Research Publication No. 2003-09
12/2003

Analysis and Critique of Mongolia's Draft Law on Information Technology

Andrew McLaughlin

Analysis and Critique of Mongolia's Draft Law on Information Technology

Andrew McLaughlin
Berkman Center for Internet & Society
Harvard Law School
21 December 2003

I. Introduction

Mongolia's Ministry of Infrastructure has proposed a Draft Law on Information Technology that is now being considered by Mongolia's State Great Khural, the country's parliament.[1]

The core conclusion of this analysis and critique[2] is that the Draft Law as it now stands would do significant harm to Mongolia's vibrant and promising information and communication technology (ICT) sector. For the reasons detailed in this analysis, the Draft Law should be substantially revised and rewritten. To fulfill its responsibilities as the guardian of the people of Mongolia, the Great Khural must give careful consideration to each of the many policy choices that would be codified in the provisions of the Draft Law. An alarmingly high portion of the policy choices in the Draft Law will cause harm to Mongolia's national Internet and e-commerce sectors and to its future as a competitive player in the global information and communication technology markets. Many provisions are confused and confusing, apparently reflecting a lack of technical understanding.

At home, the Draft Law would crush e-commerce with unnecessary regulatory burdens, block effective deployment of new technologies and infrastructures, raise the costs of Mongolia's ICT enterprises, restrict the range and reduce the quality of communications services, and increase the monthly bills for Mongolian users. If the Draft Law is approved and implemented as it is currently written, Mongolian citizens will be saddled with fewer choices, older technology, slower connectivity, higher prices, irrational limits on technology, and more bureaucracy. Perhaps worst of all, the Draft Law's burdensome regulations are so vague and

---

[1] Ministry of Infrastructure of Mongolia, Draft Law on Information Technology (September 2003), English translation available online at <http://cyber.law.harvard.edu/mongolia/draft-law-sep03.html>.

[2] This analysis and critique was prepared at the suggestion of several colleagues and partner organizations both inside and outside of Mongolia, including the Open Society Institute (which provided funding for it), the Global Internet Policy Initiative (GIPI), a number of Internet service providers, and the Mongolian Information Development Association (MIDAS), a non-profit technology policy research and advocacy organization. My thanks to each of them. I also wish to acknowledge the ongoing financial and intellectual support of the Berkman Center for Internet & Society at Harvard Law School.

expansive that they will undoubtedly open new vistas for governmental abuse and corruption. For Mongolia, the net result would be a costly tragedy of short-sightedness and a squandering of potential: with its high levels of education, literacy, and technical skills, the country is well-situated to be a highly competitive player in the global market for ICT services.

Mongolia deserves much better than the broken legal framework of the Draft Law on Information Technology. If the country is to foster entrepreneurship, local enterprise, and low-cost, high-quality ICTs for all Mongolians, the Draft Law must be thoroughly reconsidered and rewritten.

II. Summary of Findings and Recommendations

General. The Draft Law's terminology and definitions are too often confused, vague, inaccurate, incomplete, imprecise, contradictory, and/or simply missing.

Independent Regulator. The Communications Regulatory Commission (CRC) should be granted full, actual, meaningful independence to do its work without the influence or interference of the Ministry of Infrastructure. Unless the CRC can be turned into an independent and expert national regulatory authority, the Great Khural should craft detailed legislation that sets the precise policy objectives and procedural requirements that must be applied by the CRC on matters such as setting tariffs and fostering network interconnection on reasonable terms.

Dispute Resolution. The courts, not the CRC, are the proper forums for the adjudication of disputes between licensees and their customers.

Electronic Signatures. The Draft Law's chapter on electronic signatures is a hopelessly confused mess that would wreak tremendous damage to Mongolia's Internet economy; it should be deleted and replaced in its entirety.

E-Commerce. The Draft Law should be revised to provide that contracts in electronic form are legally valid, that they can serve as the basis for legal actions, and that electronic documents are admissible in court to prove the terms of the agreement between the parties.

Licensing of Information and Communications Services. "Information technology services" should not be licensed in the same manner as "communication services." Indeed, Internet service providers (ISPs) should not be subjected to any licensing requirement. If a licensing scheme must for some reason be imposed, Mongolia should establish a general authorization (i.e., class license) model that does not require prior discretionary approval by the CRC, thereby minimizing bureaucracy and opportunities for abuse.

ISP Liability. The Draft Law should provide explicit liability protection for network intermediaries, such as ISPs.

Interconnection Pricing and Accounting. All telecommunications service providers should be required to adhere to transparent, consistent, and comparable financial reporting standards.

.mn Country-Code Top-Level Domain. A government attempt to seize the .mn top-level domain could generate catastrophic instability, and is an all-around bad idea. Instead, the Mongolian government should work cooperatively with the current manager of .mn, along with the leading Internet community stakeholders, to develop a broadly representative and accountable not-for-profit entity that can assume responsibility for policymaking and operational oversight.

Role of Parliament. Mongolia's State Great Khural must play a much more active role in formulating national policy on information technology, writing needed legislation, and conducting oversight of the government's actual implementation of the law. Reliance on the Ministry of Infrastructure is not appropriate in light of its intimate financial link to Mongolia Telecom.

Executive Branch Management. The Mongolian government should consider appointing a Chief Information Officer and/or Chief Technology Officer to lead institutional information technology implementation efforts inside the Mongolian government.

National ICT Committee. The National Committee of Information and Communication Technology is a good idea, but will require dedicated staff support to be effective.

National ICT Park. Enterprises located in the National ICT Park should not be given special government subsidies (direct or indirect) that are not available to businesses located in other buildings.

Public Access to Information. The exceptions to citizens' right of access to e-government information should be narrowed and clarified; and the process for adjudication of disputes should be reconsidered and rewritten to give jurisdiction to the courts.

III. Analysis and Critique of the Draft Law on Information Technology

The Draft Law on Information Technology consists of ten chapters and 56 articles. This analysis proceeds section-by-section. The translation on which it based is available online at <http://cyber.law.harvard.edu/mongolia/draft-law-sep03.html>.

- ***Chapter One: General Provisions***
    - ***Article 3: Legal Terminology***

The first chapter of the Draft Law begins with some general language about the purpose of the Draft Law, the primacy of international treaties, and the definitions of specific terms. In translation, it is difficult to critique the definitions. However, it appears that several of the definitions are unnecessarily vague and, therefore, open to misinterpretation and abuse. Precision and specificity are particularly important where the definitions draw the line between legal and illegal conduct.

Article 3.1.4 - For example, *Article 3.1.4* defines "illegal use of information" as "illegal access to information system and data base taking advantage of skills and knowledge of using information methods, tools and software." Even discounting for the fog of translation, the definition borders on the tautological. Ordinarily, legal prohibitions on "unauthorized access" to computers and computer networks include the element of intent (i.e., what did the trespassing user intend to do?), in order to distinguish between malicious hacking and inadvertent stumbling. By contrast, the Draft Law's definition turns on the use of "skills and knowledge," which provides little clarity and, therefore, little certainty for courts and no protection for innocent individuals. Even an accidental computer trespasser takes advantage of "skills and knowledge."

Article 3.1.5 **-** *Article 3.1.*5 defines "electronic documents or records" as "information in electronic form on a computer." Generally speaking, a broad and inclusive definition of an "electronic document" is appropriate for this kind of legislation. However, the Draft Law's definition lacks an element that is common in laws to legitimate electronic signatures, namely, that legal recognition attaches only to documents whose properties allow their authenticity to be determined. In this way, the law recognized only those electronic documents that can be somehow authenticated, whether through digital signature, electronic signature, or otherwise.

Of greater concern are the Draft Law's deeply flawed definitions relating to electronic signatures and digital certificates. At root, they appear to embody some fundamental misunderstandings about the purpose, use, and technical nature of electronic signatures and digital certificates. This analysis addresses these definitions' shortcomings below, in the discussion on Chapter Seven (Electronic Signatures).

Article 3.1.12 - In *Article 3.1.12*, the Draft Law defines the term "informatics" in a fairly unconventional way: "systematic social, economic, scientific and technical activities aimed at creating a favorable environment for meeting the information needs and rights of citizens, state organizations and legal entities through creation and use of information sources". Generally speaking, "informatics" refers to the branch of computer science dedicated to managing, organizing, analyzing, and presenting information. For the sake of consistency, it would probably be better to use the standard definition, or employ a different term (such as "information society"). The term is employed in the Draft Law not in the context of computer science, but, for example, in directing the cabinet member in charge of information technology to approve a work plan, budget, and security policy for informatics. For the sake of clarity, either the definition or the substantive references should be changed.

Article 3.1.13 - In *Article 3.1.13*, the definition of "information" is given as "data, which is not dependent on the known conventions in his/her representation." Again, even accounting for the vagaries of translation, this is an unusual definition. It would likely be confusing to a judge or magistrate lacking training in the peculiarities of information technology. A more standard, and more easily comprehensible, definition might be: "'Information' is data, text, images, sounds, codes, computer programs, software, databases, or the like." (See, e.g., the U.S. federal law on electronic signatures, 15 U.S.C. § 7006 (2002)).

Article 3.1.14 - The definition of "factual information" in *Article 3.1.14* is confusing, and the term does not appear anywhere else in the Draft Law. Accordingly, it should be dropped (unless, of course, the confusion stems from translation).

Article 3.1.15 - In *Article 3.1.15,* the Draft Law defines "information system" in a way that might better fit "digital network" or "network information system". Generally, laws on information technology contain a definition that distinguishes digitally networked information systems. In the United States, for example, the federal Communications Act uses the term "interactive computer service," as distinct from "information content providers" and "access software providers." (See, e.g., 47 U.S.C. § 230). To be prudent, the Draft Law should be revised to utilize a consistent and comprehensive set of terms and definitions, carefully distinguishing between the different roles of the various entities comprising the Internet and its component networks and service providers.

Article 3.1.16 - The Draft Law's definition of "confidential information" in *Article 3.1.16* incorporates by reference "the relevant law of Mongolia." Accordingly, it will be important to ensure that there exists elsewhere in Mongolian law a relevant and applicable definition of "confidential information." The definition needs to be tailored to the specific target of the provision. Most countries' legal systems employ several definitions of "confidential information", depending on

the context. For example, securities exchange laws and laws protecting trade secrets may define "confidential information." Laws to protect data privacy define the types of information that government agencies and/or companies in the business of collecting personal data are permitted to disclose, to whom, and under what conditions. What is confusing (and problematic) about the inclusion of a general, non-contextual definition at *Article 3.1.16* is that a more detailed definition appears later in the Draft Law at *Article 16.12*, in the context of a planned e-Governance Information Database: "Confidential information shall comprise documents, data and information related to privacy of state and organizations and individuals which have been legally identified as prohibitive to expose for not damaging rights and reputation of individuals and for the interest of national defense and security and social order." That latter definition makes relatively good sense in the context of a government database containing personal information from and about citizens (although the definition is so general as to gives exceptionally wide discretion to the government to determine what pieces of information can be withheld from public review). Absent context, the Draft Law's general definition of "confidential information" is likely to generate more confusion than clarity. It should be dropped in favor of specific definitions that are tailored to their legal contexts.

Arts. 3.1.19 & 3.1.20 - *Articles 3.1.19* and *3.1.20* set forth definitions of "sender of electronic data message" and "receiver of electronic data message" that appear to be designed to relieve "intermediaries" of liability for the actions of the originators of communications. This principle ("Don't shoot the messenger!") is extremely important. In light of the technical architecture of the Internet (in which communications typically travel across numerous intervening networks that exercise no control or scrutiny over the contents of the data packets), Internet service providers (ISPs) and other network intermediaries should be protected against liability for the actions of others. Because ISPs are not creating, controlling, or reviewing the contents of the traffic over their networks, they should not be held legally responsible for it.

For the sake of comparison, following are two examples of legal provisions that protect intermediaries from legal liability:

- Germany: "Providers shall not be responsible for any third-party content to which they only provide access." Sec. 5(3), Information and Communication Services Act.

- USA: "No provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider." Sec. 230, Communications Act (47 U.S.C. § 230)

Currently, the Draft Law does not include any such explicit intermediary liability protection clause such as these. It simply states definitions that might (or might

not) be interpreted to create such a shield. If an objective of the Draft Law is to create ISP and intermediary liability protection (as I believe it should), then the Draft Law should state it directly and unmistakably.

Moreover, the definitions in *Articles 3.1.19* and *3.1.20* use odd language that may imply some meanings that do not fit the purposes of the Draft Law. The Draft Law defines "sender" to be the person or entity that "is legally entitled to send" the communication. I can think of no reason why the definition should not specify the person or entity that *actually sent* the communication, rather than whomever was "legally entitled to send" it. (One can imagine a person sitting down at a friend's unattended desktop computer and sending out some falsified emails to others; the owner of the computer is the person "entitled to send" emails from that machine, but it is her friend who, in fact, sent the email. The Draft Law could be interpreted to regard the owner, rather than the emailing friend, as the "sender.") Being entitled to do something is not the same as doing it; it is the actual act, not the entitlement, that should carry any legal consequences.

Likewise, the definition of "receiver" refers to the person or entity that "is intended by the sender to receive" the communication. Here again, for the sake of clarity, the definition should specify that the recipient is the person or entity that *actually received* the communication. At a minimum, the definitions should show an understanding of the potential difference between an intended recipient and an actual recipient. On the Internet, there may be a big difference between the two, and most information technology statutes distinguish them carefully.

Article 3.1.21 - The definition in *Article 3.1.21* is alarming. First, the term "e-commerce runner" has no apparent precedent. Perhaps a term such as "licensed e-commerce provider" would better fit the intended definition. Second, and more importantly, the definition implies that a state license will be required to engage in e-commerce. (*Article 40.1* does not clarify the issue, at least not in translation). A universal licensing scheme for e-commerce could potentially devastate the expansion and use of the Internet by Mongolia's private sector. As new advances in wireless networking becomes commonplace realities – and as the Internet becomes a truly pervasive presence – virtually any business in Mongolia (restaurants, taxis, food stores, banking services) can use the Internet to conduct transactions. To imposing a separate licensing requirement on every business that wishes to start creating economic value by using the Internet to interact with customers would add a tremendous and unnecessary disincentive on businesses to do exactly that. In light of Mongolia's remote location and small population, the country should be working to remove barriers to e-commerce, not to impose a massive barrier in the form of a universal licensing scheme.

Article 3.1.23 – The Draft Law's definition of "intermediary" in *Article 3.1.23* (as translated) is simply wrong, as it includes senders or receivers as intermediaries. For a better definition, see Article 12 of the European Union's Electronic Commerce Directive, which provides that ISPs are not liable for information

transmitted on their networks, provided they do not initiate the transmission, do not select the receivers of the transmission, and do not select or modify the information in the transmission. This exemption of liability extends to the automatic, intermediate, and transient storage of the information, provided it is not stored for any longer than "reasonably necessary."

- ***Chapter Two: Authority of the State Administration in Information and Technology***

    - ***Article 4: Authority of the State Great Khural***
    - ***Article 5: Authority of the government***

Articles 4 and 5 are recitations of the respective responsibilities of the legislative and executive branches of the Mongolian government for "information and technology." This phrase is problematic, in that each term alone is too broad, conceivably encompassing all information and all technology. The Draft Law does not purport to cover press and media regulation, or mining technologies. The Draft Law should be limited to the intersection of the two terms: information technology. Given the confusing and unconventional definition of "information" at *Article 3. 1.13*, it would be better for the recitation of authority to state clearly that the scope of the Draft Law is "information and communication technology," accompanied by an appropriate definition in *Article 3*. "Information and communication technology" is a widely-used and well-understood term, and provides the proper focus for the Draft Law. There are numerous references to "information and technology" throughout the Draft Law; these should all be changed to "information and communication technology" (commonly abbreviated as "ICT").

Together, *Articles 4 and 5* specify that the legislative branch (the Great Khural) is responsible for setting state policy and establishing the legal rules, while the executive branch (the government) is responsible for implementing the policy and enforcing the law. In addition, *Article 5* gives several specific jobs to the government: (a) to establish a national committee on "information and technology" (which, as noted, should rather use the phrase "information and communication technology")[3], (b) to create a "fund for public service" (presumably a universal service fund), and drafting regulations for its use, and (c) "to promote and facilitate any organization, enterprise, individual and legal entity that are effectively introducing information and technology."

That last provision, *Article 5.1.4*,[4] is a critically important component of the Draft Law, and should be highlighted. It commits Mongolia's government to support

[3] Rather than repeat this comment every time the term "information and technology" appears in the Draft Law, I will simply assume that the phrase can be corrected and will instead use the term "information technology" in its place.

[4] The government "shall exercise … authority … to promote and facilitate any organization, enterprise, individual and legal entity that are effectively introducing information and technology."

those organizations and individuals that are bringing ICTs to the Mongolian people, businesses, universities, and government. It reflects a basic recognition that affordable and reliable ICTs, together with robust entrepreneurship, are essential to the economic future of the country. In a sense, many of the criticisms of the Draft Law set forth in this paper are due to the failure of specific provisions to meet the objective stated in *Article 5.1.4.*

- ***Article 6: Authority of the member of the government in charge of information and technology***

Article 6 defines the responsibilities and authority of the Mongolian Cabinet official in charge of information technology. There appears to be a basic and inconsistent overlap between the stated responsibilities of the Great Khural and those of the responsible Cabinet official. As I am not an expert in Mongolian constitutional law, I do not if this apparent conflict is real or explainable under settled principles of Mongolian jurisprudence.

The issue is whether the Great Khural or the executive branch has ultimate responsibility for setting state policy on information technology. *Article 4.1* states that the Great Khural "shall define a state policy" for information technology; at the same time, *Article 6.1.2* states that the Cabinet member must "develop a coherent and consistent state policy on information technology." As I understand the Mongolian system, it would be better (and more accurate) to specify that the Great Khural has the authority to set state policy for ICTs; the Cabinet member's job is to implement that policy and, in cases where policymaking authority is explicitly delegated by the Great Khural to the government, to draft the specified policies and regulations.

The importance of this point lies in the fact that even though Mongolia's parliament is formally the supreme authority in Mongolia, there is considerable evidence that Mongolia's executive branch has acted (and is acting) in ways that are inconsistent with the laws and policies established by the Great Khural. The Great Khural does not have a tradition of vigorous oversight of the executive branch to assess compliance and implementation of state policies and laws. The Draft Law should not suggest that the Cabinet member has independent policy-making authority; rather, the executive branch should be bound to implement the legislation approved by the Great Khural, and to undertake policymaking only where clearly delegated by the legislature.

Several provisions in *Article 6* are useful. For example, *Article 6.1.3* calls upon the Cabinet member in charge of information technology to "promote competitiveness in information technology market." Indeed, it would be an improvement if the provision were strengthened so that all department-level decisions relating to ICTs were required to consider and report the likely impact on market competition.

Article 6.1.8 provides that the Cabinet member will pursue training in information technology for "professional staff." If the meaning of "professional staff" encompasses the Mongolian government across all departments, then this provision could be quite significant. *Article 6.1.9* appears to go well beyond the Mongolian government, though, calling on the designated Cabinet department to develop a work plan and overall budget for "informatics," pointing to the unconventionally broad definition of "informatics" in *Article 3.1.12*.

There is some danger in such a wide mandate. My recommendation is for the Mongolian government to focus its immediate efforts on the use of information technology to support its own functions and operations. As a consumer of services, and as the operator of potentially the largest network and information system in the country, the Mongolian government can help to shape and bolster a competitive domestic market for ICTs. It makes sense to have the Cabinet department responsible for information technology assume a general role in advocating for cost savings and efficiency improvements within the functions of government through the implementation of information technologies, and to support those efforts with training. However, a powerful alternative strategy would be for the Mongolian government to appoint a Chief Information Officer (CIO) and/or Chief Technology Officer (CTO) to lead institutional information technology efforts inside the Mongolia government (these would be operational, not policy-making, postitions). The CIO or CTO could be located within a Cabinet department, or could lead a cross-departmental government ICT services support unit reporting directly to the prime minister.

Several provisions in *Article 6* are at least slightly confusing. For example, *Article 6.1.5* refers to "public service." I presume that this is a mistranslation of the "universal service" concept.

Several ensuing sections are problematic, or worse.

Article 6.1.7 calls upon the Cabinet member in charge of information technology to "ensure the reliability, efficiency and quality of information technology services and control the security of electronic signature and information relations." This provision goes far beyond the appropriate role for government in ICTs. Government's job is to enable encourage, not to "ensure," the reliability, efficiency and quality of ICT services. In a competitive market, Mongolian citizens can choose the providers that offer the right trade-offs among cost, reliability, efficiency, and quality. The verb "ensure" implies a much heavier role for the Mongolian government than is healthy. Mongolians must keep in mind that they are competing against countries that impose very few regulations and restrictions on their ICT industries; if Mongolia wants to be at the forefront of economic development and growth, it must avoid heavy regulation and allow its citizens to develop and offer entrepreneurial new services and to make consumption choices within the broad confines of an open and fair market. The role of the Cabinet department should not be to "ensure" outcomes, but to

promote competition, create incentives for deployment of the latest technologies, and encourage the private sector to follow international best practices in business and technology. For the Cabinet department to act as a guarantor of reliability, efficiency, and quality would require heavy-handed, intrusive, and counterproductive regulation that would put Mongolia at a competitive disadvantage compared to other developing countries.

Likewise, *Article 6.1.7's* directive to the Cabinet member to "control the security of electronic signature and information relations." This is simply an impossible charge. No one can "control" Internet security, or even the security of electronic signatures. It is up to the senders and receivers of communications (such as email and web pages) to use encryption, digital signatures, virtual private networks (VPNs), and so forth, according to their needs. Information security is not a status that can be controlled, but a set of practices by senders, recipients, and intermediaries. *Article 6.1.7* states a goal that cannot be attained, and implies an objective that should not be undertaken by a government.

Article 6.1.10 and *Article 6.1.11* places very broad duties on the designated Cabinet member to protect "information and information resources," ensure their security, and "control over security and safety of informatics," and to "ensure reliability, efficiency, and quality of informatics." These provisions are useful and positive to the extent the apply to the Mongolian government's use of ICTs. But if the intention is that a government Cabinet department is to assume responsibility for these functions on behalf of the entire Mongolian public, academic, and private ICT sectors, then the provisions have set impossible and counterproductive objectives. It is neither possible nor desirable for a government department to "control" the security and safety of Internet communications.

Mongolia is a market-based democracy seeking to achieve economic success in a highly competitive global market. As such, its government should focus on support and promotion (for example, using its role as a major potential consumer of ICTs), rather than control.

The final clause of *Article 6* is extremely unclear.[5] It appears to provide that whenever a Mongolian government department appoints or fires the management of a state-owned entity, that department must "consult" with the Cabinet member in charge of information technology. The rationale for this provision is not evident to me; it may be of little or great significance, perhaps relating to the planned privatization of Mongolia Telecom. In any event, the language, background, and objective of this clause needs clarification before it can be analyzed or critiqued.

[5] "The authorized organization shall consult with member of government cabinet in charge of information technology when appointing or resigning the management of legal entity of sole state ownership or with participation of state in ownership."

- ***Article 7: Authority of Governors***

As to *Article 7*, I reiterate a broader criticism of the Draft Law: it does not scrupulously distinguish between ICT networks owned/operated by the Mongolian government and ICT networks owned/operated by others. When the Draft Law grants powers and authorities to governmental actors, the need for precision and clarity is much greater when they apply to non-governmental networks than when they apply to governmental networks only. In order to justify and sustain investment in new technologies, non-governmental network operators (such as ISPs, banks, and universities) must be afforded protection from arbitrary government action. This is especially true where, as in Mongolia, the government owns one competitor among many -- namely, the former monopoly telecom provider. Ambiguous statutory language permits abuse.

Article 7 is a good example of ambiguous statutory language that is capable of being misapplied and abused, in this case by Mongolia's governors. *Article 7.1.2* states that Mongolia's governors are permitted to "organize repair and remedy actions of damages in information network and software caused by accidental or disastrous conditions." As applied to networks and software owned and operated by the Mongolian government, this clause makes perfect sense. However, as applied to non-governmental (i.e., private and academic) networks, this clause, on its face, gives governors the ability to take advantage of any "accidental conditions" to intervene. In the wrong governor's hands, the clause permits him/her to use an unrelated "accident" to gain access to a non-governmental network's infrastructure or, worse yet, software and data.

In order to prevent potential abuse, this clause should be either (a) limited to governmental networks, or (b) supplemented with a range of definitions specifying the specific "accidental or disastrous conditions" that can trigger action by the governors, along with the particular kinds of interventions that are permitted. The clause should not enable governmental access to ISPs' "software" without a careful, specific, and narrow set of limitations (such as in the context of a criminal investigation authorized and supervised by a neutral magistrate). Non-governmental networks should have an explicit right to contest allegedly abusive interference by governors (or other governmental agencies) in the courts.

- ***Article 8: Authority of Communications Regulatory Commission***

The provisions of the Draft Law relating to the Communications Regulatory Commission (CRC) are seriously flawed. Most troublingly, the Draft Law delegates to the CRC broad authority and discretion that would be appropriate only if the CRC were truly an independent regulator; however, because the CRC continues, as a practical matter, to be subject to the will of the Minister of Infrastructure (to whom the CRC currently reports), the Great Khural can have no

confidence that the powers granted in the Draft Law will be exercised responsibly. The Draft Law should provide more detailed policy guidance to the CRC, and should reinforce the expectation that the CRC will become an independent, neutral, and trustworthy regulator, in fact as well as in theory.

Following are comments on the specific deficiencies in the Draft Law provisions relating to the CRC:

Interconnection. *Article 8.1.4* provides that the CRC has the authority to "approve general conditions of contract on inter-connection between networks…" Presumably, this is intended to empower the CRC to establish the requirements terms, conditions, and prices for inter-network inter-connection. The reference to "contract" is not entirely clear, but presumably refers to the CRC's ability to set interconnection requirements through its licenses. This section mirrors Section 9.1.4 of Mongolia's Telecommunications Law, which provides for the CRC "to approve general terms of interconnection agreements between networks and procedures of revenue distribution."

In a country like Mongolia, with a dominant wireline monopoly telecom operator (Mongolia Telecom) and a dominant mobile phone provider (Mobicom), the rules for interconnection requirements, prices and conditions are fundamental to the success or failure of the competitive marketplace. The overall efficiency and investment-worthiness of the ICT sector will largely be determined by the ability of new operators to connect to customers of the existing operators and to share existing network infrastructure on reasonable terms and conditions and at fair prices. The alternative would be for every telecom carrier to construct its own parallel, duplicate telecommunications network infrastructure, which would be both wasteful and prohibitively expensive.

Interconnection, if handled correctly, benefits both incumbents (who gain interconnection revenues from the new market entrants as they expand the overall customer base), new operators (who are able to compete with the incumbents and each other), and consumers (who benefit from lower prices and better services). The regulation of interconnection is essential to encourage fair and efficient competition, which, in turn, will force down end-user prices, encourage expanded use of existing infrastructure, generate new investments in network facilities, and maximize overall national market growth. Dominant telecom operators must be obligated to interconnect. Reasonable cost-based accounting methods and benchmarks must be developed, in light of available data. A consistent and predictable framework for carrier-to-carrier negotiations must be established, specifying the general outlines within which interconnection agreements may be concluded. A clear and speedy procedure for regulatory intervention and decision must be defined -- along with the neutral and objective criteria that will be applied by the CRC -- in the event that the parties cannot reach an agreement. And the CRC must have the capacity to police the system and enforce the rules: it must be able to detect, block, and remedy strategic

anticompetitive interconnection behavior by the incumbent, as well as exploitative gaming of loopholes by competitors.

The Draft Law does not address any of these considerations. It may well be reasonable for the Great Khural to delegate the details of interconnection pricing and conditions to the discretion of the CRC – but not if the CRC lacks meaningful, actual independence from the Mongolian government departments that have a particular interest in Mongolia Telecom (e.g., the Ministry of Infrastructure). In essence, the Great Khural is now confronted with an extremely significant choice. It must either: (a) fundamentally reform the CRC to make it a functionally independent and expert national regulatory authority, or (b) pass detailed legislation to define the precise policy objectives and requirements that must be applied by the CRC in crafting Mongolia's system of network interconnection.

If the CRC is not fully independent, it cannot be trusted with the creation of a fair, equitable, and efficient system of interconnection prices and conditions. Accordingly, the Great Khural must itself undertake to specify the objective standards that will shape the CRC's work, and by which the CRC's work will be judged. If the Great Khural can successfully reform the structure, staffing, and operations of the CRC to make it both independent and expert, then it would be reasonable to delegate to it the details of interconnection.

It may be useful to review the detailed interconnection regimes that have been implemented by diverse governments, for example, the European Union[6], the United Kingdom[7], the United States[8], Singapore[9], Estonia[10], Turkey[11],

---

[6] *See* the 1997 European Union directive on interconnection: "Notified operators shall meet reasonable requests for unbundled access to their local loops and related facilities, under transparent, fair and non-discriminatory conditions. Requests shall only be refused on the basis of objective criteria, relating to technical feasibility or the need to maintain network integrity. Where access is refused, the aggrieved party may submit the case to the dispute resolution procedure referred to in Article 4(5). Notified operators shall provide beneficiaries with facilities equivalent to those provided for their own services or to their associated companies, and with the same conditions and time-scales."

[7] *See* "Guidelines on Interconnection and Interoperability", available at <http://www.oftel.gov.uk/publications/1999/competition/gii799.htm>.

[8] *See* 47 U.S.C. § 251 and the implementing regulations of the Federal Communications Commission, both available at <http://www.internetpolicy.net/telco/us47-251.shtml>.

[9] *See* the Reference Interconnection Offer, available at <http://www.ida.gov.sg/idaweb/pnr/infopage.jsp?infopagecategory=&infopageid=I288&versionid=1>, the Interconnect Dispute Resolution Framework, available at <http://www.ida.gov.sg/idaweb/pnr/infopage.jsp?infopagecategory=&infopageid=I161&versionid=1>, and the regulator's information site on Interconnection and Access, available at <http://www.ida.gov.sg/idaweb/pnr/infopage.jsp?infopagecategory=&infopageid=I198&versionid=1>.

[10] *See* Chapter 7 of the Telecommunications Law, available at <http://sa.riik.ee/atp/failid/Telecommunications_Act.htm>, the "Cost Accounting Methodology for Leased Line and Interconnection Service Charges," available at

Lithuania[12], Botswana[13], and Uganda[14]. Though different, these various approaches to law and regulation all highlight the importance of detailed rules, set either by the parliament or the independent regulatory authority. Though Mongolia is not a relatively populous country, there is no reason why its telecommunications and IT regulations and regulations cannot meet the high standards set by small countries like Estonia (population 1.4 million), Lithuania (3.5 million) and Botswana (1.5 million). Indeed, given the sophistication and impressive entrepreneurial success of Mongolia's ICT sector, Mongolians should demand nothing less than a first-rate, detailed, straightforward, and transparent regulatory framework. By that measure, the Draft Law, as it now stands, is a serious disappointment.

Mongolia's CRC was created by the Telecommunications Law, passed in 2001. Articles 8 and 9 of the Telecommunications Law detail the division of responsibilities between the Ministry of Infrastructure and the CRC, but fail to ensure the actual independence of the CRC from the Ministry. Moreover, the experience of the past 2 years has demonstrated without a doubt that the CRC, while staffed by well-intentioned individuals, lacks effective independence from the Ministry. The Draft Law on Information Technology provides a rare opportunity to correct this glaring deficiency in Mongolia's common regulatory framework for information and communication technologies.

On a related note, the Draft Law does not improve transparency at the CRC. On a difficult and contentious issue like network interconnection, consumer and market confidence would be greatly enhanced by a stringent requirement that the CRC give public notice and opportunity to comment on all proposed policies and rules, monitoring statistics, financial data, and implementation and enforcement activities.

Tariffs. In a similarly vague way, *Article 8.1.5* assigns to the CRC the responsibility for approving "the methodology defining service tariff for information technology and control tariff prevalent in markets." Most of the foregoing comments about *Article 8.1.4* on interconnection (especially the need for clear, consistent, predictable, objective, and transparent rules, and the evenhanded enforcement of them) apply equally to this section, and I will not

---

<http://sa.riik.ee/atp/failid/tk%20cost%20leased.htm>, and the "Procedure for estimating competition conditions and specifying telecommunications markets
for the assignment of undertakings with significant market power", available at <http://sa.riik.ee/atp/failid/tk_OTE.htm>.

[11] *See* the Ordinance on Access and Internconnection, available at <http://www.tk.gov.tr/pdf/ordinance_access_interconnection.pdf>.

[12] *See* Chapter 2, Art. 5, of the Law on Telecommunications, available at <http://www.bild.net/resources/tellit.htm>.

[13] *See* Section 47 of the Telecommunications Act of 1996, available at <http://www.itu.int/ITU-D/treg/Legislation/Botswana/law.pdf>.

[14] *See* The Telecommunications (Tariffs and Accounting) Regulations of 2003, available at <http://www.ucc.co.ug/draftreg/tariffsAndAccounting.doc>.

repeat them. In light of Article 9.1.5 of the Telecommunications Law, it appears that this section is designed to extend the existing division of administrative tasks into the field of "information technology."

The Draft Law fails to state minimum substantive or procedural standards for the CRC's tariff-setting work. In general, telecommunications tariffs should be driven by market forces. Careful regulation of tariffs, however, may be needed to protect the interests of residential and rural customers. Even there, however, the Great Khural should establish as the national policy of Mongolia that telecommunications tariffs (particularly the charges imposed by the incumbent fixed line monopoly) will be reasonable, transparent, non-discriminatory, and calculated on the basis of actual costs. Mongolia Telecom (and any other dominant market actors) should be required to establish separate accounts for specified telecommunication services in order to prevent anti-competitive cross-subsidization and/or under-pricing. All telecommunications service providers should be required to adhere to transparent, consistent, and comparable financial accounting and reporting standards.

Here again, the essential point is that the Great Khural must specify these basic policies, requirements, and expectations, unless and until the CRC can be made to achieve full, actual independence from the Ministry of Infrastructure. Unlike the CRC (which is accountable to the Ministry of Infrastructure), the Great Khural (which is accountable to the people of Mongolia) is well-positioned to make policy in the best interests of all Mongolians.

Domain name administration. In *Article 8.1.6*, the Draft Law gives the CRC the authority to "approve [a] general plan of domain addresses, make registration and issue the addresses." In other words, the Draft Law intends that the CRC will take direct control of management and operations for the .mn top-level domain (TLD), forcing out the longstanding administrator – regardless of the wishes of the Mongolian Internet community. For a number of reasons, this is an unwise idea and should be deleted from the Draft Law.

First, the operation of a top-level Internet domain name registry requires extensive technical and management expertise. Most governments lack the necessary skills and capabilities to register domain names via the Internet, maintain databases, propagate TLD zone files in DNS, and handle customer interactions with current and prospective registrants. Based on my observations, the government of Mongolia has neither the technical infrastructure nor the customer service capability to undertake direct management and operation of the .mn registry.

Second, the most important feature of the .mn domain is long-term stability. Domain name registrants must have absolute confidence that their .mn domain names will work every day, 24 hours a day, without error or interruption. Long-term technical stability requires long-term organizational stability. Experience

worldwide has taught that direct governmental operation of a TLD is less stable and reliable than management by a community-based institution (typically a not-for-profit entity) that is representative of the various sectors of the local Internet community. It would be very harmful to the stability of a TLD to have management or policy changes every time there is an election and a new government or new minister comes to power. Some governments have treated their national TLD as a political prize, with the winning party controlling the jobs and the revenues (if any) that accompany it. Very often, government-run TLDs are subject to corruption, favoritism, unequal treatment, technical incompetence, and poor customer service. When a government-administered TLD starts to break down, customers will simply switch their domain names from the national TLD to a global TLD, such as .com, .org, .info, or .biz. The result is that registration fees get paid to global registries, rather than staying in the country. In other words, government mismanagement of a top-level domain inevitably results in the export of funds that ought to be staying within the country.

Of course, corruption, favoritism, unequal treatment, technical incompetence, and poor customer service can characterize a private-sector TLD manager, too. What, then, is the best structure to ensure long-term stability, low prices, fair treatment, technical excellence, and responsive customer service? Based on the past decade of domain name management experience worldwide, the most consistently reliable structures are non-profit institutions built around a representative, multi-sector policymaking committee. In this model, the top policymaking committee for the TLD is comprised of representatives of the key stakeholders in the local Internet community: ISPs, academic institutions, technical experts, the government, NGOs, and individual, organizational and business domain name registrants. In Brazil, for example, the policies for the .br registry are set by the Brazilian Internet Steering Committee,[15] which consists of several members appointed by each of those stakeholder groups. The Committee determines the rules for .br registrations, and is responsible for designating the entity to manage technical operations and provide customer services. The Committee operates in an open and transparent fashion, publishes detailed financial data, and gives every member of the Brazilian Internet community an opportunity to participate in its policy development and review processes. Compared to government institutions, these types of community-based institutions have historically done a much better job of assuring the long-term stability, technical excellence, and high-quality customer service of a country-code TLD.

The .mn top-level domain was delegated in March 1995 to Mr. Enkhbat Dangaasuren, who remains the responsible administrative contact. Currently, the institutional home for .mn is Datacom Co. Ltd., based in Ulaanbaatar. Since 1995, Datacom has operated the .mn TLD in a responsible and technically competent manner, making significant investments in the hardware, software, and connectivity required to provide excellent service to the Mongolian Internet

[15] *See* Comitê Gestor do Internet no Brasil, homepage at <http://www.cg.org.br>.

community. Over the past year, there have been serious discussions within the Mongolian Internet community about the need to transition the administration and policymaking functions for .mn from Datacom to a more broad-based, community-oriented setting. Fortunately for Mongolia, Enkhbat is willing to engage in these discussions, and has indicated that he is willing to work toward that objective. In other words, the current manager of .mn is willing to cooperate in creating a multisectoral TLD management structure that is open to all sectors of the Mongolian Internet community, including the government, ISPs, academic institutions, NGOs, and individual, organizational, and business users. Such an approach would be greatly preferable to a forcible takeover by government.

Third, the .mn registry is already located inside Mongolia, meaning that it is fully subject to Mongolian law and regulation. There is simply no pressing reason for the Mongolian government to seize control of the .mn TLD. If anything goes terribly wrong with the management or operation of the .mn TLD, the government has the necessary power and authority to step in. To date, there has been no crisis or evidence of mismanagement. There is no imperative for the government forcibly to take over a technical and customer-service operation that is now functioning well, and that will likely be transitioned in the near future toward an even more representative community-based management structure.

Fourth, it is not a trivial matter to seize control of a TLD. It cannot be done by flipping a switch on a computer. The TLD's current administrative organization is the only entity that actually has all of the data about the registrants of .mn domain names. Without the full cooperation of that entity, there is a danger that the TLD would have to be re-built from nothing, which would be a near-total catastrophe for the Mongolian Internet, banking, and academic sectors, and for anyone else who depends on a .mn domain. It is for these reasons that the global technical coordinating body for the domain name system – the Internet Corporation for Assigned Names and Numbers (ICANN) – pushes local Internet communities to resolve disputes about the management of a country-code TLD within the nation itself. Under the ICANN policies, the views of the government are taken very seriously, but are not alone decisive. A government cannot simply pick up the phone and demand that ICANN redelegate it to a government agency. As a technical matter, such a transfer is not possible without the cooperation of the current manager; and as a policy matter, the Mongolian government would have to demonstrate that the proposed seizure of the CRC is supported by the stakeholders of the Mongolian Internet community.[16] As one commentator has noted, global best practices have evolved to favor TLD management structures that "(1) embody the principle of private sector self-regulation, with the government playing a supportive but non-intervening role; (2) operate through

[16] See ICANN's "Internet Domain Name System Structure and Delegation" (ICP-1), available online at <http://www.icann.org/icp/icp-1.htm>. For an excellent explanation of the ICANN redelegation process, see Global Internet Policy Initiative, "Redelegation of Country Code Top Level Domains," (May 2003), available online at <http://www.internetpolicy.net/practices/030200cctld.pdf>.

open, transparent and inclusive processes; and (3) clearly benefit the local Internet community."[17]

In short, the Mongolian government should work cooperatively with the current manager of .mn, rather than making a unilateral move to seize control without consultation. A smart and forward-looking Mongolian government would cooperate with Mongolia's Internet stakeholders and help to build a community-based, multi-sector non-profit entity that can reliably administer and operate the .mn registry over the long term. As a first step, *Article 8.1.6* should be deleted from the Draft Law; and the National ICT Committee should undertake, as one of its next priorities, a dialogue with Datacom and Enkhbat and a broad consultation with the Mongolian Internet community to determine the best administrative structure for the long-term stability of the .mn TLD.

Resolution of disputes between license holders and users. In *Article 8.1.9*, the Draft Law states that that CRC will have the authority to settle disputes between "holder of license and user." This provision is entirely vague and, as a result, susceptible to abuse. To give the CRC a power to resolve disputes between "license holders" and "users" (presumably meaning customers of the license holder) gives tremendous power to the CRC without any guidance, limitation, or standards of adjudication. For example, is the CRC to resolve a billing dispute between an ISP and one of its subscribers? A customer's service complaint about a mobile phone company? The clause gives no clarity about the subject matters for CRC dispute resolution, or the standards that the CRC is to apply in making its decisions. There are no provisions for due process, nor any protections for license holders or users. In general, resolution of individual customer disputes is outside the competence of the CRC. Moreover, the CRC certainly lacks enough staff to become a effective adjudicative body for customer complaints.

However, it might be a good idea for the CRC to have a separate unit of several staffers that will investigate customer complaints and make recommendations to the CRC as to whether or not the license holder at issue is fulfilling the terms of its license. Based on the complaint and the investigation, the CRC could then seek to enforce the provisions of the license directly against the licensee. As a result of that proceeding, the licensee might agree to make refunds to one or more customers, or might upgrade service in a particular area. But it is important to recognize that license enforcement is different from the resolution of individual disputes between licensees and their customers. The CRC should be an independent regulatory body that implements the laws of Mongolia, not a judicial body with the power to adjudicate individual disputes. That means that the CRC should have the ability to receive and investigate customer complaints, and to enforce the terms of its licenses, but not the ability to act like a court and resolve individual disputes. Fundamentally, it would be unfair for the CRC to be the

[17] *Id.*, at 6.

issuer of licenses **and** the adjudicative body that decides disputes between license holders and their customers – that is what courts are for.

For the CRC to become an adjudicative body, the Great Khural would have to define the full set of substantive rules, procedural requirements, rights of appeal, filing periods, and so forth. A better system would be to allow the CRC the right to investigate complaints, negotiate compliance, and, if necessary, enforce its licenses by bringing legal actions through the court system.

Indeed, the Great Khural might consider the creation of an standing alternative dispute resolution system – for example, binding arbitration by a dedicated and independent panel of arbitrators – that would quickly resolve ordinary customer disputes with license holders. But such a system would have to be carefully constructed by the Great Khural to define the subjects that could be addressed, to set the possible remedies and maximum monetary awards, and to assure due process, impartiality, and fair rules of decision.

In short, adjudication of disputes between license holders and their customers should not be placed in the hands of the CRC without any further guidance. *Article 8.1.9* should be deleted or completely rewritten to address all of the critical missing components.

Digital Signatures. *Articles 8.1.10-.12* refer to digital signatures, which this paper addresses in the discussion of Chapter Seven, below.

○ *Article 9: National Committee of Information Technology*

Article 9 of the Draft Law establishes a national advisory committee on information technology, chaired by the Prime Minister and consisting of equal numbers of members from "state organizations, business organizations, education and science institutes, and NGOs." The secretariat function is to be provided by the Ministry of Infrastructure (specifically, its Information and Communications Technology Policy Coordination Division).

In this Article, the Draft Law formalizes the mission and structure of the currently-existing National Committee of Information and Communication Technology. The National ICT Committee is a good idea: it is useful to have a high-level forum in which the key stakeholders of the Mongolian Internet economy can discuss both pressing issues and long-term strategies, exchange information and learn from each other, and develop positive and cooperative relationships.

In view of the past two years of experience, however, the National ICT Committee has not lived up to its promise. It has held few meetings, and produced little substantive output. In part, this is because the chairman and members of the committee are extremely busy individuals with many competing demands on their time and energy. But primarily, it is because the Committee

has not had the benefit of dedicated staff support. In that context, it is essential for the National ICT Committee to have adequate secretariat staffing to develop its agenda, conduct research, organize meetings, and so forth. The amount of personnel can be small – perhaps a single full-time employee of the Ministry of Infrastructure.

Therefore, in addition to designating the Ministry of Infrastructure to perform secretariat functions for the National ICT Committee, the Great Khural might wish to specify a minimum amount of staff resources to be dedicated to it. Otherwise, there is a real danger that the National ICT Committee will be perceived by the staff of the Ministry of Infrastructure as an unwanted additional burden, and so continue to be neglected. Without an energetic and competent secretariat staffer, the National ICT Committee will likely fail to achieve its potential.

- ***Article 10: National Information Technology Park***

In *Article 10*, the Draft Law establishes a National Information Technology Park as "a state-owned, non-profit service organization with duties of creating and developing a favorable environment for information and communications system and network and facilitating information technology businesses."

Designed properly, a National IT Park can be a useful tool to foster new technology enterprises. A National IT Park can, for example, allow a number of start-ups to pool their purchasing power to obtain low-cost, high-speed Internet connectivity. Likewise, co-locating new start-ups together in a common facility allows entrepreneurs to share ideas, barter services, pool labor, create new joint ventures, and feed off of each other's energy.

However, there is a potentially serious downside to any scheme that provides subsidies only to those businesses that are located in the National IT Park. Subsidies tend to distort a market and create an uneven competitive playing field, regardless of whether they are direct (such as special tax breaks) or indirect (such as reduced-cost rent or Internet bandwidth). The result of such subsidies is that a new start-up's ability to gain admission to the National IT Park becomes a significant factor in whether or not it will be able to succeed. A business that is admitted to the National IT Park will benefit from the subsidies, while all other businesses must pay the higher, market-rate costs for rent, phones, Internet connectivity, and so forth. In effect, the business in the National ICT Park will have been granted a special subsidy by the government, simply by virtue of its physical location. Likewise, *Article 10.2.4* provides that the National IT Park will assist businesses located in the park to obtain contracts with state organizations and international agencies – without making the same offer to businesses that are *not* located in the National IT Park.

With their lower costs and special access to services and government contracts, businesses located at the National IT Park will have a highly valuable competitive

advantage relative to any competitors that lack the luck (or the diplomatic skills or, in the worst-case scenario, the willingness to pay bribes) to obtain a place there. Fundamentally, it is a bad idea to make the manager of the National IT Park the gatekeeper to success. Under *Article 10* as currently written, the manager of the National IT Park effectively becomes responsible for picking winners and losers – with the Park itself becoming the vehicle for central planning and control.

In short, special subsidies given on the basis of physical location are inherently irrational, from an economic point of view, and are likely to create serious market distortions. Businesses located in the National IT Park will have an inherent competitive advantage that does not derive from their innovations, prices, or quality of services. All those not located in the National IT Park will be forced to compete at a hefty disadvantage. That would make no sense, and would certainly harm Mongolia's global competitiveness in the long term.

A better solution is for the government to make subsidies available across the board, to all start-ups and businesses in the same position. For example, if the government wants to subsidize Internet connectivity for start-ups, the subsidy should be available to businesses both inside and outside the National IT Park. Alternatively, the government might allow for the creation of more than one non-profit IT parks, leaving it up to Mongolia's entrepreneurs to join together to share working space and connectivity costs – with the government defining a package of rent subsidies, connectivity subsidies, and tax breaks that apply to any businesses located in a qualifying IT Park. The point is that government subsidies must be made available to all businesses within a particular category, and not only to those that happen to gain admission to a particular building.

This is not to say that the National IT Park is a bad idea. Properly managed, a National IT Park can be an important mechanism for accelerating entrepreneurial growth in the technology sector. To be successful, the National IT Park should be careful to structure its subsidies so that they will be available to any qualified business that wishes to take advantage of them. The National IT Park might provide "connectivity vouchers" to businesses that cannot fit in its building, which could be used to offset the cost of Internet connectivity at any location; or it might make a commitment to expand and obtain new office space of equivalent quality when the initial building reaches capacity. The principle of fair and equal availability is especially true for tax incentives: any tax breaks that are given to businesses located at the National IT Park should also be afforded to any other businesses that compete in the same market.

- ***Chapter Four: Licensing***

Chapter Four of the Draft Law provides that the CRC will have the responsibility to "issue a license for information technology services and electronic signature." The Chapter further states that "information technology services" are to be

treated as "communications services" and subjected to the same licensing requirements specified in the Communications Law.[18] Finally, the Chapter provides that "Internet café services shall be registered only."

This Chapter of the Draft Law should be eliminated, or at least significantly altered. It would be a serious mistake for the Mongolian government to adopt a licensing regime that regards Internet service providers (ISPs) and other ICT businesses as "communications services." There are several reasons:

Vagueness. The Draft Law is vague as to its overall scope. The Draft Law does not include a definition of "information technology service," which could conceivably extend to every person or business that operates a web server, mail server, or even a home Ethernet hub. This vagueness is worrying because of the recent incidents when the CRC claimed that special licenses would be required to operate each and every Internet service protocol – meaning that separate licenses for HTTP (web), FTP (file transfer), NNTP (news) and SMTP (email) would be required. Such a requirement would be totally unique in the world. The CRC later dropped these particular licensing plans, but the episode demonstrates that the Great Khural cannot simply trust the CRC to correctly interpret the undefined term "information technology service." If the Great Khural is truly determined to require government licensing of ISPs (a bad idea, as outlined below), the Draft Law should include a clear definition of "internet service provider" and unambiguous language to specify that the licensing requirement extends to ISPs only, and not to every Mongolian who happens to operate Internet servers, business email services, or home networks. This is an extremely important point: Mongolia's impressive ICT sector is poised to flourish and grow, but will instead wither and die if it is burdened with the world's most restrictive licensing scheme (which is what the vague language of the Draft Law currently permits, and what the CRC evidently intends).

The harm of ISP licensing. More fundamentally, there is no compelling justification for subjecting ISPs and other ordinary ICT services to any special licensing requirement. In the most advanced economies of the world, ISPs and other ICT services are not required to obtain any special license in order to operate.[19] It is important to note that ISPs in these countries are not "unregulated". Rather, ISPs and other ICT services are simply subjected to the ordinary set of business laws and regulations that apply generally to all private-sector enterprises. In most countries, there is at least some legislation that specifically relates to ISPs and/or other ICT services – for example, a law specifying the standards that must be met by law enforcement agencies to obtain

[18] Communications Law of Mongolia, Articles 12 ("License"), 13 ("Documents for Application of License"), 14 ("Issuance of License and Refusal of License Application"), and 15 ("Revocation of License").

[19] In the United States, for example, no license or authorization is required to operate as an ISP. The United States regulatory authority has determined that the public interest does not require "information services" to be licensed or regulated.

access to an ISP's customer data. These laws are applied without the need for the ISP to have a special operating license.

The rationale for eliminating (or, at least, not extending) Mongolia's ISP licensing requirement is not merely the usual American-style obsession with deregulation. Rather, it is grounded is hard data, solid reasoning, and a decade of practical experience. A recent study by World Bank economist Scott Wallsten demonstrates that "countries that require formal regulatory approval for Internet Service Providers (ISPs) to begin operations have fewer Internet users and Internet hosts than countries that do not require such approval." [20] The study is especially impressive because it utilizes a unique set of data provided directly by regulators and controls for factors such as "income, development of the telecommunications infrastructure, ubiquity of personal computers, and time trends."[21] The study's results are sobering and instructive, and should be taken very seriously by the Mongolian government.

It may be helpful to review a bit of the theory that underlies the regulation of telecommunications and Internet services.[22] From an economist's perspective, government regulation is a blunt instrument that imposes significant costs on the economy, and should only be used to correct for market failures – for example, natural monopoly situations where increasing returns to scale mean that a single monopoly firm can supply the entire market at lowest cost. In the pre-Internet world, the regulation of telecommunications (and the licensing of telecommunications providers) was required to correct for the classic monopoly power of the incumbent telecom company. To be viable, new market entrants must obtain the ability to call the customers of the incumbent monopoly, which means that the new entrants must be allowed to interconnect their networks with the incumbent's. The incumbent monopolist has little incentive to do so, so most countries have responded with a regulatory and licensing system that requires the incumbent telecom to open its network to interconnection with authorized (licensed) competitors, under more- or less-defined terms and conditions.

If regulation and licensing have often been necessary to correct for market failure in the telecommunications industry, should not ISPs (or other ICT services) be subjected to the same requirements? There are several compelling reasons why the Internet sector should be treated differently from telecoms.

First, regulatory authorities often do a poor job of regulation. They can easily become "captured" by the very businesses they are supposed to regulate, meaning that the regulator acts to protect the incumbent monopoly, not to serve

---

[20] Scott Wallsten, "Regulation and Internet Use in Developing Countries" (World Bank working paper, draft published December 2002).
[21] *Id.*, at 1.
[22] *Id.*, at 6. This paragraph is a paraphrase of Wallsten's paper, to which I am indebted for providing such a succinct summary of the economic theory behind telecommunications regulation.

the public interest. This does not necessarily mean that the regulator is malevolent or corrupt, but that the incumbent monopolist is able to take advantage of its superior information, expertise, political influence, and financial muscle. In the case of Mongolia, it must be acknowledged that the CRC is not an independent regulatory authority, and that the Mongolian government and its Ministry of Infrastructure retain a powerful financial interest in Mongolia Telecom.

Second, licensing requirements are regulatory barriers that create opportunities for corruption, even where the requirement is imposed with the best of intentions. As stated by Wallsten, "they increase the number of interaction points between government and industry where bribes may be required for firms to begin or continue operations."[23] While there is no doubt that the current staff of the CRC is professional and well-intentioned, it would be a mistake for Mongolia to simply ignore the very real possibility that a licensing scheme for ISPs and ICT services will foster the kinds of bad incentives that will lead to petty (or even large-scale) corruption in the future.

Third, there is no technical rationale for licensing ISPs or ICT services. In the pre-Internet world, there was a need to break open the monopolists' tight control over the existing network infrastructure. In the Internet sector, there are no similar barriers to entry. ISPs can join the global Internet readily and easily, simply by contracting with domestic or international upstream providers. Where switched voice services (i.e., access to the public switched telephone network) are not at issue, there is no technical or economic requirement for the regulatory authority to mandate interconnection among ISPs by means of a licensing regime. Moreover, there is no technical or economic justification for Mongolia to limit the number of companies that are able to compete in the ISP market. The open and voluntary nature of the Internet is such that every new network that joins the Internet increases its overall value and utility.

As noted above, most of the advanced economies in the world do not require ISPs or ICT services to obtain individual licenses. It is no coincidence that their Internet sectors are the most advanced, delivering high-quality, high-speed connectivity to citizens at the lowest cost. There is no reason for Mongolia to treat its Internet sector any differently. To date, Mongolia's low level of Internet regulation and ISP licensing has produced a vibrant technology sector that should be the envy of most other countries in its size and income range. To move in the opposite direction now would be a disaster for Mongolia's technology future.

Alternative to licensing: General authorization. If the Great Khural nevertheless determines that some level of ISP licensing is required, it should consider a widely-used alternative to individual licensing: the general

[23] *Id.*, at 6-7.

authorization.[24] Under this approach, the Mongolian government would create a class license that states all of the terms and conditions that are applicable to ISPs (for example, annual licensing fees, consumer protection conditions, and limitations on liability). Any entity would be allowed to sell Internet services, subject to the terms of the class license. The key feature is that that no prior authorization or approval by the regulator is required. An ISP can simply start to operate without having to wait for a licensing decision. In a general authorization scheme, there is no discretion on the part of the regulatory authority to deny or withhold a license. On the other hand, the regulator is authorized to enforce the terms of the general class license against any ISP that violates them.

If the CRC is concerned about the need to obtain special licensing fees from ISPs, a generally authorized class license would be the best approach. In that scenario, an individual can walk into the CRC office, fill out a 1-page registration form, pay the required annual licensing fee, and then immediately begin operations as an ISP. Legally, the class license is treated as a contract that is created upon submission of the registration form. In a general authorization (class license) scheme, there is no need for the company to convince the CRC to make a favorable decision; therefore, there is no possibility for the regulator to act in an arbitrary or abusive manner. Though the CRC staff are surely people of good will and professionalism, it must once again be emphasized that the CRC lacks true independence from the Ministry of Infrastructure, which has an undisputed financial stake in the success of Mongolia Telecom against its competitors. A general authorization system would allow the CRC to focus on its important work and to collect any necessary licensing fees, without becoming a bottleneck that inhibits the growth and development of Mongolia's ICT sector.

The alternative is individual operator licenses, where each ISP must negotiate separately with the CRC and obtain its discretionary approval. Individual operator licenses are a very bad idea. They allow the regulator to treat similarly-situated ISPs differently, or to favor the incumbent monopoly. There is little transparency, certainty, or predictability to the system. By contrast, a generally authorized class license sets a level competitive playing field, and gives everyone in the Mongolian Internet community (ISPs, investors, government agencies, and users) a clear picture of an ISP's legal rights and obligations.

- ***Chapter Five: E-governance Information System***
- ***Chapter Six: E-governance Information Database***

Chapters Five and Six define an elaborate set of objectives, rules and requirements for the Mongolian government's own information technology systems. There appears to be little of controversy here, and much to praise.

[24] For a good overview of the advantages and disadvantages of various ISP licensing alternatives, see Global Internet Policy Initiative, "Licensing Options for Internet Service Providers" (September 2002), available online at <http://www.internetpolicy.net/standards/licensingoptions.shtml>.

These Chapters represent a strong commitment by the Mongolian government to make information and services available online. Still, there are a few serious problems with the current language of the Draft Law.

Citizen access to information. The Draft Law appears to create a presumption of free access by Mongolian citizens to all non-confidential e-government information. This would be a significant victory for transparency in the Mongolian government. But much will depend upon the meaning of "confidential" – that is, upon what information can be withheld by the Mongolian government -- and on the manner in which disputes over that designation are settled. Troublingly, the list of exceptions to citizen access stated in *Article 17.4* are quite vague and broad. For example, an exception is given for "cases which might adversely affect national security and social order." That is classic censorship-friendly statutory language that appears to be rooted in Mongolia's authoritarian past, and not reflective of its democratic ideals. Nearly anything can be kept secret on the ground that disclosure "might adversely affect … social order."

Equally bad, the Draft Law provides almost no detail about the procedure for adjudicating disagreements about access to e-governance information. Says *Article 17.6*: "High level organization and officer shall settle disagreement and claim against the decision prohibiting open access of information." In a stable democracy, the proper institution to resolve a dispute between the executive branch and a citizen is the independent judiciary. Chapter Six of the Draft Law instead appears to make the government agency itself the judge of whether its information can be withheld from the public.

Data privacy protection. Another missing component of Chapters Five and Six is a set of specific protections for the privacy of all personal data of Mongolian citizens that is placed in governmental databases. Any law providing for the creation of national e-governance databases should include detailed standards for the handling and protection of citizens' personal data, along with sanctions for unauthorized disclosure and misuse. In *Article 22.1.5*, the Draft Law makes it illegal "to unveil [the] secret of state, organizations, and individuals," but nowhere defines what constitutes "secret" information of individuals.

In short, the Draft Law should be revised to narrow and clarify the exceptions to the presumption of citizen access to e-government information; and the process for adjudication of disputes should be reconsidered and rewritten to give jurisdiction to the courts. In addition, comprehensive data privacy definitions and protections should be added.

Technical language. As an aside, there seems to be some confusion in Chapter Six about how governments will go about using online networks, as a practical matter. For example, in *Article 18.1* the Draft Law states that

"information in e-governance information system shall be exchanged through e-mail in file form (non-paper technology) and signature, organization seal, and mark shall be secured by secret code." It is certainly a good idea to specify that online transfers of information in government databases must be done using data encryption. But it would be surprising to specify that the transfers must be done via email, rather than, for example, secure FTP or other file transfer protocols. The intent of this clause appears to be good, but the language needs to be rewritten to make it fit the realities of the Internet. References to "e-mail" should be revised to embrace any appropriate electronic method of transferring files.

Similarly, *Article 18.2* of the Draft Law provides that "secret codes", which presumably includes the private encryption keys of government agencies and employees, "shall be included in list of confidentiality of state and organizations." The meaning of this provision is unclear: either it means that private encryption keys and passwords are "confidential" and therefore not subject to public disclosure (which is an entirely reasonable and appropriate provision), or it means that they must be submitted to some sort of central list or registry. The clause should be clarified. Moreover, the second possible interpretation points out the need for the Mongolian government to have a comprehensive system of encryption key management – something that ought to at least be mentioned in the Draft Law.

- ***Chapter Seven: Conditions for Use of Electronic Signature***

The most confused, confusing, and technically erroneous portion of the Draft Law is Chapter Seven, dealing with electronic signatures. This Chapter is almost completely wrongheaded, and appears to be based on a set of fundamental misunderstandings about the nature and use of electronic signatures. Chapter Seven is so poorly conceived and written that, if approved in its current form, it would stand as an embarrassment to Mongolia. The draft provisions would be the digital equivalent of a law that regulates how an automobile mechanic should go about repairing a horse.

The Great Khural should delete Chapter Seven entirely from the Draft Law and start over, replacing it with a new chapter that is based on a detailed understanding of the technology, a careful study of the relevant policy options, and a clear sense of the underlying legal, economic, and regulatory objectives. In other words, the Great Khural should start again from scratch, this time with the benefit of expert technical and legal input.

As currently drafted, Chapter Seven contemplates that Mongolian citizens and businesses will physically go to an authorized Certification Authority, which will issue an "electronic signature" that can be used – indeed, must be used – to consummate online transactions. The Certification Authority is required to keep a paper copy of the electronic signature, marked with an official signature, the associated holder's identifying information, and the public encryption key. The

Draft Law further provides that it is illegal to create, use, or distribute an electronic signature through any other means.

For the reasons outlined below, this is a nonsensical scenario that would serve no practical purpose, is technically unworkable, and would, as formulated in the Draft Law, affirmatively damage the ability of Mongolians to build a functioning online economy.

It is hard to know why the Mongolian Department of Infrastructure got this area of law and technology so completely wrong. One likely factor was the cutting and pasting of legislative provisions from other countries (portions of Chapter Seven close resemble legislation in Singapore, Malaysia, and India). Combined with a lack of technical understanding, this drafting technique has produced a Chapter in which the definitions do not match the operative clauses, and the operative clauses do not match reality. It would a serious mistake for Mongolia to cobble together legislation by copying language from other countries' laws. In part, this is because Mongolia's laws should fit Mongolia's unique needs, requirements, and legal system. But most importantly, this is because "electronic signature" laws have largely proven to be useless failures in nearly every country that has adopted them. Mongolia should learn from the mistakes of others, rather than blindly repeat them.

The following paragraphs outline some of the most obvious flaws in the Draft Law's electronic signature provisions. Rather than dissect Chapter Seven of the Draft Law line-by-line, this paper seeks to identify its major conceptual flaws, pointing to specific examples in the text.

Definitions: "Electronic signatures" "digital signatures" and "digital certificates." The core flaw of the Draft Law's chapter on "electronic signatures" is that it conflates three different concepts: electronic signatures, digital signatures, and digital certificates. Each of these three can play a role in electronic transactions, and each is readily distinguishable. But Chapter Seven of the Draft Law confusingly lumps them all together in an often-incompatible and incoherent mess. It will be helpful, then, to start with the correct definition of the three terms.

An *electronic signature* is any personal symbol or string of characters attached to an electronic communication that (a) identifies and authenticates a particular person as the source of the messages, and (b) indicates that the person approves of the information contained in the message.[25] It can be as simple as a personal identification number or graphical image of the person's handwritten signature attached to the end of an electronic message. Electronic signatures

[25] For example, Singapore defines "electronic signature" as "any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record." Electronic Transactions Act of 1998, available online at <http://www.ida.gov.sg>.

are simply a sign of intent: evidence that the person who added the signature meant to express his or her approval of it. Electronic signatures alone cannot verify that the message has not been altered. National e-commerce legislation typically establishes a formal recognition that electronic signatures are every bit as valid as handwritten signatures. Often, such laws create a rebuttable presumption of validity – that is, a presumption that can be negated with evidence that the electronic signature was forged, that the message was later modified, or that the person in question did not intend to indicate his approval of the text.

A *digital signature* is an electronic signature that uses cryptographic techniques to authenticate a communication or document by validating that the signature matches the sender's publicly-available key and, in many cases, to ensure that the text of the document has not been changed since the digital signature was calculated and attached. Digital signatures are generated by a complex mathematical process that results in two paired keys: a public key, and a private key. Thanks to the wonders of mathematics, these keys are related to each other, but it is essentially impossible to calculate the private key on the basis of the public key.[26]

Here's how a digital signature actually gets used: When the sender wants to digitally sign a document (or email message or whatever), she uses special software that performs a mathematical calculation using the document and her ***private*** encryption key, and attaches the result of that calculation (the "digital signature") to the document. The recipient of the document then uses software to perform a reverse calculation using the document and the sender's ***public*** encryption key. If the document's attached digital signature is consistent with the sender's public encryption key, then the recipient has "verified" that the sender sent the document (because, presumably, only the sender knows her private key).

A *digital certificate* is like an electronic identification card that identifies that the provider of the digital certificate is, in fact, who or what it claims to be. Digital certificates are issued by Certificate Authority (which can be either a public- or private-sector entity) and signed with the Certificate Authority's private key, meaning it can be authenticated by using the Certificate Authority's public key. A digital certificate typically includes the name of the holder, the public key of the holder, a serial number, the identity of the Certificate Authority that issued it, and the digital signature of the Certificate Authority. When they are digitally signed with strong encryption, digital certificates cannot (for the most part) be altered.

---

[26] For example, Singapore defines "digital signature" as "an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine: (a) whether the transformation was created using the private key that corresponds to the signer's public key; and (b) whether the initial electronic record has been altered since the transformation was made." Electronic Transactions Act of 1998.

Most users encounter digital certificates through their web browsers: they go to a website, the web server automatically sends to the browser a digital certificate, and (without the user having to do anything) the browser verifies the digital certificate by performing a mathematical operation that authenticates its digital signature using the public key provided by the Certificate Authority. In most cases, this happens without the user even noticing; only when the certificate cannot be properly authenticated does the user get a notification to that effect.

Chapter Seven of the Draft Law uses the term "electronic signature" to refer to a "digital signature" that has been issued (in paper form!) by a state-approved Certification Authority. This is not simply an error of terminology: the Draft Law fails to include any provisions defining the legal status of (1) electronic signatures that have ***not*** been signed with public-private encryption keys, or (2) digital certificates. As a technical matter (whether the Mongolian Ministry of Infrastructure likes it or not), Mongolians are going to sign email without the use of encryption, and are going to use digital certificates to verify communications with online e-commerce websites. (They are extremely unlikely to use digital signatures to form contracts, by the way). By making no provision for true "electronic signatures" or for digital certificates, the Draft Law fails to address the two most common e-commerce authentication and verification techniques.

Equivalence of electronic signatures and paper signatures. One of the goals that national governments typically attempt to achieve through e-commerce legislation is the legal principle that courts and other government entities should accord an electronic signature the same validity by as physical signatures.[27] This is sensible, and easy to accomplish. An electronic signature is simply any kind of personal marking. Properly drafted, a law on electronic signatures simply gives a presumption of validity to any communication that appears to carry an electronic signature.[28] What is crucial, however, is the recognition that electronic signatures are easy to forge (just like paper signatures); therefore, the legal presumption of validity can be overcome by a showing that the electronic signature was forged, or that the alleged sender did not, in fact, send it.

The Draft Law, however, takes a different (and wrongheaded) approach, due perhaps to a failure to understand the difference between an electronic signature and a digital signature, and the ways in which they are commonly used. In

---

[27] For example, Singapore simply provides that "where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law." Electronic Transactions Act of 1998.

[28] The European Union calls this the "non-discrimination principle." *See* the European Union's EU Directive 1999/93 (13 December 1999) on a Community framework for electronic signatures. In the United States, section 101(a) of the Electronic Signatures in Global and National Commerce Act (E-SIGN Act) places electronic records and signatures on a legal par with their paper and ink counterparts. Public Law No. 106-229, 114 Stat. 464 (2001).

Article 23, the Draft Law provides that an electronic signature is equivalent to a paper signature **only** if (a) the official certificate was valid (i.e., not revoked) at the time the electronic signature was created, and (b) the electronic signature matches the official certificate.

In other words, the Draft Law would give no legal weight to an email from a customer to a seller that places an order for goods to be purchased and delivered, unless that email was digitally signed with a state-issued encryption key. Indeed, according to *Article 24.2*, it would be illegal for the customer to send the email with any other type of signature, including, apparently, typing his name at the bottom.[29] This would be a bizarre and unprecedented system: Mongolia, alone of all the countries of the world, would make it illegal to sign any communication, or to conduct any online transactions, except in a manner that allows an officially-issued digital encryption signature to be attached. It would be illegal to use ordinary, plain text email to order goods or services; it would likewise be illegal to place an order online through a web page. What makes the scenario of the Draft Law even more absurd is the reality that almost no Internet users worldwide actually have digital signatures – and a truly miniscule number have ever used them. Over the past several years, the technology has proven itself too complicated and clumsy to catch on with ordinary users.

Instead, the Draft Law should recognize the differences between electronic signatures, digital signatures, and digital certificates, and treat them differently, according to their different properties and uses. For the reasons noted above, Mongolia's Law on Information Technology might sensibly include a provision for the recognition of electronic signatures as equivalent to paper signatures.

A "digital signature" is not a signature. It is important to understand that a digital signature is not a signature, in the conventional sense. A cryptographically-generated digital signature uses two different but mathematically related blocks of code: The public key and the private key. Here is an example of a public key:

> -----BEGIN PGP PUBLIC KEY BLOCK-----
> Version: PGP 8.0.2
>
> mQGiBDwGp2kRBAD+MMvGMjelgShh3OzWEnf6B9/BXp3xMomFt60ThdNrivaxTX9e
> GEMVpg1FEjwUz5hG8zOrjmb31l3LxAwI+8aySSZtUhlxeViZQYx2OjZJfKYj3TnF
> 9nlcZw9T/T3EHasYI64YhlyUt6+qzYDKQz/W3BGshTijBLFgJDZDFWB53QCg/4nr
> cNbjwjw/Tu338xPoJYXZPVsEAI9lygEJH/AGRgQJY2aQ++TXK/s06Rogaelajckv
> LOzdvcF8b2W63Rvs+HemNCuN7aGqWMeWTcg4nk7gTlAFxpDaZdl0wvIiPAoVGE3B
> HuEgJV7gX8rAbGW2T07YTPW56mCsWvOUpGjHM83m0hDnAdn4LZYEa6c6TYEPQ8/j
> H1w8BACuVaF5Fc58Cs24bm5gmxLMFHI5KhjyvSvzF+jIIUv8c8tsAiemjXkHZRbB
> 9r31VC4mR0sGZQrVBKuHczL0CJW7qhhh1P2y0eke+5+B1rNPGXBFKU2ayQF7FJQb
> qpdPAdCyVQZvpSuhNW105cAZabw3KGKA4sD4UKzo3N+o6Dx8iLQhQW5kcmV3IE1j
> TGF1Z2hsaW4gPGFqbUBpY2Fubi5vcmc+iQBOBBARAgAOBQI8BqdpBAsDAgECGQEA
> CgkQSU4b+NDNo9aU1QCfWQSbvWZ6qFETr87ilzbtv4TPzNoAoK1/TyBsWTnjvPOT
> Bfi7K3mLB9w6uQINBDwGp2kQCAD2Qle3CH8IF3KiutapQvMF6PlTETlPtvFuuUs4

[29] Says *Art. 24.2*: "Creation, use and distribution of signature without certified means shall be prohibited."

INoBp1ajFOmPQFXz0AfGy0OplK33TGSGSfgMg71l6RfUodNQ+PVZX9x2Uk89PY3b
zpnhV5JZzf24rnRPxfx2vIPFRzBhznzJZv8V+bv9kV7HAarTW56NoKVyOtQa8L9G
AFgr5fSl/VhOSdvNILSd5JEHNmszbDgNRR0PflizHHxbLY7288kjwEPwpVsYjY67
VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBgRjXyEpwpy1obEAxnIByl6ypUM
2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6q6Jew1XpMgs7AAICB/42GIWgiAMI
kb0/OKvsxjUAy7AH9yZbc0OLdpnUdC20x8HDY7Z3IoVwOpLPnsOkOc2gKzLqo6gg
xW4FUWP7ies53DGgxqdxvLA4kHAi0Sp5Nov6mvhgP6qLVM9ydcnTdeDBtnVfst8q
gOvR+Rs0VYBd4tJbc4hYKfeJIAxOATdmBHoQ9vv1ewM2iKeFim9b2xhiv/KwBvpI
aF5z7qOuuHWaQ2ZNFtcsaSUqQQe4fJ2qud1al9WtdR7ksAk8iacEahEhm4Z2uHEG
KHQ3GaIzN6BE6u237WzhOFnu88etzzMekkU63cBLkfxQ0W4GADKbNOr8ApY90t4w
uAWzG6Kt1YzRiQBGBBgRAgAGBQI8BqdpAAoJEEIOG/jQzaPWe7AAoKhSWySP9w4s
JUn7HOPXCUPBl5gDAKCL/J7mdA7sBzdNQHLp6fzI3t5ooQ==
=TM/I
-----END PGP PUBLIC KEY BLOCK-----

For obvious reasons, this is not something that a person can memorize. It must be stored on a computer (or disk or removable hard drive). A private key is an even *longer* block of code, and must also be stored on a computer (or disk or removable hard drive).

As noted above, a "digital signature" is a block of code that is generated by performing a mathematical operation that uses both the document (or message) and the sender's ***private*** key. A recipient "verifies" the signature by using the document and the sender's ***public*** key. Those mathematical operations are complex and must be performed by a piece of software on a computer.

The point is that a digital signature can establish that a communication was signed using a private encryption key. But it cannot establish that the person sitting at the computer on which the key is stored was the person to whom the key is registered. In the words of encryption expert Bruce Schneier, "while a digital signature authenticates the document up to the point of the signing computer, it doesn't authenticate the link between that computer and [the sender]."[30] In other words, the use of the digital signature does not guarantee that the communication is actually from the person it seems to be from: someone else might have sat down at the sender's computer and signed a document or message using her private key.

The Draft Law fails to recognize this fundamental limitation of digital signatures. Indeed, the Draft Law makes the theft and hijacking of private keys almost a certainty: it would require Mongolian citizens to obtain their private keys from an office, in paper format. In the rest of the world, public and private keys are generated electronically, communicated through secure online channels, and stored electronically in hidden, secure locations. In the bizarre universe contemplated by Chapter Seven, Mongolian citizens would have to have paper documents with both public and private encryption keys, making it virtually certain that many private keys will be discovered and misused.

---

[30] Bruce Scheier, "Why Digital Signatures Are Not Signatures," Crypto-Gram Newsletter (15 November, 2000), available online at <http://www.schneier.com/crypto-gram-0011.html#1>.

Prohibition on use of non-official electronic signatures. If Mongolia simply passed a law that made digital signatures untrustworthy and useless, it would be a tragedy; but the Draft Law would make that bad situation exponentially worse by **prohibiting** any Mongolian citizen from using any other type of electronic signature, digital signature, or digital certificate.[31] Most ordinary Internet users sign their emails and online documents without the use of cryptographically-generated public/private key pairs, usually by typing their names at the bottom; the Draft Law would make that illegal. As a result, Mongolian citizens would be prohibited from conducting ordinary transactions with each other via email. Likewise, most e-commerce websites use digital certificates generated by private companies (for example, VeriSign) to assist with the authentication of transactions; the Draft Law would also make that illegal (meaning, at a minimum, that no Mongolian could legally conduct online transactions with non-Mongolian parties).

E-commerce (and e-government) depends upon trust. Sellers and buyers (and citizens and officials) must be able to trust that their communications are secure and authentic. Electronic signatures, digital signatures, and digital certificates each have a role to play in fostering trust among players in the Internet economy, because each provides certain levels of security and authentication in certain situations. As currently written, Chapter Seven of the Draft Law would eliminate the use of two of those tools, would make the third both mandatory and untrustworthy, and would prohibit the use of any alternatives. The result would be enormous long-term harm to Mongolia's economic future.

Certification Authority. For the task of generating, issuing, and archiving digital signatures,[32] the Draft Law in *Articles 25-32* provides for a two-level network of Certification Authorities.[33] At the top of the hierarchy is the "relevant state administration organization," intended to be the Controller of Certification Authorities (CCA), a to-be-created office within the Ministry of Infrastructure. The CCA would license Certification Authorities, reviewing and approving their applications, giving them official recognition, auditing their compliance with the rules, and withdrawing recognition when necessary. The officially-sanctioned Certification Authorities would supply digital signatures to Mongolian citizens according to the rules and regulations set by the CCA. The Certification Authorities would be responsible for receiving and processing formal applications, verifying the identities of those who request digital signatures, issuing and archiving paper certificates for each digital signature, and

---

[31] See *Art. 24.2*: "Creation, use and distribution of signature without certified means shall be prohibited."

[32] Chapter Seven of the Draft Law uses the term "electronic signature," but based on a confused definition that generally matches the common definition of "digital signature." In order to keep the terminology clear and consistent, the following two sections use the term "digital signature."

[33] The English version uses the term "Certification Organizations," but this appears to be a mistranslation of "Certification Authority." This kind of hierarchical system of inter-dependent certification activities is known as a "public key infrastructure" (PKI).

maintaining a governmental register of the digital certificates that have been issued.

Simply put, the Certification Authority system contemplated by the Draft Law would be a disaster. It would create an expensive bureaucracy with nothing to do. *Electronic signatures* require no cryptographic key pairs and can be created by any Internet user. *Digital signatures* require cryptographic key pairs, but these are generated by end-user software and/or free online public services -- there is no requirement for governmental involvement. *Digital certificates* are supplied in the marketplace by any number of private companies, depending upon the particular purpose – again, without need for governmental involvement.

Several countries have, in recent years, established two-level systems of Certification Authorities, with a governmental Controller at the top -- for example, India, Malaysia, and Singapore. In its consideration of the Draft Law, Mongolia's Great Khural should take a close look at their experiences: in every case, the model has been a disappointment and, most would argue, a failure. Typically, their digital signature and digital certificate laws were passed at the height of the Internet stock market frenzy, in 1999-2000. As in the business sphere, the bloated expectations of the regulators have since been deflated. Those nations have not developed vibrant networks of Certification Authorities, and the offices of the Controllers have had essentially nothing to do. The bureaucracies have proven burdensome and expensive, with no evident benefit to the national Internet economy.

By contrast with India, Malaysia, and Singapore, Mongolia is a small nation with a small internal market. There is simply no reason for it to spend scarce governmental resources to create a Controller of Certification Authorities. If the model did not work in large countries with huge Internet sectors, it will certainly be a failure in Mongolia. If experience is any guide, very few companies will seek to become accredited Certification Authorities in Mongolia for the purpose of selling digital certificates; the process of licensing them should take no more than a few hours each. The idea that the CCA could recover its costs from licensing fees is laughable: from, at best, a tiny handful of licensees could be drawn only a small amount of money.

On the other hand, over the past few years a number of countries have concluded that citizen trust in e-commerce can be enhanced by creating a voluntary system of governmental approval for Certification Authorities that meet certain standards.[34] The laws often provide that government agencies or contractors can only use digital certificates purchased from authorized Certification Authorities; or that online transactions using government-approved Certification Authorities are presumptively valid and enforceable. However,

[34] For example, the European Union's EU Directive 1999/93 (13 December 1999) on a Community framework for electronic signatures calls for EU member states to create systems of "voluntary accreditation."

these countries have never attempted to prohibit any digital signatures and certificates issued from any other source -- they have all recognized that there are many contexts in which individuals and companies will want to (or have to) use non-government-endorsed certificate providers. This approach provides incentives, but not requirements; it grants modest legal benefits to users of officially-sanctioned Certificate Authorities, but does not penalize or prohibit the alternatives.

Many other countries, such as the United States, have not attempted to regulate digital signatures or certificates in any way. They leave it up to individual users to determine which online services, sites, and communications to trust. Given that the world's most advanced Internet economies (large and small) have survived and thrived without government regulation of digital certificates, Mongolia would do well to consider their example. Even if Mongolia were to determine that some sort of governmental approval would help to encourage trust and support e-commerce activities by Mongolian citizens, the scheme must be voluntary, non-exclusive, and low-cost. Any other approach will certainly be a waste of government resources and a heavy burden on Mongolia's e-commerce economy.

Nobody actually uses digital signatures. Finally, it is worth pointing out that very few Internet users in any country have ever actually used digital signatures. Those who use digital signatures tend to be technically-skilled Internet professionals who want to authenticate or encrypt their email communications with each other. Digital certificates are widely used by e-commerce and e-government websites, but not by individual users. There are many potential explanations for this state of affairs (for example, the concepts are confusing, and the software is not very user-friendly), but the simple reality is that digital signatures have not been embraced by users as a daily tool for making contracts or transacting business with their governments.

In formulating its Law on Information Technology, Mongolia must look outside its borders and take account of the real experiences of other countries, and not simply attempt to cut-and-paste elements of their 1999 Internet-bubble laws.

- ***Chapter Eight: E-commerce***

In stark contrast with the mess of Chapter Seven on electronic signatures, *Chapter Eight* sets forth a reasonable and coherent legal framework for Internet-based commercial transactions.

Most of the provisions of Chapter Eight merit praise. *Article 34* defines e-commerce broadly ("technical and program tools for receipt, transfer, storage and process using digital documents") and specifies that digital documents may be used "in activities of all sectors." In *Article 35*, the Draft Law articulates a positive and forward-looking set of e-commerce principles "whereby rights of participants

are equally provided, freedom and activities of contract is not impeded and transaction of goods, services and finance is made without delay." *Article 36* allows for negotiation through the exchange of electronic documents. *Article 38* permits parties to store documents in electronic format when required by law, subject to several common-sense provisos. *Article 41* gives legal recognition to contracts formed through exchange of electronic documents.

However, one provision in Chapter Eight is alarmingly misguided, at least as it appears in the English translation. *Article 42.1* is the exact opposite of what the Draft Law appears designed to accomplish; the clause is so anomalous that mistranslation is the only rational explanation. In the English translated version, *Article 42.1* states: "Contract form being in electronic form cannot serve a basis for dispute and not admissible to court related to conditions and duties of the contract between involved parties when e-commerce contract was proved to have been established through electronic documents." If this clause, as written, is what the Ministry of Infrastructure intended, it is a grave mistake. To make a contract formed by electronic communications inadmissible in court would undercut the entire purpose of Chapter Eight, and contradict the basic principles stated in *Articles 34* and *35*. If a contract formed through electronic communications cannot be proven and enforced in court, then no electronic contracts will be created; if electronic contracts cannot be enforced, then no one in Mongolia will engage in e-commerce transactions.

If Chapter Eight is to have any meaning at all, *Article 42.1* must be revised to state the reverse: that contracts in electronic form are legally valid, that they can serve as the basis for legal actions, and that electronic documents are admissible in court to prove the duties, obligations, and terms of the agreement between the parties.

A few further suggestions for improvement of Chapter Eight follow.

The Draft Law's *Article 37* attempts to draw a distinction between original electronic documents and copies. *Article 37.1* states that "[a]ll electronic documents certified by digital signature shall constitute an original document,"[35] while *Article 37.2* states that "the copy of original document is treated as ready when electronic documents are put on paper form and signed by authorized person." The reason for this distinction is not evident from the text of the Draft Law, and it appears to serve no useful purpose. In light of the foregoing critique of Chapter Seven of the Draft Law, this provision should be deleted and replaced with a broad recognition that gives full legal standing to electronic documents.

---

[35] The fact that Chapters Eight and Nine refer to "digital signatures" – a term which does not appear in Chapter Seven and which consequently has no definition in the Draft Law – rather than "electronic signatures" supports the theory that much of the Draft Law was stitched together from pieces of other nations' laws, without much thought for consistency or harmonization of the various elements into a coherent whole.

For example, Mongolia's e-commerce environment would benefit from a simple law providing that "a signature, contract, record or other document may not be denied legal effect, validity or enforceability solely because it is in electronic form."[36] Such a statute might be subjected to specific qualifications for particularly significant documents such as wills, marriage contracts, divorce settlements, adoption papers, documents transferring title to land, and legally mandated notifications to consumers (such as those required by the consumer protection code). In addition, Mongolia should specify that the use of electronic documents must be voluntary, with the consent of both parties. (Otherwise, a company might attempt to claim that it gave notice to consumers simply by posting a document online).[37]

Article 40 would benefit from some clarification. The current language states that "[e]-commerce can be run by enterprises, citizens and legal entities which are entitled to do so by the present law and other relevant laws," which could be interpreted to imply that special permission is required. A better phrasing might be: "E-commerce can be performed by enterprises, citizens, and legal entities in connection with any activities not specifically prohibited by the present law or any other relevant laws."

Article 41.3 apparently addresses the recognition to be accorded to signatures on electronic documents: "When signed by authorized person e-commerce contract in writing shall be treated as valid." This provision would make sense if the definition of "signature" is something akin to "electronic signature" as discussed in the analysis of Chapter Seven above. For example: "any personal symbol or string of characters attached to an electronic communication that (a) identifies and authenticates a particular person as the source of the messages, and (b) indicates that the person approves of the information contained in the message."

Article 41.3 should be adjusted to clarify that a contract created in e-commerce by exchange of electronic documents will be treated as valid where both parties have indicated by electronic signature their intent to form a contract. The objective is to give legal effect to the expressed intent of the parties to an electronic contract in the same manner that a court would give legal effect to the written signs that evidence intent on a paper contract. (Note that there is no place in this discussion for "digital signatures," which are specialized electronic signatures that use cryptographic techniques to validate that the signature matches the sender's public encryption key).

- ***Chapter Nine: Information Resources***

The Draft Law's Chapter Nine sets rules and standards for the handling of "information resources" in the possession of the government. As with Chapter

[36] Language suggested by Global Internet Policy Initiative, "E-commerce/Digital Signatures" (2003), available online at <http://www.internetpolicy.net/e-commerce>.
[37] See *id.*, for a good discussion of relevant considerations, with links to useful references.

Eight, most of the provisions in Chapter Nine are reasonable and appropriate. A few, however, warrant revision.

On the positive side, Chapter Nine does a solid job of articulating a property-based model of information resource management, stating that citizens and businesses retain ownership of the information that they provide to the government,[38] and that ownership of information resources can be transferred.[39]

Of enormous importance, *Article 50.1* of the Draft Law creates a broad right of presumptive public access to government information: "Information resources other than those which are substantiated and limited as stated in the law shall be open and accessible to the public." *Article 51* gives shape and specificity to this right, instructing government agencies that "[s]tate organizations, citizens and legal entities shall be equally entitled to use of state information resources other than the ones which refer to state secret." *Article 51.3* clarifies that commercial distribution of government-generated information is permissible, enabling Mongolian companies to develop innovative new services based on government information. *Articles 51.4* and *51.5* impose some citizen-friendly obligations on the government agencies that maintain information resources, including a duty to "distribute [to] users a list of information and information services and regulation and condition for access to information resources without charge," and to "provid[e] conditions which enable fast, efficient, and full scale receipt of information by users."

Equally encouraging are *Articles 52* and *53*, which appear to establish expansive governmental duties of disclosure and citizen rights of access. *Article 52* provides that the all parts of the government must "create information resource on activities and functioning of itself and subsidiary agencies which will be accessible to public. As well, within given authority they will provide the public with information on related human rights, citizen duties, freedom, human security and other issues of public interest." *Article 53* grants to each Mongolian citizen a basic right to see government-held records relating to him or her:

> 53.2 Unless otherwise stated in the law, citizens, enterprises and organizations shall be entitled to access to information resources for the purpose of ensuring the reliability and comprehensiveness of information on themselves. They shall also be entitled to be aware of who has used the information on themselves and when and why it was used.
>
> 53.2 Unless otherwise stated in the law holder of substantiated documents on citizen shall be obliged to show detailed information without charge when the citizen demands so.

[38] *Article 48.2*.
[39] *Article 48.7*.

For a country that suffered so many years of repressive authoritarian rule, it is impossible to overestimate the importance of an enforceable right to demand that the government reveal to you what it knows about you. Moreover, these measures have the potential to enhance significantly the day-to-day transparency and accountability of the Mongolian bureaucracy.

As always, of course, the devil is in the details of implementation – an expansive interpretation of "state secret" would render these rights (and, indeed, all of Chapter Nine) essentially meaningless. In the coming years, it will be essential for Mongolian citizens to hold their government to the promises made in this portion of the Law on Information Technology.

Two sections of Chapter Nine warrant serious reconsideration and revision:

In *Articles 47.3* and *47.4*, the Draft Law conditions the validity of electronic documents on their being "signed" or "certified by electronic signature." In light of the lengthy critique of the Draft Law's provisions on electronic signatures, above, these clauses should be revised to recognize the full range of other methods of authentication and validation of electronic documents. On a pragmatic level, the Great Khural should gather input on the real-world document storage and authentication practices and policies of other governments.

Article 48.5 requires the government to register all "state-owned information resources" in "the list of state property" and put them "under state protection as stipulated in the law." This seems impractical, at best: is the government supposed to list in the registry each and every electronic document in its possession? A more practical approach might be to require the government to identify and describe each individual government-administered database, and to list each database in the registry of state property.

APPENDIX A

Draft Law on Information Technology
Index of Provisions

Full text of English translation available at <http://cyber.law.harvard.edu/mongolia/draft-law-sep03.html>.

- Art. 28: Activities of certification office
- Art. 29: Duties and responsibilities of certification office
- Art. 30: Duties and responsibilities of holder of signature certificate
- Art. 31: Invalidating the signature certificate
- Art. 32: Terminating activities of certification office
- Art. 33: Cases allowing substitute for seal

Chapter 8: E-Commerce

- Art. 34: E-commerce environment
- Art. 35: Regulatory principles of e-commerce
- Art. 36: Principle of negotiation in writing on the basis of electronic document exchange
- Art. 37: Original and copy of electronic documents
- Art. 38: Storing electronic documents
- Art. 39: Sending electronic documents
- Art. 40: Legal status of e-commerce runners
- Art. 41: Establishing a contract through exchange of electronic documents
- Art. 42: Acknowledgement of duties by involved parties
- Art. 43: Regulation for establishment of e-commerce
- Art. 44: Legal relations of electronic documents in bank transactions
- Art. 45: Program and Methodology
- Art. 46: Storing electronic documents of inter-bank payment and allocating of bank statements

Chapter 9: Information Resources

- Art. 47: Legal basis of information resources
- Art. 48: Ownership of information resources
- Art. 49: Referring information resources to national wealth
- Art. 50: Rights of access to information resources
- Art. 51: Exercising the right of accessing to information resources
- Art. 52: Duties of information provision
- Art. 53: Access to information resources
- Art. 54: Rights and duties of holder of information resources
- Art. 55: Ownership right of information technology tools

Chapter 10: Validity of the Law

- Art. 56: Effectivity of the Law