MWF

Mobile & Wireless Forum

DIRBS PAKISTAN

CASE STUDY

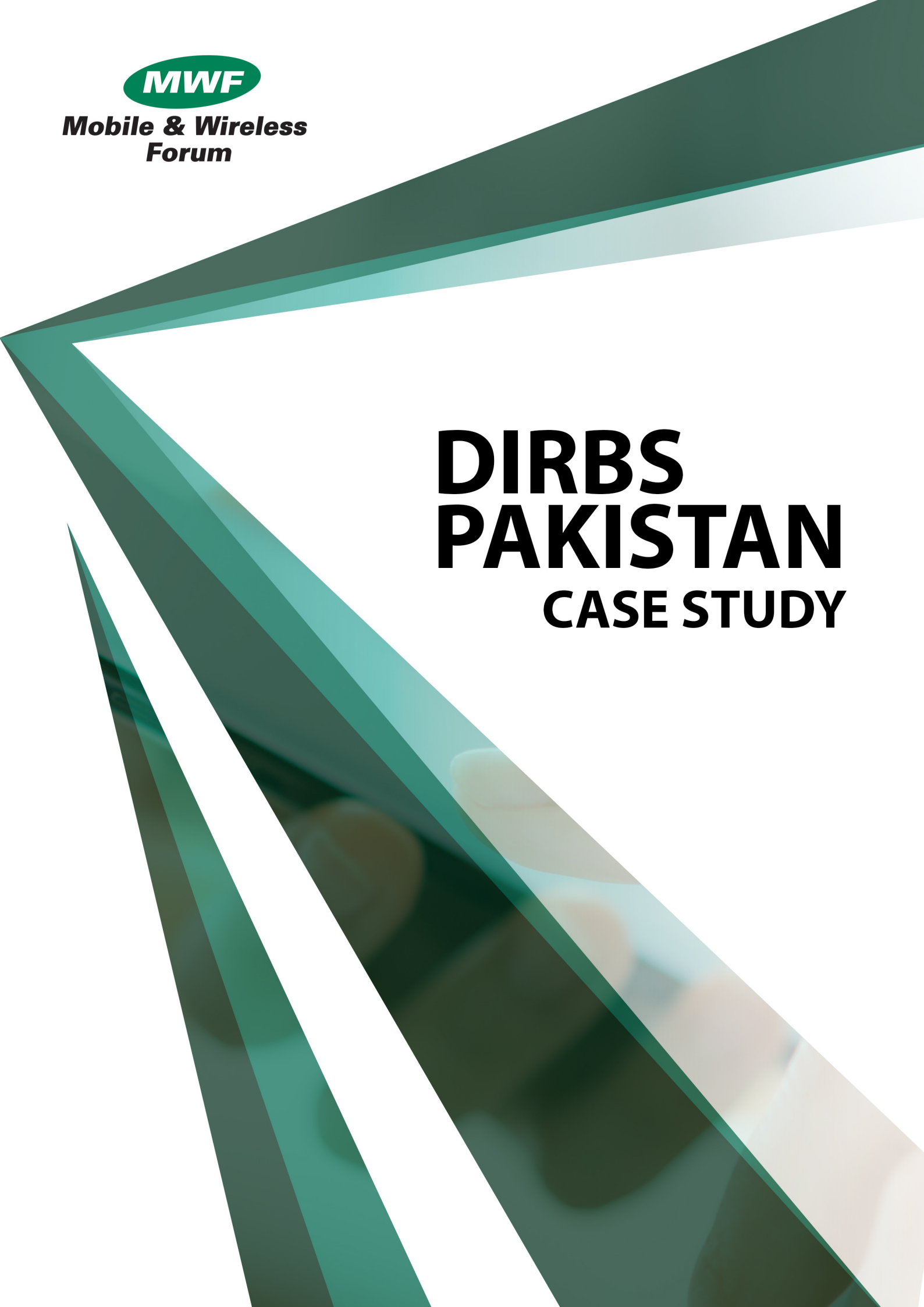


TABLE OF CONTENTS

EXECUTIVE SUMMARY

Pakistan has experienced tremendous mobile phone growth with the introduction of 3G/4G mobile networks. The country operates as an open-market meaning that the supply and availability of devices was separated from the mobile services offered by the mobile network operators. Thus consumers would source their own devices, but in doing so, this also allowed counterfeit devices as well as devices that were not legally imported onto the local market.

Pakistan recognized the impact that these devices were having on the local market and as part of the 2015 Telecommunications Policy committed itself to addressing the situation and ensuring that it cleaned up the market.

The Device Identification, Registration and Blocking System (DIRBS) is an open source server-based software platform intended to address counterfeit, illegal and stolen mobile devices in a country and was adopted for use in Pakistan with great success. Implementation of DIRBS helped clean-up the local market of counterfeit devices, reduced the theft of mobile devices, ensured legitimate device importations and increased government revenue. It also helped create additional local business opportunities and all without having any adverse impact on subscriber growth or consumer choice.

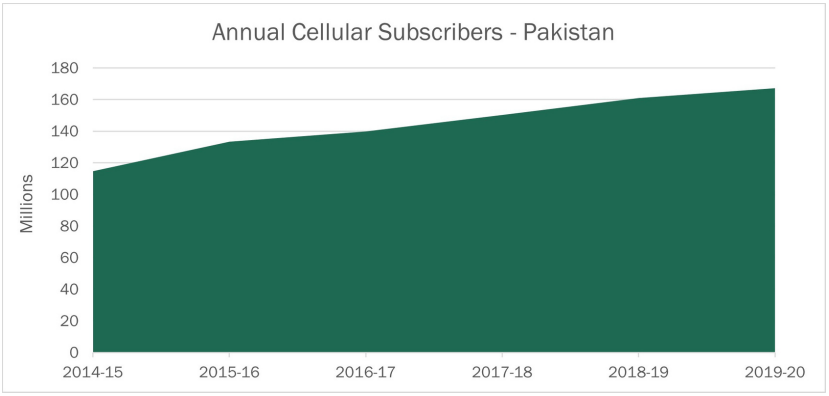
This case study examines the background to the introduction to DIRBS, the policy framework, challenges and how these were addressed, as well as going into the DIRBS system itself. Ultimately through the examination of Pakistan's implementation of DIRBS, this case study highlights how DIRBS can assist governments confronting similar challenges to those faced by Pakistan.

PRE DIRBS

PAKISTAN COUNTERFEIT MOBILE DEVICE MARKET OVERVIEW

Pakistan has experienced tremendous mobile phone growth with the introduction of 3G/4G mobile networks where the mobile market has always functioned as an open-market with the supply and availability of devices through independent importers, distributors, and retailers detached from the mobile services offered by the mobile network operators. This open-market allows operators to focus on the provision of network services and consumers are free to source their devices as they like. However, this model provided opportunity for those who wanted to avoid the legal importation route to bring in counterfeit goods thereby avoiding import duties and misleading consumers as to the nature of the device that they were purchasing. The overall worldwide impact of counterfeiting on smartphone sales is estimated at 184 million units, valued at 45.3 billion EUR or 12.9% of total sales. Pakistan is estimated to have 23.8% of lost sales in the country.[1] The illegal import and counterfeit devices were impacting the government, and the industry in a very significant manner. This open-market model also meant that the Pakistan Telecommunications Authority (PTA), the national regulator, lacked an effective way to regulate the devices that were coming into the market along with limited enforcement resources.

The open market also meant that the theft and resale of stolen mobile devices, already a significant problem in major cities was a growing public policy problem. The combination of all these factors encouraged a growing market for counterfeit and stolen devices that the Government of Pakistan committed itself to resolve in its 2015 Telecommunications Policy.



Source: PTA

[1] EU IPO study: https://euipo.europa.eu/tunnel web/secure/webdav/guest/document_library/observatory/resources/research-and-studies/ip_infringement/study11/smartphone_sector_en.pdf

TECHNOLOGY SOLUTIONS

The problems associated with counterfeit mobile devices and the need to eliminate them from the market have long been recognized in Pakistan.

As part of the 2015 Telecommunications Policy, the Government committed to ensuring the use of legal mobile phones and eliminating fake and fraudulent devices from the market. As a result of the adoption of this Policy and further consultation the PTA developed the necessary regulatory framework in September 2017 to ensure illegal, stolen, and counterfeit phones do not get access to mobile networks in the county and started to study and look for a suitable technical solution.

SOLUTION SELECTION CONSIDERATIONS

In seeking a system that can tackle counterfeit devices as well as help reduce street crime associated with mobile phone theft, there are a number of considerations that any solution should be able to offer:

- Convenient for all stakeholders, especially the consumers
- Flexible/Configurable to adapt to local country regulations and policy decisions
- Standalone system alleviating the need for mobile network integration and interoperability that cause unnecessary cost, capacity constraint and resource burden on the regulators, operators, or other stakeholders
- Provides tools for users to check device validity before purchase
- Provide a cost-effective solution for all stakeholders

The PTA realized there were hardly any tried-and-tested solutions available internationally to counter the black market in Pakistan. Some countries that had implemented solutions either did not produce any positive impact in their markets or the results on the mobile market were not available. Additionally, Pakistani mobile phone market had peculiar issues which required a customized solution.

It was estimated that a large percentage of handsets on the networks in Pakistan would fall under the definition of non-compliant phones. However, the operators were reluctant to part with a large customer base if the government were to decide to block the existing non-compliant devices fearing a decline in the subscriber base. A regulation to provide amnesty to all existing devices on the networks and present in the country addressed that concern.

Information sharing between different government entities was also necessary to introduce an online easy-to-use device registration system.

These requirements necessitated development of legal instruments/protocols based on which a technical solution could be developed. PTA assisted by CACF worked to draft a viable regulatory framework and the regulations required a technical solution to support various aspects of system implementation including:

- Device analysis and identification without the need to connect to MNOs live networks
- Amnesty to existing non-compliant or illegal devices
- An online device registration system
- An online device verification System
- Support for lost and stolen mobile phone system

DIRBS was assessed as meeting all criteria along with the ability for full customization and availability of the source-code to the government that provides code transparency and independence from being locked into any single proprietary vendor's solution.

DIRBS IMPLEMENTATION

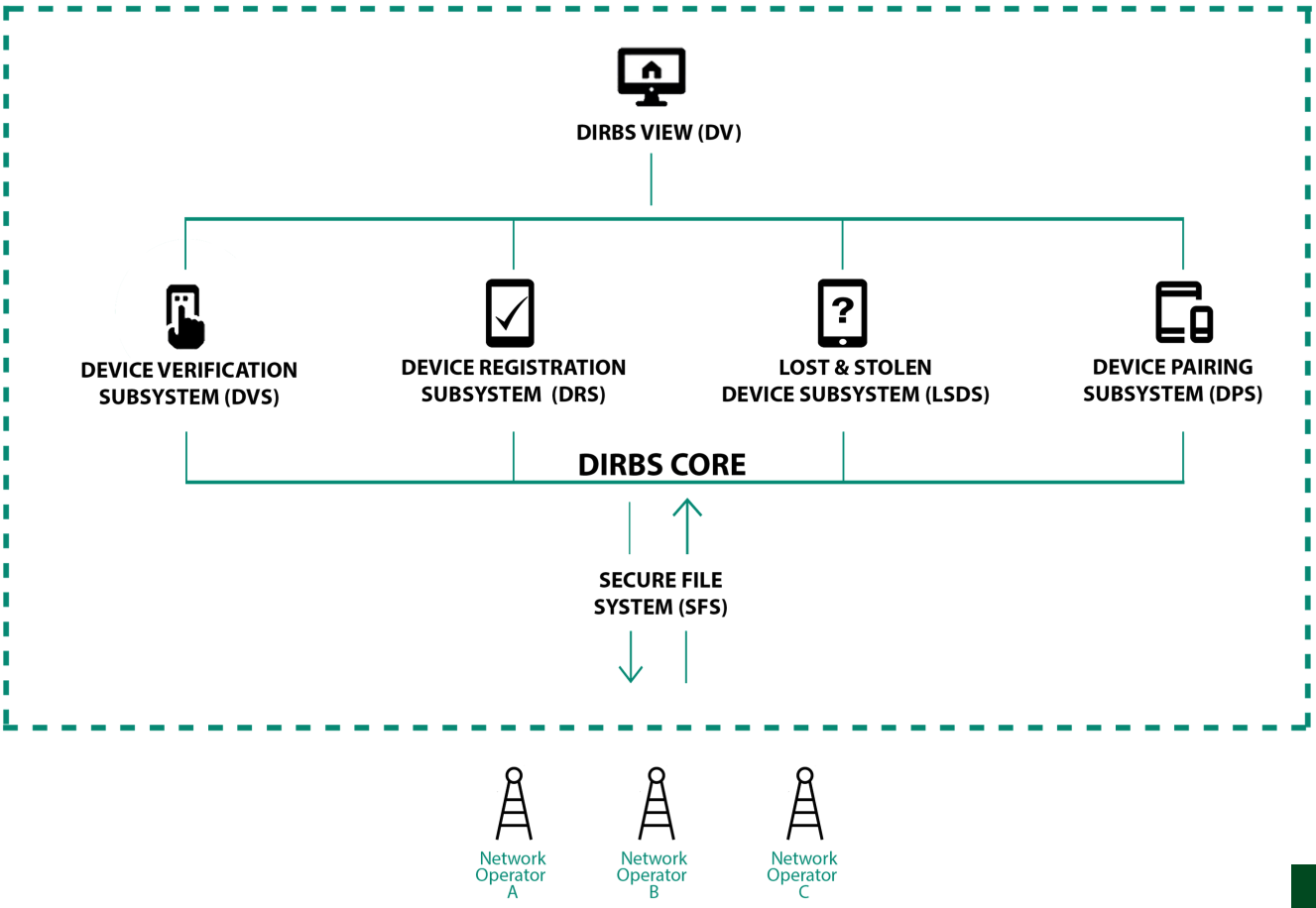
WHAT IS DIRBS?

Device Identification, Registration and Blocking System (DIRBS) is a server-based software platform intended to address counterfeit, illegal and stolen mobile devices in a country. The DIRBS software platform is available as open source to assist governments, regulators, and others in their efforts to combat the improper use of counterfeit, illegal and stolen devices on mobile networks.

The platform is consistent with the International Telecommunication Union's recommendations for addressing illegal and non-type approved devices in a country. DIRBS open-source software is available and can be freely downloaded from GitHub by visiting the following link: www.github.com/dirbs

An overview of the DIRBS system is as follows:

OVERVIEW OF DIRBS COMPONENTS



DIRBS works with three key attributes of a device extracted by each MNO from its CDR data and provided to DIRBS to perform analytics. These attributes include the device identifier i.e. the IMEI, the IMSI and MSISDN for any chargeable activity during each day.

The **Device Verification Subsystem** checks the International Mobile Equipment Identity (IMEI) number of a device on a network to see whether it in the approved format and whether the device has been approved for use by the national regulator (typically done as part of a type approval process with the OEM/importer). Fake, Duplicated, and incorrect IMEI's can therefore be flagged.

The **Device Registration Subsystem** is an online system which provides an interface to OEMs/importers/ individuals to register their devices with PTA and obtain a Certificate of Compliance (CoC) for their devices. Upon issuance of CoC the devices are permitted to operate on the MNOs networks. Devices which do not have CoC are blacklisted whenever observed operating on the mobile networks.

The **Lost & Stolen Subsystem** handles reports of lost and stolen devices and then adds these devices to the national and international blacklists, thereby ensuring that these devices cannot be used on any mobile network in the country or any other country subscribing to the international blacklist.

The **Device Pairing Subsystem** allows for the devices and subscribers' IMSIs to be paired according to policy decisions made. For instance, if a decision is made to allow all existing non-compliant devices to remain operational for their current subscribers irrespective then this subsystem will handle that arrangement.

The **Secure File Subsystem** is the encrypted file and data exchange that takes place between networks and DIRBS, allowing data to be exchanged and resulting blacklist and exception list to be implemented on each mobile network.

Finally, the **DIRBS View** module provides a graphical user interface for administrators and national regulators to see how the system is operating and to monitor the overall effectiveness of the program.

DIFFERENT TYPES OF NON-COMPLIANT IMEIS		
Malformed IMEIs - Do not meet format requirements MNV12KvuGS8WRTY 1122334455667788 11111	**Misused IMEIs** - Old TAC used on a newer device 491234567891234	**Transient IMEIs** - Equipment constantly changes IMEIs
Invalid IMEIs - Not allocated by the GSMA 351234567891234	**Duplicate IMEIs** - Same IMEI cloned on multiple devices 356938035643809 356938035643809 356938035643809	**Non-Approved IMEIs** - Non-homologated/Type Approved illegal imported

AWARENESS CAMPAIGN

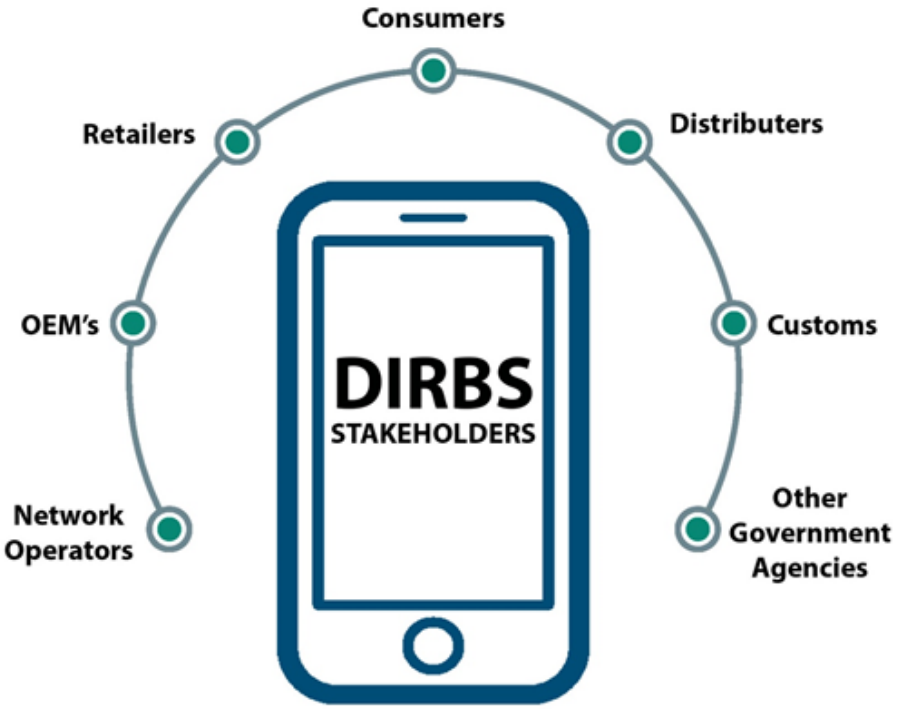
PTA had decided early on that stakeholder awareness and acceptance would be key to the successful implementation of DIRBS. To this end PTA engaged in an extensive awareness campaign for all stakeholders through traditional print and television as well as online and social media.

Consumers needed to be informed about the deployment of the system, what was going to happen to devices not registered and the fact that there was an amnesty for existing registered devices. They also needed to know then how the system would protect them going forward and how they could check if a device was legitimate.

To assist consumers, PTA sent SMS messages to every mobile phone in the country encouraging them to check the status of their device. Consumers could likewise send an SMS to check the IMEI of their device or access the PTA website or use the specially developed Android App.

Workshops were also held for those stakeholders within the industry including OEM's, Distributors, Retailers and Network Operators. OEM's, Distributors and Retailers needed to know what would be expected of them in terms of registering new devices imported into the country while mobile operators needed to incorporate parts of the DIRBS system into their own operations, especially the notification to the users of non-compliant devices, and the ultimate blocking of devices that remain unregistered as well as those the blocking of those devices reported as stolen.

Then there were the other governmental stakeholders such as Customs officials, and other government staff. Understanding the DIRBS system and what it would entail was again crucial for a smooth and efficient implementation.



Fraudulent Mobile Devices Impact All Stakeholders			
Government - Security - Tax Revenue -Non-compliant device ecosystem	**Manufacturers / Importers** - Loss of sales - Unfair competition and pricing pressure	**Operators** - QoS - Network Capacity/Spectrum - Interference	**Consumers** - Poor performance and reliability - Personal security - Privacy issues

REGULATIONS REQUIRED FOR SYSTEM IMPLEMENTATION

Pakistan adopted a Telecommunication Policy in 2015 that amongst other aspects committed the PTA to developing a framework that would see type approval of devices based on international standards incorporated into law, the blocking of devices with duplicate, fake or non-standard identifiers and those that had been reported as stolen. The framework was to be developed in consultation with all stakeholders and involved obligations on mobile licensees to ensure that the use of devices in Pakistan complied with the objectives set out in the Policy[2].

Following the adoption of the policy, and consultation with stakeholders, PTA published the Mobile Device Identification, Registration and Blocking Regulations to establish and give force to the framework outlined in the Telecommunications Policy. The link to PTA DIRBS regulation is available here: https://www.pta.gov.pk/assets/media/dirbs_amendment_reg_311218.pdf

IMPLEMENTING DIRBS

As a major policy initiative with wide ranging implications for operators, retailers, and the public, DIRBS was implemented in two phases. These were:

Phase1:
During this phase, non-compliant IMEIs seen on mobile networks were given amnesty. These non-compliant mobile devices were identified and paired with users' IMSIs. These devices' IMEIs were added in the 'Exceptions List' and they were permitted to remain unblocked for as long as they were used with the paired IMSIs. This ensured the existing users could continue to use their devices without disadvantage. IMEIs of lost and stolen devices were provided to the operators on a daily basis and blocked.

Phase 2:
This phase involved the blocking of non-compliant devices except those paired with existing users in phase 1. Owners of new non-compliant devices activated during this phase were given 60 days to register their devices. If such a device was not registered within the 60 days period, the device's IMEI was blacklisted and blocked by the operators. Users of non-compliant devices were informed of the status of their devices and the grace period through auto generated messages.

[2] See section 9.6 of the Telecommunications Policy 2015, Ministry of Information Technology, Government of Pakistan. https://usf.org.pk/UserFiles/file/Telecommunications%20Policy%20-2015%20APPROVED.pdf

Users of devices with duplicated IMEIs were notified to provide proof of the authenticity of the device to PTA within 15 days of the receipt of an SMS. Users of such devices must provide their identification and proof of purchase (original receipt/ warranty / or another such document) and photos of the device and its packaging. PTA could also ask for a physical inspection to determine the legitimacy of the device.

This process was designed to identify the genuine device from cloned ones which had duplicate IMEIs. As these devices were receiving the messages when first activated on the network, it was reasonable to assume that the devices had recently been purchased and opened and therefore the owners would have the requested items in their possession.

Throughout the implementation, users could also query the status of their device and receive a response back from DIRBS.

DIRBS System Responses to IMEI Queries:

Compliant/PTA Approved Device: The mobile device is PTA approved and legally imported into Pakistan
Device IMEI is Valid: Meaning that the IMEI of the mobile device is valid but it is not PTA approved.
Non-compliant Device: This means that it is not a PTA approved mobile device as the IMEI on the device is not
valid – and that may be because it is non-standard or duplicated.
Blocked device: The IMEI is reported as stolen and not allowed for usage/services.

IMPLEMENTATION – KEY POLICY DECISIONS

One of the first questions that needed to be addressed by PTA in seeking to clean-up the mobile device market in Pakistan was how to avoid significant disruption to the connectivity of consumers who may or may not have known that their device was illegitimate, fake or not PTA approved.

The PTA took the view that this was an issue that could be managed by allowing devices to be paired with their current users through the subscriber's IMSI – the unique number identifying a subscriber stored in the SIM card. Consumers were therefore permitted to register their usage of their device (whatever its status) prior to the DIRBS system becoming fully operational. Once registered to the user, the device would be regarded as compliant (for DIRBS purposes) for the life of that device with that user. If the user changed devices, then the old device could not be paired with a new user and would become useless.

In this way the problem of existing illegitimate devices in the market solved itself over a period of time without any inconvenience caused to consumers.

IMPLEMENTATION – INTERNATIONAL ROAMING

When first proposed, there were questions about how foreign visitors ('international roamers') using their own devices would be treated under the DIRBS system, since their devices would not be PTA approved because they were never imported into the country in accordance with PTA's DIRBS and Type Approval Regulations.

PTA resolved this issue within the program's Standard Operating Procedures. Essentially when a device is brought into a country by a visitor using their home country SIM, the IMSI of the user identifies their home network, and so the pairing of the IMEI and IMSI could be allowed to receive service in line with existing roaming regulations.

If the visitor opted to put a local SIM into the device, they would fall within the DIRBS framework. If the device were genuine, even if not PTA approved, the user would receive a message requiring them to register the device on the system. Failure to do that within 60 days of notification would see the device blocked. If the device were non-compliant it would be blocked 1 day after notification.

IMPLEMENTATION – KEY MILESTONES

As can be seen from the roadmap above, implementation of the full DIRBS system was a multi-year effort, beginning in 2015 with the adoption of Telecom Policy on Non-Compliant Mobile Devices. The conceptualization of DIRBS project started in 2016 and design and development continued till end of 2017. Interfacing and integration with external stake holders (Customs, Immigration, Operators, and Importers) took place throughout the implementation phase and the project became fully operational on 23rd April 2019.

STANDARD OPERATING PROCEDURES FOR DIRBS

In order to ensure a smooth implementation, a detailed set of Standard Operating Procedures (SOP's) was developed in consultations with MNOs and OEM and mandated by PTA. The SOP detailed the obligations of different parties with particular focus on mobile network operators (MNOs) since they were critical to the functioning and effectiveness of DIRBS. The SOP's specified amongst other things, that:

- MNOs had to implement the blacklist and exception list on their EIRs as and when provided by the PTA.
- All MNOs had to validate and upload relevant data to DIRBS servers, through secure connectivity between DIRBS and each MNO, as per the requirements specified in the SOP documentation, including the timelines by which this was to be done each day.
- It was the responsibility of MNOs to ensure secure IT connectivity for uploading of data from their respective networks and that this was established and maintained by each MNO with DIRBS.
- Once received, data would be further subject to validation and any discrepancy found will lead to DIRBS generating and transmitting a notification to the relevant MNO.
- MNOs had to ensure 99.9% connectivity uptime with DIRBS.
- MNOs, Type Approval Holders and Distributors had to train their Customer Service Centre and Help Line agents to handle DIRBS related queries and/or complaints by customers.
- There were designated points of contacts for all MNOs, Type Approval Holders, and Distributors with regards to DIRBS interactions and designated IT persons nominated at MNO's.

Fraudulent Mobile Devices Impact All Stakeholders			
Government	**Manufacturers / Importers**	**Operators**	**Consumers**
• Develop Regulatory Framework for device registration and blocking of Non-approved, Illegal and Stolen devices • Implement Standard Operating Procedure • Deploy and Administer a technology platform to enforce regulations	• Obtain Device Type Approval from the Government / Regulator • Register all devices to be imported • Register all locally manufactured devices	• Provide Device related Network Data to the government • Ensure EIRs support Blacklisting of valid & invalid IMEIs and Device Pairing • Notify subscribers of their device status via SMS as required	• Verify Device authenticity via SMS, App, Web • Register individually imported device(s) • Report Device Theft to authorities • Submit proof (invoice) for Genuine Devices, if required

Source Material and Resources
The Regulations and SOP documentation for Pakistan's implementation of DIRBS is available from the following links: https://pta.gov.pk/media/dirbs_reg_120917.zip https://www.pta.gov.pk/assets/media/dirb_amendment_reg_211217.zip https://www.pta.gov.pk/assets/media/dirbs_amendment_reg_311218.zip http://dirbs.pta.gov.pk/DIRBS_SOP_29_July_2019.pdf

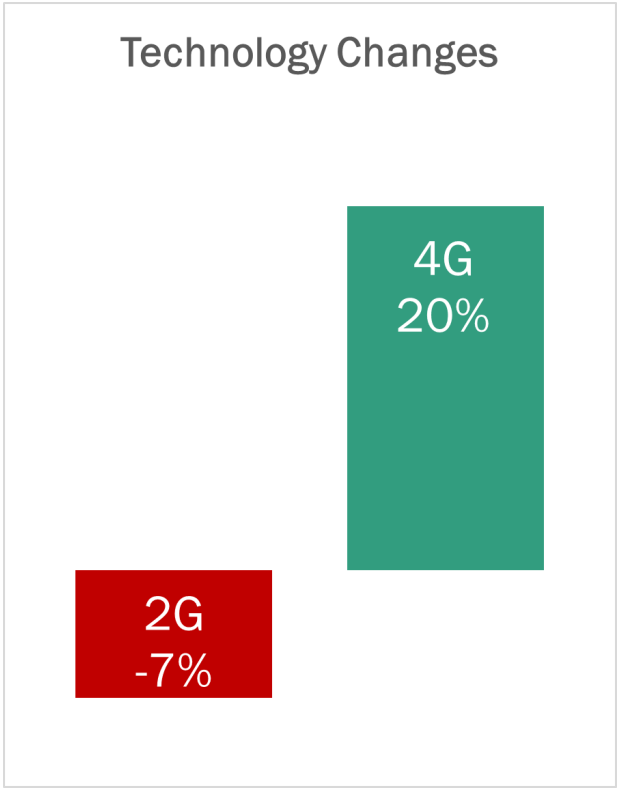
DIRBS OUTCOMES

SUBSCRIBER GROWTH

Despite initial fears from the countries network operators that DIRBS would have an adverse impact on subscribers, the reality was quite the opposite. During the first year, Pakistan's subscribers grew by 10.7M subscribers.

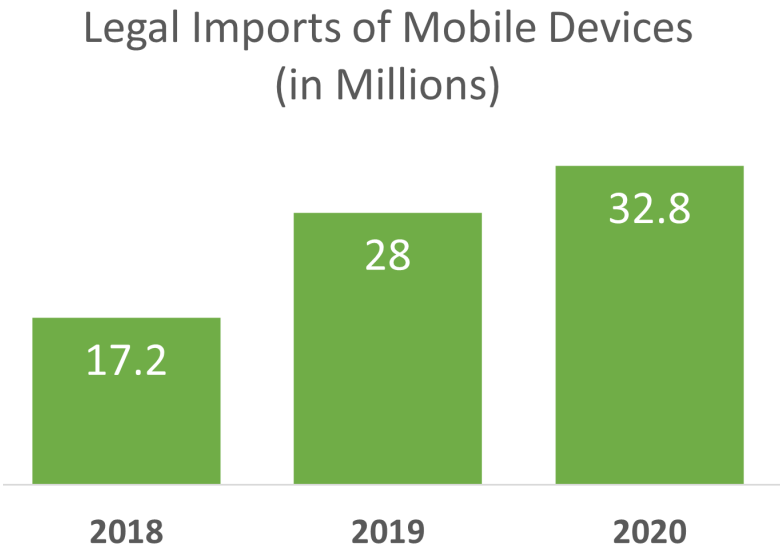
TECHNOLOGY CHANGES

Another interesting outcome was the change in the technology mix that resulted from the introduction of DIRBS. Due to the blocking of the large number of illegal and counterfeit devices, consumers updated their devices and as a result the prevalence of 2G devices fell by 7% in the market while more advanced 4G devices grew an impressive 20% in one year.



LEGAL DEVICE REGISTRATIONS

Despite difficult economic conditions in Pakistan during the first year of implementation, the legal device imports increased from 17.2 million devices in 2018 to 28m in 2019, a 62.7% increase. In 2020, legal device imports had increased by a further 32.83 million (as of December 2020).



CLEANING THE MARKET

The introduction of DIRBS helped achieve several of PTA's policy objectives, including the cleaning up of the mobile device market in Pakistan, particularly in the prevalence of fake and counterfeit devices. A total of 24.3 million fake IMEI's were removed from the national market, with 53 million IMEIs blocked.

The difference between the number of fake IMEIs and the total number of IMEIs blocked shows the degree to which devices were being imported illegally into Pakistan.

PTA has reported that the Government has collected the equivalent of $567m USD in customs duties from January 2019 through to November 2020 representing a 309% increase over the amount collected in 2018. More than $56m USD was also collected under the individual category during the same period - where previously there was no revenue collected at all.

53 MILLION TOTAL BLOCKED IMEI'S

24.3 MILLION FAKE IMEI'S

LOST AND STOLEN DEVICES

DIRBS proved itself to be an important tool in the fight against street crime. Since implementation, DIRBS has allowed 175,000 Devices to be blocked that were reported as stolen. As with other countries that have implemented blacklisting or blocking of stolen devices, it did not take long for the criminals to realize that stolen devices had little to no value, because of the blocking that occurs following a report of a device being stolen.

To truly put an end to the problem, regional blacklisting also needs to be implemented to prevent stolen handsets from being shipped to nearby countries. But the results in Pakistan show that the fight can be won.

OEM

DIRBS also resulted in positive outcomes for Original Equipment Manufacturers (OEM's) who had previously had to face unfair competition from illegally imported devices that avoided import duties. DIRBS ensured that the marketplace was even and also had the benefit that consumers became much more aware of the problems and risks associated with counterfeit devices, thereby stimulating demand for genuine devices.

IMPACT ON RELATED ACTIVITIES

Implementation of DIRBS also created a level playing field for establishment of local assembly plants for mobile device assembly that resulted in local job creation. Manufacturing now takes place in 29 local assembly facilities, which have produced over 20m devices since 2019 and generated more than 5000 new jobs.

Local manufacturing is actively encouraged by PTA and the government has adopted a Mobile Device Manufacturing Policy. Enabling regulations are also available online at: https://www.pta.gov.pk/assets/media/mdm_regulations_29012021.pdf

Tweet by Minister for Industries, (Pakistan Govt) Acknolweding that DIRBS has opened doors for Local Manufacturing in Pakistan

MWF RECOMMENDATIONS

Pakistan's implementation of DIRBS has been a great success. It has helped clean-up the local market of counterfeit devices, reduced the theft of mobile devices, increased OEM importations and government revenue, and created opportunities for local manufacturing of devices without having any adverse impact on subscriber growth. As a result, the MWF makes the following recommendations:

- Governments should carefully study the successful implementation of DIRBS in Pakistan and follow suit to ensure they benefit equally from the implementation of such a system.

- Governments should encourage adjacent business models that help increase mobile broadband connectivity by leveraging successful implementations of technical solutions like DIRBS.

- Consumers should be encouraged to check the authenticity of their devices by checking device IMEIs on OEM provided websites as well as in-country websites if provided by the government.

CONTACT US:

Mobile and Wireless Forum

www.mwfai.org

@MWFUpdates

enquiries@mwfai.org