

# Access to E-records by Taxing Authorities: A Case for Pakistan (Part II)

---

*Article by: Adil Waseem*

All tax authorities to e-commerce transactions should investigate the record retention requirements of each other's respective jurisdictions.

In September 1998 Revenue Minister Dhalinal of Canada;

"...Interpretation Circular 78-10RS and 779R (Book and Record Retention/Destruction) will be revised to explain the Department's views with respect to the electronic environment. Revenue Canada will work with authorities in other OECD Countries relating to information exchange as they currently do under the WTO and NAFTA relating to customs and excise matters such as Rules of Origin of Goods. Revenue Canada also believes that there are adequate search and seizure powers under the Criminal Code and the Income Tax Act to deal with the difficulty of accessing encrypted information."

An electronic signature may be proved in any manner, in order to verify that the electronic document is of the person that has executed it with the intention and for the purpose of verifying its authenticity or integrity or both.

Presumption relating to advanced electronic signature, in any proceedings, involving an advanced electronic signature, it shall be presumed unless evidence to contrary is adduced, that the electronic document affixed with an advanced electronic signature, as is the subject-matter of or identified in a valid accreditation certificate is authentic and has integrity; The advanced electronic signature is the signature of the person to whom it correlates, the advanced electronic signature was affixed by that person with the intention of signing or approving the electronic document and the electronic document has not been altered since that point in time.

Although digital signature technology has been available for some time, it has only recently become feasible to use digital signatures to authenticate a document. This breakthrough has made digital signatures one of the most important areas of development within electronic commerce. It is important because the technology, and the law governing it, must develop in a way that promotes, or at the very least does not inhibit, the growth of electronic commerce.

## Encryption

The role of encryption and digital signatures go hand in hand in the authentication of records. The cryptography provides the technology used in digital signatures as well as for encryption. Encryption transforms an electronic document unreadable, thereby providing another level of security and increasing the attractiveness of the Internet as a means of transferring confidential data of the type often used in electronic commerce making the access to data possible for purpose of locating of database.

## Clipper Chip

The government should make consistent attempts to introduce legislation on the clipper Chip, or a similar alternative. The Clipper Chip is a device enabling the government to gain access to communications by obtaining a key held by two escrow agents. The technical aspect of clipper chip is well known to information technology experts. But for legal profession it is device by that the record can be authenticated and verified.

## Computer Forensics

There is numbers forensics that performs their legal duties regarding digital discovery of the documents. When we look into the legal history of these digital discovery authorities, their function as certified authorities to all document produced in digital form developed with advanced with electronic communication. The assistance of computer forensics is employed by foreign courts for purpose of getting forensic view about the e-data or electronic evidence.

The Computer Forensics authorities' employs various tools for purpose of verification of documents, starting from identify, acquire, restore, and analyze electronic documents for their admission and production before court of laws. There verification of documents is not limited to local disk data but even the remote server data is verified. From authentication of record to local hard drive to remote server, the certified forensic discovery authorities help in testifying acquired from data from NT, Novell, UNIX, and Linux servers and PCs, among others.

## Identification

There procedure adopted by the digital discovery authorities start from electronic discovery is identification. The electronic discovery is the identification of likely sources of relevant information comparing it with original electronic document. The identification of computer document and its comparison with original record through critical step to help ensure that data is not overlooked and each aspect of date is properly maintained and there is no tampering of database while its production before court of law. There view about the electronic document are requested of disk or

remote documents and go on-site to inventory the data and look for hidden sources of taxpayer for evasion of record. In many cases, they present a written e-discovery report of web site and its links with database where it has been hosted.

#### Acquisition

The Identification of electronic documents is only the first step for proper identification of website link with data base. Once identified, the second step that they have to follow to gather the relevant information for authentication of the electronic evidence as to judge the reliance of the evidence. They take care to collect relevant information for coming to right conclusion regarding the authenticity of e-documents. They take care to avoid tampering of record and to maintain defensible chain-of-custody. There are three critical procedural phases judging the reliance of the electronic evidence and its presentation before the court of laws. Computer forensics employs uses forensically tools, their written protocols and internal procedures ensure that their work product with stands scrutiny in all jurisdictions where it is going to be presented before the court.

#### Restoration

There are many hidden sources of electronic evidence that can not be retrieved without seeking the assistance of the authorities of foreign jurisdiction. Once information regarding the evidence existed out state jurisdiction gathered, document must have to follow the same procedure of as defined in acquire. Rather it is foreign jurisdiction or not, important information is not retrieved without tested forensic procedures and documentation. The computer forensics helps courts to avoid any unnecessary production of documents, while ensuring that potentially relevant documents are presented, including encrypted, compressed, and password-protected files, are presented before court properly.

#### Searching

Another method is used is filtering of electronic database received in electronic discovery. While undergoing search of the electronic evidence, the computer forensics uses a variety of methods, tools and appropriate search technique to widows and other operating system for increasing reliability of electronic document to the court of law. The electronic forensics authorities are given number of powers in connect with assessing the reliance of the electronic and figuring out the hidden sources of evidence.

#### Production

The production and admission before the court of law is primary function of these forensics authorities and the computer forensics produces legal documents of data to court by their certification. They are granted certification power by statute or they are working independent autonomous bodies being famous for their impartial reports, they are often asked by court to give opinion about the electronic having agreed by both parties to suit. They produce copies of the data selected for review and offer recommendations and certification regarding the nature of electronic database to be viewed organizes data as evidence.

#### Verification

The computer Forensics perform number of function, one of them is offering detailed written certified reports and analyses to courts to just adjudication of matter. As being declared as "friend-of-the-court" experts, they assists judges with the interpretation electronic evidence being presented in court proceedings and the testimony of other electronic discovery experts. The court often needs the opinion of these experts regarding the building of the electronic evidence and reliance. For getting appropriate and meeting the reliance standard, although careful attention to detail in the early stages of electronic discovery builds solid expert testimony. The real aim of computer forensics to assist the court in reaching just conclusion regarding production of data as evidence but in Pakistan we have not yet legislated on role of computer forensics as expert role for identification, production and its admission before the court of law.

#### Legislative proposals

The legal requirement to get access to information or database for the purpose of authentication of record which is in electronic form it can only be met by providing access to the information in paper or other non-electronic form; but, if the maintenance of the integrity of the database cannot be assured, the person who must get access to the data must notify every person to whom access is required to be provided of that data base as evidence; and if requested to do so, provide access to the information in electronic form.

The form and means of access to the information reliably assures the maintenance of the integrity of the information, given the purpose for which, and the circumstances in which, access to the information is required to be provided; and the person to whom access is required to be provided consents to accessing the data in that electronic form .But the question of out cross border jurisdiction of taxing authorities is not possible unless international treaties are signed and tax laws are amended for the purpose of empower the tax administration to get access e-transaction database which is located at remoter server.

The mentioned below are my legislative proposals that can address the legal issue of access to e-records.

The Legislation of privacy and securities issues

Legislation has been suggested to address "privacy issues raised by the practices of the Internet industry, including the gathering of information about individuals' patterns of access to Internet sites ." Most of the central and local legislation, however, doesn't prohibit independent third parties from gathering and disseminating your personal information to the millions on the net.

#### Amending Sale Tax Act 1990

The section 25 of sale tax act only deals with accessibility of sale tax officer to records of electronic data base where no specific direction is available for the getting access to record which has kept at remote server.

Here we need to insert the words 'or hosted in remote web server' in section 25 of the Sale Tax Act 1990.,

"...A person who is required to maintain any record or documents under this Act or any other law shall, as and when required by an officer of Sales Tax, produce record or documents which are in his possession or control or in the possession or control of his agent; and where such record or documents have been kept on electronic data or hosted in remoter web server, he shall allow access to such officer of Sales Tax and use of any machine on which such data is kept."

The insert of appropriate wordings will enhance the power of tax administration for purpose of getting access to e-transaction data base.

#### Amending Income tax ordinance 2001

The accessibility income tax officer to get access to e-records which has kept at remote web server is ineffective by non-existent of statutory words, phrase or clause in clause (a) subsection (1) section (175) of income tax ordinance. I recommend the same phrase as I have recommended in section 25 of sale tax act of 1990.

"...In order to enforce any provision of this Ordinance , the Commissioner or any officer authorised in writing by the Commissioner for the purposes of this section – (a) shall, at all times and without prior notice, have full and free access to any premises, place, accounts, documents or computer or remoter web server...";

I will describe in second chapter, how the code criminal procedure can be made effective for search authorization of e-records uploaded at remoter server.

#### The gauging the effectiveness of legislative proposals

There are various standards for determining the effectiveness of the legislative proposal, first-practicability-whenver the legislation is promulgated that must be feasible to enforce it. We how to determine rather any such amendment is put in operation will serve the good or not? Rather any such facility is available for tax officer to access the e-records hosted at remote server, if no, then how these legislative provision can made effective? There is one simple answer to this question by increasing the efficiency of taxing officer. Secondly, predicting the proposed amendment by its intrinsic structure, what could be best substituted phrase that can remove deficiency of enacted provisions? That is 'hosted at remote web server'?

#### Summary

There are various devices are used for getting access to e-records, like encryption, clipper chip and computer forensics, and to extend legal right to access the e-records, we need to make appropriate statutory amendments in tax laws. The writer is an advocate of High Court and practicing immigration and corporate laws in Pakistan since September 2001. Author can be contacted by Adil Law Company (Advocates and Immigration lawyers) Office No.3 2nd Flr Hafeez Chambers 85 The Mall Rd Lahore Pakistan Telephone: +9242-6306195 +9242- 6360108 Fax: + 9242 6360108 Cell: +92300 4254910 E-mail: adil.waseem@lawyer.com