Contribution by DotConnectAfrica Trust to the Call for Comments on Combating counterfeit and substandard ICT devices (Geneva, Switzerland)

2014

Background and Objectives.

Substandard and fake ICT products are a serious issue that impacts developed and developing economies, the ICT industry, as well as the consumer population around the world. The costs and negative effects of substandard and fake ICT products on all stakeholders are broad and numerous—ranging from lost taxes, royalties and other revenues; decreased sales, prices and operations; erosion of brand value, goodwill and reputation; reduced incentive to innovate and invest; lower employment and economic growth rates; network disruptions and interoperability challenges resulting in poor quality of service delivery and reception; and risks to health, safety and environment. According to the International Chamber of Commerce (ICC), the value of counterfeit products globally is expected to exceed USD 1.7 trillion by 2015.

This was recognized by the ITU Plenipotentiary Conference 2010 when it adopted Resolution 177 and by the new Resolution of the World Telecommunication Development Conference (Dubai, 2014) on "The role of telecommunications/information and communication technologies in combating and dealing with counterfeit telecommunication/ICT devices".

The objectives of this ITU event are threefold, namely to: (1) discuss the global scope and impact of counterfeiting and substandard ICT products on various stakeholders; (2) highlight the common concerns, challenges, initiatives, practices and opportunities of the various stakeholders in their fight against counterfeiting and substandard ICT products; and (3) examine the possible role of ICT standards development organizations (SDOs) and in particular the ITU, as part of the global strategy and solution to curtail counterfeiting and substandard ICT products as well as to assist members in addressing their concerns regarding counterfeit devices.

DotConnectAfrica Trust is a millennial organization that has the African Vision embedded in its inception and looks to create a continental domain and registry that will not only revolutionize but also create a platform that will nurture all other facets of African socio-economic development.

Introduction of DotConnectAfrica

DotConnectAfrica Trust is an independent, non-profit and non-partisan organization that is based in Port Louis, Mauritius (Reg. ID. CT8710DCA90) with its registry operations located in Nairobi, Kenya. Its main charitable objects are: (a) for the advancement of education in information technology to the African society; and (b) in connection with (a) to provide the African society with a continental Internet domain name to have access to Internet services for the people of Africa as a purpose beneficial to the public in general.

As an independent Non-Profit, non-partisan entity, DCA Trust intends to utilize surplus proceeds from the registry operation accruing to the Trust Fund for Charitable projects. Funds will be regularly allocated to different corporate social responsibility programs. Specific projects will be identified, and supported. As the first gTLD for Africa, it will aim at bridging the digital divide that exists between other regions of the Internet community and Africa by promoting the use of ICT for development. DotAfrica gives a positive branding opportunity for Africa that will benefit all Africans and in the use of technology to power their businesses.

DotConnectAfrica and its Principal and Members have in the past has worked or been advisors with International organizations such as Organization for Africa Union (OAU) aka Africa Union, United Nations Economic Commission for Africa UNECA), and International and regional organizations such as the Corporate Council on Africa (CCA), Internet Corporation of Assigned Names and (ICANN), The International Telecommunication Union (ITU), The Internet Society (ISOC), Internationalized Domain Resolution Union (IDRU), Internet Business Council for Africa (IBCA), and various private sector technology companies in Africa and internationally, with a view to increase synergy that encourages all stakeholders to participate in this dialog, in particular the African Diaspora.

In 11 July 2012, the ITU Council decided that the Draft of the future ITRS be made publicly accessible for an open consultation process, where all stakeholders could express their views and opinions on the content of the Draft of the future ITRs or any other matter related to WCIT. DotConnectAfrica as a concerned stakeholder in the ICT sector of the African continent submitted several recommendations to that effect. DCA's contribution has been published at ITU's Public Views and Opinions page. We also submitted our comments to the ITU Council

Working Group on international Internet-related public policy issues (CWG-Internet : Public Consultation (March 2014). Read our comments here[1]

Topic:

Counterfeiting means to imitate devices. Counterfeit products which are fake replicas of the real product are often produced with the sole intent of taking advantage of the superior value of the imitated product. This is therefore a fraud, an act of deceiving or misrepresenting by presenting an intentional perversion of the truth intended to induce a person to part with something of value.

The Anti-Counterfeit Agency (ACA) in Kenya has said the most affected items were medicinal drugs, electronics, CDs and pirated software, alcoholic drinks, mobile phones and farm inputs.[2]

Most products that face counterfeiting in ICT's include Mobile phones, hand held devices, Batteries, Cameras, printer cartridges and toners. In East Africa and specifically Kenya, Trade in counterfeits has grown into a Sh70 billion annual business, rivaling key foreign exchange earners like tourism, tea and horticulture. A KPMG and AGMA report estimated that 8% to 10% of all goods in the IT industry sold worldwide were counterfeit and counterfeiting led to a loss in revenue of US$100 billion to the IT industry in 2007.[3]

The IACC (International Anticounterfeiting Coalition) estimates that brand holders lose approximately $600 billion of revenue annually due to counterfeiting. [4] According to the study of Counterfeiting Intelligence Bureau (CIB) of the International Chamber of Commerce (ICC) Counterfeiting accounts for between 5 - 7% of world trade, worth an estimated $600 billion a

[1] DotConnectAfrica Contributes to the ITU CWG-Internet: Public Consultation (March 2014) http://www.dotconnectafrica.org/wp-content/uploads/2014/03/DotConnectAfrica-Contributions-to-ITU-CWG-Internet-Public-Consultation-_March-2014_.pdf

[2] Kenya loses Sh70bn in counterfeit trade http://www.businessdailyafrica.com/Counterfeit-trade-on-Kenya-list-of-top-forex-earners/-/539546/1684296/-/pgx605/-/index.html

[3] Technical Report on Counterfeited and Substandard ICT Equipment http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=9974

[4] The IACC (International Anticounterfeiting Coalition) estimates http://www.edn.com/design/consumer/4368557/Advanced-security-prevents-counterfeit-products

year. It has to be stopped, and the CIB is a focal point for those wanting to fight this growing problem. [5]

The Imaging Supplies Coalition, has estimated worldwide impact of counterfeiting as $3.5 to $5 billion annually. It's an industry often targeted by counterfeit distributors because "fake" toner is often indistinguishable until it is used, and not often scrutinized by the consumer. But it comes at a price – including invalidating equipment warranties and inconsistent or poor print quality.[6]

The influx of counterfeit and malicious hardware and software into the Federal Government supply chain may not receive the same attention as other types of cyber threats, but this state of affairs is very real and may be more prevalent than many understand.

The East African Community (EAC) is conducting a study on how the region can adopt a harmonized law to protect brand owners from counterfeit goods. Strong anti-counterfeiting policy in the region is essential if the EAC wants to attract more foreign rights holders as it moves to establishing a common market in 2010. [7]

Effects of using Counterfeit ICT products

Most ICT devices that have hit the market include mobile phones and smart devices, , Cameras, Printer consumables such as toners and cartridges, memory sticks, drives, monitors, networking equipment such as Cat-5/Cat-6 structure cabling, switches and routers.

Such devices lead to,

-Poor quality of service leading to higher dropped calls and higher incidences of poor reception.

- Cheap sub-standard materials used to manufacture substandard phones have been shown to contain dangerous levels of metals and chemicals especially Lead (Pb), mercury, cadmium

[5] Counterfeiting Intelligence Bureau (CIB) http://www.iccwbo.org/products-and-services/fighting-commercial-crime/counterfeiting-intelligence-bureau/

[6] Supplies counterfeiting in the world wide imaging supplies market is estimated at $3.5 billion annually http://www.isc-inc.org/news/2014_conference_recap.html

[7] Fresh move to harmonize anti- counterfeiting law in east Africa http://www.worldtrademarkreview.com/Blog/detail.aspx?g=0315b206-8ec3-4c50-9703-eec9950d3c20

which are up to 40 times higher than industry standards," According to the Mobile Manufacturers Forum (MMF)[8] Health effects such as the possibility of the substandard materials that are used to make counterfeit phones possibly leading to illness.

- Substandard batteries and chargers which have not been tested to comply with the strict safety certifications that genuine mobile phone products must adhere to and are often made from cheap components most often could suffer from short circuits, overheating and thus catch fire.

-Substandard mobile devices also run on inferior operating systems susceptible to fraudulent applications which, when downloaded, encourage cyber crime where they collect and send sensitive and personal data to criminal gangs without the users knowledge

-Some of these counterfeit networking products were made with copper-clad aluminum (or steel) conductors that outwardly look like genuine copper wiring, yet exhibit poor conductivity, problems making punch block terminations and offer too much resistance to support POE (Power Over Ethernet) applications which is a favored technology in IP systems.

-Mismarking of cables in standards observation such as marking a cables as a 24 gauge when actually they were non-specific 26 AWG.

- Rampant network disruptions and interoperability challenges that result in poor quality of service delivery and reception of signals, it is been noted that there is significantly reduced network coverage as more substandard devices connected to the network.

Use of ICTs, standards and other technologies are currently being used, or could be used in the future, as tools to fight counterfeit and/or substandard ICT devices.

Efforts which have so far been made to likely fend of increasing use of counterfeit products, especially in the African countries such as Kenya include

-Denial of service to NEW counterfeit mobile phones through identification of unregistered IMEI.

[8] Mobile Manufacturers Forum (MMF) Secretary General Michael Milligan http://spotafakephone.com/docs/eng/PR_MMF-Counterfeit-mobile-phones-USD-6-billion-drain-on-global-economy_EN.pdf, http://www.gsma.com/publicpolicy/buying-a-counterfeit-mobile-phone-could-be-deadly

-Setting up of an SMS collaborative platforms that will help consumers in authentication of the ICT consumer products were buyers can confirm the authenticity of the product portfolio in case of doubt. Such organizations include, East African Cables (EAC) Zinduka verification steps[9] and Royal Philips "Buy Original" campaign.[10]

-Use of innovative hologram security stickers

-Use of the QR Code where buyers can scan the code to protect their printers. Companies such as HP ask users to download the HP SureSupply app, or use any generic QR code reader, and scan the code on the cartridge's security label.[1]

- Embedded, secure microcontroller devices which can be used to communicate with a secure chip in the ink/toner cartridge or the battery pack. The controller incorporates firmware to allow strong authentication between the printer and the cartridge or the system and the battery pack and can lock out cloned counterfeit products. Such a scheme, though, requires a communication channel between the printer and the cartridge or the host and the battery, and that requirement means the use of at least one or two more pins on both ends, which also drives up the system cost.

-Use of the Neat Field Technology that could help eliminate the pins but can be a slightly higher-cost approach. Such examples of use of the wireless NFC technology, the NFC-enabled product and incorporation of a standardized secure contactless tags and readers could help in enforcing ant counterfeiting efforts.

-Use of cryptography digital signatures and certificates are provided to offer the robust protection to devices thereby thwart counterfeiters in the grand scheme, such products are then activated online.

Other efforts to fight counterfeit products in collaboration with stakeholders

[9] East African Cables (EAC) Zinduka verification steps http://www.eacables.com/index.php?option=com_content&view=article&id=115%3Azinduka-anti-counterfeit-campaign&catid=1%3Alatest-news&Itemid=1

[10] Royal Philips "Buy Original" campaign http://www.lighting.philips.com/main/application_areas/assets/Final_Digital_Projection_Lamp_Module_replacement_folder.pdf http://www.cio.co.ke/news/top-stories/philips-to-launch-sms-platform-to-curb-counterfeit-products http://www.philips.com/buyoriginal

The war on counterfeit ICT products could help in improving the bridging of the digital divide and increase the use of ICTs that are sustainable and affordable. Specifically, agencies can:

-Require that users are allowed purchasing only from authorized and trusted sources, by certifying resellers, partners and supply agencies users are able to obtain warranties and also get after sale services.

- Increase awareness and encourage information sharing by agencies with industry to that will then build into a update database which will provide legitimate vendors with better situational awareness of the operating context and about the updated surreptitious tactics, techniques, and procedures of bad actors in the market.[11]

-Create and design incentives and awards for businesses to certify their product security practices as trusted providers this will ensure that the desire to supply genuine ICT products is appreciated.

-Proper and consistent user education and awareness campaigns for authorized suppliers of IT equipment and government or interagency personnel. Such issues that could be communicated to the users for example in the case of the rampant fake mobile phone devices include: IMEI Number., users should not that every genuine mobile phone has a unique serial number to register it to a carrier network while the counterfeit often have duplicated or invalid IMEI numbers, the price of the device, If the price is too cheap, the product is probably fake. Poor quality products and packages, therefore buyers should look for inaccurate printing, misspelled words, crooked label placement and signs of defective workmanship. Lastly the buyers must be aware of the required limited warranty provisions that are available for all genuine mobile phone manufacturers offer such cover the handset, software and accessories; here most black market counterfeit products don't have these.

-Enforce quality of service standards for service providers and a constant independent review of the existing licensing regimes which can result in the reduction of licensing fees in the sector and therefore encourage more authorization.

[11] Anti-Counterfeit Awareness http://www.canon-europe.com/About_Us/About_Canon/Counterfeit/

Examples of multiagency efforts to combat Counterfeit products

The Anti-Counterfeit Agency partnership approach in the war against counterfeits should be multi-pronged and therefore guided by the realization that there is need for collaboration both within relevant government agencies, private sector and development partners. [12]

In an online posting, Xerox (NYSE: XRX) recently supported raids and prosecutions around the world to protect customers from counterfeit consumables and products, which unknowingly lead to damaged equipment, shoddy output and higher costs. [13]

The Imaging Supplies Coalition (ISC) is a non-profit trade association comprised of original equipment manufacturers of consumable imaging supplies and equipment that have joined together to protect their customers by combating illegal activities in the imaging supplies industry. Coalition members are Brother International Corporation, Canon U.S.A., Inc., Epson America Inc., HP, Lexmark International, Inc., Samsung Electronics America, Inc., Toshiba America Business Solutions Inc. and Xerox.

The Kenya Association of Manufacturers (KAM) fully supported the Anti-counterfeits 2008 Bill and invites all other stakeholders to enjoin in efforts to encourage parliament to fast track its enactment , they also declared a total war on counterfeiting. Jointly with KRA, KEBS, Police, Diplomatic missions and Government have promised to institute co-ordinate profiling of perpetrators of the vice.[14]

[12] Anti-Counterfeit Agency partnership http://www.aca.go.ke/index.php?option=com_content&view=category&layout=blog&id=91&Itemid=474

[13] Xerox Fights Back Against Black Market Printer Supplies http://news.xerox.com/news/Xerox-fights-back-against-black-market-printer-supplies

[14] KAM fully supports the Anti-counterfeits 2008 Bill http://www.kam.co.ke/index.php/press-releases/129-press-release-on-the-anti-counterfeit-bill