Tampering with Computer Source Code

This document is an extract from the book *Cyber Crime & Digital Evidence – Indian Perspective* authored by Rohas Nagpal. This book is available as courseware for the **Diploma in Cyber Law** and **PG Program in Cyber Law** conducted by Asian School of Cyber Laws

www.asianlaws.org

8. Tampering with Computer Source Code

According to section 65 of the IT Act

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.—For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Computer source code is the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Computer source code need not only be in the electronic form. It can be printed on paper (e.g. printouts of flowcharts for designing a software application).

Let us understand this using some illustrations.

Illustration 1

Pooja has created a simple computer program. When a user double-clicks on the hello.exe file created by Pooja, the following small screen opens up:

Hello World

The hello.exe file created by Pooja is the executable file that she can give to others. The small screen that opens up is the output of the software program written by Pooja.

Pooja has created the executable file using the programming language called “C”. Using this programming language, she created the following lines of code:

```
main()
{
        printf("hello, ");
        printf("world");
        printf("\n");
}
```

These lines of code are referred to as the source code.

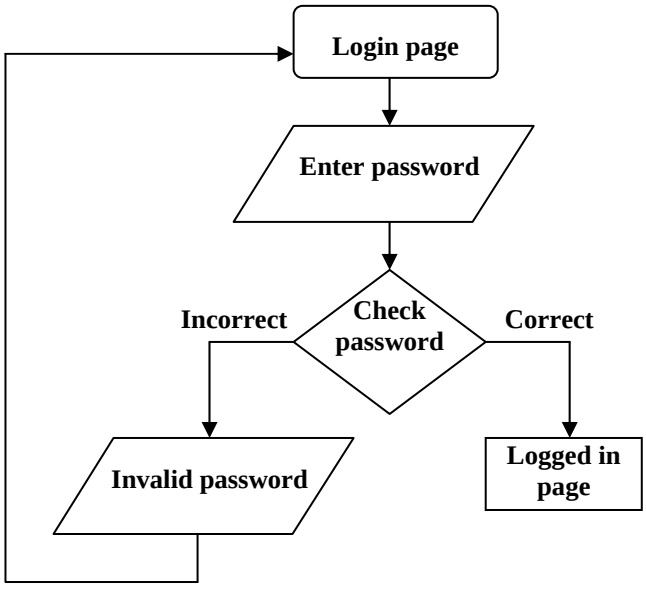
Illustration 2

Noodle Ltd has created software for viewing and creating image files. The programmers who developed this program used the computer-programming language called Visual C++. Using the syntax of these languages, they wrote thousands of lines of code.

This code is then compiled into an executable file and given to end-users. All that the end user has to do is double-click on a file (called setup.exe) and the program gets installed on his computer. The lines of code are known as computer source code.

Illustration 3

Pooja is creating a simple website. A registered user of the website would have to enter the correct password to access the content of the website. She creates the following flowchart outlining the functioning of the authentication process of the website.



She takes a printout of the flowchart to discuss it with her client. The printout is source code.

This section relates to computer source code that is either:

1. required to be kept (e.g. in a cell phone, hard disk, server etc), **or**
2. required to be maintained by law

The following acts are prohibited in respect of the source code

1. knowingly concealing or destroying or altering
2. intentionally concealing or destroying or altering
3. knowingly causing another to conceal or destroy or alter
4. intentionally causing another to conceal or destroy or alter

Let us discuss the relevant terms and issues in detail.

Conceal simply means "to hide".

Illustration
Pooja has created a software program. The source code files of the program are contained in a folder on Pooja's laptop. Sameer changes the properties of the folder and makes it a "hidden" folder.

Although the source code folder still exists on Pooja's computer, she can no longer see it. Sameer has concealed the source code.

Destroys means "to make useless", "cause to cease to exist", "nullify", "to demolish", or "reduce to nothing".

Destroying source code also includes acts that render the source code useless for the purpose for which it had been created.

Illustration 1
Pooja has created a software program. The source code files of the program are contained in a folder on Pooja's laptop. Sameer deletes the folder. He has destroyed the source code.

Illustration 2
Pooja has created a software program. The source code files of the program are contained in a folder on Pooja's laptop. Sameer deletes one of the source code

files. Now the source code cannot be compiled into the final product. He has destroyed the source code.

Illustration 3

Pooja is designing a software program. She draws out the flowchart depicting the outline of the functioning of the program. Sameer tears up the paper on which she had drawn the flowchart. Sameer has destroyed the source code.

Alters, in relation to source code, means “modifies”, “changes”, “makes different” etc. This modification or change could be in respect to size, properties, format, value, utility etc”.

Illustration

Pooja has created a webpage for her client. The source code of the webpage is in HTML (Hyper Text Markup Language) format. Sameer changes the file from HTML to text format. He has altered the source code.

Tampering with Computer Source Code (Summary)

Actions covered	Knowingly or intentionally concealing, altering or destroying computer source code (or causing someone else to do so).
Penalty	Imprisonment up to **3 years** and / or fine up to **Rs 2 lakh**
Relevant authority	Judicial Magistrate First Class
Appeal lies to	Court of Session
Investigation Authorities	1. Controller of Certifying Authorities (CCA) 2. Person authorised by CCA 3. Police Officer not below the rank of Deputy Superintendent
Points to mention in complaint	1. Complainant details 2. Suspect details 3. How and when the contravention was discovered and by whom 4. Damage suffered 5. Other relevant information

Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh & Anr.
2005CriLJ4314

IN THE HIGH COURT OF ANDHRA PRADESH
Cri. Petn. Nos. 2601 and 2602 of 2003
Decided On: 29.07.2005

Appellants: **Syed Asifuddin and Ors.**
Vs.
Respondent: **The State of Andhra Pradesh and Anr.**

Summary of the case

Tata Indicom employees were arrested for manipulation of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocomm.

The court held that such manipulation amounted to tampering with computer source code as envisaged by section 65 of the Information Technology Act, 2000.

Background of the case

Reliance Infocomm launched a scheme under which a cell phone subscriber was given a digital handset worth Rs. 10,500 as well as service bundle for 3 years with an initial payment of Rs. 3350 and monthly outflow of Rs. 600. The subscriber was also provided a 1 year warranty and 3 year insurance on the handset.

The condition was that the handset was technologically locked so that it would only work with the Reliance Infocomm services. If the customer wanted to leave Reliance services, he would have to pay some charges including the true price of the handset. Since the handset was of a high quality, the market response to the scheme was phenomenal.

Unidentified persons contacted Reliance customers with an offer to change to a lower priced Tata Indicom scheme. As part of the deal, their phone would be technologically “unlocked” so that the exclusive Reliance handsets could be used for the Tata Indicom service.

Reliance officials came to know about this “unlocking” by Tata employees and lodged a First Information Report (FIR) under various provisions of the Indian Penal Code, Information Technology Act and the Copyright Act.

The police then raided some offices of Tata Indicom in Andhra Pradesh and arrested a few Tata Tele Services Limited officials for re-programming the Reliance handsets.

These arrested persons approached the High Court requesting the court to quash the FIR on the grounds that their acts did not violate the said legal provisions.

Issues raised by the Defence

1. Subscribers always had an option to change from one service provider to another.

2. The subscriber who wants to change from Tata Indicom always takes his handset, to other service providers to get service connected and to give up Tata services.

3. The handsets brought to Tata by Reliance subscribers are capable of accommodating two separate lines and can be activated on principal assignment mobile (NAM 1 or NAM 2). The mere activation of NAM 1 or NAM 2 by Tata in relation to a handset brought to it by a Reliance subscriber does not amount to any crime.

4. A telephone handset is neither a computer nor a computer system containing a computer programme.

5. There is no law in force which requires the maintenance of "computer source code". Hence section 65 of the Information Technology Act does not apply.

Findings of the court

1. As per section 2 of the Information Technology Act, any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and the devices which are programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer system in a computer network.

2. The instructions or programme given to computer in a language known to the computer are not seen by the users of the computer/consumers of computer functions. This is known as source code in computer parlance.

3. A city can be divided into several cells. A person using a phone in one cell will be plugged to the central transmitter of the telecom provider. This central transmitter will receive the signals and then divert them to the relevant phones.

4. When the person moves from one cell to another cell in the same city, the system i.e., Mobile Telephone Switching Office (MTSO) automatically transfers signals from tower to tower.

5. All cell phone service providers have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider.

6. System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Every cell phone operator is required to obtain SID from the Government of India. SID is programmed into a phone when one purchases a service plan and has the phone activated.

7. Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. ESN is a permanent part of the phone.

8. Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. MIN is programmed into a phone when one purchases a service plan.

9. When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing.

10. If the phone cannot find any control channels to listen to, the cell phone displays "no service" message as it is out of range.

11. When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's location in a database, knows which cell phone you are using and gives a ring.

12. So as to match with the system of the cell phone provider, every cell phone contains a circuit board, which is the brain of the phone. It is a combination of several computer chips programmed to convert analog to digital and digital to analog conversion and translation of the outgoing audio signals and incoming signals.

13. This is a micro processor similar to the one generally used in the compact disk of a desktop computer. Without the circuit board, cell phone instrument cannot function.

14. When a Reliance customer opts for its services, the MIN and SID are programmed into the handset. If some one manipulates and alters ESN, handsets which are exclusively used by them become usable by other service providers like TATA Indicom.

Conclusions of the court

1. A cell phone is a computer as envisaged under the Information Technology Act.

2. ESN and SID come within the definition of “computer source code” under section 65 of the Information Technology Act.

3. When ESN is altered, the offence under Section 65 of Information Technology Act is attracted because every service provider has to maintain its own SID code and also give a customer specific number to each instrument used to avail the services provided.

4. Whether a cell phone operator is maintaining computer source code, is a matter of evidence.

5. In Section 65 of Information Technology Act the disjunctive word "or" is used in between the two phrases –

    a. "when the computer source code is required to be kept"

    b. "maintained by law for the time being in force"

www.asianlaws.org

Head Office

6th Floor, Pride Senate,

Behind Indiabulls Mega Store,

Senapati Bapat Road,

Pune - 411016.

India

Contact Numbers

+91-20-25667148

+91-20-40033365

+91-20-64000000

+91-20-64006464

Email: info@asianlaws.org

URL: www.asianlaws.org