Government Information Quarterly 26 (2009) 398–406

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Regime formation and consequence: The case of internet security in the East-Asia 'Four Tigers'

Yong Jin Park

Department of Communication Studies, University of Michigan, Ann Arbor, 1648 McIntyre Drive Ann Arbor, MI 48105, USA

ARTICLE INFO

Available online 21 January 2009

Keywords:
Information privacy
Internet security
Encryption
Asian Pacific Economic Cooperation
East Asia developmental model

ABSTRACT

The purpose of this article is to identify the process in which each nation appropriates a new technological force challenging regulatory regimes. Departing from regime theory, this paper critically assesses the interaction between Asian Pacific Economic Cooperation and the East-Asia 'Four Tigers' in formulating Internet security policy. A particular concern is about the formation of global information policy regime that arbitrates the tension between citizens' right to privacy and free information flow. This paper argues that the potential of the greater protection of information privacy are curtailed as market incentives of information flow dominate over the region's policy effort. A 2003 Bangkok meeting epitomizes such policy formulation in the interaction between international and national regimes that are particular to the region's regulatory legacies. Implications are discussed in terms of the function of industrial legacies in new information policy.

1. Introduction

How do we balance free information flow and the protection of personal information in an open digital network? The internet presents a paradox for policymakers. First, the digital landscape established the virtual marketplace that placed commercial transactions beyond geographical boundaries. Second, it became highly contentious to establish a policy standard that incorporates conflicting rules deriving from various nation-states. The paradox is twofold — whether nation-states, in response to the borderless nature of new technology, can maximize global market potentials while addressing democratic interests of citizens.

This paper examines the impact of regulatory legacies on internet security policy that regulates information flow. A particular concern is about the formation of international and national information policy regimes that arbitrate the tension between citizens' right to privacy and commercial incentive for free information flow. This article takes a two-step approach, moving from (1) the process of the interaction between international and national entities (regime formation) to (2) the consequence of such formulation within which each nation operates (regime impact) (Braman, 2004). Thus, this article aims to address the regime formation at the two levels and to triangulate central arguments in integration:

1. At the international level, how do different nations create a harmonized information policy in which different regulatory regimes can be coordinated?
2. At the national level, what is the function of distinctive regulatory legacies in generating particular policy choices?

1.1. Framework

International regime theory (IRT) posits that an effective policy develops when the consensus on a set of principles or norms emerges in a particular area of concern. Regime, in this sense, indicates the formation of cognitive frameworks or norms that are tacitly accepted as a global policy agenda (Braman, 2004). Note the linkage between the national and the international actors in defining the acceptable forms of policy problem and solution (Cogburn, 2003). Here the linkage plays the role of a set of beliefs and value systems in promoting or hindering a certain policy orientation in a given area. In other words, an international policy regime and its norm building process can revitalize or curtail particular regulatory principles and serve as a powerful constraint for national actors in formulating a new policy.

Frieden and Martin (2002) suggested the function of the three elements at the stage of policy inception:

(1) The strategic international setting.
(2) The state interests.
(3) The regulatory beliefs and ideas that deal with policy uncertainties.

The product of such elements explains why certain nations make particular policy choices in certain ways. A similar logic is applied to the tension between a global force and local ideals in adopting new technology, and how such interaction can produce nation-specific appropriations (Sandivig, 2003). To put it differently, a new regime can be effective in a certain group of nations that are willing to

E-mail address: parkyo@umich.edu.

0740-624X/$ – see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.giq.2008.03.006

correspond with (1) emerging global norms and (2) perceived common interests that are advanced in international arena. In short, the autonomous role of the state is critical in activating and exercising the principle that is developed globally in the interest of the nation-state (Cogburn, 2003; Hosein, 2004).

1.2. Application

This paper centers on the 2003 Asian Pacific Economic Cooperation (APEC) Bangkok meeting, the first 'Expert Seminar' that aimed to harmonize internet security technical standards at the working group level. The strategic aim, drawing upon a transnational event, is to illustrate the region's policymaking process and to explore the nature of a global policy consensus among the three tiers (i.e. developed, developing, and underdeveloped economies). Note the unique position of the 'Four Tigers' (S. Korea, Hong Kong, Chinese Taipei, and Singapore) in the apparent digital divide between the north and south. As the particular transnational event epitomizes the digital disparities in the region, the question is how the industrial success of the 'Four Tigers' is translated into the internet in the tension between economic and social goals.

In fact, communication policy is the choice between two contrasting goals (Napoli, 2001). On the one hand, policy goals pursue socially desirable ideals (e.g. FCC diversity and localism principles in the U.S.). On the other hand, there is the policy incentive to promote economic efficiency of new media institution that is yet to be evolved. The internet and its open architecture recast this tension into the conflict between citizens' right to privacy and commercialized data flow. The central objective of this paper is then:

1. Policy formation: To identify the emergent regime in appropriating this tension at the APEC and the 'Four Tigers' levels.
2. Policy consequences: To assess how such appropriation hinders or promotes a particular policy vision of the internet.

In sum, this study aims to illustrate the function of regulatory legacies in new information policy that is being formulated within a broad framework of international policy regime.

1.3. Contribution

International regime theory provides theoretical underpinnings for our research. Far from a dogmatic application, however, IRT is critically applied to incorporate the active role of state actors embedded in regulatory legacies (see Cogburn, 2003). Note the rationale behind this. First, it is to make a realistic assessment of how a policy consensus in the bargaining is incorporated into a distinctive set of tech-policy actions that are common to a region (Venturelli, 2002). Second, it intends to provide the linkage between the transnational setting and nation-states (Frieden & Martin, 2002), as opposed to most studies in internet policy, which focus on the one in the sacrifice of the other. The East-Asia industrial legacies are operationalized as the active regime that incorporates the APEC tech-policy consensus. In this way, this paper modifies the premise of regime theory to the particularities of the 'Four Tigers' and examines the moderating role of the emergent regime in the construction of new technology.

1.4. Structure

This article has the three sections. The first part, in a historical analogy to the infrastructural development in the US, examines the regulatory challenge that internet poses for the region's policymakers. The second part assesses the formation of the current policy regimes that appropriate such challenges at (1) the APEC and (2) the 'Four-Tigers' levels. The last part discusses the consequences of the region's information regime formation. The main thesis is that the potential of the greater protection of information privacy are curtailed as market incentives of free information flow dominate the region's policy effort. This paper attributes such policy formulation to the interaction between international and national regimes that are particular to the region's regulatory legacies.

2. Methodology

The method adopted in this paper is both holistic and historical in nature. The year 2003 contextualizes the period in which the internet security debate heated in the aftermath of the 9/11 (in 2001). The APEC and the 'Four-Tigers' are chosen for the case in order to fill the absence of scholarly endeavors that examine internet policy in a regional block of 21 member-states around the Pacific Rim. An archive with a comprehensive database is constructed based on documents from the three sectors: (1) governmental memos and media releases at both APEC and national levels, (2) press reports in industry trade magazines, and (3) policy reports and surveys from the civic NGO sector.

The aim is to reconstruct the internet policy debate through the lens of the Pacific Rim and its sub-region. For this, the article employs qualitative policy analysis of the secondary sources archived. This approach is limited in its scope in that the interpretive analysis does *not* permit ethnographical insights as with in-depth interviews. Further, the complied data are confined in the specific context, *not* necessarily suitable for generalization to other regions. Instead, the goal is the synthesis of available policy materials that warrants holistic understandings at meta-level (see Lindloff, 1995). This entails the inter-contextual data collection and analysis regarding policy practices around internet security, rather than its micro technical aspects.

3. The push from new technology

3.1. Encryption: new and old policy challenges

The notion of encryption is not new. In the old, analog world, maintaining the integrity, authenticity, and security of original messages and contents has always been a concern for regulators. The postal system, for example, is built on the idea of a 'common carrier' (Pool, 1983). That is, the role of a transmitter (courier) is confined by regulatory bodies to deliver a message from an original sender to a targeted receiver without altering, intercepting, and manipulating its content. Note the two assumptions behind the function of 'common carrier': (1) the integrity of the original content, and (2) the reliability of the delivery network (Garfinkel & Spafford, 1997). Cryptographic methods were developed in public and private sectors to ensure the confidentiality of the message. In the history of war, the military has been interested in cryptography (mathematical formulas) as a way of scrambling messages so that only a targeted recipient can interpret them.

The internet amplified this regulatory concern. First, the open nature of the internet, of which the message delivery is based on packet-switching, became architecturally vulnerable to eavesdropping during transmission (Abbate, 1999). Second, the authenticity and the integrity of messages, as they travel through digital networks, are hardly guaranteed with binary 'codes' and 'bits' susceptible for manipulation. Third, in the interface between the network backbone and the message, encryption (i.e. envelope seal in digital form) can be easily broken or tampered without users' awareness (Kerr, 2003) (see Table 1). Further challenges lie in the borderless nature of the internet.

Table 1
Transmission in old and new media

	Postal mail	Email and internet
Envelope layer	Post marks, stamps and seals	IP addresses, email headers, etc
Content layer	The contents of the letter	Email messages and communication between any two computers
Delivery Layer	Letters and packages	Internet packets

(Modified from Kerr, 2003).

Government approved encryption, no matter how sophisticated, becomes less relevant as a message goes through the transnational network in which standards may be incompatible or counteractive (Dempsey, 2003).

3.2. Incentive for standardization

The evolution of communication infrastructure (e.g. canals, railroads, and highways) always paralleled marketplace development (Bar, 2001; Sawhney & Wang, 2005). First, canals, then railroads were used to link centers of river and cargo traffic, and to create extensive networks that support a market system (Sawhney, 1999). In particular, the US 1887 Interstate Commerce Act was a trans-state rulemaking effort to establish the stability and predictability of commerce in a market that was integrated with the deployment of railroad (Horwitz, 1989). The Interstate Commerce Commission (ICC) functioned to establish operational efficiency by preempting erratic freight rates or rebates among states. The objective was clear: to ensure the interoperability of a new infrastructure system. In other words, the late 19th Century railroad system arrangements including signaling, standard time zones, and scheduling, were the result of regulatory cooperation that aimed for the expansion of unified marketplaces beyond geographical constraints (Friedlander, 1995).

3.3. Pan-Pacific cyber-market integration

An analogy should be made on cyber-market integration. Here the road is digital and the market is transnational. APEC, not the Interstate Commerce Commission (ICC), is in charge. According to Bar (2001), electronic marketplace systems develop based on the infrastructure that can deliver the security of information flow between sellers and buyers, the relationship amplified in a direct 'end-to-end' architecture. In fact, one of the first commercial services by telegraph operators in the 19th century was the transmission of individual credit records for banks operating interstate (Standage, 1998). Imagine the vulnerability of the open internet when transactional records are sent from a user in Los Angles to a vendor in Bangkok.

Critical is the locus of the internet encryption (as an envelope layer) that resides on a layer in between layers of the network (Abbate, 1999). That is, encryption functions to maintain the integrity of the system that connects (1) the backbone below and (2) its commercial applications above. Standardizing the encryption layer preempts the inconsistencies of technicalities across local markets and ensures the growth of commercial applications. The APEC Privacy Initiative stated:

> The potential of electronic commerce cannot be realized without government and business cooperation to develop and implement technologies and policies. … APEC economies realize that a key part of these efforts must be cooperation to balance and promote both effective privacy protection and the free flow of information in the Asia Pacific region (APEC, 2004a).

In short, the formulation of an APEC standard is logical prior to the integration of the virtual markets, that is, the secure flow of marketplace information across borders (see Corbitt & Thanasankit, 2002; Greenleaf, 2004).

4. The global techno-policy

4.1. Former colonies and colonists in Bangkok 2003

It was ironic that Asia's former colonists gathered in Bangkok to discuss the future of cyber-networks in their former colonies. The conference was symbolic. First, it was the first 'Expert Seminar' at the APEC working group level that aimed for a unified cyber security standard regime. Second, the meeting was to operationalize the principles of the EU cyber crime convention in the context of the Asian Pacific rim. In sum, the forum offered the venue (1) to translate previous agreements (e.g. Cyber Security Strategies[1]) from the summit to the working group level and (2) to initiate ensuing institutional efforts to harmonize technical inconsistencies prior to the implementations in member states.

4.2. Form vs. content

The APEC E-Security Task Force organized the Bangkok Meeting (APEC, 2003a). The meeting was hosted by Thailand's National Science and Technology Agency, but funded by the Computer Crime and Intellectual Property Section of the US Department of Justice. Participants included the delegates of Asian South Economic Association Nations (ASEAN) as well as those from the 'Four Tigers,' the US, Japan, and Britain (as a special participant). The forum operated with a multi-funding mechanism that facilitated the involvement of nation-actors in different power roles. Note the institutional characteristics of the forum. There are two reasons for this. First, the APEC itself is designed to promote institutional consensus building, rather than legally binding agreements (Aggarwal & Morrison, 1999). Second, different levels of infrastructure and economic power within the region make it difficult to formulate any uniform solution (Aalberts & Der Hof, 1999; Dempsey, 2003). The E-security Working Group President Westby observed, "My experience is that the legal frameworks in many countries are woefully deficient. Many developing countries are not now working on an international level, and they need help on how to do that. Just having a point of contact [APEC meeting] is probably something that hasn't occurred to most of them" (Krebs, 2002).

In this regard, the APEC cyber security regime is an institutional mechanism that 'educates' the region's developing nations about marketplace norms in order to potentially define policy standards in member states. Thus, the emphasis is on the 'form' that encourages the consensus building process, not the 'content' of policy that entails enforcement or implementation from one nation to another (see Klein, 2005; Mueller, Mathiason, & McKnight, 2004). Consequently, it is not surprising that the contents of APEC joint resolutions are generalized and lack enforcement powers.

4.3. Action plan

The joint statement forged at the Bangkok meeting indicated the very nature of 'normative appeals' in the APEC regime. The statement encouraged the formation of "comprehensive legal frameworks to combat cybercrime and to build law enforcement units capable of investigating cybercrime" (Legard, 2003). Other objectives included (1) to assist countries to develop a legal framework, and (2) to enhance understandings and cooperation between industry and law enforcements (APEC, 2003b).

So far there have been at least five cyber security conferences at the working group or ministerial level. A keyword search of 'e-security' in the official APEC website generates more than 20 policy documents written by either individual member-states or working groups. Nevertheless, the evidence that the APEC meetings exercised direct influence on national cyber security and encryption policy is slim. Neither did APEC produce any concrete policy resolution or timeline that to be implemented in member-states.

In fact, the survey of the APEC suggested that only a few advanced nations adequately implemented e-security measures in 2003–4, the

[1] Cyber Security Strategies, endorsed in 2002, is by far the most comprehensive guidelines for APEC member states (APEC TEL, 2002). Specific proposals include: (1) increase in cooperation in cyber-crime investigation, (2) improvement in interactions between law enforcement and industry, and (3) promotion of public awareness/sharing information in cross-jurisdiction cyber-crime.

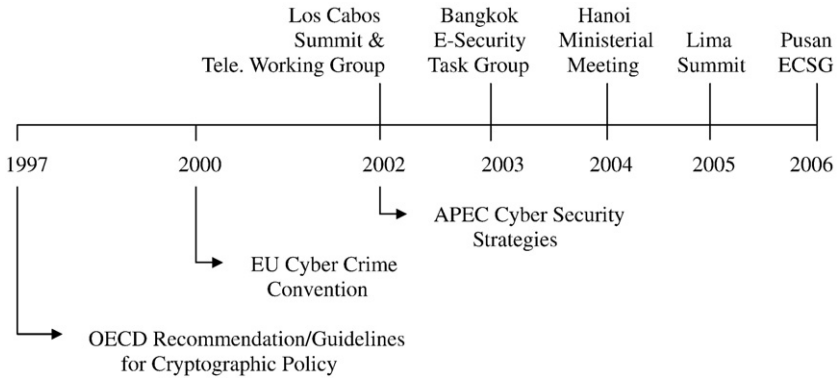

Fig. 1. Timeline of APEC cyber security regime. *Note*. ECSG refers to Electronic Commerce Steering Group, APEC.

period after Cyber Security Strategies was first formulated in Shanghai (2001) (APEC, 2003b; 2004b; Sadowsky, Dempsey, Greenberg, Mack, & Schwartz, 2003). Furthermore, as of this writing, no further development has been made at the APEC level. Note a succession of 'training' sessions at the multi-level of APEC regime since the 1997 OECD Guidelines (Fig. 1). However, this is not a comprehensive list. In 2003, for instance, there were two more technical seminars (July and August) and one summit (October) in Bangkok alone. The point is to indicate the symbolic function of consistent transnational efforts addressing market interoperability in the absence of effective formal agreement or concrete proposals (see Dempsey, 2003; Lewis, 2003).

Rather, the effect of the APEC regime is on the principle. The regime provides the frame of a set of beliefs and norms from which the member states draw their own policies. Note the primary function of the APEC from its very inception, that is, that APEC is originated to solidify the regional diffusion of market liberalism (Beeson & Jayasuriya, 1998). In this sense, the APEC is a "meta-regime" that functions in cognitive frameworks driven by the principles and norms of intraregional trade (Aggarwal, 1993). Now the internet moves the meta-regime into the cyber marketplace. It simply puts a symbolic marker of the market rationale behind "comprehensive cyber security laws on par with existing international standards of Council of Europe Cyber-crime Convention" (the White House, 2002). In short, what's being formulated in APEC policy forums is a broad framework in which nation-states are encouraged to adopt locally. Alternative policy visions are curtailed with the promotion of the market-friendly policy position.

5. National appropriation

5.1. Common threads of East-Asian information policy

Variations in policy enforcement exist into minute details in both the mechanical and legal spheres. Nevertheless, the parallels of cyber security policy among the 'Four Tigers' are astounding:

- Policy (digital signature) based on the modification of the PKI standard.
- Rapid government-driven policy implementation.
- Emphasis on market infrastructure and transactional activities over information privacy concerns. (Modified from Venturelli, 2002)

These commonalities, in fact, weave through internet security policy formation in the 'Four Tigers' as described in the following sections.

5.2. South Korea

The Korean cyber-marketplace is primarily supported by two legislations: (1) digital signature and (2) the Communication Secret Protection Law (which provides legal remedies for users who seek financial compensations for unlawful breach of transaction data). The Korean government is one of the most active entities moving to legalize and implement 'paperless' signature (e.g. Digital Signature Act 1999) that is legally binding both online and offline (NIDA, 2006).

5.3. Singapore[2]

The main encryption legal statue is the 1998 Electronic Transaction Act, passed the same year as the US 'E-sign' (Global and National Commerce Act by the Clinton Administration). The 'Electronic Contracts Certification Authority' presides over digital signature and authentication of electronic documents (AGC, 2007). The Computer Misuse Act (1998) also addresses criminal offence such as unauthorized access or modification of the contents of computers and networks.

5.4. Taiwan/Chinese Taipei

The government enacted the Digital Signature Act in 2001, followed by the Computer Data Protection Act. These formulate the criminal codes in electronic transactions. For instance, any unauthorized access or online fraud conviction carries a maximum penalty of seven years imprisonment (Ou, Shan, & Ho, 2004).

5.5. Hong Kong/China

In Hong Kong, cyber-crime is treated in the same manner as offline financial fraud. For example, the Electronic Transaction Ordinance (2000) covers online data-related offence and imposes a maximum penalty of ten years imprisonment. In addition, the government actively enacted the "Digi-Sign E-Certificate" program (digital signature electronic certificate) that issues 'e-cert' for the verification of user identities over the public data networks (Wu, 2000).

5.5. Policy contrasts

Here it is necessary to reconstruct the policy stance of 'Four Tigers' at the time of the Bangkok Meeting. Note the contrast between other APEC member states and the 'Four Tigers.' First, the U.S. and the E.U. are sharply divided over the encryption standard (Andrews, 2000). Second, the ASEAN, despite its earlier resolution of cyber security coordination, falls behind in the infrastructure readiness that can capture its policy goals (Gomez, 2004). Prior to 2003, however, the 'Four Tigers' had already begun to implement the PKI standard in its legislations. In short, the policy regimes of the 'Four Tigers' moved,

[2] Singapore is a member of ASEAN. However, its membership is not so much about its economic or infrastructural status as about the geographical proximity to South East Asian nations. Also note that the status of Chinese Taipei is represented as a ministerial, not summit, level official in the APEC.

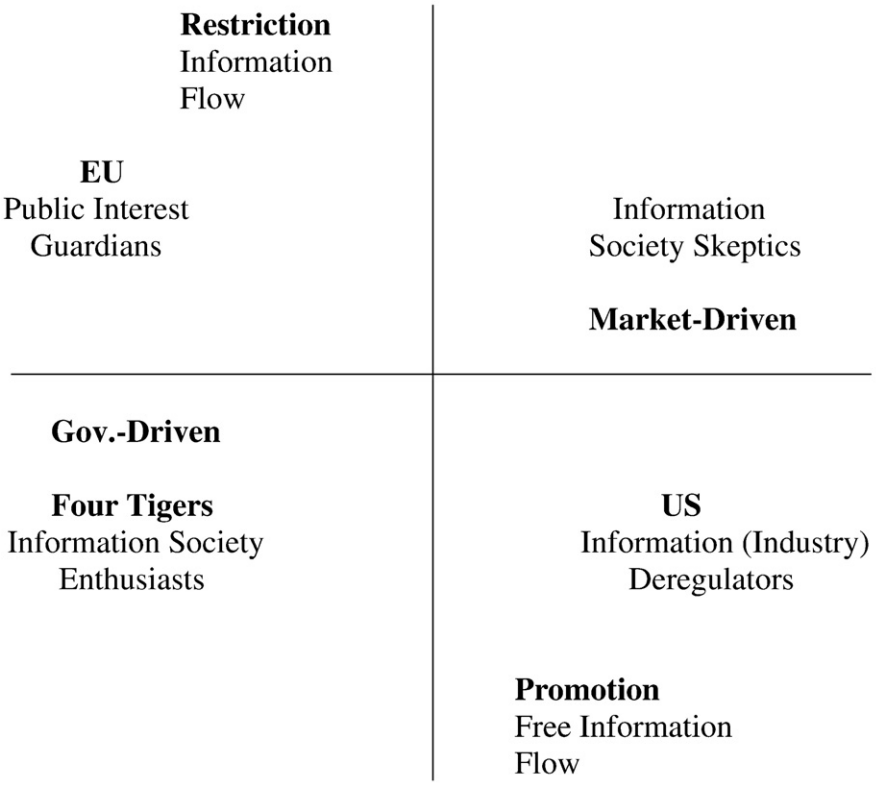

Fig. 2. Dimension of information policy. (Modified from Dutton et al., 1996).

ahead of the tangible APEC policy consensus, toward an interoperable legal framework within the Pan Pacific single market.

Compare the rush of the 'Four Tigers' and the clash between the U.S. and the E.U. (Andrews, 2000; Spyrelli, 2002). On the one hand, the liberal U.S. policy tends to favor information flow over citizens' privacy rights, that is, to the advantages of law enforcement agencies and commercial firms (Tygar, 2003). On the other hand, the E.U. Directive (and the E.U. Cyber Crime Council) restricts flow of information with the recognition of information privacy as a human right (Maxwell, 2002).[3] What the 'Four Tigers' opt for is the third alternative, one in which government favors corporate-friendly information flow (see Fig. 2). This is different from the E.U. in that the restriction of information flow is far less stringent. The approach also deviates from the U.S. because the government, not the market, takes initiative in constructing the protocol of information flow.

5.6. Industrial legacies

A central feature of the 'Four Tigers' is the development of markets through effective adaptations of technologies already pioneered in the advanced nations. This developmental model takes the form of government-led industrial policy (Amsden, 1989; Venturelli, 2002; Wade, 1995), typically with the national initiatives that aim to maximize the ability of key private firms in order to increase national competitiveness as quickly as possible (Johnson, 1982; Vogel, 1998). This was the mindset behind 'Catch Up Capitalism' in post WWII East Asia (Okimoto & Saxonhouse, 1987):

- First, rapidly build up national highway systems.
- Second, 're-engineer' imported technologies by adding values.
- Together, maximize the efficient flow of goods (that were 're-manufactured') for a market system.

In contemporary attitudes by political elites toward new technologies, as in the post WWII East, the infrastructure is to be 'programmed' to champion the nation's strategic industry and survival (Evans, 1995; Saxenian, 2006; Woo-Cummings, 1999).

In this sense, the 'sweeping' adoption of a techno-policy standard (PKI) is not surprising. It agrees with the industrial developmental model of most East Asia nations (Evans, 1995; Venturelli, 2002). The policy standardization serves as a fast solution for e-commerce industry development (see Fig. 3), given the amount of time and

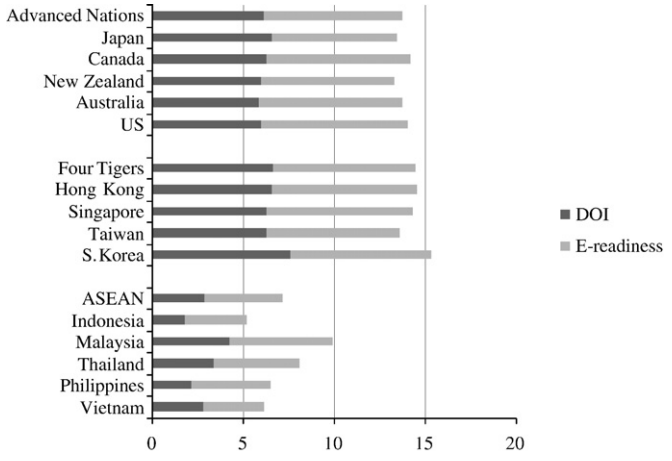

Fig. 3. Different tiers of selected APEC economies and ecommerce readiness. *Notes*. a. E-readiness (Economist, 2004) measures a set of factors that indicate market amenability of Internet-based opportunities in each nation. b. Digital Opportunity Index (ITU, 2007) measures the degree of Information Society readiness at (1) infrastructural, (2) business, and (3) access levels. DOI is converted into the scale equivalent to e-readiness.

[3] The tension between information flow and rights-to-privacy is well recognized in the APEC Privacy Initiative, the 1998 E.U. Data Directive, and the 1980 OECD Guidelines. Here information flow refers to the transfer, appropriation, and retention of personally identifiable data for commercial or political surveillance purposes.

energy saved for devising regulatory options that are workable with other nations. Policy priority is on the infrastructural standardization to 'catch up,' not the maturity of the civic codes to be evolved on the top of infrastructure. Rather, civil rights demands are deemed 'too chaotic' to harness within a highly formulated policy (Johnson, 1982). Above all, a central, hierarchical, and highly coordinated economic effort is hardly in accordance with alternative visions that regard the internet as democratic mediums spreading individual rights (Pool, 1983).

5.7. Civic codes

Here it is crucial that the 'Four Tigers' internet e-security legislations are formulated in a closer alliance with the U.S. than the E.U. (Lewis, 2003).[4] Note, however, the criticism over the U.S. key recovery system (that bases its digital signature act) for the restrictions on encryption technology. According to Andrews (2000), the U.S. key recovery system had been criticized for "vesting vast powers in third-party agents who have neither the incentive nor knowledge to contest any government intrusion." In fact, the US government had supported escrowed encryption (i.e. the standard with a central party holding users' keys for easier access) (EPIC, 2000; Etzioni, 2004). Consider the regime characteristic of the Chinese/Taipei, HK/China, and S. Korea, all adjacent to, or part of a communist regime. For decades, the governments have taken for granted information surveillance over citizens' political activities (Chin, 2005). One of the arguments in this paper is that this ideological stance at least provides ample grounds upon which e-security policies, favorable to information flow, are easily built over commercialized nets (see George, 2003; Lee, 2004 for Korea).

The reference point for comparison is the OECD principle. The 1997 OECD Guidelines recognized that, "Fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic method" (OECD, 1997 as cited in EPIC, 2000). The E.U. Cyber Crime Council is the closest in the policy commitment to the OECD standard, while the U.S. leaves much of protection to the private sector and self-regulatory policies (Spyrelli, 2002). The 'Four Tigers' policy stance remains far lower in terms of individual rights than the E.U., but perhaps more or less equivalent to that of the US.[5]

In 2006, Privacy International ranked overall surveillance practices in Singapore as 'black,' that is, an endemic surveillance society. In Taiwan, about 13,834 wiretaps were approved in 2003 alone for the reason of "national security" or "social order" (EPIC, 2005). Moreover, one policy evaluation of 20 nation-states graded the levels of privacy protection in Singapore, Taiwan, HK/China, and S. Korea as F, D, D, and C –, far below those of most E.U. nations and the U.S. (Mohl, 2005).

In fact, the PKI is an ambiguous technology (Castells, 2003). On the one hand, it can be used to preserve confidentiality, but it can also provide the basis of advanced tracking and identification. In other words, the mere presence of e-security legislations (or PKI) does not indicate the level of information privacy protection. To repeat, the 'fast' implementation of the PKI is not (as is often claimed by the 'Four Tigers') equivalent to strong privacy protection (Mohl, 2005; see NIDA, 2006). Rather, it is important to recognize that such implementations happened in the absence of strict regulations of the secondary use of personal data. That is, with no legal due process regulating the flow of information, control resides in proprietary codes of a network server in which one is allowed to cancel anonymity with ease (Lessig, 2000). It is like having a protective seal, but a third party can easily obtain permission to open the seal and appropriate the contents inside the envelope (see Etzioni, 2004). In short, the security (encryption), to be effective, should reside in the continuum of privacy protection (information flow).

The proposal is that policy orientation embedded in regulatory legacies explains why and how internet security regimes are being operated in particular ways. The critique by Jackson (2005) is poignant here. For him, the 'Multimedia Super Corridor' initiative of Malaysia exemplified the tendency of developing nations to risk their economic aspirations rather than exclude certain social values. Jackson asked, "For whom is freedom and mobility enhanced, and for whom is it constrained" within the national ambition of constructing a techno-pole? Note that most ASEAN members regard the 'Four Tigers' as the model for their economic 'leapfrogging' (Henke & Boxill, 2000), that is, policy discourse in developing nations tends to disregard civic demands while championing infrastructure readiness. It is no surprise that ASEAN also rectified its own cyber security treaty in 2003 (Gomez, 2004). Yet its regime is confounded by (1) infrastructural readiness far below that of the 'Four Tigers,' and (2) the stagnant internet security implementation process (APEC, 2004b). Moreover, there is no comprehensive data protection equivalent to that of the E.U. Directive. In sum, the regulatory commitment to citizens' rights to privacy remains immature as the policy priority is on the deployment of the internet, not on the incorporation of civil rights demands. Perhaps, it is accurate to say that there exists another tier of nations aiming to 'catch up' within the 'Catch Up Capitalism' of the APEC.

The crucial point is this: the type of debate between the U.S. and the E.U. over citizens' rights to information privacy has been nearly absent in the 'sweeping' policy (PKI) implementations of the 'Four Tigers.' Rather, new technology policy is formulated in industrial terms that aim for market interoperability, not for the maturity of civic society that is also to be evolved in the cyberspace (see Yang, 2005 for Greater China region). Note that e-security legislation is not about how the use of personal information should be governed. Rather, it is about maintaining the integrity of the original message at the level of infrastructure and concerns illegal activities such as tampering or hacking. To put it bluntly, the 'Four Tigers' are active in e-security/digital signature because it concerns transactional activities and perceived economic values. Consequently, the policy effort to balance between information flow and rights to privacy is almost ignored, but for different reasons than in the U.S.

6. Policy implications

6.1. Process: regime formation

The 2003 Bangkok Meeting epitomizes the kind of consensus to which the APEC nations are heading in aiming for the Pan Pacific marketplaces. On the one hand, the nature of the institutional setting at the international level generates no definitive policy consensus beyond general principles and norms of marketplace ideals (see Hosein, 2004). On the other hand, at the national level, the regulatory legacies that are geared toward industrial leapfrogging reinforce the policy deployment of new technologies. This fills the absence of effective agreement in the international realm (see Cogburn, 2003). In terms of the APEC e-security policy battle, the net result for the 'Four Tigers' is the hyper-activation of industrial legacies that rationalize the domination of commercial codes over civil rights concerns.

Horwitz (1989) offers a critical point regarding late 19th century America when he recalls the facilitation of the interstate

[4] It is important to note the significant impact of US policy within the APEC since its inception. In fact, even prior to 9/11, the U.S. had exercised its diplomatic and economic influence to persuade other nations to adopt its restrictive standard (EPIC, 2000). Unlike the E.U., the U.S. policy had stood against uninhibited use of encryption with no central registration. As of this writing, however, no clear development was reported in this regard as the Patriot Act did not include any specific clause in this matter (see Etzioni, 2004).

[5] This comparison is offered in a relative sense. The difference we cite concerns the level of information privacy protection embedded in a policy vision. Thus, given the differences in actual enforcement among the E.U. nations, it is not intended to promote the E.U. as an ideal, (Andrews, 2000).

infrastructure (e.g. canal, railroad, and postal services) in an early form of the capital market system. In fact, the state actively intervened in order to consolidate market-friendly infrastructural conditions. For example, the rules such as public subsidies or rate balance were formulated for the stimulation of economic conducts by private entities. Here it can be argued that the late 19th century market intervention in the U.S. took a similar form of industrial legacies as the 'Four Tigers' in the late 1970s. The legitimization of the state alliance with private interests always took a form of the state building embodied in commercial rationale. Critical here is the role of 'administrative rationality' in appropriating new technology according to market potentials (Horwitz, 1989). In other words, the very function of industrial legacies lies in its rationality in providing a firm foundation behind market-favored state intervention.

In this regard, it is a mistake to perceive the process of the 'Four Tigers' online security policy formulation as a zero-sum game. It is never a one-way imposition from a few APEC superpowers. Neither is the case of the states acting on behalf of elite commercial interests 'captured' by transnational e-commerce industry. Rather, it is a voluntary solution for the 'Four Tigers' to develop policies that comply with transnational marketplace norms and principles. In other words, new information policy regime evolves within a broad framework of the norm-building process through which nation-states interact (Braman, 2004; Cogburn, 2003). Accordingly, the states' active incorporation of the APEC agenda is to be understood as (1) the extension of the 'logic of industrialization' into cyberspace and (2) the strategic adaptation that aims for efficiency rather than civic societal concerns.

6.2. Consequence: commercial protocol

The transnational desire to establish robust e-commerce environments has generated two contrasting results. First, there was the hyperactive norm-building process of homogeneous e-security measures (public key/digital signature). Second, the prompt policy response happened in sharp contrast with the inactiveness in formulating strict measures over the secondary use of personal data. In short, the commercial code that favors free flow of information is being constructed as the de facto protocol in the region (see Kammerer, 2006).

Regarding the function of the APEC e-security regime in the context of the APEC Privacy Initiative, Greenleaf (2004) widely criticized the Initiative for its level of privacy protection that is far weaker than that of the 1998 EU Directive (EPIC, 2005; Heisenberg & Fandel, 2004). The scope of protection in the Initiative is minimal and does not cover comprehensive surveillance activities in the private sectors (Laurant, 2005). In this regard, the logical architecture of the APEC internet marketplaces looks as follows:

- In the top layer, industrial self-regulation is being encouraged under the lowest common protection standard.
- In the middle layer, the APEC e-security consensus pushes for the adoption of a standardized technical code (PKI).
- In the bottom layer, there is a physical network driving the convergence of the virtual marketplaces, yet its development is markedly uneven along the Pacific Rim (see Fig. 4).

It is important to note how the top two layers governing information flow is structured in conjunction with one another. For instance, the E.U. PKI is being implemented in compliance with the E.U. Data Directive. What matters is this configuration of protection embedded in the pattern of the layers, because information flows, not in isolation of each layer, but in combination with other layers (Lessig, 2000). Put differently, the very reason the E.U. protection regime is solid is that the strict measures of the secondary use of data are mandated to operate with the PKI. With the 'built-in' standard secondary to that of the E.U. (Greenleaf, 2004), the APEC regime configuration is, not of balance, but of bias toward data flow. In short, the protection of information privacy, by its policy design, is weak.

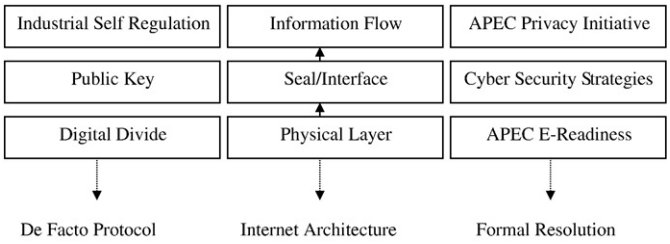

Fig. 4. APEC regimes in three logical layers.

According to Gandy (1993), Bentham's Panopticon is a social construct rather than a pure engineering consideration. Foucault (1995) himself noted that the architectural configuration itself does not automatically lead to the tyranny of surveillance (Agre, 1999; Marx, 1995). Rather, the surveillance embedded in the architecture is the function of the regime that has a particular ideological bias (Mansell, 1996). Recall the history of radio in the U.S., in which the commercialization of the public spectrum is construed in the 1927 Radio Act (Douglas, 1989; Hargittai, 2004; Streeter, 1996). The argument here is that the commercial code favoring flow of information is the construct of the regulatory regime that encourages a particular design of the otherwise democratic sphere.

7. Conclusion

7.1. The construction of the marketplace protocol

Departing from regime theory, this study brings critical attention to the function of regulatory legacies in new information policy being formulated within a broad framework of international policy regime. The market-oriented policy protocol in the 'Four Tigers' confirms the claim that the regulatory legacies embedded in each nation operate in interaction with the particularities of emergent regional policy demands. Thus, it is arguable that the construction of new technology is an artifact of deliberate policy choice rather than the pure push from the technology itself. Simply put, different regulatory regimes are likely to harness the democratic potentials of the internet in different ways (see Edwards, 2003; Sawhney, 1999).

In this regard, the untested hypothesis that new technology brings liberalizing potentials to developing nations should be revisited. Effects of new technology are conditional upon institutional variables and are not monolithic (Castells & Cardoso, 2005; Fisher, 1998; Neuman, 1991). Note the contradiction between the infrastrusctural success that even surpasses those of advanced nations, and the inaction towards civil rights in the 'Four Tigers.' The success is within the fixed policy framework that reproduces the condition of the economic rationale of industrialization. Further marginalization of civil rights protection accelerates, rather than decelerates, among the national entities whose championing new technology is advanced in such regulatory legacies.

Acknowledgments

An earlier draft of this article was presented at the annual meeting of International Association of Mass Communication Researchers (IAMCR), Taiwan in 2005. The author is indebted to Dr. Steven Jackson and Dr. W. Russell Neuman at the University of Michigan for their guidance and support.

References

Aalberts, B. P., & Der Hof, S. (1999). Digital signature blindness: Analysis of legislative approaches toward electronic authentication.*The EDI Law Review*, *7*(1) Retrieved July 2005, from http://www.buscalegis.ufsc.br/arquivos/Digsigbl.pdf
Abbate, J. (1999). *Inventing the internet.* Cambridge, MA: MIT Press.
Aggarwal, V. (1993). Building international institutions in Asia-Pacific. *Asian Survey*, *33* (11), 1029–1042.

Aggarwal, V., & Morrison, C. (1999). APEC as an international institution. In I. Yamazawa (Ed.), *APEC its challenges and tasks in the 21st century* (pp. 298–324). New York: Routledge.

Agre, P. (1999). The architecture of identity: Embedding privacy in market institutions. *Information, Communication and Society*, *2*(1), 1–25.

Amsden, A. (1989). *South Korean and Taiwanese development and the new institutional economics.* New York: Oxford University Press.

Andrews, S. (2000). Who holds the key? — A comparative study of US and European encryption policies.*The Journal of Information, Law and Technology*, *2* Retrieved August 2006, from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/andrews/

APEC Telecommunications and Information Working group. (2002). APEC Cyber Security Strategies: Business Facilitation on Steering Group. Retrieved August 2006, from http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf

APEC. (2003a). Strengthening international law enforcement cooperation to prosecute cyber criminals, hackers and virus authors. Media Releases. Retrieved August 2006, from http://www.apec.org/apec/news___media/2003_media_releases/180703_sin_strengthening_international_law.html

APEC. (2003b). Cybercrime legislation and enforcement capacity building project. E-Security Task Force Conference Report. Retrieved August 2007, from http://web.archive.org/web/20041215030512/http://www.apectelwg.org/apec/atwg/report1.htm

APEC. (2004a). APEC ministers endorse the APEC privacy framework, Media Releases. Retrieved November 2004, from http://www.apec.org/apec/newsmedia/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html

APEC. (2004b). Survey of cybercrime legislation — Final report: E-security task group. Retrieved August 2007, from http://web.archive.org/web/*/http://www.apectel28.com.tw/document/webword/estg/telwg28-ESTG-07.doc

Attorney General's Chamber. (2007). Singapore statue online. Retrieved August 2007, from http://statutes.agc.gov.sg/non_version/cgi-bin/cgi_retrieve.pl?actno=REVED-88&doctitle=ELECTRONIC%20TRANSACTIONS%20ACT%0a&date=latest&method=part&sl=1

Bar, F. (2001). The construction of marketplace architecture. *Tracking a transformation: ecommerce and the terms of competition in industries* (pp. 27–49). Washington, DC: Brookings Institution Press.

Beeson, M., & Jayasuriya, K. (1998). *The political rationalities of regionalism: APEC and the EU in comparative perspective.* London, UK: Routlege.

Braman, S. (2004). *The emergent information policy regime.* UK: Palgrave Macmillan Ltd.

Castells, M. (2003). *The internet galaxy.* New York: Oxford University Press.

Castells, M., & Cardoso, G. (2005). *The network society: from knowledge to policy.* Jhu-Sais: Center for Transatlantic Relations.

Chin, S. J. (2005). Diverging information societies of the Asia Pacific. *Telematics and Informatics*, *22*, 291–308.

Cogburn, D. (2003). Governing global information and communications policy: emergent regime formation and the impact on Africa. *Telecommunications Policy*, *27*, 135–153.

Corbitt, B., & Thanasankit, T. (2002). Acceptance and leadership — Hegemonies of e commerce policy perspectives. *Prometheus*, *20*(1), 39–57.

Dempsey, J. (2003). Creating the legal framework for information and communications technology development: The example of E-signature legislation in emerging market economies. *Information Technologies and International Development*, *1*(2), 39–52.

Douglas, S. (1989). *Inventing American broadcasting, 1899–1922.* ML: The Johns Hopkins University Press.

Dutton, W., Blumler, R., Garnham, N., Mansell, R., Cornford, J., & Peltu, M. (1996). The politics of information and communication policy: the information superhighway. *Information and communication technologies: visions and realities* (pp. 387–406). New York: Oxford University Press.

Edwards, P. (2003). Infrastructure and modernity: force, time, and social organization in then history of sociotechnical systems. In T. Misa, P. Brey, & A. Feenberg (Eds.), *Modernity and Technology* (pp. 185–225). Cambridge, MA: MIT Press.

Electronic Privacy Information Center (EPIC). (2000). Cryptography and liberty 2000: An international survey of encryption policy. Retrieved August 2007, from http://www2.epic.org/reports/crypto2000/overview.html#Heading2

Electronic Privacy Information Center (EPIC). (2005). Privacy and human rights report 2005: Country report. Retrieved August 2006, from http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-542783&als[theme]=Privacy%20and%20Human%20Rights

Etzioni, A. (2004). *From empire to community.* New York: Palgrave Macmillan.

Evans, P. (1995). *Embedded autonomy: states and industrial transformation.* Princeton, NJ: Princeton University Press.

Fisher, C. (1998). *America calling: a social history of the telephone to 1940.* Berkeley: University of California Press.

Foucault, M. (1995). *Discipline & punish: the birth of the prison.* New York: Vintage Books.

Friedlander, A. (1995). *Emerging infrastructure: the growth of railroads.* Virginia: Corporation for National Research Initiatives.

Friedman, J., & Martin, L. (2002). International political economy: global and domestic interaction. In I. Katznelson, & H. Milner (Eds.), *Political science: the state of the discipline* (pp. 118–146). New York: W.W. Norton & Company.

Gandy, O. (1993). *The Panoptic sort: a political economy of personal information.* Boulder, Co: Westview Press.

Garfinkel, S., & Spafford, G. (1997). *Web security and commerce.* CA: O'Reilly & Associates, Inc.

George, C. (2003). The Internet and the narrow tailoring dilemma for "Asian" democracies. *The Communication Review*, *6*(3), 247–268.

Gomez, J. (2004). Dumbing down democracy: Trends in internet regulation, surveillance and control in Asia. *Pacific Journalism Review*, *10*(2), 130–150.

Greenleaf, G. (2004). The APEC privacy initiative: 'OECD Lite' for the Asia-Pacific? *Privacy Law & Business*, *71*, 16–18.

Hargittai, E. (2004). *The changing online landscape: From free-for-all to commercial gatekeeping.* In P. Day & D. Schuler, Community practices in the network society: local actions/global interaction (pp. 66–76) New York: Routledge.

Heisenberg, D., & Fandel, M. -H. (2004). Projecting the EU regime abroad: The EU data protective directive as global standard. In S. Braman (Ed.), *The emergent global information policy regime* (pp. 109–209). UK: Palgrave Macmillan Ltd.

Henke, H., & Boxill, I. (2000). *The end of the 'Asian model'?* The Netherlands: John Benjamins Publishing Company.

Horwitz, R. (1989). *The irony of regulatory reform: the deregulation of American telecommunications.* New York: Oxford University Press.

Hosein, I. (2004). The sources of laws: Policy dynamics in a digital and terrorized world. *The Information Society*, *20*(3), 187–199.

International Telecommunication Union. (2007). The digital opportunity index. World Information Society Report. Retrieved August 2007, from http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07-chapter3.pdf

Jackson, S. (2005). Technopoles and development in a 'borderless world': Boundaries erased, boundaries constructed. In H. Nicole & I. Townsend-Gault (Eds.), *Holding the line: borders in a global world* (pp. 308–330). Vancouver, BC UBC Press.

Johnson, C. (1982). *MITI and the Japanese miracle: the growth of industrial policy, 1925–1975.* Stanford, CA: Stanford University Press.

Kammerer, P. (2006). *Privacy on parade: many Asian countries are failing to safeguard their citizens' rights in the digital age. South China Morning Post.*

Kerr, O. (2003). Internet surveillance law after the U.S. *Patriot Act: the big brother that isn't. Northwestern Law Review*, 607–673.

Klein, H. (2005). Understanding WSIS: An institutional analysis of the UN world summit on the information society. *Information Technology and International Development*, *1* (3–4), 3–13.

Krebs, B. (2002). US aiding Asia-Pacific anti-cybercrime efforts. Washington Post. Retrieved July 2005, from http://seclists.org/isn/2002/Aug/0050.html

Laurant, C. (2005). International developments in privacy laws. Based on the findings of EPIC's annual survey. Retrieved August 2007, from http://www.thepublicvoice.org/events/ibero4th/laurant.pdf

Lee, K. S. (2004). Surveillant institution eyes in Korea: From discipline to a digital grid of control. *The information Society*, *20*, 187–199.

Legard, D. (2003). Security group furthers plans to combat cybercrime: Countries need to pass wide-ranging laws, cooperate openly. InfoWorld. Retrieved July 2005, from http://www.infoworld.com/article/03/07/29/HNcombatcrime_1.html

Lessig, L. (2000). *Code and other laws of cyberspace.* New York: Basic Books.

Lewis, J. (2003). *Cyber security: turning national solutions into international cooperation.* Washington, D.C.: Center for Strategic and International Studies.

Lindloff, T. (1995). *Qualitative communication research methods.* CA: Sage.

Mansell, R. (1996). Designing electronic commerce. In R. Mansell, & S. Roger (Eds.), *Communication by design: the politics of information and communication technologies* (pp. 15–43). Oxford: Oxford University Press.

Marx, G. (1995). The engineering of social control: The search for the silver bullet. In J. Hagan & R. Peterson (Eds.), *Crime and inequality* CA: Stanford University Press.

Maxwell, R. (2002). The marketplace citizen and the political economy of data trade in the European Union. In J. Lewis & T. Miller (Eds.), *Cultural policy: a critical reader* (pp.149–160). Malden, MA: Blackwell.

Mohl, B. (Sept 14, 2005). *Markey files legislation to protect privacy of personal data overseas*. The Boston Globe.

Mueller, M., Mathiason, J., & McKnight, L. (April 26, 2004). *Making sense of "Internet Governance:" defining principles and norms in a policy context. Internet Governance Project, Syracuse University The Convergence Center. V 2.0.*

Napoli, P. (2001). *Foundations of communications policy: principles and process in the regulation of electronic media.* NJ: Hampton Press.

Neuman, W. R. (1991). *The future of the mass audience.* New York: Cambridge University Press.

National Internet Development Agency of Korea (NIDA). (2006). Survey on the information and communication. Retrieved August 2007, from http://www.nic.or.kr/english/

Okimoto, D., & Saxonhouse, G. (1987). Technology and the future of the economy. In K. Yamamura, & Y. Yasuba (Eds.), *The political economy of Japan: the domestic transformation* (pp. 385–419). CA: Stanford University Press.

Ou, C. -M., Shan, H. -L., & Ho, C. -T. (2004). Government PKI deployment and usage in Taiwan. *Information and security: an international journal*, *15*(1), 39–54.

Pool, I. S. (1983). *Technologies of freedom.* Cambridge, MA: Harvard University Press.

Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B. J., & Schwartz, A. (2003). Information security and government policy. Information Technology Security Handbook. Retrieved August 2007, from http://www.infodev-security.net/handbook/

Sandivig, C. (2003). Introduction to the special issue: Policy, politics, and the local Internet. *The Communication Review*, *6*(3), 1–6.

Sawhney, H. (1999). Patterns of infrastructure development in the US and Canada. In H. Sawhney, & G. Barnett (Eds.), *Progress in communication science: advances in telecommunications* (pp. 71–91). Stamford, CT: Ablex.

Sawhney, H., & Wang, X. (2005). Battle of systems: Learning from erstwhile gas–electricity and telegraph–telephone battles. *Prometheus*, *24*(3), 235–256.

Saxenian, A. (2006). *The new Argonauts: regional advantage in the global economy.* MA: Harvard University Press.

Spyrelli, C. (2002). Electronic signatures: A transatlantic bridge? An EU and US legal approach towards electronic authentication.*The Journal of Information, Law and Technology*, *2* Retrieved January 2004, from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/

Standage, T. (1998). *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers.* New York: Walker and Company.
Streeter, T. (1996). *Selling the air: a critique of the policy of commercial broadcasting in the United States.* Chicago: University of Chicago Press.
The Economist. (2004). The 2004 e-readiness rankings: A white paper from economist intelligence unit. Retrieved August 2006, from http://www.investinestonia.com/pdf/ERR2004.pdf
The White House. (2002). Fact sheet: APEC leaders' retreat, counterterrorism, US accomplishments. Retrieved January 2004, from http://www.whitehouse.gov/news/releases/2002/10/20021026-6.html
Tygar, D. (2003). Technological dimensions of privacy in Asia. *Asia-Pacific Review*, *10*(2), 120–145.
Venturelli, S. (2002). Inventing e-regulation in the US, EU and East Asia: Conflicting social visions of the information society. *Telematics and Informatics*, *19*(2), 69–90.
Vogel, S. (1998). *Freer Markets, More Rules: Regulatory Reform in Advanced Industrial Countries.* New York: Cornell University Press.
Wade, R. (1995). *Governing the market: economic theory and the role of government in East Asian industrialization.* New Jersey: Princeton University Press.
Woo-Cumings, M. (1999). *The developmental state.* New York: Cornell University Press.
Wu, R. (2000). Electronic transactions ordinance — Building a legal framework for e-commerce in Hong Kong.*The Journal of Information, Law and Technology*, *1* Retrieved August 2007, from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_1/wu/
Yang, K. (2005). A comparative study of Internet regulatory policies in the Greater China region: Emerging regulatory models and issues in China, Hong-Kong SAR, and Taiwan. *Telematics and Informatics*, *24*, 30–40.

Yong Jin Park is a Ph. D Candidate in Department of Communication Studies at the University of Michigan. His research centers on social and policy implications of new communication technologies. His previous research spans the field of information policy, media institutions, and new media users. His works will appear in Journal of Communication, Sociology Compass, the Information Society and Info: Journal of Policy, Regulation and Strategy for Telecommunication (all forthcoming in 2008). He also presented a number of articles in such conferences as TPRC, IAMCR, MPSA and AEJMC. His work on the impact of duopoly ownership (currently under review) was cited in numerous policy reports to the FCC media ownership hearings. Also he contributed to East-Asia sections of 2006 Privacy and Human Rights Report: EPIC (Electronic Privacy Information Center). Currently, he is working on his dissertation that seeks user-driven policy solutions for Internet privacy. He holds a MA from Annenberg School for Communication at the USC.