

## Digitizing The Land of Genghis Khan: Reforming Mongolia's Internet Law to Achieve Growth in E-Commerce

Stephen Errol Blythe  
Tarleton State University  
USA

### ABSTRACT

In the digital age, the E-signature has replaced the handwritten signature. Since 1995, there have been three generations of E-signature law: the first mandated use of the digital signature, the second recognized the legal validity of all types of E-signatures, and the third recognizes all types of E-signatures, but gives preferred status to the digital signature. Mongolia's Electronic Signature Law (ESL) is third-generation; it recognizes all types of E-signatures but favors the use of the digital signature. Accreditation requirements are specified for Certification Service Providers (CSP), the issuers of certificates and verifiers to third parties that a digital signature is that of a specific subscriber. The CSP is responsible for maintaining the security of information that it receives from its subscribers. The CSP must inform the subscriber of any limitations on the use of the certificate. If a CSP issues a certificate, it must meet stringent security requirements which can only be achieved with a digital signature. CSPs must maintain a publicly accessible repository of certificates and the public keys which relying third parties can use to decrypt a subscriber's message. A CSP may incur legal liability for publishing a certificate with inaccurate information or for not issuing a private key to the subscriber corresponding to the public key in the repository. The ESL recognizes the legal validity of certificates issued by CSPs in foreign countries. The author recommends reformation of Mongolia's E-commerce law by adding: (1) consumer protections for E-commerce participants; (2) several new computer crimes; (3) information technology courts; (4) mandatory E-government; and (5) explicit long-arm jurisdiction.

**KEYWORDS:** Mongolia, E-Commerce, E-Signature, Law

### OBJECTIVES OF THE ARTICLE

The objectives of this article are to (1) introduce the reader to Mongolia and its economy; (2) describe the three generations of electronic signature law; (3) analyze Mongolia's Electronic Signature Law ("ESL"), and (4) make recommendations for reformation of Mongolia's E-commerce law.

### MONGOLIA: THE ECONOMY AND INTERNET INFRASTRUCTURE

Since its peaceful democratic revolution in 1990, Mongolia has been making the difficult transition from a centrally-planned economy to a more modern open-market economy. The ex-communist Mongolian People's Party (MPP) has competed for political power with the Democratic Party (DP) and several other smaller parties. In Mongolia's most recent parliamentary elections in 2016, the MPP won overwhelming control of Parliament, largely pushing out the DP. However, a DP member, Khaltmaa Battulga, was elected President of Mongolia in 2017.<sup>1</sup>

Mongolia borders on China and Russia and is slightly smaller than the U.S. state of Alaska and about twice the size of Texas. Mongolia's Gross Domestic Product (GDP) was almost \$40 billion in 2019 and GDP per capita in 2019 was \$12,317. The GDP recently grew at an annual rate of 5.1%. The sectors contributing to Mongolia's GDP are agriculture, 12.1%; industry, 38.2%; and services, 49.7%. The value of Mongolian exports is approximately \$7 billion per year; those goods are primarily coal, copper, gold, iron, and crude petroleum.<sup>2</sup>

More than two-thirds of Mongolians live in urban areas. The largest city is the capital, Ulaanbaatar, with a population of 1.6 million.<sup>3</sup> Broadband services have become available in urban areas and the government supports the improvement of broadband availability and access.<sup>4</sup> Almost two-thirds (61%) of Mongolians use the internet. Internet cafes are popular in urban areas and have begun to spread to other parts of the country. As the internet infrastructure develops, E-commerce is becoming more and more popular.<sup>5</sup> To stimulate the growth of E-commerce, reform of Mongolia's E-commerce law is needed.

### THREE GENERATIONS OF ELECTRONIC SIGNATURE LAW

#### *First Generation: Digital Signature Required*

In 1995, the U.S. State of Utah became the first jurisdiction in the world to enact an electronic signature law.<sup>6</sup> In the Utah statute, digital signatures were required and other types of electronic signatures were not recognized.<sup>7</sup> The authors of the Utah statute believed, with some justification, that digital signatures provide the greatest degree of security for electronic transactions.

<sup>1</sup> U.S. Central Intelligence Agency, "Mongolia," THE WORLD FACTBOOK, 30 June 2021; <https://www.cia.gov/the-world-factbook/countries/mongolia/>.

<sup>2</sup> Id.

<sup>3</sup> U.S. Department of Commerce, MONGOLIA COUNTRY COMMERCIAL GUIDE: E-COMMERCE; <https://www.trade.gov/mongolia-country-commercial-guide>.

<sup>4</sup> Global for Merchants, SELLING ONLINE IN MONGOLIA; <https://merchants.global.com/en-us/sell-online/mongolia>

<sup>5</sup> U.S. Department of State, Bureau of East Asian and Pacific Affairs, BILATERAL RELATIONS FACT SHEET: MONGOLIA, 24 June 2021; <https://www.state.gov/u-s-relations-with-mongolia/#:~:text=U.S.%20MONGOLIA%20RELATIONS,relationship%20to%20a%20Strategic%20Partnership>.

<sup>6</sup> UTAH CODE ANN. 46-3-101 *et seq.*, 1995. This first-generation statute was repealed in 2000 and replaced with the Uniform Electronic Transactions Act, a second-generation model law. UTAH CODE ANN. 46-4-101 *et seq.* (2000).

<sup>7</sup> Id.

Utah was not alone; other jurisdictions granting exclusive recognition to the digital signature include Argentina,<sup>8</sup> Bangladesh,<sup>9</sup> India<sup>10</sup>, Malaysia,<sup>11</sup> Nepal,<sup>12</sup> New Zealand<sup>13</sup>, and Russia.<sup>14</sup>

Unfortunately, these jurisdictions' decision to allow the utilization of only one form of technology is burdensome and overly restrictive. Forcing users to employ digital signatures gives them more security, but this benefit may be outweighed by the digital signature's possible disadvantages: more expensive because of the fee paid to the certification authority; lesser convenience due to being forced to use a certification authority; forcing users to use one type of technology to the exclusion of others when another type of technology might be better suited to a particular type of transaction; use of a more complicated technology which may be less adaptable to technologies used in other nations, or even by other persons within the same nation; inappropriate risk allocation between users if fraud occurs; and the potential disincentive to invest in the development of alternative technologies.<sup>15</sup>

### ***Second Generation: All Types of E-Signatures Accepted***

Jurisdictions in the Second Generation overcompensated. They did the complete reversal of the First Generation and did not include any technological restrictions whatsoever in their statutes. They did not insist upon the utilization of digital signatures, or any other form of technology, to the exclusion of other types of electronic signatures. These jurisdictions have been called "permissive" because they take a completely open-minded, liberal perspective on electronic signatures and do not contend that any one of them is necessarily better than the others. The United States of America<sup>16</sup> is a member of the second wave; the overriding majority of its jurisdictions (forty-five states, the District of Columbia, and the Territories of Puerto Rico and the Virgin Islands) have enacted the Uniform Electronic Transactions Act (either in its entirety or with minor amendments), a permissive second-generation model law.<sup>17</sup> Australia has also enacted a second-generation statute.<sup>18</sup>

The disadvantage of the permissive perspective is that it does not take into account that some types of electronic signatures *are* better than others. A PIN and a person's name typed at the end of an E-mail message are both forms of electronic signatures, but neither can even approach the degree of security that is provided by the digital signature.

### ***Third Generation: Acceptance of All E-Signatures, With Preference for Digital***

Singapore led the Third Wave. In 1998, that country adopted a compromise, middle-of-the-road position for the various types of electronic signatures. In terms of the relative degree of technological neutrality, Singapore adopted a "hybrid" model—a preference for the digital signature in terms of a greater legal presumption of reliability and security, but not to the exclusion of other forms of electronic signatures.<sup>19</sup> The digital signature is given more respect under the Singapore statute, but it is not granted a monopoly as in Utah. Singapore allows other types of electronic signatures to be employed. This technological open-mindedness is commensurate with a global perspective and allows parties to more easily consummate electronic transactions with parties from other nations.<sup>20</sup>

In recent years, more and more nations have joined the Third Generation. They recognize the security advantages afforded by the digital signature and indicate a preference for the digital signature over other forms of electronic signatures. This preference is exhibited in several ways: (1) utilization of a digital signature using a PKI system is explicitly required for authentication of an electronic record; (2) utilization of a digital signature with PKI seems to be necessary for an electronic record to comply with any statutory requirement that a record is in paper form; and (3) for a signature in the electronic form to comply with a statutory requirement that a pen-and-paper signature is affixed, it must be a digital signature created with PKI. Nevertheless, the Third Generation jurisdictions do not appear to be as technologically restrictive as those in the First Generation. They do not compel the E-commerce participant to use only the digital signature, *instead* of other forms of electronic signatures, as the State of Utah did in its original statute of 1995.

The moderate position adopted by Singapore has now become the progressive trend in international electronic signature law. The hybrid approach is the one taken by the European Union's E-Signatures Directive,<sup>21</sup> Armenia,<sup>22</sup> Azerbaijan<sup>23</sup> Barbados,<sup>24</sup> Bermuda,<sup>25</sup> Bulgaria,<sup>26</sup> Burma,<sup>27</sup> China<sup>28</sup> Colombia,<sup>29</sup> Croatia,<sup>30</sup> Dubai,<sup>31</sup> Egypt,<sup>32</sup> Finland,<sup>33</sup> HongKong,<sup>34</sup> Germany,<sup>35</sup> Hungary,<sup>36</sup> Iran,<sup>37</sup> Jamaica,<sup>38</sup> Japan,<sup>39</sup> Jordan,<sup>40</sup> Lithuania,<sup>41</sup> Pakistan,<sup>42</sup> Peru,<sup>43</sup> Poland,<sup>44</sup> Sloven

<sup>8</sup> Argentine Republic, DIGITAL SIGNATURE DECREE 2628/2002, 19 December 2002. The original act was amended by DIGITAL SIGNATURE DECREE 724/2006 on 8 June 2006.

<sup>9</sup> Bangladesh, INFORMATION TECHNOLOGY (ELECTRONIC TRANSACTION) ACT 2000 (Draft).

<sup>10</sup> Republic of India, THE INFORMATION TECHNOLOGY ACT, 9 June 2000.

<sup>11</sup> Republic of Malaysia, DIGITAL SIGNATURE ACT, 1997.

<sup>12</sup> Federal Democratic Republic of Nepal, ELECTRONIC TRANSACTIONS ORDINANCE NO. 32 OF THE YEAR 2061 B.S. (2005 A.D.), ss 60-71.

<sup>13</sup> New Zealand, ELECTRONIC TRANSACTIONS ACT 2000.

<sup>14</sup> Russian Federation, ELECTRONIC DIGITAL SIGNATURE LAW, Federal Law No. 1-FZ, 10 January 2002.

<sup>15</sup> Amelia H. Boss, "The Evolution of Commercial Law Norms: Lessons To Be Learned From Electronic Commerce," 34:3 BROOKLYN JOURNAL OF INTERNATIONAL LAW 673, 689-90 (2009).

<sup>16</sup> For analysis of American law, see Stephen E. Blythe, "E-Commerce and E-Signature Law of the United States of America," THE UKRAINIAN JOURNAL OF BUSINESS LAW, Kiev, Ukraine, November, 2008. For concise coverage of American, British, European Union and United Nations law, see Stephen E. Blythe, "Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security," 11: 2 RICHMOND JOURNAL OF LAW AND TECHNOLOGY 6 (2005).

<sup>17</sup> United States of America, National Conference of Commissioners on Uniform State Laws, UNIFORM ELECTRONIC TRANSACTIONS ACT, 7A U.L.A. 20 (Supp. 2000).

<sup>18</sup> Commonwealth of Australia, ELECTRONIC TRANSACTIONS ACT 1999.

<sup>19</sup> Singapore's lawmakers were influenced by the U.N. Model Law on E-Commerce. See United Nations Commission on International Trade Law ("UNCITRAL"), MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT ("MLEC") G.A. Res. 51/162, U.N. GAOR, 51st Sess., Supp. No. 49, at 336, U.N. Doc. A/51/49 (1996).

<sup>20</sup> Republic of Singapore, ELECTRONIC TRANSACTIONS ACT (Cap. 88), 10 July 1998, amended in 2010.

<sup>21</sup> EUROPEAN UNION DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 13 DECEMBER 1999 ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES, (1999/93/EC)—19 January 2000, OJ L OJ No L 13 P.12.

<sup>22</sup> Republic of Armenia, LAW ON ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE, 2002.

<sup>23</sup> Republic of Azerbaijan, THE LAW OF THE AZERBAIJAN REPUBLIC ON DIGITAL ELECTRONIC SIGNATURE, 2003.

<sup>24</sup> Barbados, ELECTRONIC TRANSACTIONS ACT, CAP. 308B, 8 March 2001.

<sup>25</sup> Commonwealth of Bermuda, ELECTRONIC TRANSACTIONS ACT 1999.

<sup>26</sup> Republic of Bulgaria, LAW ON ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE, 2001.

<sup>27</sup> The Union of Myanmar, ELECTRONIC TRANSACTIONS LAW, The State Peace and Development Council Law No. 5/2004, The 12 Waxing of Kason 1366 M.E., 30 April 2004.

<sup>28</sup> People's Republic of China, Order No. 18 Of The President, LAW OF THE PEOPLE'S REPUBLIC OF CHINA ON ELECTRONIC SIGNATURE, adopted at The 11th Meeting of The Standing Committee of The Tenth National People's Congress of The People's Republic of China, Promulgated 28 August 2004, Effective 1 April 2005.

<sup>29</sup> Republic of Colombia, LAW REGULATING DATA MESSAGES, ELECTRONIC TRADE, DIGITAL SIGNATURES AND CERTIFICATION ENTITIES, 13 January 1999.

<sup>30</sup> Republic of Croatia, ELECTRONIC SIGNATURE ACT, 17 January 2002.

<sup>31</sup> Emirate of Dubai, LAW OF ELECTRONIC TRANSACTIONS AND COMMERCE NO. 2/2002, 12 February 2002.

ia,<sup>45</sup> South Korea,<sup>46</sup> Taiwan,<sup>47</sup> Tunisia,<sup>48</sup> Turkey,<sup>49</sup> the United Arab Emirates,<sup>50</sup> Vanuatu<sup>51</sup> and in the proposed statute of Uganda.<sup>52</sup> Many other nations have adopted the hybrid approach; Mongolia is one of them.

## MONGOLIA'S E-SIGNATURE LAW

Mongolia enacted its Electronic Signature Law (hereinafter “ESL”) on December 15, 2011, and it was amended on December 31, 2015.<sup>53</sup> Definitions of important terms are provided: electronic signature, digital signature, cryptography, electronic document, private key, public key, digital signature holder, digital signature certificate, and others.<sup>54</sup> The Communications Regulatory Commission (Commission) is empowered to implement the ESL and may promulgate regulations to that effect.<sup>55</sup> The ESL allows E-signatures and E-documents attested with a certificate issued by a Certification Service Provider (CSP) to be used for all legal purposes, except for the communication of state secrets and whenever a notarized document or signature is required.<sup>56</sup> The ESL recognizes certificates issued in foreign countries.<sup>57</sup>

### *Validity of E-Signatures*

E-signatures and E-documents may be used in place of handwritten signatures and paper documents and have the same degree of legal validity.<sup>58</sup> All types of E-signatures are recognized, but a preference is given to the digital signature; in other words, Mongolia's ESL is third-generation.<sup>59</sup> For example, in the case of a contract, a “certified” E-signature (with relatively greater security features) must be used to sign the E-document.<sup>60</sup> A contract “under seal” must use a certified E-signature.<sup>61</sup> The digital signature must allow its user to be able to determine: (a) if the content of an attached E-document has been changed; (b) the identity of the certificate holder; (c) whether it is genuine, and not fraudulent; (d) whether the private key has been illegally used; and (e) whether the confidentiality and singularity of the private and public keys have been maintained.<sup>62</sup>

### *Certification Service Providers*

The Commission registers practicing Certification Service Providers (“CSP”).<sup>63</sup> To be registered, a prospective CSP must have sufficient expertise; reliability; sufficient financial resources; high-quality technical products; and other qualifications according to the ESL.<sup>64</sup> CSP's must continuously be able to prove that they are qualified to operate under the ESL.<sup>65</sup> A CSP is allowed to issue a certificate only after the subscriber has provided sufficient identification and other personal information.<sup>66</sup> The CSP is bound to maintain the confidentiality of this information, but the CSP must divulge it to law enforcement authorities if they request it.<sup>67</sup> To prevent forgery, the CSP must ensure the security of the signature codes at all times and use only reputable personnel.<sup>68</sup> The subscriber will be given ownership of the private key and must be kept informed of the degree of security of the private key.<sup>69</sup> The subscriber must maintain the confidentiality of the private key.<sup>70</sup>

The certificate must contain the subscriber's name or pseudonym; signature-test code, and the related algorithms; certificate number; dates of validity; the name of CSP and its location; any limitations on usage or monetary amount; and any special attributes of the subscriber.<sup>71</sup> The CSP must post information relating to the certificates on the CSP's website.<sup>72</sup> The CSP is mandated to invalidate the certificate if the requirements of the ESL are not complied with, and the subscriber also has the right to invalidate it.<sup>73</sup> The subscriber has the right to access his file kept by the CSP,<sup>74</sup> and the CSP is not allowed to use the subscriber's

<sup>52</sup> Arab Republic of Egypt, LAW NO. 15/2004 ON E-SIGNATURE AND ESTABLISHMENT OF THE INFORMATION TECHNOLOGY INDUSTRY DEVELOPMENT AUTHORITY (ITIDA), 2004.

<sup>53</sup> Republic of Finland, Ministry of Justice, ACT ON ELECTRONIC SIGNATURES, 2003.

<sup>54</sup> Hong Kong Special Autonomous Region, People's Republic of China, ELECTRONIC TRANSACTIONS ORDINANCE, Ordinance No. 1 of 2000.

<sup>55</sup> Stephen E. Blythe, “A Critique of the German Electronic Signature Law and Recommendations for Improvement,” a paper presented and published in the PROCEEDINGS OF THE ACADEMIC AND BUSINESS RESEARCH INSTITUTE INTERNATIONAL CONFERENCE, San Antonio, Texas USA, March 22-24, 2012.

<sup>56</sup> Republic of Hungary, ACT XXXV of 2001 ON ELECTRONIC SIGNATURE, 2001.

<sup>57</sup> Islamic Republic of Iran, ELECTRONIC COMMERCE LAW OF THE ISLAMIC REPUBLIC OF IRAN.

<sup>58</sup> Jamaica, ELECTRONIC TRANSACTIONS ACT, Act 15 of 2006.

<sup>59</sup> Japan, LAW CONCERNING ELECTRONIC SIGNATURES AND CERTIFICATION SERVICES, promulgated 24 May 2000, effective 1 April 2001.

<sup>60</sup> Hashemite Kingdom of Jordan, ELECTRONIC TRANSACTION LAW NO. 85 OF 2001.

<sup>61</sup> Republic of Lithuania, LAW ON ELECTRONIC SIGNATURE, No. VIII—1822 (July 11, 2000), As Amended, No. IX—934 (June 6, 2002).

<sup>62</sup> Islamic Republic of Pakistan, ELECTRONIC TRANSACTIONS ORDINANCE, 2002.

<sup>63</sup> Republic of Peru, LAW REGULATING DIGITAL SIGNATURES AND CERTIFICATES, 28 May 2000.

<sup>64</sup> Stephen E. Blythe, “Fine-Tuning Vietnam's Electronic Transactions Law In Order To Promote Growth of E-Commerce,” a paper presented at the conference of the Eurasia Business and Economics Society, Warsaw, Poland, November 1-3, 2012.

<sup>65</sup> Republic of Slovenia, Centre for Informatics, ELECTRONIC COMMERCE AND ELECTRONIC SIGNATURE ACT, 2000.

<sup>66</sup> Korean Legislation Research Institute, DIGITAL SIGNATURE ACT NO. 5792, STATUTES OF THE REPUBLIC OF KOREA, Vol. 16 (II), pp. 1217-1220 (1999).

<sup>67</sup> Republic of China, ELECTRONIC SIGNATURES ACT, 2002.

<sup>68</sup> Republic of Tunisia, ELECTRONIC EXCHANGES AND ELECTRONIC COMMERCE LAW, 9 August 2000.

<sup>69</sup> Republic of Turkey, ELECTRONIC SIGNATURE LAW, 2004.

<sup>70</sup> United Arab Emirates, FEDERAL LAW NO. (1) OF 2006 ON ELECTRONIC COMMERCE AND TRANSACTIONS, 30 January 2006.

<sup>71</sup> Republic of Vanuatu, ELECTRONIC TRANSACTIONS ACT (Act. 24 of 2000).

<sup>72</sup> Republic of Uganda, ELECTRONIC SIGNATURES ACT, Draft, 2004.

<sup>73</sup> Republic of Mongolia, Communications Regulatory Commission of Mongolia, LAW OF 15 DECEMBER 2011 ON ELECTRONIC SIGNATURE (“ESL”), 2011; <https://crc.gov.mn/en/k/2lq/1q>.

<sup>74</sup> ESL art. 4.

<sup>55</sup> ESL art. 34.

<sup>56</sup> ESL art. 3, 6.

<sup>57</sup> ESL art. 17.

<sup>58</sup> ESL art. 5.

<sup>59</sup> ESL art. 5.

<sup>60</sup> ESL art. 6.

<sup>61</sup> ESL art. 8.

<sup>62</sup> ESL art. 7.

<sup>63</sup> ESL art. 21, 34.

<sup>64</sup> ESL art. 19.

<sup>65</sup> ESL art. 11.

<sup>66</sup> ESL art. 10.

<sup>67</sup> ESL art. 29.

<sup>68</sup> ESL art. 29.

<sup>69</sup> ESL art. 29.

<sup>70</sup> ESL art. 16.

<sup>71</sup> ESL art. 11.

<sup>72</sup> ESL art. 9.

<sup>73</sup> ESL art. 13, 14.

<sup>74</sup> ESL art. 16.

data for any purpose not related to the CSP's business.<sup>75</sup> If the CSP fails to abide by the ESL, the CSP is liable to third parties incurring damages as a result thereof.<sup>76</sup>

A CSP planning to go out of business must inform the Commission. Those CSPs must inform their subscribers and must revoke all certificates that have been issued. Furthermore, they must find another CSP to assume their responsibilities.<sup>77</sup>

#### ***E-Government***

Rudimentary E-government is included in the ESL. Public officials are mandated to record their official work in electronic form, and they are only allowed to use digital signatures; they may not use other E-signatures.<sup>78</sup>

#### ***Enforcement of the ESL***

The ESL does not contain computer crimes, but it does provide fines. If an imposter CSP operates without a license, the illegal income from his activities shall be confiscated. If an individual, a fine shall be imposed equal to 10 to 15 times the minimum wage; if an entity, a fine shall be imposed equal to 20 to 25 times the minimum wage.<sup>79</sup>

A public official disclosing information from a private key shall be fined. If an individual, the fine will be 3 to 5 times the minimum wage; if an entity, the fine shall be 20 to 25 times the minimum wage.<sup>80</sup> A public official who uses an E-signature that is not a digital signature, or a public official who does not record official work in electronic form, shall be fined. If an individual, the fine shall be 3 to 5 times the minimum wage; if an entity, the fine shall be 5 to 10 times the minimum wage. A public official who fails to fulfill the demands of a state inspector shall be imposed a fine of 3 to 5 times the minimum wage; if an entity, the fine shall be 5 to 10 times the minimum wage.<sup>81</sup>

A CSP who does not fulfill his legal obligations under the ESL shall have his license revoked and all income from his business shall be forfeited. If an individual, he shall be fined 10 to 15 times the minimum wage; if an entity, it shall be fined 15 to 25 times the minimum wage. A CSP who does not suspend the holder of a certificate for violating its terms shall be fined 10 to 15 times the minimum wage. A CSP who does not suspend a certificate at the expiration of its term shall be fined 3 to 5 times the minimum wage. A CSP who does not inform the holder that his certificate has been suspended will be fined 5 to 10 times the minimum wage.<sup>82</sup>

A person making unauthorized changes to an E-document by breaching the ESL shall be fined 5 to 10 times the minimum wage. If a public official, the fine shall be 10 to 15 times the minimum wage; if an entity, the fine shall be 20 to 25 times the minimum wage.<sup>83</sup>

### **RECOMMENDATIONS FOR REFORMATION OF MONGOLIA'S E-COMMERCE LAW**

#### ***Add: Consumer Protections in E-Commerce Contracts***

Mongolia currently requires internet advertisers to identify themselves, provide their contact information, and provide a memorandum to customers when they make an internet payment.<sup>84</sup> However, Mongolian internet purchasers need more protection. As a model, Mongolia can look to Tunisia for an example of a nation with good consumer protections for E-commerce buyers. All of Tunisia's E-commerce consumer protections are commendable: (1) buyers have a "last chance" to review the order before it is entered into; (2) they have a 10-day window of opportunity to withdraw from the agreement after it has been made; (3) they have the right to a refund if the goods are late or if they do not conform to the specifications, and (4) the risk remaining on the seller during the 10-day trial period after the goods have been received.<sup>85</sup>

#### ***Add: Several New Computer Crimes***

The following computer crimes should be recognized: (a) Unauthorized Access to Computer Material; (b) Unauthorized Tampering with Computer Information; (c) Unauthorized Use of a Computer Service; (d) Unauthorized Interference in the Operation of a Computer; and (e) Unauthorized Dissemination of Computer Access Codes or Passwords. The Singapore Computer Misuse Act can be used as a model.<sup>86</sup>

#### ***Add: Information Technology Courts***

Because of the specialized knowledge often required in the adjudication of E-commerce disputes, Information Technology Courts should be established as a court-of- first-instance for them. The I.T. Courts would be tribunals consisting of three experts. The chairperson would be an attorney versed in E-commerce law, and the other two persons would be an I.T. expert and a business management expert. The attorney would be required to hold a law degree and be a member of the bar with relevant legal experience; the I.T. person would be required to hold a graduate degree in an I.T.-related field and have experience in that field,

<sup>75</sup> ESL art. 32.

<sup>76</sup> ESL art. 29.

<sup>77</sup> ESL art. 29.

<sup>78</sup> ESL art. 6.

<sup>79</sup> ESL art. 36.

<sup>80</sup> Id.

<sup>81</sup> Id.

<sup>82</sup> Id.

<sup>83</sup> Id.

<sup>84</sup> Republic of Mongolia, Communications Regulatory Commission of Mongolia, LAW OF 30 MAY 2002

ON ADVERTISEMENT, Art. 12, 2002; <https://crc.gov.mn/en/k/x8>.

<sup>85</sup> Republic of Tunisia, ELECTRONIC EXCHANGES AND ELECTRONIC COMMERCE LAW, 2000.

<sup>86</sup> Republic of Singapore, COMPUTER MISUSE ACT (Cap. 50A), 30 August 1993.

and the business management expert would be required to hold a graduate degree in business administration and have managerial experience. The E-commerce law of Nepal can be used as a model.<sup>87</sup>

#### **Add: Mandatory E-Government**

To reduce cost and to make governmental functions more convenient for citizens, E-government needs to be emphasized and mandated. By established deadlines, governmental departments should begin to offer online services to citizens. Governmental communications to citizens should be in electronic form if at all possible. The best example for Mongolia to follow in the implementation of mandatory E-Government is Puerto Rico; its Electronic Government Act is exemplary.<sup>88</sup>

#### **Add: Explicit Long-Arm Jurisdiction**

Because so many of the E-transactions will occur between Mongolians and parties outside the borders of the nation, it would be prudent for Mongolia to formally state its claim of “long-arm” jurisdiction against any party who is a resident or citizen of a foreign country, so long as that party has established “minimum contacts” with Mongolia.<sup>89</sup> Minimum contacts will exist, for example, if a cyber-seller outside of Mongolia makes a sale to a party living within Mongolia. In that situation, the cyber laws of Mongolia should apply to the foreign person or entity outside of Mongolia because that person or firm has affected Mongolia through the transmission of a message that was received in Mongolia. The foreign party should not be allowed to evade the jurisdiction of the Mongolia courts merely because they are not physically present in the country. After all, E-commerce is an inherently international phenomenon.

### **CONCLUSIONS**

Mongolia’s E-Signature Law is third-generation; it recognizes the legal validity of all types of E-signatures but gives a preference to the digital signature. The statute focuses on the regulation and required business practices of Certification Service Providers, but does not devote enough attention to other important issues. Mongolia’s E-commerce law should be reformed by adding: (1) consumer protections for E-commerce participants; (2) several new computer crimes; (3) information technology courts; (4) mandatory E-government; (5) and explicit long-arm jurisdiction.

### **REFERENCES**

- Berman, A.B. (2001). International Divergence: The “Keys” To Signing on the Digital Line—The Cross-Border Recognition of Electronic Contracts and Digital Signatures. *Syracuse J. Int’l L. & Com.* 28, 125,143-44.
- Blythe, S.E. (2005). Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security. *Richmond Journal of Law and Technology* 11(2), 6.
- Blythe, S.E. (2005). Electronic Signature Law and Certification Authority Regulations of Hong Kong: Promoting E-Commerce in the World’s “Most Wired” City. *N.C. J. L. & Tech.* 7, 1.
- Blythe, S.E. (2006). Taiwan’s Electronic Signature Act: Facilitating the E-Commerce Boom With Enhanced Security. *Proceedings of the Sixth Annual Hawaii International Conference on Business* (2006).
- Blythe, S.E. (2006). Computer Law of Tunisia: Promoting Secure E-Commerce Transactions With Electronic Signatures. *Arab L. Q.* 20, 317-344.
- Blythe, S.E. (2006). A Critique of India’s Information Technology Act and Recommendations for Improvement. *Syracuse J. Int’l L. & Com.* 34, 1.
- Blythe, S.E. (2006). Cyber-Law of Japan: Promoting E-Commerce Security, Increasing Personal Information Confidentiality and Controlling Computer Access. *J. Internet L.* 10, 20.
- Blythe, S.E. (2006). “Pakistan Goes Digital: The Electronic Transactions Ordinance as a Facilitator of Growth for E-Commerce,” *J. Islamic State Practices in Int’l L.* 2(2), 5.
- Blythe, S.E. (2006). Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality. *Ohio No. U. L. Rev.* 33, 525-562 (2006).
- Blythe, S.E. (2006). The Tiger on the Peninsula is Digitized: Korean E-Commerce Law as a Driving Force in the World’s Most Computer-Savvy Nation. *Houston J. Int’l L.* 28(3), 573-661.
- Blythe, S.E. (2006). South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga. *J. So. Pacific L.* 10(1).

<sup>87</sup> Kingdom of Nepal, ELECTRONIC TRANSACTIONS ORDINANCE NO. 32 OF THE YEAR 2061 B.S. (2005 A.D.), s 60-71.

<sup>88</sup> Commonwealth of Puerto Rico, ELECTRONIC GOVERNMENT ACT (“EGA”), Act No. 151 of 22 June 2004; <http://www.oslpr.org/download/en/2004/0151.pdf>.

<sup>89</sup> The Republic of Tonga is an example of a nation that has claimed long-arm jurisdiction over E-commerce parties, and its statute may be used as a model. See, Stephen E. Blythe, “South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga,” 10:1 JOURNAL OF SOUTH PACIFIC LAW (2006), a publication of the School of Law, University of the South Pacific, Emalus Campus, Port Vila, Republic of Vanuatu.

- Blythe, S.E. (2006). Tehran Begins to Digitize: Iran's E-Commerce Law as a Hopeful Bridge to the World," *Sri Lanka J. Int'l L.* 18.
- Blythe, S.E. (2007). Azerbaijan's E-Commerce Statutes: Contributing to Economic Growth and Globalization in the Caucasus Region. *Columbia J. East European L.* 1(1) 44-75.
- Blythe, S.E. (2007). The Dubai Electronic Transactions Statute: A Prototype for E-Commerce Law in the United Arab Emirates and the G.C.C. Countries. *J. Econ. & Admin. Sciences* 22(1),103 (2007).
- Blythe, S.E. (2007). China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce. *Chicago-Kent J. Intellectual Prop.* 7, 1.
- Blythe, S.E. (2007). Hungary's Electronic Signature Act: Enhancing Economic Development With Secure E-Commerce Transactions. *Info. & Comm. Tech. L.* 16(1), 47-71 (2007).
- Blythe, S.E. (2007). Lithuania's Electronic Signature Law: Providing More Security in E-Commerce Transactions. *Barry L. Rev.* 8, 23.
- Blythe, S.E. (2007). Slovenia's Electronic Commerce and Electronic Signature Act: Enhancing Economic Growth With Secure Cyber-Transactions. *I.C.F.A.I. J. Cyber L.* 6(4) 8-33.
- Blythe, S.E. (2008). Bulgaria's Electronic Document and Electronic Signature Law: Enhancing E-Commerce With Secure Cyber-Transactions. *Transnat'l L. & Contemp. Problems* 17(2), 361.
- Blythe, S.E. (May, 2008). Armenia's Electronic Document and Electronic Signature Law: Promotion of Growth in E-Commerce via Greater Cyber-Security. *Armenian L. Rev.*
- Blythe, S.E. (August, 2008). Croatia's Computer Laws: Promotion of Growth in E-Commerce Via Greater Cyber-Security. *European J. L. & Econ.* 26(1), 75-103.
- Blythe, S.E. (May, 2008). E-Signature Law and E-Commerce Law of the European Union and its Member States. *Ukrainian J. Bus. L.* 22-26.
- Blythe, S.E. (2008). Finland's Electronic Signature Act and E-Government Act: Facilitating Security in E-Commerce and Online Public Services. *Hamline L. Rev.* 31(2), 445-469.
- Blythe, S.E. (2008). On Top of the World, and Wired: A Critique of Nepal's E-Commerce Law. *J. High Tech. L.* 8(1).
- Blythe, S.E. (2009). The New Electronic Commerce Law of the United Arab Emirates: A Progressive Paradigm for Other Middle Eastern Nations to Emulate. *Proceedings of the Annual International Conference on Global Business*, Dubai, United Arab Emirates.
- Blythe, S.E. (2009). Computer Law of Colombia and Peru: A Comparison With the U.S. Uniform Electronic Transactions Act. A book chapter in *Internet Policies and Issues*, Frank Columbus, Ed., Nova Science Publishers, Inc., New York NY USA.
- Blythe, S.E. (2009). The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control. *Proceedings of the Tenth Annual Conference of the International Academy of African Business and Development*, Kampala, Uganda.
- China, Hong Kong Special Autonomous Region. (2000). *Electronic Transactions Ordinance*, Ord. No. 1, s 2.
- Chung, R.C.Y. (2003). Hong Kong's "Smart" Identity Card: Data Privacy Issues and Implications for a Post-September 11<sup>th</sup> America. *Asian-Pacific L. & Pol'y J.* 4, 442.
- European Union. (1999). *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework For Electronic Signatures (1999/93/EC)*—19 January 2000, OJ L OJ No L 13 p.12.
- Fischer, S.F. (2001). California Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation. Association of American Law Schools 2001 Annual Meeting, Section on Law and Computers, *B.U. J. Sci. & Tech. L.* 7, 229, 233.
- Froomkin, A.M. (1996). The Essential Role of Trusted Third Parties in Electronic Commerce. *Or. L. Rev.* 75, 49, 58.
- Glopal for Merchants, Selling Online in Mongolia; <https://merchants.glopal.com/en-us/sell-online/mongolia> .
- Hallerman, D. (June 1, 1999). Will Banks Become E-commerce Authorities? *Bank Tech.News*, 12.
- Hogan, T.C. (2000). Now That the Floodgates Have Been Opened, Why Haven't Banks Rushed Into the Certification Authority Business? *N.C. Banking Inst.* 4, 417, 424-25.



- Nepal, Kingdom of. (2005). Electronic Transactions Ordinance No. 32 of the Year 2061 B.S., s 60-71. An official English version was released by the Nepal Ministry of Law, Justice and Parliamentary Affairs and was published in the *Nepal Gazette* on 18 March 2005.
- Poggi, C.T. (2000). Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation. *Va. J. Int'l L.* 41, 224, 250-51.
- Pun, K.H., Lucas Hui, K.P. Chow, W.W. Tsang, C.F. Chong & H.W. Chan. (2002). Review of the Electronic Transactions Ordinance: Can the Personal Identification Number Replace the Digital Signature?, *Hong Kong L.J.* 32, 241, 256.
- Roland, S.E. (2001). The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues? *Suffolk U. L. Rev.* 35, 625, 638-45.
- Ross, C.M. (2005). Probate—Taylor v. Holt—The Tennessee Court of Appeals Allows a Computer Generated Signature to Validate a Testamentary Will. *U. Memphis L. Rev.* 35, 603.
- Singapore, Republic of. (1993, revised 2007). *Computer Misuse Act*, Cap. 50A. Retrieved from: <https://sso.agc.gov.sg/Act/CMA1993> .
- Singapore, Republic of. (1998). *Electronic Transactions Act*, Cap. 88.
- Smedinghoff, T.J. (1999). Electronic Contracts: An Overview of Law and Legislation. *PLI/P*, 564, 125.
- Stern, J.E. (2001). Federal Legislation: The Electronic Signatures in Global and National Commerce Act. *Berkeley Tech. L.J.* 16, 391, 395.
- Tang, D.K.Y. (1999). Electronic Commerce: American and International Proposals for Legal Structures. *Regulation and Deregulation: Policy and Practice in the Utilities and Financial Services Industries* 333 (Christopher McCrudden Ed.).
- Tunisia, Republic of. (2000). *Electronic Exchanges and Electronic Commerce Law*, art. 25-37.
- Turkey, Republic of. (2004). *Electronic Signature Law*, art. 14.
- United Nations, Commission on International Trade Law. (1996). *Model Law on Electronic Commerce with Guide to Enactment*, G.A. Res. 51/162, U.N. GAOR, 51<sup>st</sup> Sess., Supp. No. 49, at 336, U.N. Doc. A/51/49.
- United States of America, Central Intelligence Agency, “Mongolia,” *The World Factbook*, 30 June 2021; <https://www.cia.gov/the-world-factbook/countries/mongolia/> .
- United States of America, Department of Commerce, Mongolia Country Commercial Guide: E-Commerce; <https://www.trade.gov/mongolia-country-commercial-guide> .
- United States of America, Department of State, Bureau of East Asian and Pacific Affairs, Bilateral Relations Fact Sheet: Mongolia, 24 June 2021; <https://www.state.gov/u-s-relations-with-mongolia/#:~:text=U.S.%2DMONGOLIA%20RELATIONS,relationship%20to%20a%20Strategic%20Partnership> .
- United States of America. (2007). 10 L.P.R.A. s 4081 et seq.
- United States of America, Commonwealth of Puerto Rico. (June 22, 2004). *Electronic Government Act*, Act No. 151. Retrieved from: <http://www.oslpr.org/download/en/2004/0151.pdf>.
- United States of America, State of Utah. (1999). *Utah Code Annotated* 46-3-101 et seq.
- United States of America. (1998). *Uniform Commercial Code* Sect. 2-201, 2-209.
- Wright, B. (2001). Eggs in Baskets: Distributing the Risks of Electronic Signatures. *West L.A. L. Rev.* 32, 215, 225-26.
- Zaremba, J. (2003). International Electronic Transaction Contracts Between U.S. and E.U. Companies and Customers. *Conn. J. Int'l L.* 18, 479, 512.