2011 International Conference on Software and Computer Applications
IPCSIT vol.9 (2011) © (2011) IACSIT Press, Singapore

A Guideline to Enforce Data Protection and Privacy Digital Laws in Iran

Tahereh Hasani

Asia Pacific University College of Technology and Innovation, Kuala Lumpor, Malaysia
Tahereh.Hasani@gmail.com

Ali Dehghantanha

Asia Pacific University College of Technology and Innovation, Kuala Lumpur, Malaysia
ali_dehqan@ucti.edu.my

Abstract. in the Iranian cyber law, no law has been enacted to protect the personal data of the people when a theft of personal data occurs. This paper will suggest a guideline for applying and enforcing the data protection and privacy digital laws in Iran. By enforcing the suggested guideline we achieve a means to process data strictly by commercial sectors for commercial activities in sectors of tourism, finance, insurance, telecommunications, and such other commercial transaction sectors.

Keywords— Data Protection, Privacy, Digital Laws, Iran

I. Introduction

The lack of attention to privacy in constitution and legal documents of Iran caused to very poor privacy protection in the country. i.e. [1] discusses that the use of identification mechanisms like biometrics or CCTV cameras with no specific privacy protection mechanism is very common.

In theory the future "data protection law" would be able to protect personal information and privacy of consumers where transactions over a network, collection, storage, retrieval and dissemination of personal data. However due to constant disapproval and contradicting view points from various governmental parties, approving the data protection law has been constantly delayed.

Comparing EU and American laws regarding privacy shows that in US the federal government regulations protect the data privacy while in EU specific right sets and some principles for controlling private information has been set regardless of the data type (public or private) [2].

The approach of Iran's data protection law will be a combination of both as the government aims to provide a data protection law that helps to regulate the treatment of personal data for both the public and private sector, as well as for data collection by the government Internal Security Act (ISA).

The underlying problem however is that while the data protection law has been awaiting approval, there has been rampant consumer data theft in the Iranian market. It has been known that the information of consumers has been sold to willing buyers for as low as 1 Rial, resulting in data theft, scams, spamming, fraud, and identity theft [3] while there is no law in place to punish those steal personal data.

This paper serves as to review and recommend a solution for the personal data protection plan in Iran, which caters for everyone and not just enterprises.

Lots of international bodies including Article 12 of the Universal Declaration of Human Rights and Article 17 of the United Nations International Covenant on Civil and Political Rights [4] acknowledged the privacy right by stating: "No one shall be subjected to arbitrary interference with his privacy, family, home or

correspondence or to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." The international concept of "the right to privacy". This international constitution is resulted from U.S common law and usually plays an important role in managing privacy all around the world.

When it comes to our personal data and protecting it in Iran, it is understandable that there is none in existence. Legally, it would be a crime to sell out a person's personal data or information to any outside party. With regards to the banking acts in the country, it is illegal to do so, but it only means that it's a crime to sell customers personal data if you're an employee of a bank.

So if you're personal data has been leaked or sold-out from an employee that's working in your telecommunications line company or your membership club and you would like to make a complaint or file a police report. There is no known law or act at the moment that will back you up.

There may be no effects since the absence of a data protection act, but in reality companies have suffered losses due to the lack of a law that protects the personal data. According to **a** KPMG survey [5] which are done in 2004, when the lack of a data protection act was not yet known to the mass public:

- 83% of respondents acknowledge fraud in their organization
- 17% suffered losses of $ 1 million
- 87% of fraud was done internally
- 38% consider intellectual property to be at risk of theft or fraud.

Aside from the numbers alone, companies identify their intellectual property as being at risk the most. Since the absence of a data protection act financial and information loss occur with much of the crimes that took place being unable to be enforced. Among 17% of respondents from the KPMG fraud survey, the following percentile shows how their personal and private information had been abused.

- 55% acknowledge that an abuse of password or access privilege from their employees.
- 23% said there was manipulation of the weakness in the current IT systems in their company.
- 27% accredit the breach of information through hacking.
- 68% of the respondents accredited the crimes to be committed by internal users within their organization.

The current lack of data protection act in Iran caused a very uncontrolled usage of private customers data by banks, developers, and other enterprises that lead to leaking of the data as well [9]. Even for some cases like banking environments that should follow international rulings like the BAFI act (Banking and Financial Institution acts), these acts are weakly enforced.

The absence of the data protection act has allowed forms of data theft to go unpunished and needs to be erected to govern private data processing the processing of personal data such as in countries like Emirates, and Turkey.

The data protection act should be able to control collection, preservation, and using and implementation of personal data by any parties. Therefore, privacy of all individual data would be guaranteed by creating a set of common regulations for handling and management of private data.

The data protection act would apply to all personal data, which by all means would indicate any recorded information in a document. The processing and management of these documents by automatic or non-automatic means should be regulated in a way that no private or individual data would be extractable by linking the information. This should cover all indications of intentions or individual expressions in relation to their private information.

The data protection act will apply to any information or opinion which are processed by either online or offline means. Information which is used in the data protection act is information that relates to a person either living or deceased and from which the person's identity is ascertainable. Information in the data protection act includes all opinions, statements of intentions, and all form of personally identifiable information both recorded online and offline.

The data protection act will be used to regulate the usage of personal data for data subjects by the data users. The data subjects in this instance is the individual who is the subject of the personal data, while the data users are individuals, and/or organizations who controls the collection, holding, processing, or usage of any personal data.

II. Review and Analysis of the Draft Cyber Law

The below provisions are mentioned in the current draft; however, lacks enough details and therefore are quite misleading.

- Unauthorized access to computer material
- Unauthorized usage and modification of computer material.
- Unauthorized access with the intention to commit or facilitate offences
- Password Sharing
- Threatening to damage a computer or data
- Compromising confidentiality
- Obstruction of computing services
- Obstruction of justice
- Geographical coverage

Upon initial comparisons to the United States of America's cyber law, the following provision seems to be missing in the Iranian version and needs to be addressed in the Iranian cyber law as well. These provisions and the pertaining sections in the current draft will be discuss more further in this paper

- Access to information and data related to national security
- Compromising Confidentiality
- Trespassing
- Duping
- Intentional damage
- Intentional access and intentional damage
- Intentional access and unintentional damage
- Password sharing
- Threatening to damage

In this part, we highlight and discuss the major flaws in Sections 3 to 11, which are related to common cyber laws and which must be improved**.**

A. Issues in Section 3 of the Current Draft Act

Section three in the draft cyber law focuses on preventing "unauthorized usage of material stored in a computer". Language can be often a problem in the legal domain, especially when it comes to technical terms. The title itself, in Section 3 creates a doubt since it specifically uses the term "unauthorized". However, it is not only outsiders who try to access data or computer that they are not supposed to access. Both insiders and outsiders are involved in the real cases. This section needs to clearly explain both "Unauthorized" and "Privilege Escalation".

B. Issues in Sections 4 and 5 of the Current Draft Act

Section 4 focuses on preventing unauthorized access to computers or data with the intention to commit or facilitate offences. Due to the critical nature of the subject matter, a cyber law cannot be left ambiguous. It is critically important to differentiate between damages due to reckless or irresponsible computer usage and intentional damages. Furthermore, this section must define what constitutes to be "damage" and what is meant by "fraud". Section number 16 of the draft act gives the definitions of the key terms; however, the aforementioned have not been included.

Section 5 goes in line with Section 4 thus adding the prevention of unauthorized modification to material stored in a computer. Then again, the bill fails to specify what constitutes to be a modification, is it changing the contents in a file? Or does a mere time stamp modification constitute to be an offence? Such questions can be raised since gadgets such as iPods tend to automatically synchronize, thus changing the time stamps on the files stored in it.

C. Issues in Sections 6 and 7 of the Current Draft Act

These two sections are focused on preventing unauthorized obstruction to a computing service or function. Under United States of America's Computer Fraud and abuse act**,** Section 1030, Sub section 5, it strictly focuses on protecting government material. Learning from the American act, the Iran Act must also contribute

not only to protect the private sector, but as well to protect government property and data. Furthermore, the act should explain what constitutes to be obstruction of a computing service.

D. Issues in Section 8 of the Current Draft Act

Section 8 states that unauthorized sharing or password trafficking either to gain an unlawful benefit, undergo an unlawful purpose or to facilitate access to a computer or information in a computer knowingly that it could harm another person.

Since the main aim of this section is to prevent facilitation of unauthorized access, the section needs more input to fulfill the anticipated need. First of all, different methods of authentication such as usage of passphrase, digital signatures, and digital finger prints must be explored and explained.

E. Issues in Section 9 of the Current Draft Act

This section states the penalties for crimes committed involving protected computer. The term "Protected Computer" under this section refers to computer used for the following purposes:

- Iran nation security, protection or international relations.
- A source for criminal justice data collection.
- Such tools that provide services to telecommunication infrastructure, banking, financial services, public basic needs/services, public travel or information infrastructure.
- Used by public protection services; i.e Iran police services, healthcare and emergency services protection and protection of the systems.

In this section, the term "Protected Computers" has been used in a notably arguable way in terms of technical specifications. Computers which are password protected, antivirus installed, anti malware software installed and other security measures take are not considered as protected computers. This weakens the power or reduces the provisions of jurisdictions, thereby encouraging offenders to attack normal residents whose computer are "not protected" under this statue.

F. Issues in Section 10 of the Current Draft Act

Section 10 focuses on preventing aiding and abetting of cyber crimes. Subsection "b" in section 10, states that "the place where the guilty party was while committing the crime is of interest". It is critically important to avoid ambiguities in the statement. The statement must be able to express what it wants to achieve and why it wants to address the anticipated issue.

G. Issues in Section 11 of the Current Draft Act

This section covers the territorial scope of the act. Subsections "a" and "b" explain the geographical areas of coverage within this act, however turns out to be extremely ambiguous. This section required much revision since it tends to mislead. The Iranian authorities must be given rights to investigate or take action only under Iranian jurisdictions. If the crime happened in another country and if the offender was in a country other than Iran, at the time of crime, then it should not be a concern for the Iranian authorities. However, if the offence directly or indirectly harms anything or person under the Iranian Jurisdictions and provisions, then they must act on it.

H. Intellectual Property Protection

It is fair to say the country currently, has no respect to intellectual property since it has no laws that could possibly protect ones' intellectual property. The very existence of a copyright Law will promote the progress of useful art [4][10], as said in the US constitution on copyrights. This will also help investigators and law enforcement authorities in protecting the victims and prosecuting the offender. Patents and Trademark laws must also be put into place in order to support intellection property protection. For an example, if someone in Iran creates a website and uses the name of another company, the victim and his right cannot be protected since there is no Intellectual Property protection law in the Iran. Not to mention Privacy laws. The current main constitution gives the right for freedom on

To complete the Iran cyber law, the above mentioned areas has to be amended into the constitution. To get a clear view of the whole scenario, below listed are some of the common types of cyber crimes.

- Corporate Espionage

- Child Pornography
- Denial of Service attacks
- Other types of computer hacking
- Copyright, Patent, Trademark Infringement
- Piracy
- Fraud

Based on the above small list of possible or rather ongoing crimes listed above, it is clear that the maximum intended outcome or benefit from the cyber law may not be achieved without adding those missing areas into the constitution.

III. Proposed Guideline for Data Protection

Data protection act ensures privacy of data in collection, storing, and transition by different public and private entities. The law should cover the processing of private data, protection for individuals whose data was being processed, uphold individual rights, and prevent data abuse if approved [6].

Under the data protection act 1998 in the United Kingdom [7], it is specified that personal data must be:

- Processed fairly and lawfully.
- Obtained for specified and lawful purposes.
- Adequate, relevant, and not excessive.
- Accurate and up-to-date.
- Not kept any longer than necessary.
- Processed in accordance with the data subjects rights.
- Securely kept.
- Not transferred to any other country without adequate protection in situ.

The Privacy International states that the legislation which has implication to privacy includes Computer Crimes Act 1997, Digital Signature Act 1997, Communication and Multimedia Act 1998, Penal Code, Official Secrets Act 1972, National Land Code 1965, the Consumer Protection Act 1999, and the Banking and the Financial Institutions Act 1989[8].

With such requirements in lieu, we propose a guideline to apply such requirements and embody it within the Iranian data protection act is shown in subsection (A) (1-8)

A. Proposed Guideline

The proposed data protection act requires compliance with various principles in areas. Such compliance can be reviewed from the United Kingdom data protection act, where the act had to be lawful and compliant to other laws, human rights, and in accordance to the collection, holding, and processing of personal data.

1) Collection of Personal Data

In this occurrence, the collection of personal data has to fair and lawful to the data subject and the data collector. When collecting personal data, the data subject has the right to be informed whether it is obligatory or voluntary for them to supply personal data.

When personal data is collected, the data subject must be informed:

- The choice to supply personal data voluntarily or obligatorily.
- The purpose for collecting data.
- The persons/organization personal data may be transferred to.
- The users' right to access the personal data.
- The users' right to correct the personal data.

2) Purpose for Collecting of Personal Data

There must be a lawful and specified purpose for the collection of personal data from the data subjects. For the collection of personal data, there must be:

- One or more specified and lawful purpose for collection of data.
- A related function or activity for data collection.
- Adequate, relevant but not excessive in relation to the purpose of collecting personal data

3) Usage of Personal Data

The personal is to be used for the sole purpose of collection. In no instance should the personal data that was collected be used for another purpose other than what was stated to the data user.

4) Disclosure of Personal Data

The personal data is not to be disclosed without consent or authority from the data user, unless:

- Disclosure is made for the purpose it was collected for.
- Disclosure is made with a court or police order for investigations.
- Disclosure is due to the request of the ISA

5) Accuracy of Personal Data

All practice shall be done towards ensuring that the personal data is accurate, complete, relevant, non-misleading, and is up-to-date with regards to the purpose it was collected for the purpose intended.

6) Personal Data Witholding Duration

The personal data shall not be kept for a longer period of time than it was intended for. The data shall not be kept longer than it is necessary for the purpose it was collected for. Withholding of data for a period that exceeds the terms and conditions as stated will be viewed as a violation of personal data, and organizations caught doing so will be fined.

7) Personal Data Access and correction

The individual should be informed by the data collector whether his/her personal data is being held, or kept. The data user also has the right:

- To have access to his/her personal data
- To be informed that his/her personal data is being processed.
- To be informed on the logic involved in processing his/her personal data.
- To have his/her personal data corrected.
- To be informed on the purpose his/her personal data is being held.

8) Personal Data Security

The personal data of data users must be kept with upmost security and to ensure that there is confidentiality of personal data. All known steps shall be taken to ensure that security is placed in order to prevent accidental loss, unauthorized access, or intended data theft.

The following procedures require attention and more focus in securing personal data:

- accessing personal data,
- processing personal data,
- deleting personal data,
- modification of personal data,
- destruction of personal data
- storage of personal data,
- security measures in physical equipment,
- transmission of personal data

B. Exemptions in the Data Protection Plan

The following event that a person's personal data can be revealed should be limited to the following, and with a grounded reasoning for doing so

Such exemptions to revealing personal data are:

- National security
- Crime and taxation
- Health
- Judicial appointments
- Employment matters
- Financial and credit status
- Intelligent service

If a police officer or inspector is to conduct a search and seizure, they shall be accompanied with a witness to the search and seizure, a search warrant of reasonable cause, and the access to the personal data required in the search and seizure, and investigation.

IV. Means of Enforcing the Data Protection Act

A. Implementation

Implementing the data protection laws will require organizations to invest in equipment to enforce the regulation of data protection and the uphold code of practicing it.

Company administrators will have to undergo training in order to reprogram and reengineer the business process of processing data in their company in order to meet the satisfactory requirement of the data protection act.

The commission would have to give advice and recommendations to organizations on the means of complying with the data protection act. The cost for getting companies to comply with could cost millions, and the commission.

When implementing regulations for the implementation of the act. There must be a comprehensive regulation for the public sector, and a self regulating sector specific regulation for the private sector. The main focus of the data protection act is on personal information such as credit information, medical information, and other online personal information.

B. Commision to govern Data Protection

To enforce the protection of personal data, there has to be a separate body to govern the enforcement of personal data, which is not related to any governmental body in order to prevent favoritism or corruption within governmental bodies.

The commission shall be able to have a full body to assist and lead investigations on its own, without having restrictions or face peer pressure from organizations and government bodies.

The data protection commission shall be lead by a commissioner which shall have the power to:

- Investigate reported cases.
- Search and seize evidence and personal data deemed necessary for the investigation.
- Compound organizations who malpractice personal data of data users.
- Conduct prosecutions unto the guilty parties who have caused a breach of data.

Aside from having legal jurisdiction to conduct investigations, search and seizures, and conduction prosecutions, the commissioner may carry out inspections on any data system used by the data user for the purpose of making recommendations to the data user and enforcing compliance to the data protection principles as stated earlier.

C. Codes of Practicing Data Protection

The commission will investigate, and come to a conclusion for a ‘codes of practices’ recommendation. The recommendation shall be submitted to the commissioner for further review and approval.

The commissioner shall keep an electronic and physical copy of the codes of practices, and any other copies if necessary, provided there is a valid and sound reason.

Under the code of practice, should there be a breach of the code of practice, it is recommended to charge the assailant with the maximum fine of $250,000 . An assailant who has breached the code of practice shall be taken to court and charged in regards to the malpractice or breach of the code of practice.

D. Reporting a Misconduct of Data Processing

The commission shall accept reports on the misconduct of personal data being processed, review the report to verify its authenticity, and send a notification unto the person that made the report and to the assailant as mentioned in the report.

The commission shall in turn conduct a thorough investigation to find any means of misconduct in the processing of personal data whether stated on the report or not, and as the commissions investigator sees fit.

Should the commission’s investigation yield results of misconduct in the processing of personal data, the assailant shall in turn be fined depending on the misconduct, and a notice of enforcement shall be placed unto the assailant, of which the assailant must comply, else face stern reprimand.

V. Conclusion

In this paper we review the laws and suggested guideline for the Iranian data protection plan based on the United Kingdom's version of the data protection act.

In conclusion, Iran needs a strong and solid foothold in the cyber law department and in securing the personal data of its citizens as more and more information is digitalized and stored online, there will be more access to it from outside sources with no law or data protection act to stop unauthorized access to it.

For the future work the author suggests an anti spam and phishing law, wireless internet law, and a legislation that allows for every Iranian to have a right to the internet.

VI. References

[1] Centre for Independent Journalism, "Poor Privacy Protection in Iran, Says Privacy International"

[2] Jean Slammon & Juri Straff, *"Data Protection and Privacy in the United States and Europe",* pg17

[3] Joseph Loh & Rashvinjeet S. Bedi, "*Beware, your data's on sale"*

[4] United Nations, General Assembly, 3rd Session. "*Resolution 217A Universal Declaration of Human"*

[5] KPMG, *"Fraud Survey 2004"* http://www.kpmg.com.au/aci/docs/Fraud-Survey-2004.pdf, Pg 12

[6] Iran Ministry of Justice , "*Parliament: Personal Data Protection Law Finalised",* http://www.Iranian.org/legal/general_news/parliament_personal_data_protection_law_finalised.html

[7] Giam Say Khoon, husna Yusop, *"Years Away from Data Protection Bill"*, Pg2, http://www.Iranian.org/index2.php?option=com_content&do_pdf=1&id=9868

[8] Caslon.com, *"Caslon Analytics: Privacy Guide",* http://caslon.com.au/austprivacyprofile3.htm.

[9] Lee Min Keong, *"Iran to enforce data protection law",* http://www.zdnetasia.com/news/business/0,39044229,62058458,00.htm

[10] Cornell University Law School, "United States Constitution," Retrieved October 14, 2009 from the world wide web: http://www.law.cornell.edu/constitution/constitution.article.html