



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 Issue: VII Month of publication: July 2019

DOI: <http://doi.org/10.22214/ijraset.2019.7146>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Cell Phone Surveillance & Tracking

Ajit Kumar¹, Dr. Anita Soni²

²T.I.T Group of Institutions

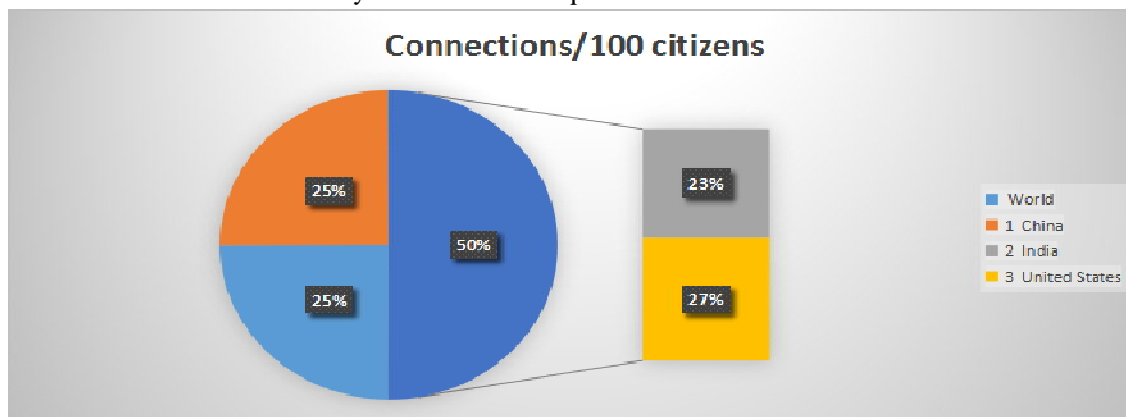
Abstract: *This paper provides an overview of the police department use of new technologies to monitor and track the movements of people using cell phones or smart phones. A Police Department applied a method for tracking as a any crime cases. Cellphone surveillance (also known as cellphone spying) may involve the tracking, bugging, monitoring, interception and recording of conversations and text messages on mobile phones. A distinction is made between major crime (e.g. theft, murder, violent assault, rape, etc.) and volume crime (e.g. domestic burglary, shoplifting, etc.). Illustrative systems that are in practical use for tackling both major and volume crime are described. A topic of current research is the use of tracking techniques for automatically detecting patterns in reported crimes. The paper concludes by looking at the problems and benefits such systems may bring.*

Keywords: *Mobile Phone, Police Department, Tracking Criminals, Crime, misplace.*

I. INTRODUCTION

In today’s lifestyle, Mobile phones have really changed the way of communications. Cell phones are the most used communication tools in today life. Mobile phones are at the center of everyone’s lives today. You have your complete life documented on your mobile phone—private photographs, contacts, bank details, browsing history, personal emails, phone logs and almost all your personal information. Mobile phones are used widely in our day-to day lives giving us the freedom to communicate anywhere and at any time. With the growing importance of mobile phones the handset has become a valuable item particularly in terms of the personal data or information stored in it and for this reason, the mobile phone theft has become a serious problem.

List of countries by number of mobile phones connections/100 citizens in use.



But India lost 3 million active mobile connections in January 2018, with Airtel, Idea, Reliance Jio and Vodafone accounting for 85% of total active mobile connections in India, according to data released by TRAI.

“The survey results are clear: mobile phone loss and theft is a significant issue for Indians today. As smartphones become more pervasive in our lives, there is a greater need to protect the data on such devices,”

When we misplace our phone then the fear of its misused is the biggest stress for every person. The best option for us is to opt for filing a FIR because that is very easy and the procedure to file a FIR is very easy and ensures the possibility of exemption from any liability arising from the misuse of that phone. To file the FIR the person needs to go to any nearby police station where he last time had his phone with him and tell the police officer, the details of his phone like colour and model of the phone, IMEI number of the phone. If there were any witnesses present at the place where you lost your phone you can mention their names too. Or that person can file the complaint online to where he needs to register IMEI number of his phone online at the Stolen Mobile Database.

While registering your IMEI number online you need to provide your e-mail and active mobile number then you will get an SMS with a code you need to fill that code and some details then you can register your IMEI number. This registration will not lodge a complaint itself but save the phone from resale, or can be used to generate a copy of FIR.

But According to Crime in India data, 19,377 cases (in 2014) of Electronic Components Stolen were registered across the country last year, out of which 6,014 were recovered. Police promptly registers FIR in all cases, where the Mobile Phones have reportedly been stolen. The complainant is also advised to inform the Service Provider to block the SIM to prevent misuse.

Moreover, concrete steps /measures have also been taken by Police to make the public aware of their rights to lodge a complaint/FIR in Police Stations. There is a sign board in the Duty Officer's room of every Police Station, indicating the right of complainant to lodge an FIR. Efforts are made by Police to track/trace stolen mobile phones are as under:-

The Investigating Officer makes necessary efforts to track and recover the stolen mobile phones. These include contacting the service providers, ascertaining the user details of the number on which the handset is activated subsequent to this theft and visiting the address mentioned in the subscriber form. The technical knowhow pertaining to IMEI number of a stolen mobile phone is available only with the service providers and necessary follow-up of a painstaking kind is done with the service providers to scan and work upon the IMEI numbers of stolen phones, in order to trace them. Zonal Integrated Police Network (ZIPNET) has been provided which contains the details (IMEI numbers) of lost/stolen mobile handsets. Citizen are advised to check the list of stolen/list mobile handsets on the ZIPNET before purchasing a pre-owned mobile phone.

Further, the Government has emphasized that the Law Enforcement Agencies i.e. Police, Prosecution and Judiciary etc. and the Public at large may be made aware and for the effective implementation of Information Technology Act, 2000 read with Information Technology (Amendment) Act 2008 and Rules made there under, as these are effective laws to deal with matters on Crimes. Agencies like NASSCOM, NTRC, CERT-In etc. may also be taken for training. The aforesaid measures are only indicative and the State Governments/UT Administrations may consider any additional measures for the preventing & combating crime as necessary. Art.21 of the Indian Constitution says that "No person shall be deprived of his life or personal liberty except according to procedure established by law."

II. BASICALLY A FOLLOWING SERVICES THAT ARE USED IN POLICE DEPARTMENT:-

- 1) CDR (Call Detail Record)
- 2) TL (Tower Location)
- 3) PL (Parallel Listing)- Logger Machine
- 4) CAF (Customer Application Form)
- 5) SDR (Subscriber Detail Report)

A Police Department applied this method for tracking as a any crime cases. Cellphone surveillance (also known as cellphone spying) may involve the tracking, bugging, monitoring, interception and recording of conversations and text messages on mobile phones.

It also encompasses the monitoring of people's movements, which can be tracked using mobile phone signals when phones are turned on. Only an officer of the rank of Superintendent of Police — a DCP-rank officer in a commissionerate — can write to the nodal officer of a mobile network service provider seeking the CDR of persons in connection to an investigation.

III. TRACKING CRIMINALS AND CRIME

Mobile technology has become a powerful crime-fighting tool. Cell phones contain call history, contacts, text messages, web browser history, email, a Global Positioning System (GPS), and other location information that police and law enforcement agencies find valuable. Evidence from cell phones can help investigators piece together motives and events and provide new leads. By law (at least in the USA for sure, and other countries), the police can request the carrier to provide that information - based on some purpose like safety, for example, or tracking a criminal, etc.

Police sends the request to the service provider's legal department with the details of Mobile e.g. Mobile Number /IMEI number for tracking the location of the Cell Phone. Mobile service providers give the information to the police about the Mobile number from there database.

- 1) *CDR (Call Detail Record)*: Call Detail Record (CDR) is the detailed record of all the telephonic calls that pass through a telephone exchange or any other telecommunications equipment. The record is maintained by the concerned telephone exchange and contains call details such as time of the call, duration of the call, source and destination number, completion status of the call, etc. When your phone is off, police contacts your service provider to give the details of calls made in a specific duration of time. So they can get last location of yours from there. This is basically because you connect to a tower of the service provider to make calls/SMS/etc and the provider records the same. Therefore, some details regarding the call, your phone and the tower are stored with the company.



- 2) *TL (Tower Location)*: The mobile phone provider also gives to the police the location of the mobile phone while a call is being made or an SMS is being sent or received. This means, that the police can also track your movement while you use the phone. Every time someone uses a cell phone, a signal is sent out that pinpoints where the criminal/user is. In TL a following data is present MSISDN , Last Activity, Cell ID, VLR ID, IMSI, Latitude, Longitude, Google map link, and Request ID. Through a TL a police department easily reach a criminal.
 - 3) *PL (Parallel Listing)*: Cell phones are tracking and surveillance devices. Almost every person has a cellphone nowadays and carries it around all the time. The police asks the mobile phone provider for access to your phone line and is then capable of listening to every call you make. They do this based on your phone number, so if you are being surveilled and you change the phone, but keep the number, they are still listening. And they can listen to the calls you make as soon as the phone is dialing.
 - 4) *CAF (Customer Application Form)*: police can get the documents you submitted while buying the SIM card and get your details from there.
 - 5) *SDR (Subscriber Detail Report)*: A telecome company provides a following details to police department such as : Mobile Number, Detail: Name, Father Name, Address, UID-Aadhaar Card Number, Type – Prepaid/Postpaid, Activation Date, Service Provider Name – Idea/Airtel/BSNL etc.. Circle etc. Through a SDR a Police Department easily evaluate a owner of a SIM.
- When the police monitor your phone number, they also get an unique identifier of your phone. So if you change the SIM-card but not the phone and they start monitoring your new number, they know that it is the same phone.

REFERENCES

- [1] <https://www.southuniversity.edu/whoweare/newsroom/blog/fighting-crime-with-mobile-technology-137309>
- [2] <http://pib.nic.in/newsite/PrintRelease.aspx?relid=107332>
- [3] <https://blog.ipleaders.in/lost-mobile-phone/>
- [4] https://en.wikipedia.org/wiki/List_of_countries_by_number_of_mobile_phones_in_use



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)