, p. 264.

83. See FreeMarket.Net: Policy Spotlight, October-November 1997, as shown on the Americans for Computer Privacy website, http://www.computerprivacy.org/glossary/

84. Peter Wayner, "Cracked Code Reveals Security Limits," New York Times, 24 October 1997.

85. Kahn, Codebreakers, p. 984.

86. Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C (New York: John Wiley, 1994), p. 129.

87. John Markoff, " US Data Code Is Unscrambled In 56 Hours," New York Times, 17 July 1998, p. D1.

88. Daniel C. Lynch and Leslie Lundquest, Digital Money: The New Era of Internet Commerce (New York: John Wiley, 1996), p. 96.

89. Laura J. Gurak, Persuasion and Privacy in Cyberspace: The Online Protests Over Lotus MarketPlace and the Clipper Chip (New Haven, CT: Yale University Press, 1997), p. 35.

90. Ibid, p. 210.

91. Ibid, p. 212.

92. Ibid.

93. Ibid, pp. 212-13.

94. Gurak, Persuasion and Privacy in Cyberspace, p. 34.

95. Ibid, pp. 37-39.

96. Diffie and Landau, Privacy on the Line, pp. 213-15.

97. Ibid, p. 217.

98. William Jefferson Clinton, Executive Order: Administration of Export Controls on Encryption Products, 15 November 1996, http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1996/11/15/4.text.1

99. Jeri Clausing, "FBI, Security Chiefs Ask Senate for Keys to All Encrypted Data," New York Times, 10 July 1997.

100. Kenneth A. Mendelson, Stephen T. Walker, and Joan D. Winston, "The Evolution of Recent Cryptographic Policy in the United States," Cryptologia XXII, no. 3 (July 1998), pp. 193- 210.

101. Markoff 3/20/98: http://www.nytimes.com/library/tech/98/03/biztech/articles/20encrypt. htm.

102. Jeri Clausing, "Study Puts Price on Encryption Controls," New York Times, 1 April 1998.

103. Jeri Clausing, "White House Yields a Bit on Encryption," New York Times, 8 July, 1998, p. D1.

104. Elizabeth Corcoran, "U.S. to Relax Encryption Limits," The Washington Post, 17 September 1998, p. C04.

105. Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovak Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and United States.

106. http://www.wassenaar.org/docs/index1.htm

107. Mary Mosquera, "Encryption Resolution May be Sector by Sector," New York Times, 3 December 1998.

108. Jim Kerstetter, "Wassenaar Pact May Threaten Global E-Com," PCWeek, 14 December 1998, p. 48; Peter Wayner, "Germany

109. Michel Alberganti, "La France Renonce a contr™ler les communicatinos sur Internet," LeMonde, 21 January 1999.

110. Mary Mosquera, "Encryption Resolution May be Sector by Sector," New York Times, 29 July 1998. 111. Electronic Privacy Information Center, Cryptography and Liberty 1999: An International Survey of Encryption Policy (Washington, DC: EPIC, 1999), http://www.epic.org/reports/ crypto1999.htm.

112. Lance Hoffman, et al., "Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations," CPI-1999-02, 10 June, 1999; John Markoff, "Encryption Products Found to Grow in Foreign Markets," New York Times, 10 June 1999, C13.

113. Marc Rotenberg is the Executive Director of the Electronic Privacy Information Center (EPIC) http://www.epic..org.

114. Jeri Clausing, "New Encryption Rules Leave Civil Libertarians Unhappy," New York Times, 18 January 2000.

115. The full text of the new rules can be found at: http://www.bxa.doc.gov/Encryption/ pdfs/Crypto.pdf.

116. US Department of Commerce Fact Sheet on Clinton Administration Updated Encryption Export Policy http://204.193.246.62/public.nsf/docs/