CONTRIBUTION TO:

ITU EVENT ON COMBATING COUNTERFEIT AND SUBSTANDARD ICT DEVICES

ITU Headquarters, (Geneva, Switzerland, 17-18 November 2014)

Submitted by: **Mobile Manufacturers Forum (MMF)**

Contact point: **Thomas Barmüller**

Source:

Counterfeit and substandard mobile phones - A resource guide for Governments (EN)

http://spotafakephone.com/docs/eng/MMF_CounterfeitPhones_EN.pdf

COUNTERFEIT/SUBSTANDARD MOBILE PHONES

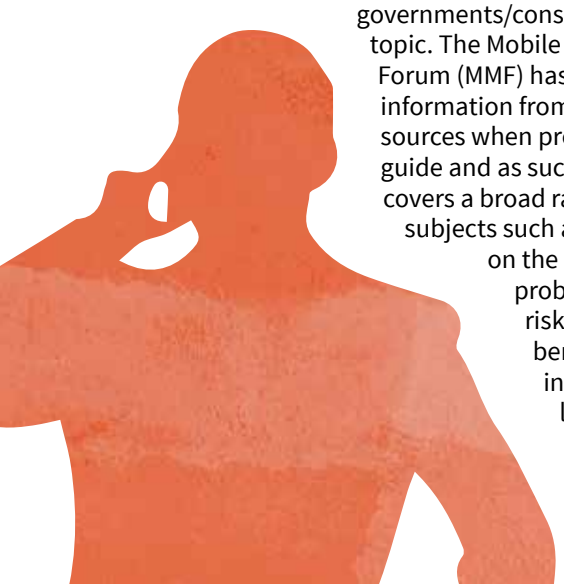
A RESOURCE GUIDE FOR GOVERNMENTS

MMF
Mobile Manufacturers Forum

1 INTRODUCTION

There has been a proliferation in recent years in the manufacture, distribution, and sale of black market mobile phones (commonly referred to as counterfeit and substandard phones). While this problem has created significant adverse consequences for society, governments do not yet fully understand the scope and nature of the problem. Governments continue to face significant challenges in finding effective solutions to this problem given the innovative and creative ways used by people and entities engaged in this illicit activity to evade enforcement/legal measures.

Despite the severity of the problem, very few resources currently exist for governments to draw on in order to understand the problem and to assist them in developing appropriate solutions. Also, there continues to be a dearth of comprehensive information educating consumers about the risks of purchasing black market cell phones. The goal of this resource guide is to create the most authoritative and comprehensive resource guide for governments/consumers on this topic. The Mobile Manufacturers Forum (MMF) has collected information from a variety of sources when preparing this guide and as such this guide covers a broad range of relevant subjects such as information on the scope of the problem, the various risks to society, and benchmarking information on legislative and technical solutions.



2 WHAT IS THE DIFFERENCE BETWEEN COUNTERFEIT AND SUBSTANDARD MOBILE PHONES?

While there are more similarities than differences between counterfeit and substandard mobile phones, it is important for governments to understand the difference. Counterfeit and substandard cell phones (which are collectively referred to as 'Shanzhai' or 'black market' products[1]) are the same in the following significant ways: the IMEIs on both categories of mobile phones are likely to be invalid[2]; both counterfeit and substandard mobile phones avoid the payment of patent royalties to the rightful intellectual right holders; both use inferior or used chipsets and other components; and, both fail to comply with applicable country legal requirements regarding sale and distribution of these devices. There is, however, an important difference, between these two subsets of black market mobile phones that is important for governments to understand because they underscore the need to craft solutions that are designed to control the distribution of both categories of handsets.

A **counterfeit mobile phone** is a product, which explicitly infringes the trademark or design of an original or authentic product. A counterfeit mobile phone copies the trademark (brand) of an original well-recognized brand, copies the form factor of the original product, and/or copies the packaging of the original product. In other words, a counterfeit mobile phone is an identical copy of the original brand or similar to the original brand (in terms of copying the trademark or the design) for all practical purposes it can be considered to be a 'copy' of the original 'branded' product. This includes, for example, those products which adopt a label felt to be amusing and humorous by playing with the established brand name (e.g. 'Nokla' or 'SunSang').

[1] The term "shanzhai' comes from the Chinese characters for "bandit' or outside of government regulation and this term is typically used to refer to fake and knockoff electronics and other products manufactured in China outside of government regulations that are widely distributed in and outside of China. The terms Shanzhai products or "black market' products are used interchangeably in this paper. Black market or Shanzhai products should not be confused with the "gray market' products, also known as the parallel market, which is the trade of a commodity through distribution channels which, while legal, are unofficial, unauthorized, or unintended by the original manufacturer.

[2] The GSMA maintains a unique system known as the IMEI Database (IMEI DB), which is a global central database containing basic information on serial number (IMEI) ranges of millions of mobile devices (e.g. mobile phones, laptop data cards, etc.) that are in use across the world's mobile networks. The IMEI is a 15-digit number that is used to identify the device on mobile networks. The GSMA provides access to the IMEI DB and its data to GSMA member mobile networks operators across the world, and to qualified industry parties (i.e. manufacturers of device management products and regulatory authorities). The network operators use the information in the IMEI DB to determine what types of devices are being used by their customers on their networks, and what features the devices support, so they can offer the latest services to their customers through their networks.

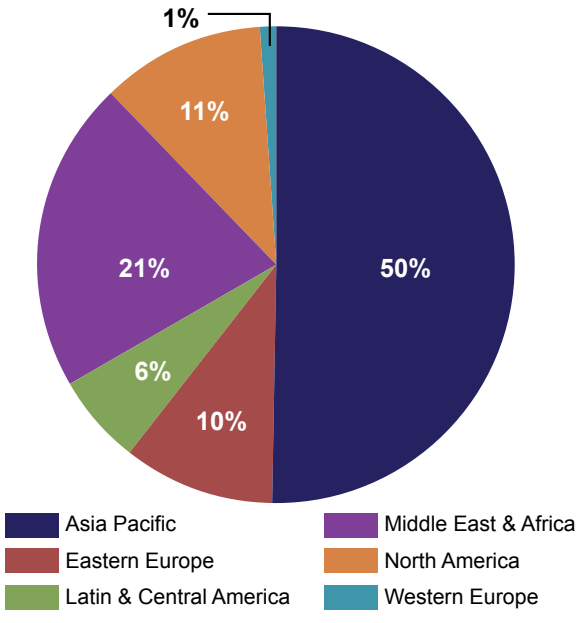
A **substandard mobile phone,** on the other hand, is a category of mobile phone which may resemble an original brand but is 'different enough' to make it difficult definitively to classify this product as 'counterfeit'. A substandard mobile phone includes, for example: 'White box' products which may appear similar in form factor to the authentic brand, but carry no explicit branding (i.e. do not explicitly counterfeit a legitimate brand, nor apply their own brand); and, 'Small Brand' products which have an unknown or little known brand that attempt to copy other brands or form factors from original products.

It is important for governments to understand, however, that except for appearance a substandard mobile phone is essentially the same as a counterfeit mobile phone in all other respects. There is a tendency on governments to focus only on counterfeit mobile phones when in fact substandard mobile phones present the same societal challenges.

3 QUANTIFYING BLACK MARKET COUNTERFEIT/SUBSTANDARD DEVICE PROBLEM: THE TIP OF THE ICEBERG

As with any trafficking in black market products, it is difficult to measure the exact size of the black market in the mobile phone sector. This is because many black market mobile phones are physically sold in 'black markets' and therefore it is inherently difficult to measure the market size of these products. A recent study by ARCchart, however, provides a starting point for determining the potential size of this problem. Specifically, the study concluded that in 2011 the number of counterfeit/substandard handsets sold globally was 125 million and this amount is expected to be 148 million units in 2013. According to ARCchart, Asia Pacific is the region with the largest proliferation of these handsets followed by Middle East and Africa, North America, Eastern Europe, Latin & Central America and Western Europe (see figure below).

The ARCchart figures are undoubtedly conservative. One of the limitations of such figures is that they only represent those products sold in traditional retail channels and do not capture those sold in the unregulated or unofficial channels, as well as those sold through the black market. Given that most of these devices are trafficked through the black market, it is reasonable and logical to assume that the data collected by ARCchart is merely the tip of the iceberg and that this problem is much bigger than what is reflected in the ARCchart figures.



There is other anecdotal evidence that sheds light on the size of the problem. During 2012 the counterfeit handset market shares in Tanzania have fluctuated between 10% and 20% of the entire market volume. This does not include sub-standard devices, only trademark infringements.

Additionally, BusinessDay in Johannesburg (March 25, 2013) reported that the Communications Commission of Kenya has stated that 3 million of the 30.4 million handsets in Kenya are counterfeit. According to the article, the Anti-Counterfeit Agency switched off 1 million counterfeit phones and seized other phones worth 5 million Kenyan shillings (~59,000 USD).

The Libyan Minister for Telecoms recently estimated that 80% of the handsets in the country were smuggled in[3], while in the United Arab Emirates, a recent single raid resulted in more than 1900 fake devices with an estimated value of about 460,000 USD being confiscated.[4]

The Federation of Indian Chambers of Commerce and Industry (FICCI) recently released a report that shows that just over 20% of the Indian mobile phone market are counterfeit/substandard products, costing industry 1.5 billion USD annually in lost sales, government 85 million USD in direct tax losses and around 460 million in indirect tax losses.

While in the United Kingdom, the 2011/12 Annual report from the IP Crime Group (part of the Home Office) revealed 125,249 fake mobile accessories, 2,012 counterfeit phones and 1,583 bogus iPhones, iPads and MP3 players were seized by the UK Border Force, and that does not include the thousands of devices and accessories seized by UK Trading Standards.

Another important source of data is GFK, one of the world's leading research companies. A special study commissioned in China concluded that the size of the black market in China in 2011 was 33.16 million units, representing sales value of 10.28 billion CNY (~1.9 billion USD). This study also concluded that the average selling price for these devices (in China) in Q4 2011 was 284 CNY (~47 USD). Combining the volume data (units sold) compiled by ARCchart with the average selling price data compiled by GFK illustrates that just the 'tip of the iceberg' represents a global problem that exceeds **6 billion dollars USD**.

On a broader scale, the Business Action to Stop Counterfeiting and Piracy, International Chamber of Commerce (BASCAP) cites a study that estimates the upper bound of the global value of counterfeit and

[3] http://www.lorientlejour.com/article/817178/sehnaoui-les-douanes-sont-une-passoire.html

[4] http://www.telecompaper.com/news/uae-cracks-down-on-counterfeit-mobile-phones--945597#.UaTVEL13Phg.twitter

pirated products in 2015 at $1.77 trillion.[5] BASCAP furthermore estimates counterfeiting and piracy costs G20 governments and consumers over €100 billion every year.[6]

4 WHAT IS THE NEGATIVE IMPACT OF COUNTERFEIT AND SUBSTANDARD MOBILE PHONES ON SOCIETY?

There are many ways in which the counterfeit/substandard mobile phone problem manifests itself negatively in society. As explained below, this problem significantly impacts consumers, governments, and private industry in a myriad of ways.

A : WHAT IS THE IMPACT ON CONSUMERS?

1 : HAZARDOUS SUBSTANCES IN COUNTERFEIT/ SUBSTANDARD MOBILE PHONES

A recent study conducted by the Nokia Institute of Technology in Brazil (INdT) on hazardous substances illustrates the potential dangers from counterfeit/ substandard phones. Specifically, the objective was to evaluate whether substandard and counterfeit phones were compliant with RoHS, the EU Directive on the restriction of use of certain hazardous substances in electrical and electronic equipment. This directive restricts the use of six hazardous materials in various types of electrical and electronic equipment.[7]

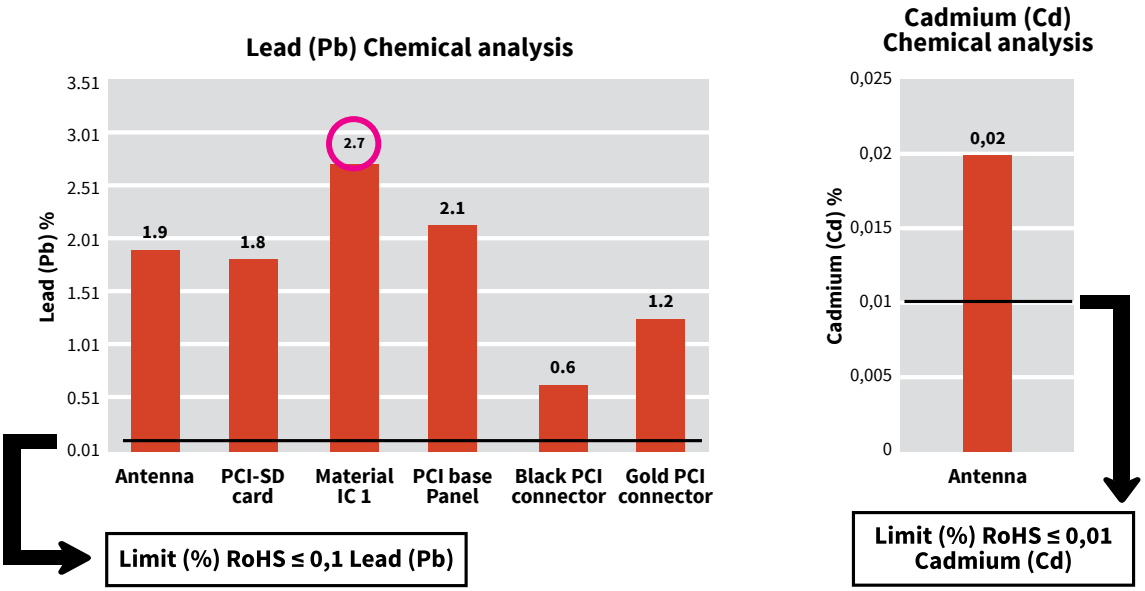
The study, using the IEC 62321 standard test method, involved testing five counterfeit phones having 158 parts (covers, displays, integrated circuits (IC), keyboard and others surface mounted (SMD) Components). The INdT study revealed the presence of two hazardous substances (lead and cadmium) in both internal and external components at concentrations much higher than the maximum values permitted by RoHS. **Figure A** below illustrates the excessive level of lead and cadmium found on internal and external components of the tested mobile phones.

Other studies conducted in other countries have confirmed the existence of hazardous substances on counterfeit/substandard mobile phones. A study was conducted in India by the Centre for Materials for Electronics Technology (C-MET), Hyderabad, to test RoHS compliance of mobile handsets being put on the Indian market. For this study (which was recommended by the Ministry of Environment & Forests (MOEF) and supported by the Indian Cellular Association (ICA)), the C-MET Hyderabad selected 15 widely available mobile phone models for testing. The phones were chosen based on their popularity, demand and availability in the market. C-MET officials were personally involved in procuring these models (3 nos. for each model) from the stores and phones both from the legal and unbranded/Chinese brands were picked up for testing. Detailed tests were conducted by IEC 62321:2006 procedures on over 150 parts (covers, displays, integrated circuits (IC), keyboard and other surface mounted (SMD) components) comprising all handsets.

FIGURE A: Test: Hazardous substances Chemical analysis

Lead with tin (PbSn) has been used as a process consumable since 1940's for soldering components into Printed Wiring Boards (PWB). If lead is found from the component solder joints, this more than likely means that the previous technology process has been used to manufacture products. This violates the RoHS restriction of not using lead in the manufacturing of EEE products.

The analytical test results are described below:

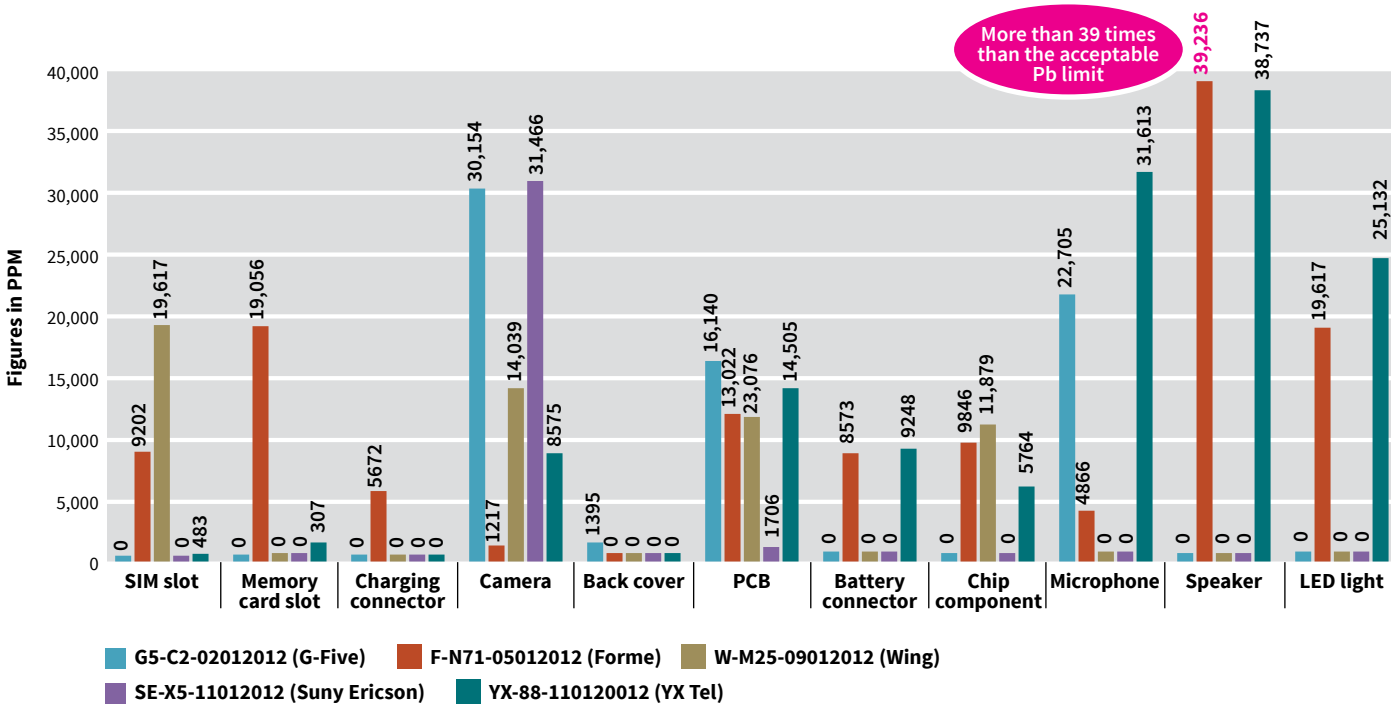


[5] http://iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/BASCAP-Research/Economic-impact/Global-Impacts-Study/

[6] http://iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/BASCAP-Research/Economic-impact/Impacts-on-Governments-and-Jobs/

[7] The EU RoHS Directive was chosen as the regulatory benchmark in this study for determining the existence of hazardous substances because it is the most well-known regulation on substance restrictions in electronics globally and it is the one which all major mobile phone manufacturers comply with. It has become the de facto global standard for mobile phones.

FIGURE B: High Lead (Pb) content found in all handsets tested - clearly amplifying their substandard character



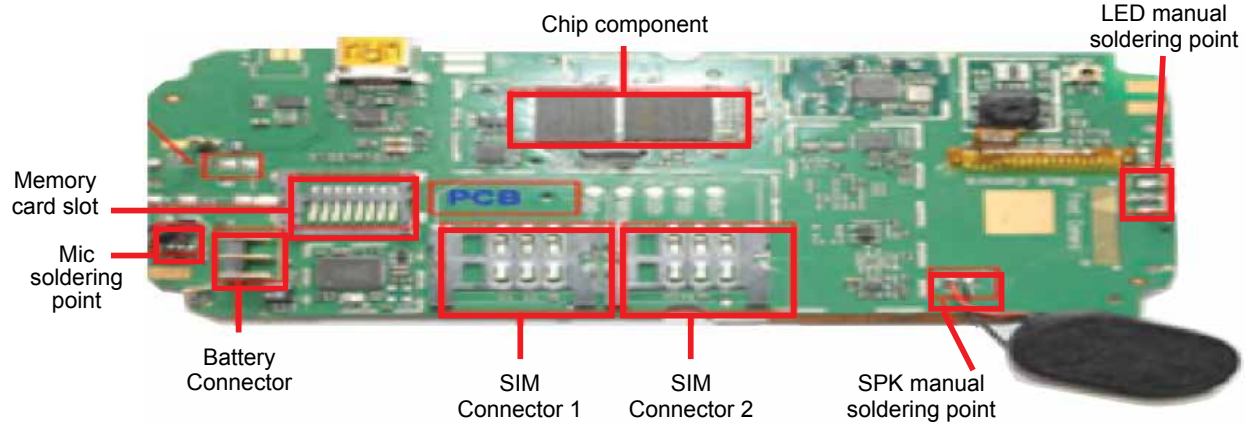
All unbranded/Chinese mobile phones were found to contain alarmingly high proportions of hazardous substances, especially lead (Pb). In some cases the values were 35-40 times higher than the globally acceptable limits for Pb. Many of the critical components like memory card slot, SIM slot, camera etc. which come in direct physical touch with consumers fared the worst in terms of hazardous material content, which obviously increases the risk much more than if the components were inside the phones. In contrast, mobile phones tested from global brands and other recognized brands were found to be within the acceptable RoHS limits and therefore safe for consumer use. **Figure B** above, summarizes the results of this study.

Figure C below demonstrates visually the areas where high concentrations of lead were found.

2 : OTHER SAFETY ASPECTS

The existence of hazardous materials in counterfeit/substandard mobile phones is not the only safety hazard that may potentially arise from the use of these products. Legitimate manufacturers must subject their products to extensive testing and compliance assessments before they can be sold. This can include compliance with national regulations, as well as low-voltage device safety requirements, audio safety requirements, electromagnetic compatibility, and RoHS (as mentioned above), amongst others. Additionally, in most countries, mobile phones must be type approved (sometimes referred to as homologation or product certification) by the telecommunications regulator. Product certification, among other things, ensures that the mobile phone performs the functions it purports to be able to perform, tests for interoperability and interference, and confirms it is safe for consumer use. In some countries even the accessories such as battery chargers and batteries

FIGURE C: Parts of the cell phone where hazardous substances are found



must also be certified by the regulator. It is safe to say that while legitimate products undergo rigorous internal and legally required approval processes before they are allowed to be sold in the country, it is probable that counterfeit/substandard mobile phones do not comply with any of these requirements.

3 : QUALITY OF SERVICE

Two recent studies confirmed what the MMF always suspected: that counterfeit/substandard mobile phones are of low quality, do not operate well, and, in fact, cause interference with network.

A : GSMA

A study undertaken for the GSM Association by Qualcomm, looked at the technical performance of 18 counterfeit smartphones alongside 3 genuine smartphones using industry standard protocols. All the testing was done in an accredited lab, with all of the devices being HSDPA-capable. Unlike the genuine devices, none of the counterfeit devices appeared to have been tested by either government or private sector labs for compliance to any legal or industry standards.

The results found that 15 of the 18 counterfeit devices would fail industry TIS (receiving sensitivity) requirements with half of the devices being 10-15dB below the reference phones. Likewise, 16 of the 18 counterfeit devices would fail transmit performance requirements with 11 of these devices being 6-13db below requirements. Both of these key indicators show a high level of degraded performance and would translate into a very high percentage of call dropouts for a user when using the device.

In addition the study then took the results of this first phase and investigated the impact that such devices would have upon a network in terms of voice and data capacity loss, data transmit speeds and impact on coverage. The results highlighted that such devices not only degrade the users experience but also create major burdens for network operators. For example, the results show that if such devices were being used in large numbers, operators would suffer a 200% loss in voice capacity and 50% loss in data capacity, with the maximum data rate on the modeled networks falling to only 250 {kilobits per second) kbps. Likewise, because of the poor performance of the devices, coverage was significantly reduced effectively creating holes in the network, necessitating more than 80% more base stations to rectify the problems.

These results highlight the considerable impact for both users as well as network operators from the widespread availability and use of such devices.

B: INdT STUDY

The INdT laboratory in Brazil also conducted a similar study on user experience. The INdT's study involved 44 counterfeit/substandard phones and conducted tests on original phones as well as a 'control group'.[8] The objective of this study was to evaluate the impact on mobile phone service performance due to the existence of counterfeit and substandard phones in the operator network. Test processes were based on 3GPP[9] testing protocols in order to compare the performance of original products versus counterfeit/substandard phones. Specifically, the following categories were tested for performance: 1) access failures 2) dropped calls 3) handover capabilities 4) transmission power capabilities 5) transmission power control and 6) access to Internet.

Consistent with the Qualcomm study, the INdT study revealed significant problems with user experience. Overall circuitry quality in counterfeit/substandard phones was found to be significantly lower than original phones and consequently these phones experienced excessively high dropped calls, access failures, as well as handover problems. The study also concluded that counterfeit/substandard phones not only degraded service quality of the user but also negatively impacted other subscribers too. Graphical representations of the results can be seen in Annex A.

The results of these two studies are significant and have broad-ranging implications for everyone. Due to performance degradation of counterfeit/substandard phones, the consumer experience is negatively impacted (excessively high dropped calls, access failures, and handover problems). These products not only thwart the Governments' responsibility to protect consumers and manage quality of service but also have severe implications for network operators given the expensive and unnecessary technical measures that are needed in order to make up for the problems caused by counterfeit/substandard phones (i.e., more antenna installations, base stations and the need for more spectrum).

4 : COUNTERFEIT/SUBSTANDARD PHONES ARE SOLD WITHOUT WARRANTY

The Qualcomm and INdT study confirm the poor quality of the counterfeit/substandard products. Yet, this problem is further compounded by the fact that these products, unlike well-known brands (which offer warranties of at least one year), obviously do not offer any consumer warranties for their products. Hence, these consumers have no recourse when counterfeit/substandard products cease to function.

[8] The original phones tested had type certification approval from ANATEL (Brazilian Telecom Regulatory Agency)

[9] The 3rd Generation Partnership Project (3GPP).

5 : SECURITY ISSUES (CYBER SECURITY, THEFT OF STOLEN PHONES, DATA-PROTECTION, ETC.)

It is hard to imagine any other device which contains more sensitive information than a mobile phone. Most people have given up on their paper address books because they are too heavy to carry around and too tiresome to update. Now they store all that information on their mobile phones, along with quick notes for themselves, the schedule of meetings and events, emails, and instant messaging. Consumers use their mobile phones well beyond calling people. They use them to shoot, store, and share photos and videos, to connect with friends and relatives via social networks, to post opinions on blogs, surf the Internet, download and listen to music, and to perform financial transactions. In Kenya, for example, more than 50% of the population takes care of all of their financial transactions through mBanking. As a result, the security related risks that arise from mobile phones need to be taken seriously.

Cybercriminals are not surprisingly increasingly committing cybercrimes by accessing mobile devices. Numerous types of malware are already circulating continuously on the Internet scanning for susceptible mobile devices. Cybercriminals use malware to infect mobile phones (malicious Trojans, viruses, spyware, worms etc.) that are designed to look for credit card numbers, social security numbers, bank account information, and other types of information. There is no way a consumer can be sure that the software in these mobile phones are not continuously scanning the information the consumer inputs on the phone for information that may allow them to commit a cybercrime or simply to invade a person's privacy. This information is then used to steal consumers' money or their identity.

Hackers are also known to disguise cyber security crimes in corrupted games which allow the criminal to take over the phone and make calls and/or send SMS messages. Hackers are also known to similarly install malware which directs the phone to send text messages to premium-rate numbers thus resulting in significant charges to the phone bill. Another form of malware that has been discovered aims to hold mobile devices for ransom. This malware, for example, could remove all the text messages from targeted phones and threaten to cripple the device unless users send money. Another malware has the capacity to act as a logger of information including remote phone monitoring, logging of incoming and outgoing SMS messages, and viewing of call history, address books, and other data.

Besides the cyber security threats, counterfeit/substandard mobile phones are potentially attractive devices for individuals engaged in organized crime. Counterfeit/substandard mobile phones are not easily tracked given the fact they have invalid IMEI numbers or no IMEI numbers.

The impact that counterfeit/substandard phones have on the growing problem of theft of mobile phones cannot be underestimated. This is a huge societal problem in all countries of the world and it is not uncommon for mobile phone theft to represent one of the top five crimes committed in any given country. The fact that counterfeit/substandard phones in most cases have no IMEI number or an invalid IMEI number (and the relative ease in which the IMEI can be changed on these devices) threatens countries' efforts to control mobile phone theft through the creation of blacklists and other similar measures.

Cyber security, protection of citizens' privacy interests, and crime control are a cornerstone of the most important public policy debates ongoing in society today. Yet, the impact of counterfeit/substandard mobile phones on these societal problems is not in the crosshairs of most governments. Many still do not recognize that a counterfeit/substandard mobile phone presents a much more important threat than other counterfeit products because it is perhaps the most important communications device of our age. More than a billion people in the world use mobile phones and if one takes the rather conservative estimate from ARCchart of 148 million counterfeit/substandard devices sold globally in 2013, one can understand the danger to security that counterfeit/substandard mobile phones present. This is a threat that must be taken seriously.

B : WHAT IS THE IMPACT OF COUNTERFEIT/SUBSTANDARD DEVICES ON GOVERNMENTS?

The impact of the counterfeit/substandard problem on governments is equally compelling. The foundation for new business development in any country is the existence of a legal protection of rights of legitimate business and the promotion of fair competition. Governments have adopted many requirements which range from adoption of consumer laws requiring warranties, regulations requiring certification of mobile phones, environmental laws, and laws protecting intellectual property, to laws relating to cyber security, and others. Counterfeit and substandard phones thwart all these government efforts because they by definition operate outside the law.

However, perhaps the most significant impact of these products on governments relates to the loss of revenue. These products typically do not pay duties and sales taxes when imported and sold and the companies involved in these operations obviously would not foolishly (for risk of capture) pay taxes on any profits. Again, using very conservative estimates, this is a 6 billion dollar problem world-wide, resulting in the loss of potentially billions in direct and indirect tax revenues every year.

C : IMPACT ON PRIVATE INDUSTRY: COUNTERFEIT/SUBSTANDARD PROBLEM RESULTS IN LOSSES FOR RIGHTS' HOLDERS

Legitimate manufacturers invest billions of dollars in research and development and millions more in ensuring that their products comply with the myriad of legal requirements imposed by specific countries. Most major manufacturers employ tens of thousands of employees in their operations. Yet, they find themselves in direct competition with counterfeit and substandard phones and suffer direct loss of sales as result of these black market products because these products have a significant competitive advantage given that they can be produced rather easily and cheaply.

The emergence a few years ago of total chip solution manufacturers in China has dramatically altered the competitive landscape in this respect because it significantly lowered barriers to market entry for black market entities. Companies which operate under a completely new business model have arisen whereby instead of merely offering a chipset like other major chipset providers the company provides customers with turnkey software solutions (chipset, hardware interfaces, and other software). This enables black market manufacturers to create and distribute counterfeit and substandard phones much easier than in the past.

The availability of turnkey solutions essentially eliminated the R&D step in the development cycle of mobile phones and black market manufacturers can now simply source the components such as displays and covers and not do much more than assemble them. This has allowed black market entities to proliferate. Without the size, R&D expenditure, regulatory costs of legitimate OEMs (original equipment manufacturers), black market manufacturers were able to easily take these products to market and profit handsomely from them. To compound this problem, these black market manufacturers pay no intellectual property royalties. In this day and age, no one can produce a mobile phone without having to pay royalties to owners of essential patents. In short, because of the emergence of turnkey solutions, counterfeit and substandard mobile phones can be produced incredibly cheap and unfairly compete with genuine products.

5 WHAT CAN GOVERNMENTS DO TO CONTROL THIS PROBLEM?

Given the growth of the counterfeit/substandard phone problem in recent years, it is obvious that enforcement efforts alone are not sufficient to control it. It is therefore necessary to explore new and creative ways to attack this issue. In this part, the MMF discusses potential solutions to the problem (in order of preference) and provides examples where similar solutions have been adopted.

A : NETWORK BLOCKING SOLUTIONS

The MMF believes the most effective way to deal with the issue of counterfeit/substandard mobile phones is to block these devices on the networks. One huge advantage that mobile phones have over other counterfeited products is that they must be activated in the network in order to function. This advantage should not be wasted. Network blocking solutions present probably the best and more effective ways for governments to control the issue. The question is what type of network blocking solution is the right one for a certain country.

1 : COUNTERFEIT/SUBSTANDARD 'FINGERPRINTING' BLOCKING SOLUTIONS

As previously mentioned, counterfeit/substandard mobile phones probably have invalid IMEI numbers. With these products either the numbers are invalid (all zeros, for example), the products have no IMEI number, or the IMEI number is a valid number but cloned from an original handset. Accordingly, this presents challenges to governments seeking to block these devices merely by using the IMEI number because the technology may not be able to distinguish which mobile phone is the one with the valid IMEI number. Moreover, having a valid IMEI cannot be deemed as sufficient to establish the legitimacy of the device because the issuance of a valid IMEI to a manufacturer for a particular model does not guarantee that the model is not counterfeit or substandard. **The GSMA for example, does not check the legitimacy of the device before issuing an IMEI number.** Indeed, it would not be surprising to find many black market models which have a validly issued IMEI. Additionally, a blocking solution based solely on IMEIs is inherently unreliable because it is fairly easy to change the IMEIs on the counterfeit/substandard phones. Thankfully new technologies have been developed to address this issue.

One technological solution (referred to as 'fingerprinting' or 'Counterfeit Identifier Platform') can identify and block counterfeit/substandard phones by blocking the IMSI of the SIM card when used in a counterfeit mobile phone by cross-checking the handset's capabilities with the expected ones. Handset capabilities used by this platform relate to information already standardized by 3GPP. This technology is designed to operate in the following manner:

a. The system checks the 'capability' database to determine if the capabilities of the phone match the listed capabilities. The technology then compares the phone's capabilities with capabilities stored in the capability database (database creation is based on information provided by the legitimate device manufacturer relating to the phone's IMEIs and capabilities). The capability database can also, for example, use other data to block phones such as whether the product is type approved or not.

b. The platform sends a request to HLR (Subscriber Database) to block the subscriber's IMSI if the capability crosscheck failed.

c. Until the user changes his/her mobile phone to one with the correct capabilities (in the capability database) the phone will remain blocked.

The technology does not necessarily have to block the mobile phones in the first instance. As a first step, the carrier can notify users with the illegal phones and request regularization (for example, give the user a chance to insert his SIM card in a legal phone). While the other solutions mentioned below can be effective in blocking substandard/counterfeit phones, this fingerprinting technology represents the 'second generation' of solutions with several countries now considering this approach.

2 : IMEI NETWORK BLOCKING SOLUTIONS

An effective option which cannot automatically distinguish valid IMEIs from invalid IMEIs but which can nonetheless be a viable and effective option for governments is the IMEI blocking solution. Many governments already have a blacklist of stolen devices (IMEI blacklist which in many cases is based on reporting by the subscriber) which is used to block devices that are purportedly stolen. A similar type of solution can also be used to block counterfeit/substandard devices.

A country can accomplish this in two different ways. It can require network operators to establish a system whereby all mobile phones activated on the network are cross-checked with the GSMA IMEI 'whitelist' database. This will allow the operator to determine which phones either have no IMEI number or an invalid number or proceed to block those phones. In the case of duplicate IMEI's, additional steps can be taken by the operator to investigate which one of the subscribers is using a valid number. The GSMA database is available at no cost to governments for this cross-checking purpose. The downside with this approach is that it does not allow cross-checking for other non-compliance such as failure of handsets to be type approved and other similar legal/regulatory requirements.

The second IMEI network blocking approach employed by some countries is perhaps best represented by the process in Ukraine and Turkey. The solutions used in both countries establish a blacklist and a 'white list' for cross-checking purposes.[10] The blacklist is focused on stolen and lost devices and the white list (which is created locally) is focused on those devices that are allowed to be sold in the country (for example, type approval and legal importation). Devices are cross-checked against both lists to determine if the mobile phone is blocked or not. This solution has the potential of screening out more devices than by simply using a blacklist but it does require establishment of the white list registry and as such creates burdensome and unwelcome obstacles for temporary visitors and importers. Additionally, as already explained, screening based purely on the validity of the IMEI may not be effective given how IMEIs are distributed.

3 : NETWORK BLOCKING BASED ON TYPE APPROVAL

Another possible measure to attack the counterfeit and substandard phone problem is to require the blocking of devices which are not type approved on the network. Given that most counterfeit/substandard devices are not type approved by the regulator, this type of network blocking implementation could be an effective means of controlling this problem. Indeed, the implementation could be done in conjunction with the network blocking solutions discussed previously. This solution was recently required by the regulator in Brazil and implementation must be completed by January 2014.

B : IMPORTATION BLOCKING SOLUTIONS

The IMEI and type approval network solutions mentioned above can also be implemented at the border in the event that network blocking is not feasible. Instead of cross-checking against the GSMA IMEI database (or database of type approved mobile phones) and blocking phones with invalid IMEIs from being activated on the network, a government may elect to block these devices at the time of importation. Both these solutions will filter counterfeit/substandard phones imported through normal 'legal' channels but obviously the effectiveness is hampered by the fact that this will not block those handsets that are imported as contraband (outside the customs process).[11]

C : DEVELOPMENT OF A COMPREHENSIVE PLAN

While the above mentioned strategies are designed to cast a wide net with new and innovative approaches, more traditional measures should also be a focus. As previously explained, the societal impact of counterfeit/substandard devices is currently misunderstood and consequently it is generally grossly under resourced. The development of a comprehensive plan is necessary in order to address this complex problem and this comprehensive plan should include, among other things, consumer awareness, greater enforcement measures, and appropriate reforms to legislation/regulations.

10 Costa Rica also requires legitimate importers to register IMEIs with the regulator which feed then into a white list of devices that can be activated on the networks. A similar approach is used in Uruguay.

11 For example imports of counterfeit/substandard phones over the courier services which is an increasingly used mechanism for importation of these phones.

1 : INCREASED CONSUMER AWARENESS

Building of awareness by government authorities on the dangers of counterfeit/substandard products is a critical component of any strategy. The demand side needs to be addressed as well and in this respect consumers need to be made aware of the serious problems posed by these products such as the safety and health threats, the poor performance of the products, the lack of warranty coverage, and equally important the security threats particularly in the area of cyber security and privacy. Consumers are generally not aware of these problems.

2 : INCREASED ENFORCEMENT

Increased enforcement is also essential. While the new approaches mentioned above can be effective options to control this problem, there are no silver bullets. A comprehensive policy must include increased resources in the form of intelligence gathering and raids with a particular focus on the huge black markets that exist in all major cities. Government authorities are not often able to collaborate efficiently across organizational jurisdictions. As the counterfeit/substandard problem impacts and cuts across a number of government authorities, establishment of cross-functional coordination mechanisms with strong industry representation is necessary. The MMF urges regulators and ICT ministries to establish national anti-counterfeiting committees to ensure development and follow-up of cross-functional action plans and the allocation of appropriate and sustainable funding mechanisms.

3 : LEGISLATIVE/REGULATORY REFORMS

The effectiveness of existing legislation/regulation should also be reviewed. Many countries do not have adequate legislation to deal with this problem. Many countries, for example, do not have legislation that makes it a crime to distribute phones with invalid or no IMEIs nor make it illegal to change an IMEI number. Another example relates to environmental controls. While many countries have laws relating to environmental waste there are no established controls for ensuring that counterfeit/substandard phones comply with these rules. Many counterfeit/substandard mobile phones are out of the reach of customs authorities because they happen to be 'in transit' through a particular country. This creates a huge loophole for criminal organizations distributing these products throughout the world as customs officials are powerless to seize obvious counterfeit products that are being shipped to a third country.

CONCLUSION

Counterfeit and substandard mobile phones represent a huge societal problem given the nature of the mobile phones and their importance in today's society. This problem touches many aspects of society including health & safety, environment, security, quality of service, loss of tax revenue, and unfair competition. It represents a multi-billion dollar industry for illegal manufacturers and it is causing billions of dollars of losses to governments, the economy, and industry. Bold action is needed by governments to control this problem as traditional tools are becoming less and less effective. Effective solutions (technological and legislative) exist and countries have already started to adopt them. Concerted action between industry and government must occur in order to adopt a solution that best suits a particular country. The MMF can assist governments in solving this problem by providing expertise and other resources.

This paper was prepared by the Mobile Manufacturers Forum - an international association of mobile or wireless communications equipment manufacturers. For more information on this important issue, please visit:

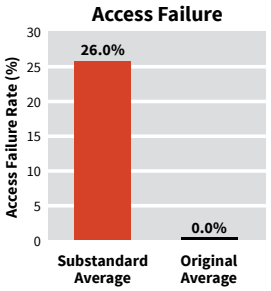
www.spotafakephone.com

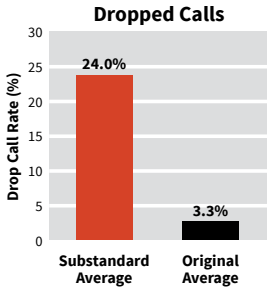
The Spot-a-Fake-Phone project is designed to help consumers learn more about the dangers associated with counterfeit and substandard devices and to help them identify these devices before they buy them.

ANNEX 1

TEST CATEGORY #1 AND #2: Access Failure and Dropped Calls

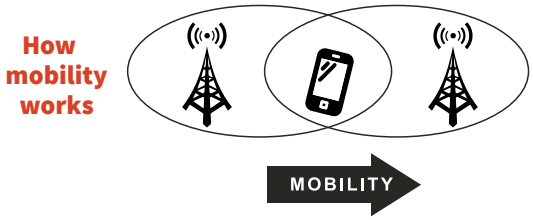
- Operators typically evaluate service quality by monitoring access failure and dropped calls:
- **Access Failure:** This category measures call attempts that fail in the network.
- **Dropped Calls:** This category measures ongoing calls that are undesirably interrupted (disconnected) from the network.
- **Results:** On both test categories, counterfeit/substandard phones performed significantly inferior to original phones with access failures and dropped call values of 26% and 24%, respectively.

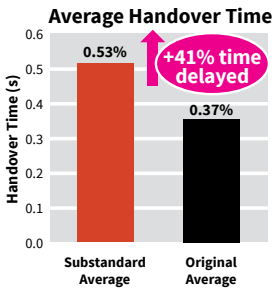


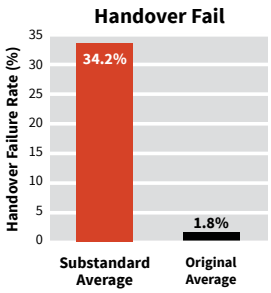


TEST CATEGORY 3: Handover Performance

- Successful phone mobility depends on the process of transferring the call from one antenna coverage to another.
- This mechanism is called **handover** and should be as quick as possible. If handover is delayed, the handover can fail and the call can be terminated (ie. dropped).

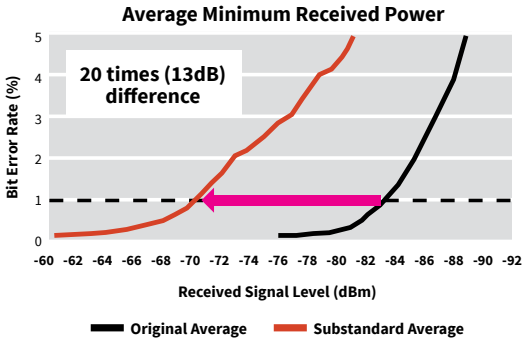


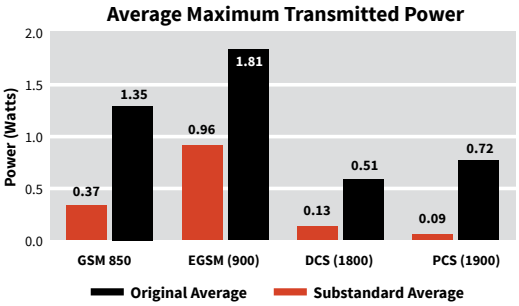




TEST CATEGORY #4: Transmission Power Capabilities:

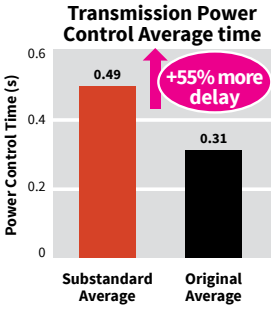
- Transmission power is critically important because it affects geographical coverage as well as quality of connection to the network.
- Maximum distance for coverage is restricted by phones:
  - **Minimum received power** from antenna tower.
  - **Maximum transmission power** to be listened by antenna.
- Maximum distance from antenna tower to phone decreases 57% for a counterfeit/substandard phone to maintain connection (voice call).

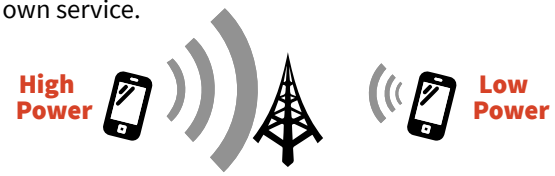




TEST CATEGORY #5: Transmission Power Control: Should my phone transmit high or low?

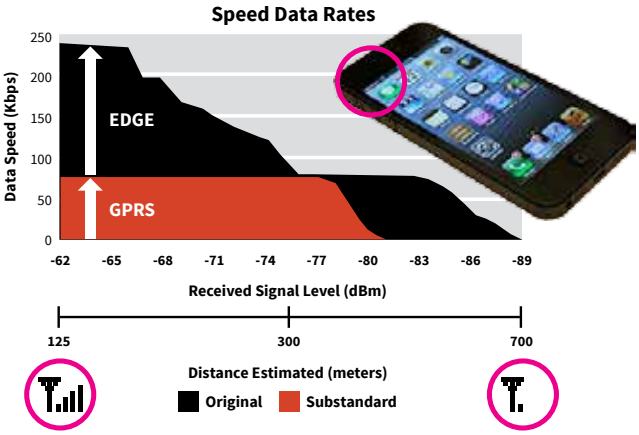
- Phone transmission power needs to be controlled.
- Control mechanism needs to be executed with minor delays.
- If too much power transmitted, handset will interfere with the other phones and if transmits too little, it will degrade its own service.





TEST CATEGORY #6:
How fast is my internet access?

- The speed of internet access is related to technology (GPRS and EDGE) available and the quality of receiver.
- Most substandard phones tested do not support EDGE technology which allows us around 200kbps.



MMF

Mobile Manufacturers Forum

Diamant Building
Boulevard Auguste Reyers 80
1030 Brussels Belgium
Telephone + 32 2 706 8567
Facsimile + 32 2 706 8569

Av. Paulista, 2300 – Piso Pilotis
CEP 01310-300 São Paulo/SP Brazil
Telephone +55 11 2847-4610
Facsimile +55 11 6847-4550

15th Floor, 100 Queen's Road Central,
Central, Hong Kong
Telephone +852 3180 9375
Facsimile +852 3180 9399

www.mmfai.org