UNOFFICIAL TRANSLATION PROVIDED BY SQUIRE PATTON BOGGS
18 SEPTEMBER 2014

Law No. (14) of 2014

Promulgating the Cybercrime Prevention Law

We, Tamim Bin Hamad Al Thani, Emir of the State of Qatar,

Having perused the Constitution;

Law No. (3) of 2004 on counterterrorism;

The Penal Code promulgated by Law No. (11) of 2004, as amended;

The Criminal Procedure Code promulgated by Law No. (23) of 2004 as amended by Law No. (24) of 2009;

The Telecommunications Law issued by Decree Law No. (34) of 2004;

The Anti-Money Laundering and Combating the Financing of Terrorism Law as issued by Law No. (4) of 2010;

The Electronic Transactions and Commerce Law issued by Decree Law No. (16) of 2010;

The proposal of the Minister of Interior; and

The draft law submitted by the Cabinet; and

Having referred to the Advisory Council;

Have promulgated the following law:

Article (1)

The provisions of the attached Cybercrime Prevention Law shall come into force.

Article (2)

All service providers addressed under the provisions of the attached Law and operating at the time of its entry into force shall remedy their status in accordance with the provisions of the attached Law within six months from the date of its operation. The Minister of Interior may extend this period up to another six months as necessary.

Article (3)

The Minister of Interior shall be responsible for issuing the decisions implementing the attached Law.

UNOFFICIAL TRANSLATION

SQUIRE PATTON BOGGS

Article (4)

Any provision in contradiction with the provisions of the attached Law shall be repealed.

Article (5)

All competent bodies, each within its area of competence, shall implement this Law. This Law shall be published in the Official Gazette.

Tamim Bin Hamad Al Thani

Emir of the State of Qatar

Issued on: 15 Sep 2014

UNOFFICIAL TRANSLATION

The Cybercrime Prevention Law

Section (1)
Definitions

Article (1)

In the implementation of the provisions of this Law, the following words and expressions shall have the meanings respectively assigned thereto, unless the context requires otherwise:

Information Technology:	Any technique, tangible or intangible, or set of methods, connected or unconnected, used to store, arrange, organize, retrieve, process, develop and exchange information based upon internally stored commands and information, including all inputs and outputs which are associated thereto, by way of wired or wireless association, in an information system or an information network.
Electronic Data and Information	Everything that can be stored, processed, created or transferred by any information technology technique, particularly any writing, photo, sound, number, letter, symbol, signal, etc.
Information Network	A network connecting more than an information technology technique to acquire and exchange information, including personal and public networks and the Internet
Information System	A set of software or hardware used to create, extract, send, receive, view, process or store information.
Information Processing	Executing a process or a set of processes in connection with data or information of an individual or otherwise, including receiving,

	collecting, storing, changing, transferring, retrieving or deleting such information.
Traffic Data	Any electronic data or information arising from any information technology technique and indicating the source and destination of the communication and the route thereof as well as the time, date, size, period, type of the service.
Official Electronic Document	An electronic instrument issued by any government authority or body or any public corporation using an information technology technique.
Website:	A place where electronic data or information are made available on the Internet through a specific address.
Cybercrime	Any act involving an unlawful use of an information technology technique, an information system or the Internet in violation of the provisions of this Law.
Capture	Viewing or acquiring electronic data or information
Electronic Transactions Card:	An electronic card issued by competent authorities and containing a magnetic stripe, a smart chip or otherwise and including electronic data or information.
The Competent Authority:	The competent authority at the Ministry of Interior.
Service Provider:	Any natural or legal person enabling users to communicate through information technology or processing any storing of information.
User Information:	Any information available to the service provider relating to the service users, including: 1) The type of the used communication service, the technical requirements and the service period; 2) The user's identity, email or geographic address, telephone number and payment details which are available based on an agreement or arrangement regarding the service; and 3) Any other information about the location in which the communication equipment are installed according to the service agreement.

UNOFFICIAL

Section (2)
Crimes
Chapter (1)
Crimes Pertaining to Hacking Information Systems, Information Programs, Information Networks and Websites

Article (2)

A person who manages through an Information Network or any information technology technique to have an unlawful access to a website or an information system belonging to a state authority, body or entity or any affiliated corporation shall be punished by imprisonment for a period not exceeding three (3) years and a fine of not more than QR500,000.

The punishment mentioned in the preceding paragraph shall be doubled if such access results in:

1) acquiring any electronic data or information:
2) acquiring any information or data pertaining to the State's domestic or foreign security or its national economy;
3) acquiring any government information which are deemed confidential by nature or by way of specific instructions;
4) cancelling, destroying, damaging or publishing such electronic information or data;
5) inflicting damage on any beneficiaries or users; or
6) acquiring undeserved money, services or benefits.

Article (3)

A sentence of not more than three years in prison and a fine of not more than QR500,000, or either of these penalties, shall be imposed on any person who (i) intentionally and illegally accesses in any way a website, an information system, an information network or an information technology technique or a part thereof; (ii) exceeds authorized access; or (iii) knowingly continues his visit or access thereof.

The punishment mentioned in the preceding paragraph shall be doubled if such access results in:

1) cancelling, deleting, adding, disclosing, destroying, changing, transferring, capturing, copying, publishing or republishing electronic data or information stored in an information system;
2) inflicting damage upon beneficiaries or users;
3) destroying, stopping or suspending a website, an information system or an information network; or

UNOFFICIAL TRANSLATION

4) changing or deleting a website or changing its content, design or way of use or impersonating its owner or administrator.

Article (4)

A sentence of not more than two years in prison and a fine of not more than QR100,000, or either of these penalties, shall be imposed on any person who unlawfully captures, intercepts or intentionally spies on any traffic data or any data being transmitted through an information network or any information technology technique.

Chapter (2)
Content Crimes

Article (5)

A sentence of not more than three years in prison and a fine of not more than QR 500,000 shall be imposed on any person who through an information network or an information technology technique sets up or runs a website for a terrorist group or organization, facilitates communication with leaders and members of such group or organization, promotes its thoughts, secures financing thereto or publishes information relating to manufacturing explosives or incendiary devices or any device that can be used in a terrorist act.

Article (6)

A sentence of not more than three years and a fine of not more than QR500,000, or either of these penalties, shall be imposed on any person who through an information network or an information technology technique sets up or runs a website to publish false news to threaten the safety and security of the State or its public order or domestic and foreign security.

A sentence of not more than a year in a prison and a fine of not more than QR250,000, or either of these penalties, shall be imposed on any person who promotes, disseminates or publishes in any way such false news for the same purpose.

Article (7)

A sentence of not more than five years in prison and a fine of not more than QR500,000 shall be imposed on any person who, through information technology techniques, produces child pornography or imports, sells, puts to sale, offers the use of, circulates, transfers, disseminates, publishes, makes available or transmits the same.

A sentence of not more than a year and a fine of not more than QR250,000, or either of these penalties, shall be imposed on any person possessing material including child pornography.

The punishments under this Article shall be imposed irrespective of the child's consent.

Under this article, a child shall be every person under the age of 18 years old.

UNOFFICIAL TRANSLATION

Article (8)

A sentence of not more than three years in prison and a fine of not more than QR100,000, or either of these penalties, shall be imposed on any person who, through an information network or information technology technique, violates social values or principles, publishes news, photos or video or audio recordings related to the sanctity of people's private or family life, even if the same is true, or insults or slanders others.

Article (9)

A sentence of not more than three years in prison and a fine of not more than QR100,000, or either of these penalties, shall be imposed on any person who uses an information network or information technology technique to threaten or blackmail another person to have him/her do or refrain from doing a certain action.

Article (10)

A sentence of not more than 10 years and a fine of not more than QR200,000 shall be imposed on any person who forges an official electronic document or knowingly uses the same.

A sentence of not more than three years in prison and a fine of not more than QR100,000, or either of these penalties, shall be imposed on any person forging an unofficial electronic document or knowingly using the same.

Article (11)

A sentence of not more than three years in prison and a fine of not more than QR100,000, or either of these penalties, shall be imposed on any person doing any of the following actions:

1. Uses an information network or information technology technique to impersonate a legal or natural person; or
2. Manages, through an information network or information technology technique, to seize, for himself or for another person, any movable or document, or secures signature of such document, by acting fraudulently, using a false name or impersonating someone.

Chapter (4)
Crimes Pertaining to Electronic Transactions Cards

Article (12)

UNOFFICIAL TRANSLATION

A sentence of not more than three years in prison and a fine of not more than QR200,000, or either of these penalties, shall be imposed on any person who:

1. Unlawfully uses, accesses or gives access to numbers and data of an electronic transaction card through an information network or an information technology technique;
2. Forges an electronic transaction card in any way whatsoever;
3. Produces or possess, without a license, devices or material that may be used in issuing or forging an electronic transaction card;
4. Knowingly uses or facilities the use of a forged electronic transaction card; or
5. Knowingly accepts an invalid, forged or stolen electronic transaction card.

Chapter (5)
Violating Intellectual Property Rights

Article (13)

A sentence of not more than three years and a fine of not more than QR500,000, or either of these penalties, shall be imposed on any person who uses an information network or information technology technique to violate or ease the violation of copyright and neighboring rights, patents, trade secrets, trademarks, commercial data, trade names, geographic indications, industrial designs or integrated circuit designs which are protected under the law in any way whatsoever.

Section (3)
Procedures

Chapter (1)
Evidence and Investigation Procedures

Article (14)

The public prosecution or any investigation officer authorized thereby may search people, places and other information systems which are relevant to the crime.

The search warrant shall be reasoned and specific, and may be renewed multiple times as long as the reasons behind such procedure still exist.

If the search results in finding devices, tools or instruments related to the crime, the investigation officers shall present the same to the public prosecution which shall take the necessary action.

Article (15)

UNOFFICIAL TRANSLATION

Any evidence collected through information technology techniques, information systems, information networks, websites, electronic information or data may not be excluded on the grounds of its nature.

Article (16)

Any evidence collected by competent bodies or investigation authorities of another state may not be excluded based on that reason as long as collection thereof is in accordance with the legal and judicial procedures pertaining to international cooperation.

Article (17)

The public prosecution may issue an order to promptly collect or record any electronic information or data, any traffic data or any content information as long as it deems so necessary for the investigations.

Article (18)

The Public prosecution may order any relevant person to present it with any relevant devices, tools, equipment, electronic data or information, traffic data, content information or any other thing that would be helpful in uncovering the truth.

Article (19)

All competent bodies shall adopt the necessary measures and procedures to protect any devices, tools, information technology equipment, information systems, electronic data or information placed under seizure until the competent judicial authorities issues a decision regarding the same.

Article (20)

Except for the professional obligations provided for in the law, failure to provide the information and documents required under this Law may not be justified on grounds of professional confidentiality.

Chapter (2)
Service Providers Obligations

Article (21)

According to the established legal procedures, a service provider shall:

1. Present the competent authority, the judicial authority or the court with all the data and information necessary to uncover the truth where so is ordered by the public prosecution;

UNOFFICIAL TRANSLATION

2. Take the necessary steps to block Internet links when so is ordered by the judicial authorities;
3. Keep user information for a year;
4. Keep on a temporary and urgent basis information technology data, traffic data and content information for a period of 90 days renewable upon a request by the competent body or the investigation and litigation authorities;
5. Cooperate with and help the competent authority with collecting and recording the electronic data or information and traffic data if so is ordered by judicial authorities.

Article (22)

The State bodies, authorities and corporations shall:

1. Adopt the necessary preventive measures to protect its information systems, websites, information networks and electronic data and information;
2. Promptly report to the competent authority any crime mentioned in this Law or any unlawful attempts regarding any capturing, intercepting or spying and provide the competent authority with any information necessary to uncover the truth.
3. Keep information technology data and user data for a period of not less than 120 days and provide the competent authority with such data; and
4. Cooperate with the competent authority to enable it to carry out its responsibilities.

Section (4)
International Cooperation

Chapter (1)
General Rules

Article (23)

The competent authority shall help the similar bodies of the other countries regarding mutual legal assistance and extradition of criminals in connection with the criminal procedures of the crimes mentioned in this Law, according to the Criminal Procedures Code, the bilateral or multilateral agreements concluded with the State and the principle of reciprocity without violating the provisions of this Law or any other law.

A legal assistance or extradition request shall not be met under this law unless the laws of the requesting country and the laws of the State deem such crime publishable or impose a punishment for a similar crime. Dual criminality shall be deemed fulfilled irrespective of whether the laws of the requesting country place the crime within the same category of crime or denominate the crime by the same terminology as the State, provided that the conduct underlying the crime is deemed a crime under the laws of the requesting country.

Article (24)

UNOFFICIAL TRANSLATION

The Public Prosecutor shall undertake the function and responsibility for receiving mutual legal assistance and extradition requests relating to the crimes provided for in this Law, and shall implement such requests or refer them to the competent body for implementation as soon as possible.

In urgent cases, such requests may be sent through the International Police Organization or directly by the foreign authority to the competent authority in the State, in which case the body receiving the request shall inform the Public Prosecutor therewith.

Requests and responses shall be sent by post or any other more expedient means that provides access to a written record of receipt or an equivalent thereto, in a manner enabling the State to verify its correctness.

Requests and their attachments shall in all cases be accompanied by an Arabic translation thereof.

Article (25)

The legal assistance and extradition requests shall include the following:

1. Identification of the entity requesting the measure.
2. The name and function of the entity undertaking the investigation or prosecution related to the claim.
3. Specification of the entity to which the request is to be directed.
4. Statement of purpose behind the request and any related remarks.
5. Supporting documentation to the Request.
6. Any known details which may facilitate the ascertainment of the identity of the relevant persons, particularly their names, social status, nationalities, addresses, locations and occupations.
7. Any known details which may facilitate the ascertainment of the identity of the relevant persons, instruments, property or belongings.
8. The legal text criminalizing the act or a statement of the law applicable to the offence, as the case may be, together with any statement of the penalty that might be imposed on the perpetrator of the offence.
9. Details of the required assistance and any special procedures the requesting country may desire to be implemented.

Article (26)

In addition to the details mentioned in the preceding Article, the requests shall in some specified cases include the following details:

1. Presentation of the requested measures where temporary measures are requested.

UNOFFICIAL TRANSLATION

2. Statement of the relevant facts and arguments which enable the judicial entities to issue a confiscation order according to the law, where a confiscation order is requested.
3. Where the execution of an order relating to temporary measures or confiscation:
    a. Attested copy of the order and a statement of the grounds for its issuance where such are not included in the order itself.
    b. Document ensuring that the order is capable of being executed, and is not ordinarily appealable.
    c. Statement of the required extent of execution of the order and the amount, relating to property value, required to be recovered.
    d. Any information relating to the rights of the third party in the instruments, proceeds, property or other related things.
    e. Original copy of the judicial verdict, an attested copy thereof, or any other documents proving that the accused has been convicted and indicating the punishment imposed, that such verdict is mandatorily executable and showing the balance of the punishment term, where the extradition of a convicted person is requested.

Article (27)

The Public Prosecutor, or the Competent Authority in its own discretion or upon a request from the Public Prosecutor, shall request additional information from the foreign competent authority where such additional information is necessary for the implementation or facilitation of the implementation of the request.

Article (28)

Confidentiality shall be observed where the request made it a condition to observe its confidentiality. Where it is not possible to observe confidentiality, the requesting authority shall be immediately notified.

Article (29)

The Public Prosecutor may withhold the referral of the request to the authorities responsible for its implementation where the measure or order therein requested could possibly substantially contradict a current investigations or claim. The Public Prosecutor shall immediately notify the authority making the request of such decision.

UNOFFICIAL TRANSLATION

Article (30)

Where a request is received from a foreign country for mutual legal assistance in connection with the offences stipulated in this law, the implementation of such request shall be in accordance with the provisions of this Chapter.

The forms of mutual legal assistance shall in particular include the following:

1. Obtaining evidence and interrogating persons concerned.
2. Assisting with the appearance of detainees, voluntary witnesses or others before the judicial authorities of the country making the request for the purpose of providing evidence or assisting with the investigations.
3. Delivery of judicial papers.
4. Execution of search and seizure operations.
5. Immediate reserve of the electronic data and information, and the participant's information.
6. Immediate collection and regiteration of pass information.
7. Inspection of property, places and information system.
8. Provision of information, expert reports and evidence proving the accusation.
9. Confiscation of assets.
10. Any other forms of mutual legal assistance which do not contradict the laws applicable in the State

Article (31)

The mutual legal assistance request shall not be refused except in the following cases:

1. Where the request is not issued by an authorized body under the laws of the country requesting assistance, or where the request is not sent in accordance with the applicable laws or its content constitutes a substantial breach of the provision of this Law or any other laws.
2. Where the execution of the request is likely to affect the security, sovereignty, public order or basic interests of the State.
3. Where the offence connected to the request is the subject-matter of a current criminal claim or has been settled in the State by a final verdict.

UNOFFICIAL TRANSLATION

4. Where there are substantial grounds to believe that the requested measure or order is addressed to the relevant person only because of his/her ethnicity, religion, nationality, race, political convictions, sex or other status.
5. Where the offence mentioned in the request is not included in the laws of the State or has no similar offences included therein in accordance with the provision of Article 23 (2) of this law. However, assistance may nonetheless be granted if it does not involve coercive measures.
6. Where it is not possible to issue an order for the execution of the requested measures by reason of limitation rules applicable on the offence prescribed in this law in accordance with the laws of the State or of the country requesting assistance.
7. Where the order requested to be implemented cannot be implemented according to the law.
8. Where the issuance of the decision in the requesting country has taken place in circumstances where no sufficient guarantees were available in connection with the rights of the accused.

Article (32)

The mutual legal assistance request shall not be refused on the basis of extremely restrictive conditions.

The decision issued in connection with the mutual legal assistance request shall be subject to appeal according to the established legal rules.

Where the request is refused the Public Prosecutor or the competent authority in the State shall immediately inform the foreign competent authority, and give reasons for such a refusal.

Article (33)

Requests for investigation measures shall be implemented according to the rules and procedures applicable in the State, unless the FCA requests the application of specific procedures compatible with such rules. The implementation of measures may be attended by a public officer delegated by the foreign competent authority.

Article (34)

UNOFFICIAL TRANSLATION

Requests for temporary measures shall be implemented according to the aforesaid Criminal Procedures Law and where the request is worded in general terms the measures most appropriate according to the law shall be implemented.

Should the requested measures not be provided for in the aforesaid Criminal Procedures Law, the authorized committee may substitute such measures with measures provided for in such Law which have an effect, as similar as possible, to that of the requested measures.

The rules relating to the lifting of temporary measures shall apply in the manner provided for in this Law, provided that the country requesting the measures is informed before lifting such temporary measures.

Article (35)

In the case the competent authority received a mutual legal assistance request for the issuance of a confiscation order; the competent authority shall transfer the request to the Public Prosecution for the issuance of the confiscation order, and shall execute such order where it has been issued.

The confiscation order shall apply to the information devices and systems and the programs and means used as mentioned in the confiscation rules provided for in this Law and situated in the State.

The competent authority shall, as they execute the confiscation order, observe the particulars on the basis of which the order has been issued.

Article (36)

Without prejudice to the rights of a bona fide owner, the State shall be authorized to dispose of the assets confiscated on its territory upon the application of foreign authorities, unless a treaty signed with the requesting country otherwise provides.

Article (37)

UNOFFICIAL TRANSLATION

The competent authority of the State may sign bilateral or multilateral agreements or measures in connection with investigation matters or the procedures in one or more countries for the purpose of forming a joined investigation teams and conducting of joint investigations.

Where no such agreements or measures exist, joint investigations may be conducted separately on the basis of every individual case.

Article (38)

The competent authority shall on its own discretion send the information obtained during the investigations and the collection of evidence, where it thinks this information may benefit the competent authorities in another country, after obtaining an undertaking of maintaining confidentiality of the information from the recipient.

Extradition:

Article (39)

Offences stipulated in this law shall be considered offences whose perpetrators may be repatriated.

For the purposes of this Law, offences stipulated herein shall not be considered political offences, offences connected to political offences nor offences with political motives.

Article (40)

The extradition request shall not be accepted in the following cases:

1. Where substantial grounds exist for believing that the extradition request is made in order to accuse or punish a person because of his/her sex, race, religion, nationality, race, political convictions, or where the execution of the order would affect his status because of any of the aforesaid reasons.
2. Where the extradition offence is the subject-matter of a claim settled by virtue of a final verdict in the State.
3. Where a person requested to be repatriated under the laws in either of the two countries, is no longer subject to trial or punishment for whatever reason including limitation or pardon.
4. Where substantial grounds exist for believing that the person requested to be repatriated has been or would be subjected to torture, cruel, inhuman or demeaning treatment and where no minimum guarantees under recognised international standards would be available for such a person under the relevant criminal procedures.
5. Where the person requested to be repatriated is a Qatari national.

UNOFFICIAL TRANSLATION

Article (41)

Extradition of offenders may be refused in the following cases:

1. Where there is a current judicial investigation in the State against the person requested to be repatriated in connection to the extradition offence.
2. Where the extradition offence was committed outside the territories of either of the two countries and the laws of the State do not provide for jurisdiction in the case of offences.,
3. Where a judicial verdict has been issued against the person requested to be repatriated. Furthermore where such person would be subjected to an unfair trial and judgment in the requesting country..
4. Where the State is of the opinion that extradition of the relevant person would be contrary to human considerations because of his age, health or other personal circumstances.
5. Where the extradition request is based on a final verdict issued in absentia due to reasons beyond the person control i.e. the person did not have sufficient time before the trial to take necessary measures for his defense, consequently failed to have the opportunity to personally review his/her case..
6. Where the State has assumed jurisdiction in respect of the offence

Article (42)

Where the extradition request is refused for reasons provided for under this Law, the case shall be transferred to the competent authority to conduct the prosecution of the person being subjected to the extradition request.

Article (43)

In the cases relating to the offences stipulated in this law, the State may assist in the extradition of offenders after receiving a temporary arrest warrant from the requesting country; provided that the person requested to be repatriated explicitly agree thereto before the authorized body.

General Provisions

Article (44)

Without prejudice to any severer penalty provided in the penal code or any other law, perpetrators of the offences punishable by this this law, shall be punished by the penalties stipulated herein.

UNOFFICIAL TRANSLATION

Article (45)

Whoever commits an act constituting an offence set in forth by any other law, using the information network or the information system shall be punished by the penalty provided for therein.

Article (46)

in conditions other than those permissible by the law, whoever divulges the confidentiality of the procedures stipulated in this law shall be sentenced to imprisonment for not more than two years or to a fine not exceeding (100,000) hundred thousand Riyals, or to both.

Article (47)

Any service provider violates any of the provisions of Article (21) of this law shall be punished with a fine not more than (500,000) five thousand Riyals.

Article (48)

Any juristic person shall be sentenced to a fine of not more than (1,000,000) one million Riyals, if any of the offences stipulated in this law committed in his name or on his behalf.

Article (49)

Whoever contributes by motivation, agreement, or assistance to the committal of a felony or a misdemeanor punishable virtue to the provisions of this law, shall be subject to the penalties provided for therein.

Article (50)

Whoever attempts to commit a felony or a misdemeanor punishable virtue to the provisions of this law, shall be imprisoned for a term not exceeding half the maximum limit prescribed for the consummate offence.

Article (51)

Shall be doubled the punishments prescribed for the offenses set forth in this law, if committed to facilitated by a public employee, taking the advantage of his powers and his authority to do so.

Article (52)

UNOFFICIAL TRANSLATION

IN the event of conviction of any of the offences stipulated in this law, in addition to the penalties stipulated in this law, the court may order to deport the non-Qatari perpetrator out of the country.

Article (53)

In addition to the penalties set forth in this law, and without prejudice to the rights of bona fide third parties, the court shall, in all cases, confiscate devices or programs or means used in, or any funds obtained form, the offences set forth in this law, and shall order the closure of the place or the block of the website where or which by the offence has occurred, as the case may be.

Article (54)

Shall be exempted from the penalties set forth in this law, whoever perpetrator(s) initiates to inform the competent authorities of any information about the crime and its participants before their knowledge thereof. The court may order may order the suspension of the execution of the penalty if the information was communicated to the authorities after they had already become aware of the crime, but in circumstances where this information led to the arrest of the rest of the perpetrators.

UNOFFICIAL TRANSLATION